UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ

INSTITUTO DE ECONOMIA

CURSO DE GRADUAÇÃO EM CIÊNCIAS ECONÔMICAS

Sérgio da Costa Lins Junior

(IN) EFICIÊNCIA ENERGÉTICA DAS REDES BLOCKCHAINS: O FIM DO PROOF-OF-WORK?

Rio de Janeiro
2023

Sérgio da Costa Lins Junior

(IN) EFICIÊNCIA ENERGÉTICA DAS REDES BLOCKCHAINS: O FIM DO PROOF-OF-WORK?

Trabalho de Conclusão de Curso apresentado ao Instituto de Economia da Universidade Federal do Rio de Janeiro – UFRJ, como exigência para obtenção do título de Bacharel em Ciências Econômicas.

Orientador: Professor Dr. Marcelo Colomer

Rio de Janeiro
2023

CIP - Catalogação na Publicação

L759(Lins Junior, Sérgio da Costa
(IN)EFICIÊNCIA ENERGÉTICA DAS REDES BLOCKCHAINS: O FIM DO PROOF-OF-WORK / Sérgio da Costa Lins Junior. -- Rio de Janeiro, 2023.
71 f.

Orientador: Marcelo Colomer.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Instituto de Economia, Bacharel em Ciências Econômicas, 2023.

1. Criptomoedas. 2. Blockchains. 3. Proof-of Works. I. Colomer, Marcelo, orient. II. Titulo.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

SÉRGIO DA COSTA LINS JUNIOR

(IN) EFICIÊNCIA ENERGÉTICA DAS REDES BLOCKCHAINS: O FIM DO PROOF-OF-WORK?

Trabalho de conclusão de curso apresentado ao Instituto de Economia da Universidade Federal do Rio de Janeiro, como requisito para a obtenção do título de Bacharel em Ciências Econômicas.

Rio de Janeiro, 14/12/2023.

MARCELO COLOMER FERRARO - Presidente
Professor Dr. do Instituto de Economia da UFRJ

DIOGO LISBONA ROMEIRO
Doutor em Economia pela UFRJ

VICENTE ANTONIO DE CASTRO FERREIRA
Professor Dr. do Instituto de Economia da UFRJ

AGRADECIMENTOS

A presente oportunidade é propícia para que eu possa expressar meus sinceros agradecimentos a todos aqueles que colaboraram de forma significativa para a realização deste trabalho acadêmico. Nesse sentido, é importante destacar a fundamental contribuição de meu orientador Marcelo Colomer, que, com sua competência, dedicação e expertise, ofereceu uma orientação precisa e assertiva, fundamental para a conclusão deste trabalho que integra duas áreas distintas de conhecimento.

Não posso deixar de reconhecer o imprescindível apoio que recebi de meus pais, Sérgio da Costa Lins e Mara Pinto Gomes Lins que sempre me incentivaram na formação do meu intelecto e na busca de meus objetivos acadêmicos, confiando em todo o meu potencial e proporcionando as condições necessárias para que eu pudesse concluir esta pesquisa. Desta forma, estendo, com muito carinho, meus agradecimentos a minha avó, Yolanda da Costa Lins, que sempre investiu na minha educação, sendo essencial em minha caminhada até aqui. Adicionalmente, agradeço ao meu tio e padrinho Alexsandro Fontenele pelo apoio.

Agradeço também aos demais professores e funcionários do Instituto de Economia da UFRJ, que disponibilizaram seu tempo, conhecimentos e recursos, de modo a me permitir desenvolver um grau de estudo consistente e aprofundado e uma visão mais holística da economia e da sociedade de um modo geral. Igualmente, não posso deixar de reconhecer o importante apoio dos meus amigos, atuais e futuros colegas de profissão, que fiz durante minha passagem na instituição, que de alguma forma contribuíram para a expansão da minha visão de mundo.

Por fim, reitero meus sinceros agradecimentos a todos os envolvidos neste processo, que foram fundamentais para a concretização deste trabalho acadêmico. Expresso, assim, minha gratidão por toda a colaboração recebida e por toda a experiência enriquecedora vivenciada.

Os maiores avanços da civilização, seja na arquitetura ou na pintura, na ciência e na literatura, na indústria ou na agricultura, nunca vieram de um governo centralizado.
Milton Friedman.

RESUMO

A presente dissertação estuda e analisa o processo de validação de transações de criptomoedas como atividade econômica, enunciando o problema do seu alto consumo energético, sugerindo alternativas menos impactantes ao sistema elétrico. O processo de validação de transações de criptomoedas é comumente denominado de mineração e consiste no emprego de poder computacional para resolver um enigma criptográfico, recebendo uma recompensa pelo esforço empregado nesta resolução. Com o aumento do grau de dificuldade da mineração de criptomoedas e da menor recompensa obtidas pelo processo de validação das mesmas, mais poder computacional é necessário para manter o nível de lucratividade, ocasionando em um aumento geral no consumo elétrico do setor. Esse estudo aborda, de modo holístico, todo o processo de validação de criptoativos, comparando as diferentes formas validadora, enunciando de forma aprofundada todo o processo técnico das diferentes validações blockchain. Os resultados desta análise mostram que o processo de mineração de criptomoedas possui um impacto massivo no consumo elétrico e deve ser levado em consideração para guiar o futuro do setor, sob a forma do rumo dos avanços tecnológicos ou regulatórios. O estudo conclui que um futuro com um uso generalizado de criptoativos na sociedade, de modo geral, depende de uma melhor eficiência energética dos mesmos, incluindo a adoção de uma matriz elétrica sustentável para o processo de validação das blockchains.

Palavras-chave: Sistema Elétrico; Blockchain; Criptomoedas

ABSTRACT

The present dissertation studies and analyzes the validation process of cryptocurrency transactions as an economic activity, enunciating the problem of its high energy consumption, suggesting less impactful alternatives to the electrical system. The process of validating cryptocurrency transactions is commonly called mining and consists of using computational power to solve a cryptographic enigma, receiving a reward for the effort employed in this resolution. With the increase in the degree of difficulty of cryptocurrency mining and the lower reward obtained by the validation process, more computational power is needed to maintain the level of profitability, resulting in a general increase in the sector's electrical consumption. This study addresses, in a holistic way, the entire crypto-asset validation process, comparing the different validator forms, enunciating in depth the entire technical process of the different blockchain validations. The results of this analysis show that the cryptocurrency mining process has a massive impact on electrical consumption and should be taken into account to guide the future of the sector, in the form of technological or regulatory advances. The study concludes that a future with widespread use of crypto-assets depends on their improved energy efficiency, including the adoption of a sustainable electrical matrix for the blockchain validation process.

Keywords: Electrical System; Blockchain; Cryptocurrencies

Sumário

Capítulo 1 - INTRODUÇÃO

O século XXI trouxe consigo transformações tecnológicas que impactaram diretamente o cotidiano das relações sociais e comerciais pelo mundo. Do início da internet da banda larga, ao primeiro smartphone, aos poucos vimos uma sociedade cada vez mais digitalizada, e com a moeda não seria diferente. Em 2008, surgiu a Bitcoin – uma proposta de moeda virtual descentralizada – com a premissa tecnológica de estabelecer uma plataforma segura de transações sem a necessidade de órgãos governamentais garantido seu valor ou uso social. Nakamoto (2008), propõe uma solução descentralizada para os meios de pagamento descentralizados, sobretudo referente ao problema de gasto duplo usando um servidor *peer-to-peer (P2P).*

Em 2008, o conceito de blockchain surge originalmente como a base operacional da Bitcoin, a criptomoeda com a maior captação de mercado (*market cap*) do mundo. Em resumo, a blockchain é uma plataforma de contratos inteligentes, que despreza a necessidade de um órgão mediador legal, capaz de registrar transações de forma descentralizada. Para que uma transação seja bem-sucedida na rede, é necessário que esta seja confirmada por múltiplos agentes validadores, tornando assim virtualmente impossível qualquer tipo de fraude do sistema, o que, por fim, a consolidou como a mais segura e rápida forma de autenticação de contratos em todo mundo.

A consolidação da tecnologia *blockchain* independente é vista por muitos governos como uma ameaça. Inicialmente, essa percepção se deve à preocupação com a possível fuga de controle estatal em relação às transações financeiras. Isso, por sua vez, poderia resultar em episódios de evasão fiscal e lavagem de dinheiro. Além disso, posteriormente, observou-se que a tecnologia *blockchain* foi responsável por diminuir a margem de segurança energética dos países que hospedam o poder de processamento da rede. Nos últimos 10 anos, o tráfego de dados, que dão origem as criptomoedas, expandiu de maneira inimaginável. Entretanto, as preocupações e críticas associadas ao elevado consumo de energia são mais recentes e datam de 2017, quando a formação de uma bolha especulativa em torno dos preços das criptomoedas tornou o processo de mineração dos novos ativos momentaneamente uma atividade com rentabilidade acima da média dos demais setores, com a mediana de ROI entre 6% e 7,5% entre os anos de 2012-2016 (DERKS et al, 2018), que precederam os primeiros estudos acerca do impacto energético do processo de mineração de criptoativos.

Mais recentemente, em 2021, novamente um ciclo de valorização dos criptoativos fez aumentar a popularidade da criptomineração como atividade econômica. Em ambas as situações, as valorizações refletiram uma maior profissionalização do segmento, significando também uma maior concentração da rede que nascera com a premissa da descentralização.

