

Mineração de criptomoedas como prática sociotécnica: comunidades, governança e dinâmica de validação distribuída

Cryptocurrency mining as a socio-technical practice: communities, governance, and distributed validation dynamics

Boanerges Alves da Costa Neto¹

v. 14/ n. 2 (2026)
Abril/Junho

Aceito para publicação em 13/04/2026.

¹Doutorando em Ciências Jurídicas pela Universidad do Museo Social Argentino, Buenos Aires. ORCID: 0009-0006-7592-1818. E-mail: bcadvogado@hotmail.com.

RESUMO: Hodiernamente, a materialização das criptomoedas trouxe à tona formas inéditas de registrar e validar transações em ambientes digitais, movendo a confiança de estruturas centralizadas para arranjos distribuídos sustentados por código e participação coletiva. Nesse diapasão, a mineração é um elemento indispensável para o funcionamento dessas redes, na medida em que organiza transações, assegura a integridade do registro e permite a continuidade do sistema. Ainda assim, sua compreensão não pode se limitar à dimensão técnica, pois a atividade se desenvolve em meio a comunidades, disputas por capacidade computacional, estratégias econômicas e processos informais de coordenação. Tendo em vista essa perspectiva, o artigo busca analisar a mineração de criptomoedas como prática sociotécnica, considerando, por um espectro, seus fundamentos conceituais e operacionais e, por outra visão, as formas de organização dos participantes e os mecanismos de governança que sustentam a validação distribuída. Para tanto, a pesquisa adota abordagem qualitativa, com caráter exploratório e explicativo, orientada pelo método dedutivo. Bem como, recorre-se à pesquisa bibliográfica e documental, com base em doutrina abalizada, estudos técnicos e produções acadêmicas que tratam da mineração, dos mecanismos de consenso, da formação de *pools* e das dinâmicas de descentralização e coordenação em redes *blockchain*. Ao longo do trabalho, fica claro que a mineração ultrapassa a ideia de simples geração de ativos digitais, funcionando como processo de ordenação e estabilização do sistema. Também, é possível observar que as comunidades de mineração se estruturam de forma heterogênea, coadunando cooperação e concorrência em um ambiente caracterizado por desigualdade de recursos e crescente especialização. No plano da governança, verifica-se que a ausência de um centro decisório não elimina a necessidade de coordenação, entretanto, a redistribui entre protocolo, infraestrutura e adesão dos participantes.

Palavras-chave: Direito digital; Tecnologias descentralizadas; Proof of work; Pools de mineração; Governança.

ABSTRACT: Nowadays, the materialization of cryptocurrencies has brought to light unprecedented ways of recording and validating transactions in digital environments, shifting trust from centralized structures to distributed arrangements sustained by code and collective participation. In this context, mining emerges as an indispensable element for the functioning of these networks, as it organizes transactions, ensures the integrity of records, and enables the continuity of the system. Even so, its understanding cannot be confined to the technical dimension alone, since the activity unfolds within communities, disputes over computational capacity, economic strategies, and informal coordination processes. From this perspective, the article aims to analyze cryptocurrency mining as a sociotechnical practice, considering, on the one hand, its conceptual and operational foundations and, on the other, the forms of organization among participants and the governance mechanisms that sustain distributed validation. To this end, the research adopts a qualitative approach, with an exploratory and explanatory character, guided by the deductive method. It also relies on bibliographic and documentary research, drawing on

<https://www.gvaa.com.br/revista/index.php/RDGP>

established doctrine, technical studies, and academic works addressing mining, consensus mechanisms, the formation of pools, and the dynamics of decentralization and coordination in blockchain networks. Throughout the study, it becomes clear that mining goes beyond the mere generation of digital assets, functioning as a process of ordering and stabilizing the system. It is also possible to observe that mining communities are structured in a heterogeneous manner, combining cooperation and competition in an environment marked by resource inequality and increasing specialization. At the governance level, it is evident that the absence of a central decision-making authority does not eliminate the need for coordination; rather, it redistributes it across protocol design, infrastructure, and participant adherence.

Keywords: Digital law; Decentralized technologies; Proof of work; Mining pools; Governance.

1. CONSIDERAÇÕES INICIAIS

A expansão das tecnologias descentralizadas alterou a forma como se produzem, registram e validam interações econômicas em ambientes digitais. Nesse diapasão, a mineração de criptomoedas passou a ser importante, porque viabiliza a emissão e a circulação de ativos digitais e, ao mesmo tempo, sustenta, por mecanismos distribuídos, a validação das transações e a estabilidade do registro compartilhado.

Contudo, essa atividade não pode ser lida apenas em sua dimensão técnica, já que se desenvolve em redes atravessadas por cooperação, disputa, coordenação tecnológica e interesses econômicos diversos. Em razão disso, a mineração deve ser entendida como prática inserida em um espaço no qual código, infraestrutura material, incentivos de mercado e ação coletiva se relacionam de forma contínua.

Por esse motivo, a compreensão do fenômeno exige o afastamento de visões mais estreitas. Durante certo tempo, a mineração foi tratada só como etapa técnica do funcionamento da *blockchain* ou como meio de obtenção de recompensas econômicas, mas essa leitura é limitada quando se observa que a atividade depende de comunidades organizadas, de formas próprias de governança e de processos de validação que só se mantêm porque há adesão real às regras do protocolo. Em redes descentralizadas, a confiança não desaparece, apenas se reorganiza, passando a se formar a partir de procedimentos verificáveis, da aceitação coletiva do *software*, da atuação de mineradores, desenvolvedores e operadores de infraestrutura e das disputas em torno da manutenção e da atualização do sistema.

É a partir daí que a pesquisa se concentra: até que ponto a mineração de criptomoedas pode ser entendida como uma prática sociotécnica, e não só uma operação computacional, quando se observam as comunidades que a mantêm em funcionamento, os arranjos de governança que orientam a rede e a lógica de validação distribuída que permite sua permanência no tempo?