Ainda que o desenvolvimento da blockchain tenha sido apoiado exclusivamente por entusiastas de criptoativos, atualmente é objeto de estudo e interesse do setor energético, contando com inúmeros projetos em implantação ou fase inicial nos quais é possível a integração entre produtor e consumidor final de energia, utilizando a infraestrutura já presente para distribuição. O amadurecimento das criptomoedas, não apenas como meio de pagamento, mas também como plataformas de smart *contracts*, traz consigo um debate sobre a sustentabilidade energética da própria rede *blockchain*.

Apesar da conjuntura mundial apresentar uma tendência a eficiência energética, de acordo com o *Energy Efficiency 2022* da IEA – que aponta para um aumento de 2% na eficiência energética em relação ao ano anterior –, o contínuo aumento por demanda elétrica das *blockchains*, destacando-se as da Bitcoin e do Ethereum, ameaça a estabilidade do Sistema Elétrico (S.E) de países hospedeiros do poder de processamento da rede como é o caso da China, que chegou a concentrar cerca de 70% do poder de rede na mineração de criptomoedas, de acordo com o *Cambridge Electricity Consumption Index* (2022).

Este estudo tem como objetivo principal investigar o impacto dos diferentes sistemas de blockchain sobre o consumo energético de diferentes países. Para isso, serão apresentados os desafios e as novas soluções associados à evolução tecnológica do processo de mineração. Desta forma, será adotada uma abordagem metodológica estruturada, com o intuito de fornecer uma análise sistemática e rigorosa sobre o tema.

A metodologia utilizada neste trabalho pode ser dividida em três etapas principais. Primeiramente, será realizada uma revisão bibliográfica técnica, de modo a conduzir o leitor aos conceitos, teorias e os diferentes argumentos relacionados ao debate acerca do consumo energético das blockchains. Nessa monografia, o uso dos termos "criptomoedas" e "criptoativos" serão utilizados como sinônimos, ainda que autores façam a diferenciação dos termos.

Em seguida, será conduzida uma coleta de dados quantitativos, incluindo uma amostragem representativa dos impactos do consumo elétrico dos diferentes modelos de *blockchains.* Nesta etapa serão considerados indicadores específicos de consumo energético, como o consumo médio em TWh – terawatts-hora –, para avaliar o impacto dessas tecnologias no sistema energético de forma geral, sobretudo em países que concentram a indústria da mineração de criptoativos. Por fim, será realizada uma análise qualitativa dos dados coletados, empregando métodos de pesquisa qualitativa, como análise da evolução do impacto da criptomineração na demanda elétrica. Isso permitirá compreender os fatores contextuais, as percepções dos usuários e as estratégias adotadas pelas organizações para lidar com o consumo energético das *blockchains*.

A monografia foi estruturada em 3 capítulos além dessa introdução e da conclusão. No primeiro capítulo, discutiremos as variantes de estruturas da rede blockchain e os diversos

métodos usados para verificar as transações e para se aumentar a segurança e integridade do sistema. No segundo capítulo, exploraremos a complexa relação entre os criptoativos e moedas privadas, examinando a trajetória de como estes ativos digitais vêm se consolidando. Por fim, no terceiro capítulo, abordaremos os problemas de consumo de energia associados às atividades de mineração dos criptoativos e discutiremos as soluções tecnológicas e regulamentárias propostas para reduzir o seu impacto energético. Através desta revisão, procuramos fornecer uma perspectiva abrangente e crítica sobre os desafios e oportunidades que o blockchain e os criptoativos apresentam para a sociedade moderna, contribuindo neste caso para um rico debate acadêmico neste campo em constante evolução.

Capítulo 2 - BLOCKCHAIN: MUITO ALÉM DA BITCOIN

A *blockchain* é apontada pela Columbia Business School (2023) como uma tecnologia disruptiva mais cativante e discutidas no cenário contemporâneo, e, todavia, não é explorada em sua totalidade e, portanto, se faz necessário desmistificar tópicos basais da mesma. Em primeiro lugar, é importante separar os conceitos da *blockchain* como tecnologia disruptiva e da *bitcoin* como a vanguarda das moedas digitais. De acordo com The Economist (2015), "para entender o poder dos sistemas blockchain e as coisas que eles podem fazer, é importante distinguir entre três coisas que são comumente confusas, ou seja, a moeda bitcoin, a blockchain específica que a sustenta e a ideia de blockchains em geral." Muito além da Bitcoin, a blockchain é cada vez mais presente em aplicações digitais, sejam financeiras ou de dados de forma geral.

Podemos definir a *blockchain* como um banco de dados virtual descentralizado, isto é, uma plataforma digital onde transações e contratos inteligentes (*smart contracts*) são registrados através de múltiplos agentes validadores, sem necessidade de mecanismos tradicionais de validação como cartórios ou bancos. Dentro da *blockchain*, todas as transações são armazenadas em blocos, ligados uns aos outros por elos, conhecidos como *hashes*. A união desses elos forma uma cadeia de blocos, de onde surge o nome da rede (*blockchain* em tradução livre), que garante o funcionamento da plataforma ao se responsabilizar com a segurança das transações de informações realizadas, seja sob a forma de contratos ou com a transferência unilateral de criptomoedas. Ao contrário de sistemas bancários, que dependem de um servidor central, os registros feitos nas novas plataformas são armazenados em diversos computadores ao redor do mundo, com seu grau de descentralização sendo determinado pelo sistema de validação da mesma. Ao operarem simultaneamente, os agentes validadores de uma determinada *blockchain* funcionam de modo a validar informações verdadeiras e impedir que sejam inseridas informações falsas, garantindo assim o funcionamento da rede.

O surgimento da *blockchain* é o pontapé inicial de um movimento de descentralização baseado na tecnologia. Através dela, tornou-se possível estabelecer relações de confiabilidade entre múltiplos agentes sem a necessidade de um mediador centralizado. De acordo com Di Pierro (2017), o protocolo *blockchain* da Bitcoin, elaborado em 2008 por Satoshi Nakamoto resolveu este problema ao divulgar publicamente as transferências, tornando a rede *blockchain* um livro-contábil descentralizado e facilmente verificável.

> O problema que Nakamoto resolveu com o blockchain foi o de estabelecer confiança em um sistema distribuído. Mais especificamente, o problema de criar um armazenamento distribuído de documentos com carimbo de data/hora em que nenhuma parte pode adulterar o conteúdo dos dados ou os carimbos de data/hora sem detecção.

> [...] Para resolver isso, o blockchain fornece um mecanismo de confiança distribuído: várias partes mantêm um registro das transações e todas as partes podem verificar se o pedido e os carimbos de data e hora das transações não foram adulterados (Di Pierro, 2017, p.1).

Se imaginássemos uma determinada rede *blockchain* como o sistema elétrico, os agentes validadores seriam as linhas de transmissão de energia (informações) entre dois ou mais pontos, essenciais para retroalimentação do sistema como um todo, garantindo que a energia (informação) seja transportada do gerador (remetente) ao consumidor final (destinatário). Estes agentes, além de levarem informações P2P (sigla referente a ponto-a-pontos em inglês), fazem parte de todo um mecanismo de validação de dados e, através dessa forma, são recompensados pelos seus esforços empregados no poder de processamento das transações, criando assim um ecossistema econômico formado por empresas especializadas em diversos segmentos, desde a mineração, segurança de dados e corretagem das moedas digitais.

Satoshi Nakamoto (2008. p.2), define a rede *blockchain* como sendo uma sequência, em cadeia, de assinaturas digitais. Cada vez que um agente remetente transfere a moeda, acaba por assinar digitalmente um *hash* – número hexadecimal determinístico – da transação anterior, junto com a chave pública do agente receptor e adicionando-os ao final da moeda. Deste modo, o criador anônimo da rede Bitcoin idealiza a blockchain de modo semelhante a um livro-contábil, sendo a criptomoeda o ativo circulante a ser transacionado e registrado dentro deste sistema.

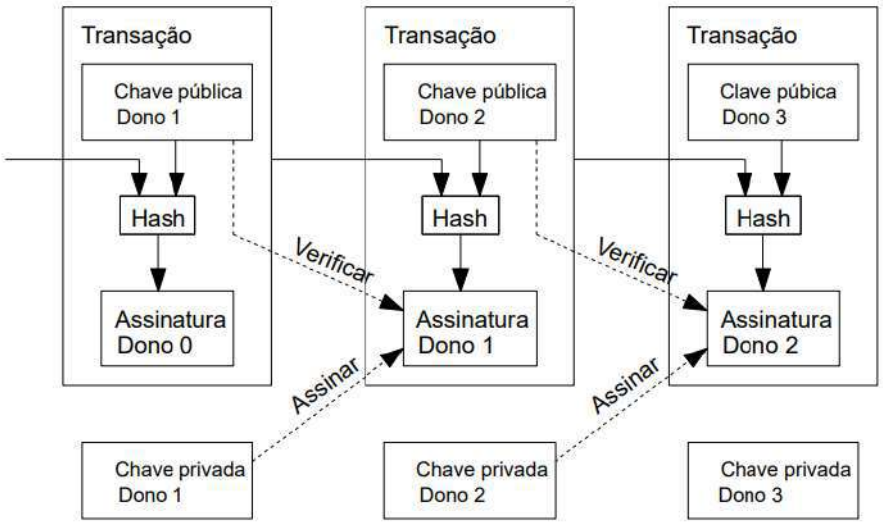


Figura 1: Esquema de transações dentro da *blockchain* da Bitcoin

Fonte: Satoshi Nakamoto (2008, p.2)

Nakamoto (2008), aponta a possibilidade de gasto duplo (double spending) por parte de um agente mal-intencionado, sendo este um dos principais desafios para a construção de um

sistema de transferências confiável e sustentável. A revolução inserida dentro da blockchain consiste justamente em elaborar uma solução alternativa descentralizada para este propósito.

> O problema, claro, é que o beneficiário não pode verificar se um dos proprietários não gastou duas vezes a moeda. Uma solução comum é introduzir uma autoridade central confiável, ou casa da moeda, que verifica todas as transações para evitar gastos duplos. [...] O problema com esta solução é que o destino de todo o sistema monetário depende da empresa que administra a casa da moeda, com todas as transações tendo que passar por ela, assim como um banco. Precisamos de uma maneira para o beneficiário saber que os proprietários anteriores não assinaram as transações anteriormente. Para nossos propósitos, a transação mais antiga é a que conta, então não nos importamos sobre tentativas posteriores de gastar duas vezes. A única maneira de confirmar a ausência de uma transação é estar ciente de todas as transações. [...] Para conseguir isso sem uma parte confiável, as transações devem ser anunciadas publicamente, e precisamos de um sistema para que os participantes concordem em um único histórico da ordem em que foram recebidos. O beneficiário necessita de prova de que, no momento de cada transação, o a maioria dos nós concordou que foi o primeiro recebido (Nakamoto, 2008, p.2. Tradução própria).

De modo a tornar a *blockchain* um verdadeiro livro-razão descentralizado e passível de auditoria por qualquer usuário da mesma, Nakamoto (2008), propõe uma solução de *timestamp*[1] (carimbo temporal, em tradução adaptada). Segundo Satoshi Nakamoto, este mecanismo de demarcação temporal resulta em um sistema completo do histórico de ações (transferências), resolvendo a questão da possibilidade de gasto duplo (*double spending*) em um sistema descentralizado de pagamentos, agregando confiabilidade ao mesmo.

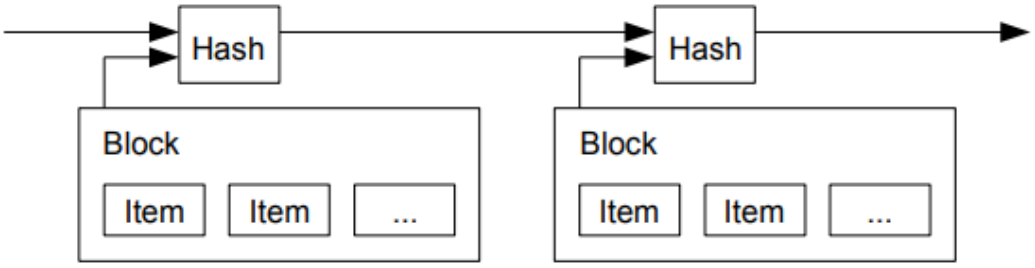


Figura 2: Esquema de carimbo temporal (*timestamp*) dentro da *blockchain* da Bitcoin

Fonnte: Satoshi Nakamoto (2008, p.2)

[1] Um servidor de *timestamp* funciona tomando um hash de um bloco de itens a serem marcados com data e hora e publicando amplamente o hash [...] O carimbo de data/hora prova que os dados devem ter existido no tempo, obviamente, para entrar no hash. Cada carimbo de data/hora inclui o carimbo de data/hora anterior em seu hash, formando uma cadeia, com cada *timestamp* adicional reforçando os anteriores. [...] Para nossa rede de *timestamp*, implementamos a prova de trabalho incrementando um *nonce*[1] no bloco até que seja encontrado um valor que dê ao hash do bloco os bits zero necessários. Uma vez que um esforço computacional foi gasto para realizar a prova de trabalho, o bloco não pode ser alterado sem refazer o trabalho. À medida que os blocos posteriores são encadeados depois dele, o trabalho para alterar o bloco incluiria refazer todos os blocos depois dele (Nakamoto, 2008. p.2. Tradução própria).

É através do sistema de *timestamp*, primeiramente adotado pela bitcoin e posteriormente difundido para as demais criptomoedas que surgiram após a criação das mesmas, que as blockchains são consideradas “vias de mão única” – isto é, após uma transferência ser aprovada por uma série de agentes validadores, um determinado montante é enviado de uma carteira A para uma carteira B, não sendo possível desfazê-la. Dessa forma, alguns autores acendem um alerta para o risco de criptoativos serem utilizados para fins ilícitos. De acordo com Liao et. Al (2016 p.2. Tradução própria), “na Bitcoin transações são essencialmente irreversíveis. Esse recurso, aliado com o pseudônimo da Bitcoin, permite que os cibercriminosos cometam fraude financeira que é virtualmente impossível de reverter e difícil de rastrear”.

Os avanços teóricos obtidos após a consolidação da blockchain proporcionaram um alicerce para o surgimento de novas propostas de blockchain cada vez mais específicas, consolidando, de fato, a tecnologia blockchain muito além da Bitcoin. De acordo com Vitalik Buterin (2014), co-fundador da rede Ethereum, Satoshi Nakamoto tem papel fundamental, como descrito em *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform:*

> A inovação proporcionada por Satoshi é a ideia de combinar um consenso descentralizado aliado com um protocolo muito simples, baseado em nós que combinam transações em um "bloco" a cada dez minutos criando um blockchain em constante crescimento, com prova de trabalho como um mecanismo através do qual os nós ganham o direito de participar do sistema. Enquanto nós com uma grande quantidade de poder computacional, temos influência proporcionalmente maior, chegando com mais poder computacional do que toda a rede combinada é muito mais difícil do que simular um milhão de nós. Apesar do modelo de blockchain do Bitcoin crueza e simplicidade, provou ser bom o suficiente, e nos próximos cinco anos se tornaria a base de mais de duzentas moedas e protocolos em todo o mundo (Vitalik, 2014, p. 4. Tradução própria).

2.1 As diferentes estruturas de rede blockchain e suas características

O processo de validação das transações é parte vital para o funcionamento das *blockchains* de maneira geral. É através deste processo, que as transações são corretamente enviadas ponto-a-ponto (P2P, *peer-to-peer*, em inglês) – isto é, de uma carteira A para um endereço B. Na medida em que as blockchains tornam-se mais populares, sua adesão e aplicação se expandiram de uma simples plataforma de pagamentos para diversos projetos que até então, não eram tecnologicamente viáveis ou funcionavam de formas mais convencionais. Desta forma, inúmeras propostas de *blockchains* surgiram com a premissa de ofertar uma melhor solução tecnológica conforme as novas demandas de aplicações se manifestaram.

Dentre as diferentes formas de validação das transações podemos destacar o *Proof-of-Work* (PoW) e *Proof-of-Stake* (PoS), cada uma com suas vantagens e desvantagens, sendo

empregadas nas maiorias das soluções *blockchains* atuais. O PoW, permite uma maior descentralização da rede, enquanto o PoS permite uma maior escalabilidade. Desta forma, os diferentes projetos *blockchains* utilizam-se de diferenciais técnicos para obter vantagens comparativas aos demais, em um mercado cambial extremamente competitivo e especulativo.

Buterin Vitalik (2021), co-fundador da rede Ethereum, propõe a existência do Trilema da Escalabilidade (figura 2), um *trade-off* entre as diferentes formas de validação atualmente empregadas dentro das redes blockchains. Desta maneira, é necessário escolher duas dentre as três características, abdicando da terceira. Ao assumir a preferência dos agentes por uma rede segura como absoluta, os usuários necessitam escolher entre a descentralização ou escalabilidade, atribuindo menor ou maior valor a estas características diante das demais propriedades da plataforma, como ilustrado a seguir:

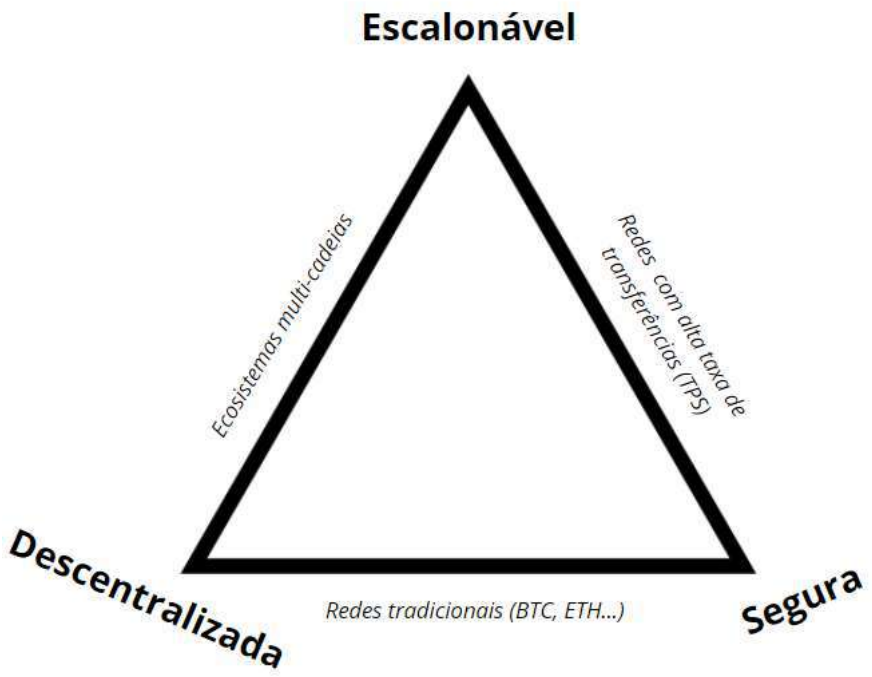


Figura 2: O Trilema da Escalabilidade
Fonte: VITALIK, Buterin. (2021) [tradução própria]

Em um cenário de livre competição entre plataformas *blockchains*, o trilema da escalabilidade atua de acordo com o uso da rede. Projetos com um alto número de usuários ou transações simultâneas - como jogos NFTs – performariam melhor em um modelo mais centralizado de *blockchain*, dada a necessidade de manter um elevado grau de escalabilidade da natureza de seu uso.