A questão surge da constatação de que a descentralização, embora frequentemente apontada como traço característico das criptomoedas, não apaga disputas, desigualdades ou formas de

coordenação. O que ela faz é mover tais elementos para outra moldura, na qual passam a surgir novos modos de organização, influência e conflito, que pedem análise mais atenta.

A partir disso, o artigo tem como objetivo compreender a mineração de criptomoedas como prática sociotécnica, considerando seus fundamentos conceituais, as formas de organização das comunidades de mineração e os processos de governança e validação distribuída que dão sustentação à rede. Com isso, o estudo não se prende à descrição do funcionamento técnico da atividade, pois busca mostrar como ela se organiza socialmente, como articula cooperação e concorrência entre os participantes e como a promessa de descentralização convive com movimentos de concentração operacional e com centros difusos de influência.

Para alcançar esse objetivo, a pesquisa segue uma abordagem qualitativa, de caráter exploratório e explicativo, orientada pelo método dedutivo. O percurso parte de discussões mais amplas sobre tecnologias descentralizadas, confiança distribuída e organização sociotécnica e, a partir desse ponto, dirige o olhar para a mineração de criptomoedas em suas formas mais aplicadas, buscando compreender como ela se estrutura e se mantém no interior das redes.

Do ponto de vista metodológico, o estudo se apoia, em primeiro lugar, em pesquisa bibliográfica desenvolvida a partir de bases acadêmicas e indexadores reconhecidos, com atenção a produções nacionais e estrangeiras situadas nos campos da tecnologia, da governança digital, da economia política das infraestruturas e dos estudos sobre *blockchain* e *Bitcoin*. Soma-se a isso a pesquisa documental, construída com base em documentos técnicos, textos fundacionais, artigos científicos, trabalhos apresentados em eventos acadêmicos e estudos voltados à segurança da rede, à descentralização e à governança dos sistemas distribuídos.

No processo de seleção do material, foram privilegiados textos ligados ao objeto em questão, principalmente aqueles que tratam da mineração, do funcionamento do *proof of work*, da formação de *pools*, da governança em *blockchain*, dos mecanismos de consenso e das tensões entre o ideal de descentralização e os movimentos concretos de centralização. Como critérios de inclusão, consideraram-se a pertinência temática, a consistência teórica, o diálogo efetivo com o problema de pesquisa e a contribuição real para a compreensão da mineração em perspectiva sociotécnica.

Em sentido diverso, ficaram de fora materiais apenas descritivos, conteúdos promocionais, publicações sem lastro acadêmico e textos que abordassem criptomoedas de maneira genérica, sem enfrentar as categorias aqui trabalhadas. A discussão é guiada, ainda, por autores dedicados à formação histórica do registro distribuído, à arquitetura do Bitcoin, à sociologia das infraestruturas digitais, à economia da mineração, à governança em *blockchain* e à segurança dos mecanismos de consenso.

A organização do trabalho acompanha esse percurso. Em um primeiro momento, são discutidos os fundamentos conceituais e a estrutura operacional da mineração de criptomoedas, com o propósito de situar historicamente o tema e delimitar seus elementos técnicos mais importantes. Posteriormente, o estudo se volta para as comunidades de mineração e para as formas de organização que surgem nesse ambiente, com atenção às relações de cooperação, disputa e concentração de poder. Na parte final, a discussão recai sobre a governança das redes descentralizadas e sobre a dinâmica da validação distribuída, destacando processos decisórios, mecanismos de estabilidade e tensões que atravessam a manutenção do sistema.

2. MINERAÇÃO DE CRIPTOMOEDAS COMO PRÁTICA SOCIOTÉCNICA: FUNDAMENTOS CONCEITUAIS E ESTRUTURA OPERACIONAL

Quando se olha para a trajetória histórica dos arranjos técnicos que tornaram possível a circulação de registros digitais confiáveis em ambientes abertos, é possível perceber que a mineração de criptomoedas não surgiu de forma repentina, tampouco pode ser entendida como consequência do mercado financeiro.

Antes mesmo do Bitcoin, já havia um percurso intelectual voltado à solução de problemas ligados à autenticação, à integridade e à marcação temporal de documentos digitais. Foi nesse caminho que a ideia de encadeamento temporal seguro de registros abriu espaço para a construção de sistemas em que a confiança passaria a depender de mecanismos suscetíveis de verificação por uma pluralidade de participantes.

A posterior aparição das criptomoedas aproveitou esse acúmulo anterior da criptografia aplicada e da computação distribuída, transformando tais ferramentas em uma infraestrutura voltada à validação econômica. Com isso, essa perspectiva histórica merece destaque porque afasta a leitura apressada segundo a qual minerar significaria apenas gerar moedas. No centro da atividade está a tarefa de ordenar eventos, impedir duplicidades e estabilizar um acordo coletivo sobre a sequência legítima das transações realizadas em uma rede aberta (Haber; Stornetta, 1991).

Foi com o Bitcoin que esse problema ganhou formulação mais clara, já que sua proposta apresentou uma arquitetura de dinheiro eletrônico *peer-to-peer* apta a dispensar uma instituição intermediária encarregada de impedir o gasto duplo. O modelo concebido não confiava a um centro administrativo a autenticação das transações.

Em lugar disso, repartia essa função entre os participantes da rede, que competem para registrar blocos e prolongar a cadeia reconhecida como válida. É exatamente nesse ponto que a mineração possui importância no sistema, pois ela aparece como o procedimento por meio do qual a

rede converte transações dispersas em um histórico comum e passível de auditoria. Ou seja, é pela mineração que consenso e segurança passam a atuar de forma integrada, unindo validação, prova computacional e emissão de novas unidades monetárias na própria lógica do protocolo (Nakamoto, 2008).

Esse arranjo ganhou pertinência em um contexto marcado pela desconfiança em relação às instituições financeiras e pela valorização da privacidade digital, da autonomia técnica e da resistência à vigilância. Por isso, o surgimento do Bitcoin não pode ser separado do universo *cypherpunk* nem do ambiente político e cultural que se radicou após a crise financeira de 2008. Desde o início, a tecnologia foi recebida como experiência social mais ampla, em torno da qual se reuniram expectativas ligadas à liberdade informacional, ao autogoverno da infraestrutura e à crítica às formas tradicionais de intermediação (Costardi, 2021).

Por isso, a mineração integra uma visão de mundo em que a produção da confiança coletiva passa a ser transferida para arranjos algorítmicos sustentados por comunidades distribuídas. Nesse ambiente, a técnica não aparece como elemento isolado, porque já surge permeada por valores, disputas e expectativas em torno da possibilidade de uma ordem econômica menos subordinada a centros decisórios tradicionais (Swartz, 2018).

Do ponto de vista conceitual, minerar significa reunir transações pendentes, organizá-las em blocos candidatos e submetê-las a um mecanismo de prova que permita à rede reconhecer um desses blocos como válido. Não se está diante de extração em sentido físico, embora a metáfora mineral tenha cumprido função importante ao transmitir ideias de escassez, esforço e recompensa. O que existe, na prática, é uma atividade voltada à verificação das regras do protocolo, à disputa pela prioridade na inclusão de blocos e à atualização contínua do livro-razão distribuído.

No plano econômico, a recompensa em moedas recém-criadas e em taxas de transação é um estímulo para que agentes anônimos, dispersos e sem vínculo prévio cooperem na manutenção do sistema. Já no plano técnico, o que se remunera é a aptidão para apresentar, dentro das regras do protocolo, uma prova aceita pela rede e, com isso, contribuir para a continuidade da cadeia. De tal modo, a mineração atua, ao mesmo tempo, como mecanismo de segurança, ordenação temporal e coordenação econômica (Ulrich, 2014).

Para Greve *et al.* (2018), essa dinâmica depende de alguns elementos sem os quais a própria ideia de mineração perde coerência. O primeiro deles é a *blockchain*, entendida como uma cadeia de blocos conectados por funções criptográficas, na qual cada novo bloco remete ao anterior e aumenta a integridade do histórico já admitido. Já o segundo é a lógica da rede *peer-to-peer*, que permite a circulação de cópias do registro entre diversos nós e reduz a dependência de um servidor único.

O terceiro é o protocolo de consenso, responsável por tornar possível que agentes que não confiam entre si cheguem a uma mesma leitura sobre o estado da rede. Em sistemas como o Bitcoin, a *blockchain* age como livro-razão distribuído e auditável, enquanto o consenso viabiliza a formação de uma memória coletiva resistente a alterações arbitrárias. É na confluência desses elementos que a mineração se situa, já que é por seu intermédio que a rede converte divergências potenciais em uma sequência estável de registros (Greve *et al.*, 2018).

No âmbito do *proof of work*, esse acordo coletivo se ampara em uma prova construída a partir do gasto de capacidade computacional, de modo que os mineradores disputam a obtenção de um valor que atenda à exigência criptográfica fixada pelo protocolo, enquanto o grau de dificuldade do problema é periodicamente ajustado para preservar certa regularidade no ritmo de formação dos blocos.

Nesse prisma, o sistema não indaga quem é o agente, tampouco sua posição institucional ou sua identidade no mundo social, pois o que realmente importa é saber se a prova apresentada satisfaz o critério anteriormente estabelecido. É daí que decorre a força do modelo e, ao mesmo tempo, uma de suas tensões mais notórias, já que a validação pode ser percebida como neutra porque se apoia em um cálculo passível de verificação, embora essa aparência de neutralidade dependa de uma base material pesada, sustentada por máquinas, consumo de energia, conectividade e capacidade financeira (Rebello *et al.*, 2021). Ou seja, a prova de trabalho não apaga relações de poder, mas as reorganiza conforme a disponibilidade de recursos computacionais e a forma pela qual o protocolo distribui incentivos.

É diante disso que o *hash rate* ganha maior destaque, porque, em sentido técnico, ele indica a quantidade de funções *hash* processadas em determinado intervalo de tempo e, em sentido sistêmico, funciona como um índice da força computacional empregada na disputa pela validação dos blocos. Igualmente, quanto maior for a participação de um agente, ou de um grupo de agentes, no *hash rate* total da rede, maior é sua chance de validar blocos e obter as recompensas correspondentes. Na experiência das criptomoedas, o poder computacional é um recurso de organização, de estratégia e de disputa dentro desse ecossistema (Gencer *et al.*, 2018).

Por essa razão, a ideia de ausência de autoridade nuclear, frequentemente apresentada como marca distintiva dessas redes, precisa ser estudada com mais cuidado, porque o fato de não existir banco central, câmara de compensação ou administrador único não equivale à ausência de coordenação. O que ocorre, em verdade, é uma redistribuição dessa coordenação entre o protocolo, os incentivos econômicos, a manutenção do código, a circulação de informações entre os nós e a adesão concreta dos participantes às versões do *software* que passam a ser socialmente aceitas.

As redes distribuídas não prescindem de autoridade. O que ocorre, na verdade, é uma reelaboração dessa autoridade em bases infraestruturais, técnicas e comunitárias. Nessa perspectiva, o consenso descentralizado não se confunde com espontaneidade social, já que depende de regras estáveis, de assimetrias de competência técnica e de mecanismos pelos quais a coletividade reconhece como legítimo determinado estado da rede. É nesse sentido que a mineração é uma forma de autoridade operativa, exercida pela capacidade de participar validamente da produção do registro compartilhado (Mucelli; Moura, 2024).

A perspectiva sociotécnica permite perceber por que a mineração não pode ser reduzida a um procedimento automático. O Bitcoin e outras redes semelhantes se estruturam a partir de arranjos nos quais máquinas, código, mercados, comunidades on-line, fóruns de deliberação, fabricantes de hardware, investidores e operadores se relacionam de maneira contínua. Assim, o sistema permanece em funcionamento porque elementos humanos e não humanos se coadunam de forma permanente, em uma dinâmica de coprodução.