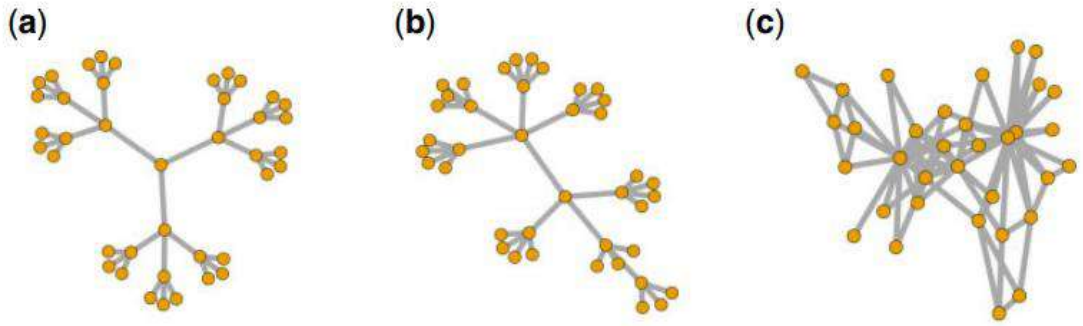


Figura 3: Diferentes arranjos de blockchain

Formas de estrutura de blockchain: a) centralizada; b) descentralizada; c) distribuída

Fonte: QuantLet/CrixToDate

A forma de validação adotada pelas diferentes redes impacta diretamente na estrutura das mesmas, conforme demostrado na Figura 3. Um sistema de validação via *proof-of-stake* (PoS) tende a um maior grau de centralização se comparado a uma rede usuária do sistema *proof-of-work* (PoW) em função das próprias características dos fenômenos intrínsecos às suas estruturações. Essas características serão mais bem analisadas ao longo desse estudo.

De forma geral, agentes racionais optam por alocar investimentos em blockchains que apresentam vantagens comparativas em relação às demais redes concorrentes. Deste modo, com a recente popularização dos *smart contracts* – isto é, contratos inteligentes validados dentro de blockchains – observada durante 2021-22, plataformas multifunção com alta capacidade de transações simultâneas receberam destaque no segmento, como a Solana.[2]

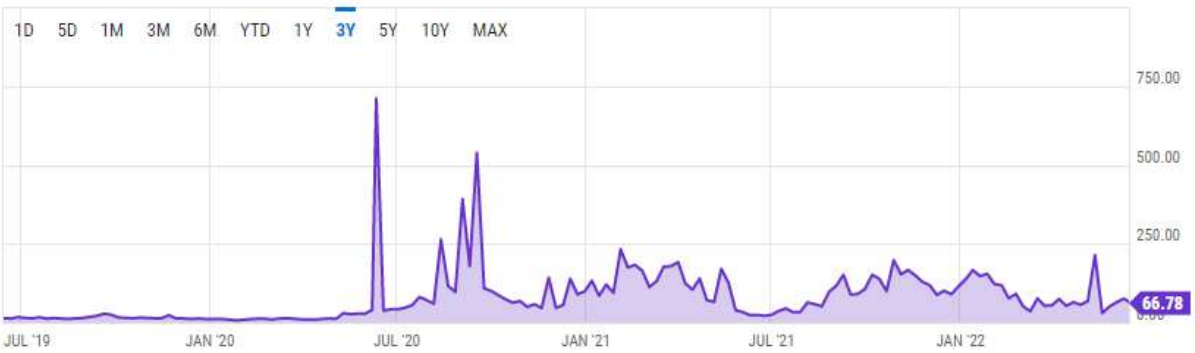


Figura 4: Evolução da taxa transacional[3] média da rede Ethereum ao longo de 2019-2022.

Índices maiores na taxa de transferência indicam sobrecarga da rede.

[2] A Solana, (SOL), por exemplo, vem ameaçando a participação da rede ERC-20, da Ethereum (ETH), no mercado dos contratos inteligentes, devido às limitações técnicas da rede ERC-20, sobretudo quanto ao número de transações simultâneas e ao custo repassado das mesmas aos usuários, conforme demonstrado pela evolução da *gas fee* - isto é, na taxa transacional da rede ERC-20 - na figura 4

[3] Taxa cobrada para realização de uma transferência na rede blockchain. Em redes como Ethereum e Polygon, é chamada de *gas fee*, em outras redes como a Solana é denominada de taxa de transação.

Fonte: Ethereum Average Gas Price | Ychart, 2022.

Nesse movimento de mercado, a demanda foi por projetos de blockchain com maior escalabilidade – isto é, que suportassem um maior número de transações ou contratos simultâneos. De acordo com o trilema da escalabilidade (Figura 2) descrito anteriormente por Vitalik (2021), agentes racionais possuiriam uma maior preferência por projetos ao mesmo tempo escaláveis e seguros, atribuindo menor peso ao fator centralização das redes *blockchain*.

O Ethereum 1.0 (PoW), que durante esse recorte (2019-2022) apresentou gargalhos técnicos, não foi capaz de suportar a demanda transacional dos *smart contracts*, acarretando maiores taxas transacionais (*gas fee*), conforme demonstrado na Figura 4. Dessa forma, foi observado a explosão de preço nos projetos baseados em *proof-of-staking* (PoS), como a Solana (SOL), criando uma pressão ainda maior na transição do Ethereum de PoW para PoS.

2.1.1 Proof-of-Work (PoW): Mineração, uma engrenagem para blockchains

O conceito de *Proof-of-Work (*PoW ou Prova de Trabalho, em tradução livre) surge com o emprego de criptografia para gerar um esforço computacional de modo a evitar ataques de *spam*[4] em servidores de e-mail, atribuindo custos operacionais a agentes mal-intencionados. (Dwork, Clayton, 1993, p.4). Em 2008, com a criação da Bitcoin, o PoW é redesenhado de modo a ser utilizado como base operacional de sua rede *blockchain*, empregando cálculos matemáticos de forma a solucionar as informações criptografadas presente em suas transações.

[4] Do inglês, termo referente a ações automatizadas indesejadas presente na internet.

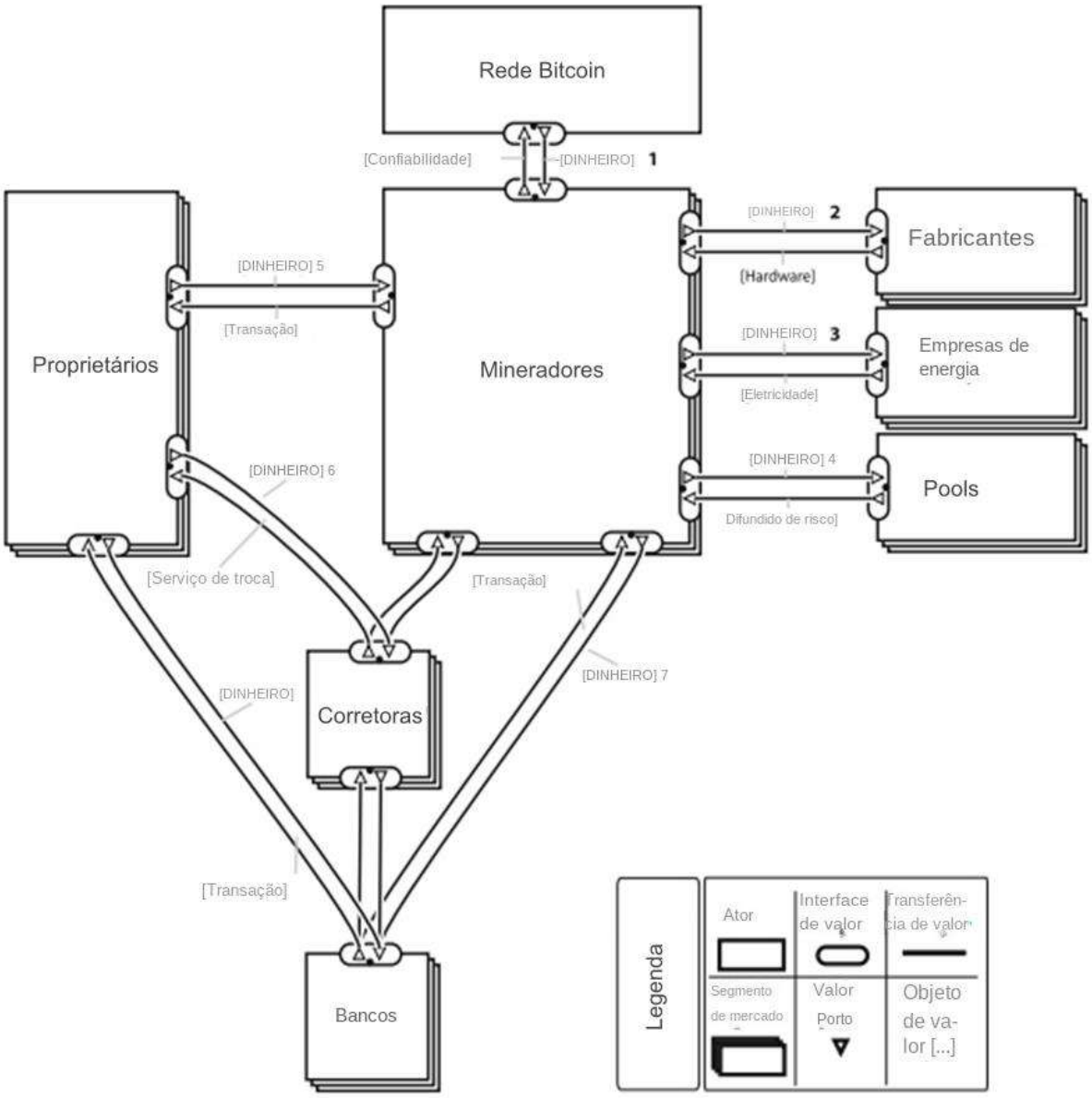


Figura 5: Fluxo de valor dentro da rede Bitcoin. Tradução própria.
Fonte: DERKS, Jona; GORDIJN, Jaap; SIEGMANN, Arjen (2018)

No sistema de validação *Proof-of-Work* (PoW ou Prova de Trabalho), a participação dos agentes validadores – estes denominados mineradores – é realizada na etapa de validação das informações inseridas na rede, como demonstrado na Figura 5, que consiste em primeiro descriptografar o bloco de informações anterior e, em seguida adicionar novas informações em um novo bloco que contará com informações do bloco anterior e, enfim, empregar poder de processamento para solucionar um novo cálculo criptografado e escrevê-lo através do algoritmo vigente na rede. O processo de resolução de equações na blockchain é muito mais complicado do que a sua verificação, por tanto, seu cálculo é feito através da tentativa de diferentes soluções até que a resposta para resolver a criptografia se mostre verdadeira.