A prova computacional, tomada isoladamente, não basta para sustentar a rede. Seu funcionamento depende de *software* atualizado, da adesão dos operadores, de compreensões compartilhadas sobre segurança e de expectativas econômicas capazes de tornar racional a permanência nesse ambiente. Sob esse ângulo, a mineração pode ser entendida como prática sociotécnica justamente porque reúne infraestrutura material e ação humana em um mesmo circuito de produção de confiança distribuída (Hayes, 2019).

Essa compreensão também permite corrigir a imagem, bastante difundida, de que o Bitcoin seria uma forma de dinheiro “sem confiança”. O que se verifica é a movimentação do lugar em que a confiança se estabiliza. Em vez de permanecer concentrada em instituições clássicas, ela passa a se distribuir entre o protocolo, as reputações técnicas, a adesão comunitária, as arquiteturas de incentivo e o monitoramento público do registro.

Ainda subsiste uma dependência de práticas sociais, arranjos organizacionais e compromissos coletivos, embora ela já não se apresente sob a forma tradicional. A mineração integra esse rearranjo, na medida em que materializa a ligação entre a prova objetiva e a aceitação social de seu resultado. Sem o reconhecimento comunitário da validade do protocolo e sem a continuidade das operações sobre a mesma cadeia, a prova computacional, por si só, não é capaz de produzir estabilidade duradoura. É nesse sentido que o consenso deve ser compreendido, ao mesmo tempo, como fenômeno técnico e social (Dodd, 2018).

Quando se acompanha a trajetória desse ecossistema ao longo do tempo, percebe-se que a mineração passou a se inserir em um cenário de crescente especialização. Nos primeiros anos, era mais estreita a proximidade entre o ideal do “par” distribuído e a realidade material da rede.

Com a valorização do ativo, o aumento da dificuldade e o desenvolvimento de *hardware* dedicado, porém, a atividade passou a exigir escala, capital, acesso a energia de menor custo e formas mais elaboradas de gestão. O imaginário da participação aberta permaneceu como referência normativa, mas a prática, pouco a pouco, distanciou-se da figura do minerador doméstico e abriu espaço para instalações industriais e cadeias produtivas orientadas exclusivamente à disputa por *hash rate* (Cardoso, 2018).

Por essa razão, a mineração está na posição limítrofe entre técnica, economia e organização social. Ela continua sendo a engrenagem responsável por assegurar a ordem das transações e a integridade da cadeia, mas, ao mesmo tempo, transformou-se em prática materializada em fazendas computacionais, contratos de energia, mercados de *hardware*, serviços de hospedagem e formas cada vez mais elaboradas de cooperação estratégica.

O percurso histórico que conduz da promessa de desintermediação à formação de novas interdependências não desmente a rede distribuída, considerando que o que ele demonstra é que nenhuma infraestrutura dessa natureza atue à margem do mundo social. Em sua acepção mais sofisticada, a mineração exprime esse ponto de encontro entre cálculo criptográfico, incentivos econômicos, cultura técnica e disputa em torno da forma legítima de organizar a confiança em ambientes digitais abertos (Cardoso, 2019).

3. COMUNIDADES DE MINERAÇÃO E FORMAS DE ORGANIZAÇÃO: COOPERAÇÃO, DISPUTA E ESTRUTURAS DE PODER

A consolidação da mineração como atividade especializada produziu uma ecologia interna de agentes bastante heterogênea. Há mineradores individuais, que operam com capacidade reduzida e mantêm relação mais direta com o ideal originário de participação aberta. Há pools, que agregam *hash rate* de múltiplos participantes e redistribuem recompensas segundo critérios predefinidos. Há, ainda, grandes operações empresariais, que combinam escala industrial, domínio logístico, negociação energética e proximidade com fabricantes ou distribuidores de *hardware*. Essa diferenciação importa porque a rede não é composta por unidades equivalentes. Os participantes ocupam posições distintas, dispõem de recursos desiguais e respondem a incentivos também diversos. A comunidade de mineração, assim, não forma bloco homogêneo, mas campo de relações no qual coexistem cooperação necessária, competição contínua e hierarquias materiais bastante visíveis (Xu *et al.*, 2020).

O surgimento dos pools responde a uma questão econômica elementar. A mineração individual submete o participante a alta variância na obtenção de recompensas, já que mesmo

contribuindo honestamente para a rede ele pode passar longos períodos sem validar qualquer bloco. Os pools reduzem essa incerteza ao permitir que vários agentes somem capacidade computacional e dividam os ganhos de forma mais previsível. Em termos práticos, trata-se de mecanismo de compartilhamento de risco, sem o qual muitos pequenos e médios participantes encontrariam dificuldade para permanecer ativos. A pool, portanto, não é simples desvio do ideal descentralizado. Em larga medida, ela é resposta organizacional racional aos custos, à aleatoriedade e à pressão competitiva intrínsecos ao proof of work (Rosenfeld, 2011).

Essa racionalidade econômica, contudo, produz efeitos ambivalentes. Se, por um lado, os pools viabilizam a permanência de agentes menores na atividade, por outro favorecem processos de agregação que podem deslocar poder de decisão e ampliar assimetrias internas. A literatura econômica tem mostrado que a centralização em pools não decorre apenas de vontade monopolística, mas do modo como risco, taxas cobradas, economias de escala e diversificação estratégica se articulam nesse mercado. Em muitas situações, a própria formação de pools ajuda a sustentar a participação distribuída, porque cria condições mais estáveis para mineradores avessos à volatilidade do retorno. Ainda assim, esse mesmo expediente pode reforçar dependências novas, tornando a autonomia do participante individual cada vez mais relativa diante dos centros de agregação de hash rate (Cong; He; Li, 2019).

A convivência entre cooperação e competição aparece, então, como traço estrutural dessas comunidades. Os mineradores cooperam porque precisam compartilhar regras mínimas, validar a mesma gramática protocolar e sustentar a credibilidade do registro coletivo. Ao mesmo tempo, competem intensamente pela obtenção de recompensas, pela redução de custos e pela maximização de sua presença no hash rate global. Não há contradição entre esses movimentos. A rede depende exatamente dessa articulação entre rivalidade econômica e adesão cooperativa a um conjunto comum de regras. O ecossistema não se mantém apesar desse atrito, mas por meio dele. Em linguagem mais precisa, a competição se desenrola dentro de uma moldura cooperativa, e essa moldura só se preserva enquanto os participantes entenderem que seguir as regras continua sendo estratégia mais vantajosa do que tentar destruí-las (Hou; Chen, 2020).