O primeiro agente a resolver a função será o criador do próximo bloco e receberá uma recompensa além das taxas inclusas nas transações processadas no mesmo. Assim que um bloco

for resolvido e aceito pela rede descentralizada, começa a corrida pelo próximo bloco. É através deste processo que ocorre o pagamento aos mineradores por sua contribuição para a rede, também chamado de incentivos.

> Por convenção, a primeira transação em um bloco é uma transação especial que cria uma nova moeda que pertencerá ao criador do bloco. Isso cria um incentivo para os mineradores ajudarem a rede, além de providenciar um meio inicial para distribuição das moedas entrarem em circulação. […] O incentivo também pode ser formado através das taxas de transferências. […]. E uma vez em que todas as moedas entrarem em circulação, todas as recompensas serão formadas por taxas de transferências, ou seja, completamente livres da inflação da moeda. […] (Nakamoto, 2008, p.6. Tradução própria).

De acordo com Nakamoto (2008, p.3), além do papel econômico fundamental para a sustentação da rede, os mineradores são essenciais para a manutenção da credibilidade do sistema. Os incentivos do processo de mineração do tipo Pow encoraja os mineradores a permanecerem honestos. Isto é, um grande minerador, ainda que mal-intencionado, agirá de forma honesta tendo em vista que será pago de forma justa pelo seu trabalho empregado e que qualquer ação que prejudique a confiança do sistema irá afetar a sua própria riqueza. Para o autor, a rede *blockchain* é nada mais que um mecanismo que atua de forma orgânica, onde o preço da moeda depende da credibilidade e, consequentemente, da demanda pelo ativo. Além disso, Nakamoto destaca que a validação pela prova de trabalho (PoW) resolve uma série de problemas de trapaças do sistema:

> A prova de trabalho (PoW*)* também resolve o problema de determinar a representação na tomada de decisão majoritária. Se a maioria fosse baseada em um endereço IP, um voto, poderia ser subvertido por qualquer um capaz de alocar muitos IPs. A prova de trabalho pode ser definida essencialmente como um CPU, um voto. A decisão da maioria é representada pela cadeia mais longa, que tem o maior esforço de prova de trabalho investido. Se a maior parte do poder da CPU for controlada por nós honestos, a cadeia honesta aumentará mais rápido e ultrapassar quaisquer cadeias concorrentes. Para modificar um bloqueio passado, um invasor teria que refazer a prova de trabalho de um bloco e de todos os blocos posteriores a ele, e então alcançar e superar o trabalho dos nós honestos. [...] Para compensar o aumento da velocidade do hardware e o interesse variável na execução de nós ao longo do tempo, a dificuldade da prova de trabalho é determinada por uma média móvel visando um número médio de blocos por hora. Se eles forem gerados muito rápido, a dificuldade aumenta (Nakamoto, 2008, p.3. Tradução própria).

Alvo de críticas por conta de sua natureza competitiva, o sistema de validação *proof-of-work* (PoW) resulta em um consumo energético elevado se comparado a demais formas de validação blockchain. Este tópico será abordado com maior ênfase no capítulo 4.

2.1.2 Proof-of-Stake (PoS): Ganhos de escala e economia de energia

O conceito de *Proof-of-Stake* (PoS – Prova de participação, em tradução livre) surge como

uma alternativa ao protocolo PoW adotado na Bitcoin, Ethereum e algumas das outras principais criptomoedas de primeira geração, como a Monero (XMR).

Para validar as transações dentro de uma blockchain, o método PoS utiliza um montante em criptomoedas sob custódia da rede – o staking – de modo similar a uma aplicação financeira em poupança. Ao realizar um aporte de um determinado montante de um criptoativo em stake, o agente se torna um validador da rede, obtendo recompensas provenientes das transações dos agentes utilizadores da plataforma.

> [...] O PoS constitui um dos poucos candidatos viáveis definidos para substituir o PoW amplamente ineficiente em um futuro próximo. O PoS aproveita os recursos virtuais indicados pela participação de um validador para resolver o problema de computação. Os s*takes* se referem aos ativos (ou criptomoedas) pertencentes a um nó. A ideia é que quanto mais *stake* um validador tiver, maior a probabilidade de ele encontrar uma solução para gerar um bloco. [...] (Wenting et al., 2017, p.4, tradução própria).

De forma antagônica ao PoW, o *Proof-of-Stake* (PoS) não resulta em um consumo impactante de energia, este fenômeno tem origem na substituição do processo de cálculo por força bruta da mineração, energeticamente dispendioso, por um sistema baseado na participação de capital dos agentes dentro de uma rede. Deste modo, a competição entre entes validadores se dá em um âmbito parcimonioso. A recompensa é, de modo geral, determinada pelo montante aportado sob a forma de ativos utilizados para contribuição da rede e pelo tempo em que estes montantes estão realizando o papel de agente validador da plataforma. De acordo com um levantamento realizado pelo Digiconomist (2023), a simples migração da rede Ethereum – atualmente validada por PoW – para PoS é capaz de reduzir seu consumo de energia em 99,95% de acordo com um levantamento da Ethereum Foundation (2021).

Analistas convergem que um maior uso das *blockchains* está ligado a soluções de escalabilidade, com tecnologias que permitam o maior número de transações em um determinado período com um menor custo operacional possível. Desta forma, os agentes do mercado enxergam com bons olhos projetos de plataformas concorrentes ao Ethereum, chamados de *Ethereum Killers* (destruidores de Ethereum, em tradução adaptada), como Cardano (ADA) e Solana (SOL). De modo reativo ao movimento de êxodo de projetos para fora de sua rede, a Ethereum se movimenta rumo ao *Proof-of-Stake* (PoS) com o objetivo de assegurar sua parcela de mercado como plataforma de contratos inteligentes (smart contracts). O futuro da moeda Ether (ETH) como reserva de valor é diretamente afetado pela fé em sua sustentabilidade e uso da plataforma.

2.1.3 Proof-of-Activity (PoA): Um modelo híbrido

O conceito de *Proof-of-Activity* (PoA – Prova de Atividade, em tradução livre) surge como

uma extensão dos protocolos PoW e PoS. Segundo Bentov et al. (2014), ao combinar ambos os métodos, o principal objetivo é mitigar o risco da centralização de uma determinada rede *blockchain,* seja através dos grandes centros de mineração (PoW) ou pela dominância de grandes carteiras no processo de *staking (PoS).*

> O objetivo do protocolo PoA é ter uma rede de criptomoedas descentralizada cuja segurança é baseada em uma combinação de PoW e PoS. Em termos gerais, os protocolos baseados em *Proof-of-Work* conferem o poder de decisão às entidades que realizam tarefas computacionais, enquanto os protocolos baseados em *Proof-of-Stake* conferem o poder de decisão às entidades que detêm participação no sistema (Bentov et al, 2014. p.2 Tradução própria).

Ao adotar mecanismos descentralizadores, a validação via *Proof-of-Activity (PoA)* mitiga os riscos de ataque de maioria (*>50% attack)* – cenário onde a maioria do poder computacional de uma rede atua de maneira maliciosa –, sendo impossível prever qual agente irá contribuir com a assinatura do bloco. Para tal, o PoA se utiliza de um artifício lógico denominado *follow-the-satoshi* (siga o satoshi[5], em tradução direta), forçando a comunicação entre os diferentes *nodes* (nós) da rede, atuando como uma ferramenta descentralizadora. Entretanto, um maior montante de criptoativos resulta em uma maior chance para a escolha pseudo-aleatória de qual agente irá validar o bloco. Bentov descreve o processo como:

> *follow-the-satoshi* [...] é escolhido uniformemente entre todos os satoshis que foram cunhados até agora. Isso é feito selecionando um índice pseudoaleatório entre zero e o número total de satoshis existentes até o último bloco, inspecionando o bloco em que esse satoshi foi cunhado e acompanhando cada transação que transferiu esse satoshi para um endereço subsequente até chegar ao endereço que atualmente controla este satoshi (Bentov et al., 2014, p.5. Tradução própria).

2.1.4 Proof-of-History (PoH): Usando o tempo como um otimizador

O conceito de *Proof-of-History* (PoH – Prova de História, em tradução livre) é primeiramente descrito por Anatoly Yakovenko (2018) *no whitepaper*[6] da Solana (SOL). Trata-se de uma forma de validação que utiliza a passagem de tempo do histórico de registro dos eventos de modo a simplificar o processo de validação das transações, evitando etapas desnecessárias e possibilitando uma maior horizontalização de uma determinada *blockchain* que a adote. Em *Solana: A new architecture for a high performance blockchain v0.8.13, (2018),* Yakovenko descreve o PoH como:

[5] Satoshi é a menor unidade divisível de uma bitcoin, sendo equivalente a 10^-8 BTC ou 0,0000001 BTC.
[6] Documento de apresentação de uma rede *blockchain*, mostrando suas novas propostas e características técnicas.

> Prova de História é uma sequência de computação que pode fornecer uma maneira de verificar criptograficamente a passagem de tempo entre dois eventos. Ele usa uma função criptograficamente segura escrita para que a saída não possa ser prevista da entrada, e deve ser completamente executado para gerar a saída. A função é executada em uma sequência em um único núcleo, sua saída anterior como a entrada atual, gravando periodicamente a saída atual e quantas vezes foi chamado. A saída pode então ser recalculada e verificada por computadores em paralelo verificando cada segmento de sequência em um núcleo separado (Yakovenko, p.3-4, 2018. Tradução própria).

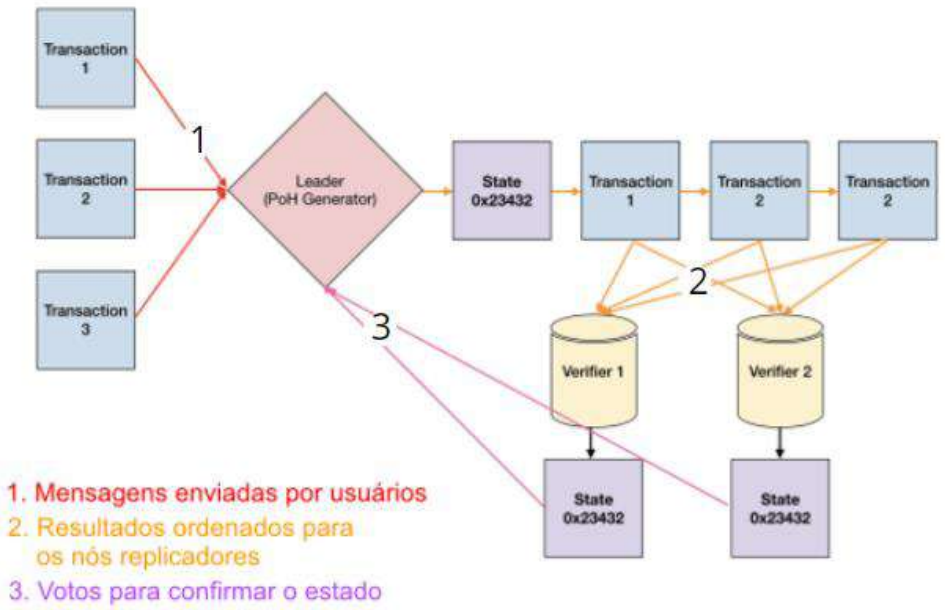


Figura 6: O fluxo de transações ao longo da rede PoH

Fonte: (YAKOVENKO, p.3, 2018)

No modelo PoH, o tempo funciona como um marcador lógico. De acordo com a Cryptopedia, cada validador de uma rede PoH possui um relógio próprio codificado por uma função de atraso verificável (Verifiable Delay Function - VDF) usando o algoritmo SHA-256, o mesmo utilizado pela Bitcoin. Desta forma, as transações dentro de uma rede PoH são registradas utilizando os hashes de um algoritmo externo como marcadores temporais. Yakovenko descreve que:

> Os dados podem ser marcados com data e hora nesta sequência anexando os dados (ou um hash de alguns dados) no estado da função. O registro do estado, índice e dados como foram anexados nas sequências fornece um carimbo de data/hora que pode garantir que os dados foram criados em algum momento antes do próximo hash que foi gerado na sequência. Este design também suporta dimensionamento horizontal já que vários geradores podem sincronizar entre si misturando seus estados em sequências uns dos outros (Yakovenko, p.4, 2018. Tradução própria).

Ao trocar informações, os agentes validadores de uma rede PoH combinam informações com base no histórico da ordem dos eventos, permitindo a escalabilidade da rede sem a perda de

confiabilidade ou dados. Segundo a Cryptopedia da Gemini Trust Company, corretora de criptoativos norte-americana, ao alcançar o consenso de blockchain via PoH, a rede Solana é capaz de alcançar tempos de confirmação notavelmente rápidos sem sacrificar a segurança da rede, preservando um grau relativo de descentralização. Deste modo:

> É possível sincronizar vários geradores de Prova de História misturando os estados de sequência de cada gerador para cada outro gerador e, assim, alcançar dimensionamento horizontal do gerador de Prova de História. Este dimensionamento é feito sem fragmentação. A saída de ambos os geradores é necessária para reconstruir a ordem completa dos eventos no sistema (Yakovenko, p.9, 2018. Tradução própria).

Tabela 1: Ilustração de uma situação de ganhos de escala horizontal da rede PoH

PoH Generator A			PoH Generator B		
Index	Hash	Data	Index	Hash	Data
1	hash1a		1	hash1b	
2	hash2a	hash1b	2	hash2b	hash1a
3	hash3a		3	hash3b	
4	hash4a		4	hash4b	

Fonte: (Yakovenko, p.10, 2018)

A horizontalização entre diferentes validadores PoH acontece conforme o esquema da Tabela 1. A ordem entre os eventos e a transitividade entre eles permite ganhos de escala ao passo que torna a rede menos centralizada. Tal qual:

> Sendo os agentes A e B validadores PoH, A recebe um pacote de dados de B (hash1b), que contém o último estado do Gerador B e o último gerador de estado B observado do Gerador A. O próximo estado hash no Gerador A depende do estado do Gerador B, então podemos derivar que hash1b aconteceu algum tempo antes de hash3a. Esta propriedade pode ser transitiva, então se três geradores são sincronizados através de um único gerador comum A ↔ B ↔ C, podemos traçar a dependência entre A e C mesmo que eles não fossem sincronizados diretamente (Yakovenko, p.10, 2018. Tradução própria).

É válido destacar as características – isto é, qualidade e defeitos – das diferentes formas de validação das redes blockchains. O *Proof-of-Work* (PoW) é alvo de críticas por conta do seu consumo energético, porém possui qualidades não encontradas em outros modais. Por exemplo, um determinado projeto PoW possui maior descentralização e segurança se comparado a um projeto PoS, que por sua vez apresentam maiores aplicações em larga escala. Deste modo, é possível supor que diferentes sistemas coexistirão dentro do ecossistema blockchain, dado que diferentes aplicações demandam diferentes arquiteturas de rede.

Capítulo 3 – ANÁLISE DA DEMANDA DOS CRIPTOATIVOS:

O aumento da popularização das criptomoedas, inicialmente como ativo reserva de valor e posteriormente como alternativa aos meios de pagamento tradicionais, inaugurou uma nova era nas finanças. Esta mudança não apenas transferiu as preocupações a respeito da segurança do sistema, mas também reviveu o debate teórico a respeito da viabilidade do uso de moedas privadas. Este capítulo explora como e por que essa mudança ocorreu.

Criptoativos se tornaram uma parcela cada vez mais proeminente do cenário moderno financeiro, com a Bitcoin, Ethereum e outras altcoins representando uma parcela significativa da capitalização de mercado (*market cap*). Neste capítulo, iniciaremos com uma revisão do debate acerca das moedas privadas, desde os postulados de Hayek, acerca da viabilidade das moedas privadas, até experiências reais em economias capitalistas desenvolvidas – como os EUA, Canadá e Suécia – durante o século XIX. Posteriormente, abordaremos a questão se a Bitcoin, Ethereum e outros ativos podem ser considerados moedas *de facto* ou ativos digitais através de uma análise técnica de suas propriedades. Por fim, introduziremos as CBDCs como o início de uma era criptofiduciária, onde os governos começam a adotar as tecnologias *blockchains* ao sistema financeiro tradicional, permitindo a implantação de políticas econômicas através da nova tecnologia.

Entender a dinâmica da demanda dos criptoativos, bem qual sua cada vez mais frequente adoção como moeda é fundamental para compreender a trajetória do impacto dos ativos digitais no setor energético, o que será apresentada no capítulo 4.

3.1 Moedas privadas e criptoativos: Hayek previu a Bitcoin?

Moedas privadas são alvo de um debate antigo entre economistas sobre sua viabilidade e impactos na esfera macroeconômica muito antes do surgimento das criptomoedas. De acordo com François R. Velde (1998), as moedas privadas lastreadas em metais preciosos – como o ouro e a prata – foram utilizadas em ampla escala durante mais de dois milênios, contando com uma ampla gama de registros históricos nos continentes europeu e asiático, mais especificamente na China. Segundo Velde (1998), em *Lessons from the History of Money:*

> O uso do dinheiro começou no século VI antes da Era Comum, onde hoje é a Turquia ocidental, quando pedaços de ouro encontrados em rios foram derretidos e transformados em pedaços de tamanho uniforme impressos com um selo. Por quase todo o tempo desde então, o sistema monetário comum foi dinheiro-mercadoria, pelo qual uma mercadoria valiosa (tipicamente um metal) é usado como um meio de troca. Além disso, a quantidade de dinheiro não estava sob o controle de ninguém; Agentes privados, seguindo incentivos de preço, tomaram medidas que determinava a oferta monetária

(Velde, 1998. P.4. Tradução Própria).