A despeito disso, o risco de concentração do poder computacional nunca desaparece. Se determinado agente ou grupo de agentes logra controlar parcela muito expressiva do hash rate, a promessa de resistência à censura, neutralidade procedimental e segurança da rede fica tensionada. O problema não se resume ao clássico ataque de maioria. Há também cenários em que coalizões menores, mas estrategicamente organizadas, obtêm ganhos desproporcionais ou induzem outros participantes a aderir a comportamentos oportunistas. A literatura sobre selfish mining mostrou, com clareza, que a segurança do sistema não pode ser descrita apenas pela fórmula simplificada segundo

a qual “menos de 50%” bastaria para afastar ameaças relevantes. A distribuição do poder computacional, a conectividade entre participantes e os incentivos postos pelo protocolo importam decisivamente (Eyal; Sirer, 2014).

Por isso, a concentração em torno de grandes pools ou operações empresariais não é mera curiosidade empírica. Ela altera a textura política da rede. Quando poucos agentes passam a controlar parcela expressiva da capacidade de mineração, aumenta a possibilidade de censura seletiva de transações, influência sobre debates de atualização do protocolo e maior capacidade de impor ritmos decisórios ao restante do ecossistema. Medições comparativas de descentralização em Bitcoin e Ethereum mostraram que a fragmentação do controle está longe de ser absoluta e que discussões públicas sobre a saúde dessas redes, muitas vezes, partem mais de pressupostos normativos do que de observação da arquitetura realmente existente. Em redes abertas, a descentralização precisa ser verificada, não presumida (Gencer *et al.*, 2018).

Esse quadro ajuda a entender por que as comunidades de mineração são atravessadas por disputas que ultrapassam a obtenção imediata de recompensas. Debates sobre tamanho de bloco, velocidade de confirmação, atualização do software, desenho dos incentivos e legitimidade dos processos decisórios mostram que a vida dessas redes não se esgota no código. Há governança da infraestrutura, e não apenas governança pela infraestrutura. Em outras palavras, o protocolo organiza parte das interações, mas os conflitos sobre a evolução do sistema dependem de arenas discursivas, lideranças técnicas, reputações acumuladas e articulações entre mineradores, desenvolvedores, operadores de nós e agentes de mercado. A comunidade, nesse cenário, funciona como instância difusa de coordenação política, ainda que rejeite formas clássicas de representação (De Filippi; Loveluck, 2016).

Nessa arena, mecanismos informais de coordenação assumem relevo. Fóruns, listas de discussão, repositórios de código, canais de comunicação entre operadores e convenções tácitas sobre comportamento esperado passam a integrar o funcionamento ordinário da rede. Muitas decisões que afetam profundamente a infraestrutura não resultam de comando soberano formal, mas de processos graduais de persuasão, adesão técnica e sedimentação comunitária. A autoridade se manifesta menos como imposição jurídica vertical e mais como capacidade de orientar interpretações legítimas do protocolo e de mobilizar apoio para certas mudanças. Em tais condições, cultura técnica, reputação e competência de implementação importam tanto quanto a força computacional propriamente dita (Werbach *et al.*, 2024).

Daí decorre uma consequência teórica relevante. A ausência de um centro administrativo não elimina figuras de ascendência nem dissolve assimetrias entre participantes. Desenvolvedores centrais, operadores de infraestrutura, grandes mineradores e agentes econômicos com elevada

capacidade de coordenação podem exercer influência decisiva sobre os rumos da rede, ainda que essa influência não assuma a forma tradicional de mando jurídico. O mito da completa horizontalidade encobre, assim, um cenário em que confiança, expertise e poder infraestrutural se distribuem de modo desigual. Em vez de negar a descentralização, esse diagnóstico a qualifica. Redes distribuídas podem reduzir dependências clássicas e, ao mesmo tempo, produzir novos núcleos de influência técnica e organizacional, cuja visibilidade pública nem sempre acompanha seu peso efetivo nas decisões do ecossistema (Walch, 2019).

Também a cultura que cerca a mineração contribui para moldar essas relações. Desde os primeiros fóruns até a consolidação de grandes operações, observa-se a persistência de valores ligados à autonomia individual, à defesa da abertura do código, à aversão à censura e à valorização da competência técnica como critério de reconhecimento. Tais valores, no entanto, convivem com pragmatismos de mercado, estratégias de proteção de rentabilidade e aceitação gradual de soluções que concentram capacidade operacional. O resultado é uma cultura tensionada entre imaginário igualitário de rede e experiência concreta de especialização, escassez de recursos e profissionalização. A comunidade de mineração não abandona seus símbolos originários, mas os reinscreve em cenário no qual máquinas, energia e capital moldam possibilidades reais de participação (Swartz, 2018).

A trajetória da mineração confirma, assim, que a descentralização é mais bem compreendida como problema de grau, arranjo e disputa do que como atributo absoluto. O protocolo abre espaço para participação distribuída, mas a forma histórica assumida por essa participação depende de fatores materiais e sociais que o código, sozinho, não controla. Pools, grandes fazendas de mineração, fabricantes de ASICs, operadores de nós e comunidades de desenvolvedores compõem uma tessitura em que cooperação, cálculo econômico, ideologia técnica e luta por influência se entrelaçam. Ler a mineração apenas como operação computacional empobrece o fenômeno. Ler apenas como conflito político também é insuficiente. O que está em jogo é a formação de uma infraestrutura sociotécnica na qual consenso, mercado e comunidade se produzem reciprocamente, dando ao ecossistema das criptomoedas sua forma histórica concreta (Hayes, 2019).

Em arremate, as comunidades de mineração mostram que a promessa de uma rede sem autoridade central não conduz a um mundo sem organização, sem coordenação e sem poder. Conduz, isto sim, a formas novas de distribuí-los, negociá-los e disputá-los. A mineração permanece, do ponto de vista técnico, como processo de validação e segurança. Mas, do ponto de vista social, ela se converteu em espaço no qual se definem pertencimentos, hierarquias, dependências e margens de influência dentro de ecossistemas digitais abertos. É nessa dupla condição, técnica e social, que seu exame ganha densidade e permite compreender por que as criptomoedas, longe de serem meros

artefatos financeiros, se afirmaram como laboratórios de organização coletiva mediados por código, infraestrutura e conflito (Dodd, 2018).

4. GOVERNANÇA E DINÂMICA DE VALIDAÇÃO DISTRIBUÍDA: PROCESSOS DECISÓRIOS E ESTABILIDADE DO SISTEMA

À medida que o ecossistema das criptomoedas amadureceu, tornou-se cada vez mais evidente que a descentralização, por si, não resolve o problema da coordenação coletiva. A supressão de um comando vertical formal não elimina a necessidade de decidir, interpretar regras, administrar conflitos e preservar a continuidade do sistema. Em redes distribuídas, a governança não desaparece. Ela muda de forma, de linguagem e de locus. Em vez de se concentrar em órgãos claramente identificáveis, passa a se manifestar por meio do protocolo, das rotinas de desenvolvimento, da aceitação comunitária do software e da capacidade prática de certos agentes influenciarem o funcionamento da rede. Por isso, o estudo da governança em blockchain exige abandonar a falsa oposição entre técnica e política, já que a própria infraestrutura passa a incorporar critérios de coordenação, inclusão, exclusão e autoridade difusa (Werbach *et al.*, 2024).

Essa particularidade ajuda a compreender por que a ausência de hierarquia formal não se confunde com ausência de poder. Redes como o Bitcoin não operam a partir de um centro institucional equivalente a um banco central, uma empresa administradora ou uma autoridade reguladora interna. Ainda assim, elas desenvolvem mecanismos de orientação coletiva, zonas de influência e práticas recorrentes de tomada de decisão. Há, de um lado, a governança pela infraestrutura, inscrita nas regras do protocolo e nas condições de validação dos blocos. Há, de outro, a governança da infraestrutura, que envolve debates sobre mudanças no código, interpretação de impasses técnicos e coordenação entre desenvolvedores, mineradores, operadores de nós, empresas e usuários economicamente relevantes. A crise em torno do tamanho dos blocos mostrou, com nitidez, que o simples fato de uma rede ser distribuída não a torna politicamente neutra nem socialmente autoexplicativa (De Filippi; Loveluck, 2016).

Os protocolos e as regras de consenso exercem, nesse cenário, função normativa. Eles não são mera descrição de procedimentos computacionais, porque delimitam comportamentos aceitáveis, fixam critérios de validade e estabelecem consequências para condutas incompatíveis com o desenho do sistema. Quando o protocolo define a forma do bloco, o nível de dificuldade, as condições para aceitação de transações e os incentivos econômicos envolvidos na mineração, ele está operando como estrutura regulatória interna da rede. Sua normatividade, contudo, difere da normatividade jurídica estatal. Não se trata de comando apoiado na coação institucional clássica, mas de um conjunto de

regras que disciplina o ambiente ao vincular participação, recompensa e legitimidade técnica a padrões verificáveis de conduta. O código, assim, adquire dimensão organizadora, sem que isso autorize tratá-lo como ordem autossuficiente ou impermeável à deliberação humana (Walch, 2019).

A estabilidade do sistema decorre, em larga medida, dessa articulação entre regra técnica e adesão social. Um bloco só se torna parte da história válida da rede porque os demais participantes aceitam as condições que tornam aquela prova reconhecível como legítima. O consenso não é simples unanimidade subjetiva, mas convergência prática em torno de um mesmo histórico transacional. Nesse sentido, a validação distribuída envolve dupla camada. Há, primeiro, a verificação criptográfica das transações e do bloco candidato. Há, depois, a incorporação desse resultado ao comportamento coletivo dos nós que continuam a construir sobre a cadeia aceita. Sem esse segundo momento, a prova isolada não se converte em estabilidade sistêmica. O consenso, portanto, é sempre processo socialmente sustentado por mecanismos técnicos de verificação (Nakamoto, 2008).

Os processos de atualização tornam essa realidade ainda mais visível. Toda vez que surge proposta de alteração relevante no protocolo, a rede é levada a confrontar não apenas uma escolha técnica, mas diferentes visões sobre segurança, escalabilidade, identidade do projeto e distribuição de custos entre os participantes. Atualizar um sistema descentralizado significa negociar continuidade e mudança em ambiente no qual ninguém detém, isoladamente, autoridade soberana para impor a solução. Por isso, disputas sobre alterações de software frequentemente expõem clivagens profundas entre grupos com interesses distintos. O conflito não se limita ao mérito funcional da proposta. Ele alcança o modo como a comunidade entende legitimidade, pertencimento e fidelidade ao desenho originário da rede (Hofman; Walters; Choi, 2021).

É nesse contexto que os forks assumem importância singular. Em termos gerais, o fork corresponde à bifurcação do caminho técnico ou normativo da rede. Algumas vezes, ele decorre de atualização compatível com versões anteriores. Em outras, traduz ruptura mais intensa, capaz de dividir a comunidade em cadeias distintas. O fork, portanto, não deve ser lido apenas como evento de programação. Ele é momento de explicitação do dissenso e de teste da capacidade de coordenação coletiva. Quando uma comunidade chega ao ponto de operar cadeias diferentes, o que está em disputa não é somente a melhor solução técnica, mas a autoridade para definir o que conta como continuidade legítima daquele sistema. A história das blockchains mostra que decisões dessa natureza emergem de processos controversos, marcados por alianças provisórias, retórica de legitimidade e disputas pela adesão dos participantes economicamente e tecnicamente mais influentes (De Filippi; Loveluck, 2016).