Ao longo do tempo, o dinheiro evoluiu de acordo com as mudanças nas conjunturas sociais e comerciais. Com a ascensão dos impérios, o aspecto do dinheiro abandona a forma de metálicas privadas e passa a apresentar a forma de moedas estatais metálicas, estampadas com símbolos nacionais de forma a assegurar seu peso e pureza em metal. Com o surgimento dos bancos privados, a moeda se converteu em títulos lastreado nas reservas metálicas destas instituições - que séculos depois viria a ser replicado pelos governos no padrão-ouro.

Recentemente, o fenômeno dos criptoativos – popularmente conhecidos como criptomoedas – reviveram o debate sobre o uso e viabilidade das moedas privadas, considerada pela maioria dos economistas atuais como uma questão pacificada –. Nos séculos XIX e XX, houve experiências de coexistência entre moedas privadas e públicas numa mesma economia como a Suécia, Canadá e Estados Unidos. Tal qual as moedas estatais, as moedas privadas necessitam respeitar as três características comuns das moedas – meio de troca, unidade de medida e reserva de valor.

Autores liberais, como Friedrich Von Hayek – defensor do livre mercado e um dos mais expoentes membros da Escola Austríaca – contribuem com uma abordagem moral cética perante o monopólio do Estado e o papel que ele exerce sobre o dinheiro. Em *Desestatização do Dinheiro* (2011), Hayek afirma que ao adotar uma moeda de curso forçado, os governos conduzem a população a problemas socioeconômicos causados por decisões macroeconômicas criadas justamente por cúpulas do governo. Desta forma, Hayek enxerga as falhas do sistema monetário como falhas governamentais, e não falhas de mercado. De acordo com o autor:

> [...] O direito exclusivo do governo de emitir e regular o dinheiro, que certamente não nos ajudou a ter um dinheiro melhor do que teríamos de outra forma e que provavelmente nos deu um dinheiro muito pior, tornou-se, indubitavelmente, um dos principais instrumentos a favor das políticas governamentais vigentes, e auxiliou enormemente o crescimento do poder do governo. Grande parte da política atual se baseia na premissa de que o governo tem o poder de criar e de fazer com que as pessoas aceitem qualquer quantia de dinheiro adicional que deseje. Por esse motivo, os governos defenderão diligentemente seus direitos tradicionais. Mas, pelo mesmo motivo, é importantíssimo que esse poder seja retirado de suas mãos (Hayek, 2011, p.37).

Para Hayek, a moeda deve ser tratada tal como uma mercadoria qualquer, possuindo maior ou menor grau de liquidez, sendo sujeita a livre competição com demais moedas dentro de uma economia. Deste modo:

> [...] Embora habitualmente se aceite o fato de que existe uma clara linha divisória entre o que é e o que não é dinheiro, e a lei geralmente tente estabelecer essa distinção –, quando se trata dos efeitos causadores de eventos monetários tal diferença não é tão clara. O que encontramos é, ao contrário, um *continuum* em que objetos com vários graus de liquidez, ou com valores que podem oscilar independentemente, se confundem um

> com o outro quanto ao grau em que funcionam como dinheiro (Hayek, 2011, p.66).

Hayek (2011), acredita que a expansão do maquinário estatal foi financiada pela capacidade interna do mesmo de cobrir déficits com emissão de montantes adicionais de moeda, geralmente em atividades improdutivas, sob o postulado de uma maior geração de empregos. É válido frisar que ele não abomina a emissão estatal de moeda, mas sim seu monopólio e uso forçado da mesma. Ao defender uma competição real entre moedas – isto é, com taxas verdadeiramente variáveis – em uma determinada economia controlada por um determinado governo, Hayek acredita na existência de um desincentivo a má alocação dos recursos por parte do Estado, pois o mesmo estaria suscetível ao êxodo do uso de sua moeda em prol da adesão de moedas alternativas. Sendo assim:

> [...] A justificativa parece estar na suposição de que deve haver apenas uma moeda uniforme em cada país e que a competição consistiria no fato de haver diversas entidades emitindo independentemente a mesma moeda. Contudo, é obviamente inviável permitir que moedas de mesmo nome, intercambiáveis entre si, sejam emitidas competitivamente, uma vez que ninguém estaria em posição de controlar sua quantidade [...] A questão a ser examinada é se a competição entre os emissores de tipos de moeda claramente distinguíveis [...] não nos daria um tipo de dinheiro que, por ser melhor do que qualquer outro que já tivéssemos tido, compensasse, em muito, a inconveniência de haver mais de um tipo de dinheiro. [...] Caberia, também, a cada emissor de uma moeda distinta regular sua quantidade de forma a torná-la mais aceitável para o público – e a competição o forçaria a agir dessa forma. [...] Parece que, nessa situação, o mero desejo de lucro já poderia produzir um dinheiro melhor do que o que o governo jamais produziu (Hayek, 2011, p.61).

3.2 Experiências práticas do uso de moedas privadas em economias capitalistas já desenvolvidas

As experiências históricas de moedas privadas em economias capitalistas já desenvolvidas são escassas e contaram com evoluções próprias, podendo destacar os casos do Canadá, Estados Unidos e Suécia. Durante o final do séc. XIX e início do séc. XX, a moeda estatal sueca – *Sveriges Riksbank* – coexistiu com uma moeda privada emitida por bancos privados – *Enskilda* –. De modo distinto à experiência sueca, as experiências canadense e americana surgiram em um contexto de ausência de moeda pública e foram mais duradouras. Deste modo:

> [...] As evidências do Canadá, Suécia e Estados Unidos mostram que notas bancárias privadas e notas bancárias governamentais podem coexistir. No Canadá, notas de banco privado e notas do governo (notas do Dominion e, mais tarde, notas do Banco do Canadá) coexistiram de 1868 a 1950. Na Suécia, notas de banco Enskilda e notas do Riksbank coexistiram de 1831 a 1903. Nos Estados Unidos, notas de banco nacional e notas de banco as notas do governo (notas do Federal Reserve) coexistiram de 1913 a 1935. No Canadá e nos Estados Unidos, as notas do governo foram introduzidas em economias que já tinham notas de banco privado servindo como importante, talvez até mesmo o

> principal meio de troca. O que a experiência sueca acrescenta ao nosso conhecimento é que as notas de banco privado podem ser introduzidas e se tornar um importante meio de troca em economias que já possuem notas governamentais bem estabelecidas desempenhando esse papel (Fung *et al*., 2018, p. 22. Tradução própria).

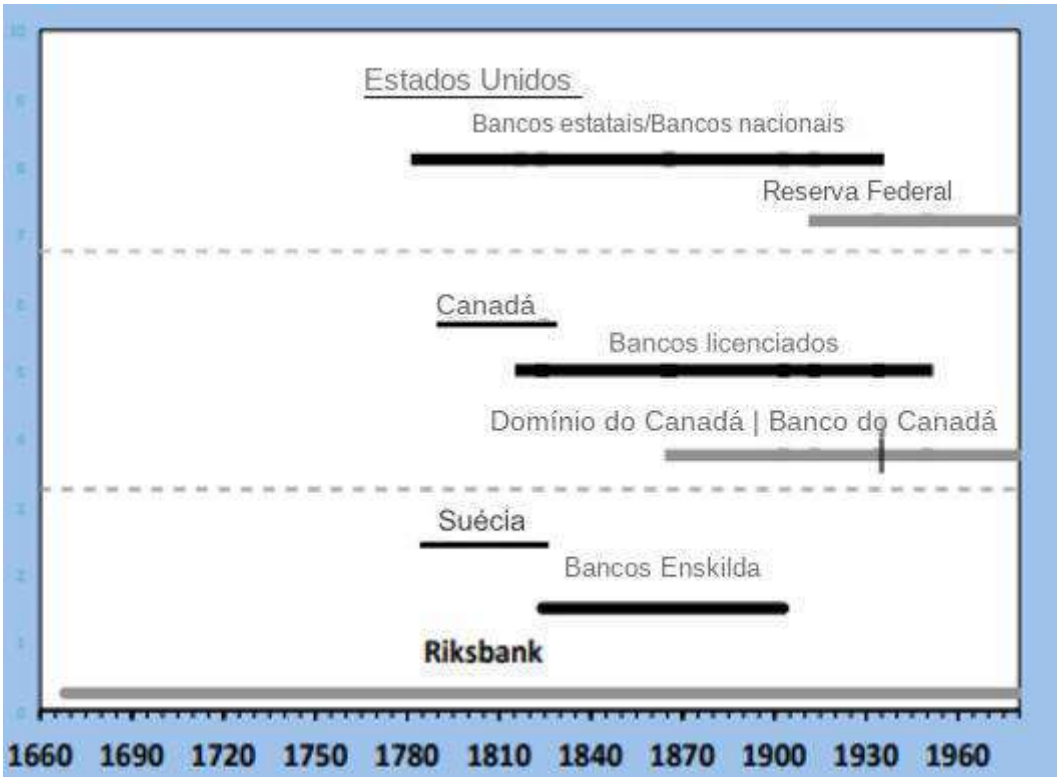


Figura 7: Linha do tempo entre notas emitidas por bancos privados (linhas pretas) e notas públicas (em cinza) nos EUA, Canadá e Suécia.

Fonte: Bank of Canada (2018) p.8. Tradução Própria.