A segurança da rede depende, por sua vez, da solidez desse ambiente de validação e verificação. Em blockchains baseadas em proof of work, a confiança operacional decorre do custo

envolvido na tentativa de reescrever o histórico aceito, somado à dificuldade de coordenar agentes suficientes para subverter a lógica ordinária do protocolo. Cada bloco validado amplia o custo de reversão e fortalece a percepção de estabilidade do registro. Ainda assim, a segurança não é estado absoluto. Ela resulta de incentivos econômicos, distribuição do poder computacional, velocidade de propagação das informações, comportamento estratégico dos mineradores e desenho do próprio protocolo. Em outras palavras, não basta afirmar que a rede é segura porque utiliza criptografia. É preciso examinar como essa segurança é produzida em condições concretas de operação (Eyal; Sirer, 2014).

A literatura sobre ataques estratégicos demonstrou, inclusive, que a estabilidade da rede pode ser comprometida antes mesmo de uma maioria absoluta de poder computacional ser alcançada. A hipótese do selfish mining foi decisiva para corrigir visões excessivamente simplificadas a respeito da segurança do Bitcoin. O estudo mostrou que grupos coordenados de mineradores podem manipular a publicação de blocos e obter rendimento superior à sua fração “justa” de poder computacional, criando incentivos para expansão oportunista da coalizão. Isso significa que a integridade do sistema não depende apenas de barrar um ataque frontal de 51%, mas de observar como o protocolo recompensa ou desestimula comportamentos estratégicos que corroem, gradualmente, a descentralização prometida. O ponto mais sensível não está apenas na violação aberta das regras, mas na possibilidade de explorá-las de forma formalmente compatível e materialmente desestabilizadora (Eyal; Sirer, 2014).

A prevenção de ataques exige, assim, um equilíbrio delicado entre incentivo econômico, arquitetura do consenso e vigilância coletiva. Validar e verificar blocos não é suficiente quando a estrutura remuneratória da rede pode estimular coordenações nocivas, concentração em pools dominantes ou estratégias de vantagem assimétrica. A segurança passa, então, a depender de monitoramento contínuo do comportamento da rede e de capacidade comunitária para reconhecer vulnerabilidades antes que se consolidem em crise sistêmica. Mesmo em ecossistemas que se apresentam como autônomos, a estabilidade concreta exige observação social permanente, produção de conhecimento especializado e disposição para rever mecanismos que se mostrem suscetíveis a exploração oportunista. A rede distribuída, nesse ponto, aparece menos como máquina autossustentável e mais como ordem em manutenção constante (Nabben, 2024).

Essa constatação conduz à tensão mais persistente do tema. O ideal normativo da descentralização convive, na prática, com formas relevantes de centralização operacional. Grandes pools de mineração, desenvolvedores com alta capacidade de coordenação, provedores de infraestrutura, fabricantes de hardware e plataformas com forte poder econômico acabam ocupando posições desproporcionais dentro do ecossistema. A descentralização segue funcionando como

referência identitária e critério de legitimidade, mas sua realização concreta se dá em ambiente atravessado por assimetrias de capital, expertise, conectividade e influência. Em vez de uma horizontalidade plena, o que se observa é uma descentralização tensionada, parcial e constantemente renegociada (Walch, 2017).

Essa assimetria se projeta diretamente sobre os processos decisórios. Embora toda alteração relevante dependa, em algum grau, de adesão difusa da comunidade, alguns atores possuem mais condições de moldar a agenda, enquadrar o debate e converter sua preferência em caminho tecnicamente executável. A autoridade prática, nesse ambiente, costuma nascer da combinação entre reputação técnica, capacidade de implementação, controle infraestrutural e posição econômica. Por isso, a governança distribuída não deve ser romantizada como deliberação perfeitamente igualitária. Ela oferece barreiras relevantes ao mando centralizado clássico, mas não suprime disputas por predominância nem impede a formação de polos de influência persistentes. O exame empírico das blockchains contemporâneas indica justamente isso, que a governança distribuída opera como arranjo híbrido, onde abertura protocolar e concentração factual coexistem em tensão permanente (Werbach *et al.*, 2024).

Sob esse prisma, a dinâmica de validação distribuída deve ser compreendida como forma historicamente situada de organização da confiança coletiva. Ela não repousa em autoridade estatal nem em hierarquia empresarial unitária, mas tampouco se resolve por simples espontaneidade técnica. Seu funcionamento depende de protocolos, incentivos, cultura comunitária, rotinas de desenvolvimento, mecanismos de verificação e estruturas materiais de poder que condicionam quem pode participar, influenciar e permanecer na rede. A governança, portanto, não se apresenta como elemento externo ao sistema. Ela integra o próprio modo de existência da blockchain, orientando tanto a produção do consenso cotidiano quanto as respostas a crises, disputas e riscos de centralização. É nesse ponto que a promessa das redes descentralizadas encontra seu teste mais exigente, porque sua estabilidade não se mede apenas pela resistência técnica a ataques, mas pela capacidade de manter coordenação legítima sem sacrificar, no plano operacional, a pluralidade que lhes dá sentido (De Filippi; Loveluck, 2016).

5. CONSIDERAÇÕES FINAIS

Ao longo do percurso desenvolvido, buscou-se demonstrar que a mineração de criptomoedas não se reduziu a um procedimento técnico de validação, nem pôde ser compreendida como um simples mecanismo econômico de geração de ativos digitais. O que se tornou mais claro, ao longo da

discussão, foi sua inserção em um arranjo sociotécnico em que infraestrutura computacional, incentivos econômicos, cultura comunitária e disputas por coordenação se coadunam.

Desse modo, a mineração passou a ser compreendida como prática situada no ponto de encontro entre cálculo criptográfico e construção social da confiança, movendo o eixo tradicional de validação das instituições centralizadas para mecanismos distribuídos, sem que isso tenha eliminado relações de poder e assimetrias internas.

Também se verificou que as comunidades de mineração, longe de formarem espaços homogêneos, passaram a reproduzir dinâmicas próprias de cooperação e disputa, nas quais a formação de *pools*, a especialização técnica e a concentração de recursos influenciaram a distribuição de poder no interior da rede. A promessa de descentralização permaneceu como horizonte normativo, mas sua realização mostrou-se condicionada por fatores materiais, econômicos e organizacionais que, com o passar do tempo, redefiniram as possibilidades concretas de participação.

No plano da governança, observou-se que a ausência de hierarquia formal não significou ausência de coordenação. Ao contrário, tornou-se visível o surgimento de formas difusas de autoridade, apoiadas no protocolo, na capacidade de desenvolvimento do código e na adesão prática dos participantes. Processos como *forks*, disputas interpretativas e atualizações do sistema mostraram que a estabilidade da rede depende de negociação entre técnica e comunidade, exigindo mecanismos de validação que fossem, ao mesmo tempo, verificáveis e socialmente aceitos.

REFERÊNCIAS

CARDOSO, Bruno Campos. Algoritmos como “máquinas de cultura”: notas sobre política e produção de consenso no sistema peer-to-peer Bitcoin. In: REUNIÃO DE ANTROPOLOGIA DA CIÊNCIA E DA TECNOLOGIA, 7., 2019, Florianópolis. **Anais [...]**. Florianópolis: ReACT, 2019. Disponível em: <https://ocs.ige.unicamp.br/ojs/react/article/view/2678>. Acesso em: 31 mar. 2026.

CARDOSO, Bruno Campos. **Governança digital e o processo de mineração**: especialização e controvérsias no sistema peer-to-peer Bitcoin. Trabalho apresentado na 31. Reunião Brasileira de Antropologia, Brasília, 2018. Disponível em: https://www.abant.org.br/files/1543880565_ARQUIVO_bruno-cardoso_2018_governanca-digital-processo-de-mineracao-bitcoin.pdf. Acesso em: 31 mar. 2026.

CONG, Lin William; HE, Zhiguo; LI, Jiasun. Decentralized mining in centralized pools. **Review of Financial Studies**, Oxford, v. 34, n. 3, p. 1191-1235, 2021.

COSTARDI, Carla Maria de Oliveira Costardi. The ideological background of bitcoin: the unintended, but predicted, convenience of anonymity for criminal activities. **Revista Brasileira de Ciências Policiais**, v. 12, n. 4, p. 75-99, 2021.

DE FILIPPI, Primavera; LOVELUCK, Benjamin. The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. **Internet Policy Review**, Berlin, v. 5, n. 3, 2016.

DODD, Nigel. The social life of Bitcoin. **Theory, Culture & Society**, London, v. 35, n. 3, p. 35-56, 2018.

EYAL, Ittay; SIRER, Emin Gün. Majority is not enough: Bitcoin mining is vulnerable. In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 18., 2014, Christ Church. **Proceedings [...]**. Berlin: Springer, 2014. p. 436-454.

GENCER, Adem Efe *et al.* Decentralization in Bitcoin and Ethereum networks. In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 22., 2018, Nieuwpoort. **Proceedings [...]**. Berlin: Springer, 2018. p. 439-457.

GREVE, Fabíola *et al.* Blockchain e a revolução do consenso sob demanda. In: SBC. **Minicursos do SBRC 2018**. Porto Alegre: Sociedade Brasileira de Computação, 2018. Disponível em: <https://books-sol.sbc.org.br/index.php/sbc/catalog/view/30/116/275>. Acesso em: 31 mar. 2026.

HABER, Stuart; STORNETTA, W. Scott. How to time-stamp a digital document. **Journal of Cryptology**, New York, v. 3, n. 2, p. 99-111, 1991.

HAYES, Adam. The socio-technological lives of Bitcoin. **Theory, Culture & Society**, London, v. 36, n. 4, p. 49-72, 2019.

HOFMAN, David; WALTERS, Ryan; CHOI, Bernard. Blockchain governance: de facto (x) or designed? In: ADVANCES IN FINANCIAL TECHNOLOGIES, 2021. **Proceedings [...]**. [S. l.]: [s. n.], 2021. Disponível em: <https://www.cs.ubc.ca/~bestchai/papers/2021-bchain-governance.pdf>. Acesso em: 31 mar. 2026.

HOU, Binbing; CHEN, Feng. A study on nine years of Bitcoin transactions: understanding real-world behaviors of Bitcoin miners and users. In: IEEE 40TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, 2020. **Proceedings [...]**. Los Alamitos: IEEE, 2020.

MUCELLI, Tadeus; MOURA, Maria Aparecida. O papel da tecnologia blockchain e do conceito de redes P2P na descentralização de acervos de arte: uma introdução ao desafio. **Revista Ibero-Americana de Ciência da Informação**, Brasília, v. 17, n. 1, p. 85-114, 2024.

NABBEN, Kelsie; DE FILIPPI, Primavera. Accountability protocols? On-chain dynamics in blockchain governance. **Internet Policy Review**, Berlin, v. 13, n. 4, 2024.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. [S. l.]: [s. n.], 2008.

REBELLO, Gabriel Antonio F. *et al.* A security and performance analysis of proof-based consensus protocols. **Annals of Telecommunications**, Cham, v. 76, n. 11-12, p. 713-739, 2021.

ROSENFELD, Meni. Analysis of Bitcoin pooled mining reward systems. **arXiv**, 2011. Disponível em: <https://arxiv.org/abs/1112.4980>. Acesso em: 31 mar. 2026.

SWARTZ, Lana. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. **Cultural Studies**, London, v. 32, n. 4, p. 623-650, 2018.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

WALCH, Angela. In code(rs) we trust: software developers as fiduciaries in public blockchains. In: DE FILIPPI, Primavera; WRIGHT, Aaron (ed.). **Blockchain and the law**. Cambridge: Harvard University Press, 2019.

WALCH, Angela. The path of the blockchain lexicon (and the law). **Review of Banking & Financial Law**, Boston, v. 36, n. 2, p. 713-765, 2017.

WERBACH, Kevin *et al.* Blockchain governance in the wild. **Cryptoeconomic Systems**, v. 3, n. 1, 2024.