Os bancos privados *Enskilda* não eram permitidos na Suécia até a proclamação real de 1824, O primeiro deles, *Skånska Privatbank* (posteriormente *Skånes Enskilda Bank*), só foi ser aberto em 1831. De acordo com Ögren (2003), em 1897, quando o *Riksbank* assumiu o monopólio da moeda, ele era superior a 26 bancos privados. Na experiência sueca, o arranjo de bancos *Enskilda* criou um sistema interbancário de modo a aumentar a aceitação e liquidez das notas privadas a fim de concorrer com as notas públicas. Desta forma, a evolução do setor privado monetário sueco criou um terreno fértil para o sistema bancário naquela economia. Sendo assim:

> [...] quando os primeiros bancos Enskilda começaram a operar, as notas do Riksbank eram o meio de troca predominante. Assim, eles tiveram que tomar medidas para ajudar a tornar suas notas competitivas com as notas do Riksbank. Aceitar as notas de outros bancos ao par pode ter ajudado os bancos Enskilda através de uma externalidade de efeitos de rede. Se o Banco A aceita as notas do Banco B ao par e o Banco B faz o mesmo, então as pessoas podem ver as notas de ambos os bancos como mais aceitáveis, aumentando a competitividade das notas de ambos os bancos em relação às notas do

governo (Fung *et al.*, 2018, p. 21. Tradução própria).

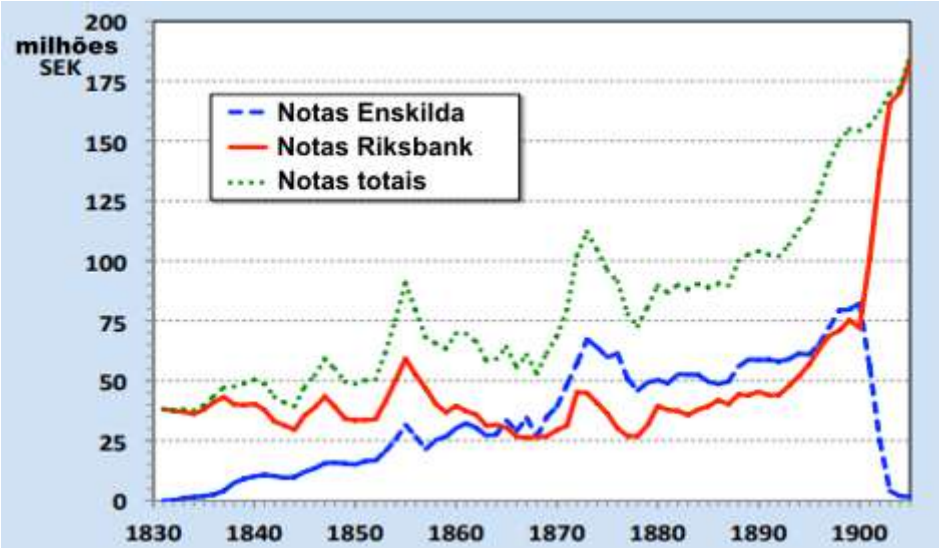


Figura 8: Evolução do montante de notas públicas (Riksbank – em vermelho) e privadas (Enskilda – em azul) na economia sueca entre 1831-1903.

Fonte: Bank of Canada (2018). Tradução própria.

As experiências das implantações das moedas privadas nas economias sueca e da américa do norte apontaram desafios, sobretudo no âmbito legal, em uma tentativa de estabelecer e garantir a segurança sistêmica. Como descrito:

> A experiência do banco sueco *Enskilda* sugere ainda que a legislação governamental, ao menos legislação que amplie a responsabilidade dos acionistas sem dar prioridade à nota titulares, pode ser insuficiente para garantir a segurança das notas bancárias privadas. Acionistas dos bancos suecos tinham responsabilidade ilimitada, mas os detentores de notas não tinham garantia inicial, e não havia foram as ameaças à segurança das notas bancárias discutidas acima. Da mesma forma, os acionistas dos bancos do Canadá estavam sujeitos a responsabilidade estendida, neste caso dupla responsabilidade, mas alguns detentores de notas ainda sofreram perdas. Não foi até 1881, quando os detentores de notas receberam o primeiro penhor de um ativo do banco, que as notas bancárias canadenses se tornaram perfeitamente seguras (Fung *et al.*, 2018, p.19. Tradução própria)

Deste modo, a regulação das moedas privadas teve papel crucial para assegurar a estabilidade financeira e evitar fraudes ou corridas bancárias. No caso sueco, ao estabelecer uma única moeda privada, o governo promoveu um sistema mais eficiente e confiável. O sistema Enskilda funcionou de forma solene até sua total substituição pela moeda estatal, em 1903. Já no caso canadense, após 1881 - período marcado pela regulamentação do setor - não foram registradas perdas aos detentores de notas bancárias canadenses.

3.2.1 A viabilidade de uma economia de livre competição entre moedas privadas

A livre competição entre moedas privadas tem sido matéria de estudo desde meados do século XX, com destaque para a Hayek, F. em *Desestatização do Dinheiro* (1976), onde o autor descreve a competição entre moedas privadas como "uma forma mais eficiente de trocar recursos do que se comparado à moeda estatal". De acordo com Hayek, a inflação sistêmica é resultado direto do monopólio do governo sobre a emissão de dinheiro, oriundo dá má alocação de recursos e gastos desnecessários como o financiamento de guerras ou atividades consideradas improdutivas pelo autor. Segundo ele, as moedas privadas não apresentariam esse problema pois competiriam entre si e um mercado monetário livre resultaria em moedas que apresentam vantagens em relação as outras, sobretudo no âmbito da segurança e estabilidade.

O surgimento e a popularização de criptomoedas privadas trouxeram de volta o debate sobre a viabilidade das moedas privadas em uma economia capitalista desenvolvida. De modo similar ao modelo de moedas privadas ilustrado por Hayek, as criptomoedas privadas são exógenas ao sistema monetário governamental. Entretanto, existem diferenças substanciais entre os criptoativos e as moedas privadas postuladas por Hayek. Dado o anacronismo, seria impossível imaginar a tecnologia blockchain sem a necessidade de uma figura de autoridade validadora centralizada. No modelo do autor, as moedas privadas seriam emitidas por instituições financeiras privadas, com menor ou maior regulamentação governamental.

Por outro lado, os criptoativos ainda não cumprem o papel pleno desempenhado pelas moedas privadas propostas por Hayek (1976). Para o autor, as moedas privadas seriam plenamente utilizadas como meio de troca e reserva de valor. Diferente disso, entre as criptomoedas, o observado é um maior uso das mesmas como reserva de valor em detrimento das demais funções da moeda – isto são, a de meio de troca e a de unidade de conta. As transações são baseadas no valor de uma determinada moeda corrente governamental, seja o dólar americano ou o real.

A sustentabilidade de preços é outra questão a se preocupar em uma economia aberta com moedas voláteis - sejam elas estatais ou privadas -. Nos modelos privados, sobretudo os de criptoativos descentralizados, a mudança de ânimo dos agentes detentores da custódia dos ativos é mais variável. De acordo com Fernández-Villaverde et Sanches (2019), a estabilidade monetária de moedas privadas depende da tecnologia e do custo da produção de uma unidade marginal de dinheiro em um ambiente competitivo:

> [...] Em um ambiente competitivo, a existência de um equilíbrio monetário compatível com a estabilidade de preços depende das propriedades das tecnologias disponíveis. Mais concretamente, a forma da função de custo determina a relação entre os preços de equilíbrio e o incentivo do empresário para aumentar sua oferta de moeda. Um equilíbrio

> com preços estáveis só pode existir se a função de custo associada à produção de dinheiro privado for estritamente crescente e localmente linear em torno da origem. Se a função de custo tiver uma derivada positiva em zero, então não há equilíbrio consistente com a estabilidade de preços. Assim, a visão de Hayek de um sistema de dinheiro privado competindo entre si para fornecer meios de troca estáveis não é geral (Fernández-Villaverde et Sanches, p.2, 2019. Tradução própria).

Segundo Eli Noam (2019, p.98), "a demanda por criptomoedas pode mudar drasticamente e rapidamente, iniciando um possível episódio de inflação se as pessoas tentarem se livrar de suas criptomoedas alimentando o mercado e afogando os preços". No entendimento do autor, há um desacordo sobre a origem da força de compra (demanda) dos criptoativos – se os agentes compram devido ao seu potencial como moeda ou para fins especulativos.

Em suma, o debate sobre a desestatização do dinheiro e o surgimento das criptomoedas privadas é multifacetado e contínuo. Embora as ideias de Hayek tenham moldado o debate, a evolução das novas tecnologias e as mudanças no ambiente econômico global continuam a desenvolver a discussão.

3.3 Criptoativos ou Criptomoedas? Uma abordagem teórica e analítica

Criptoativos, sobretudo a Bitcoin, têm conquistado maior atenção de investidores e do público em geral nos últimos anos. Estes ativos digitais, que operam de forma independente de instituições financeiras convencionais e governos têm revolucionado o sistema financeiro global, sobretudo na aplicação da tecnologia blockchain na validação de transações e demais contratos inteligentes. Entretanto, ainda paira o questionamento se estes ativos digitais podem ser efetivamente considerados ou não como moedas, com uma série de críticas a respeito da sua volatilidade e restrição de uso pesando contra uma ampla qualificação dos criptoativos como moedas. Nesta seção, vamos abordar de forma teórica e analítica as propriedades dos principais criptoativos de modo a melhor classificá-los dentro desta dicotomia técnica acadêmica.

Das três funções clássicas da moeda – meio de troca, unidade de medida e reserva de valor, os criptoativos – como a Bitcoin e a Ether – são capazes de desempenhar as três, com maior ou menor grau de implantação e uso dentro da sociedade. Dado o seu caráter escasso dos principais criptoativos, característica fundamental para o processo de financeirização das mesmas, seu uso como moeda corrente, é abertamente desencorajado por entusiastas, que se apoiam na premissa que uma maior adesão global aos criptoativos – alinhada com a escassez programada dos criptoativos – levaria ao processo de valorização dos mesmos. Da mesma forma, a escassez gradual na oferta (*supply*) dos criptoativos os torna uma reserva de valor de considerável interesse

e sucesso.

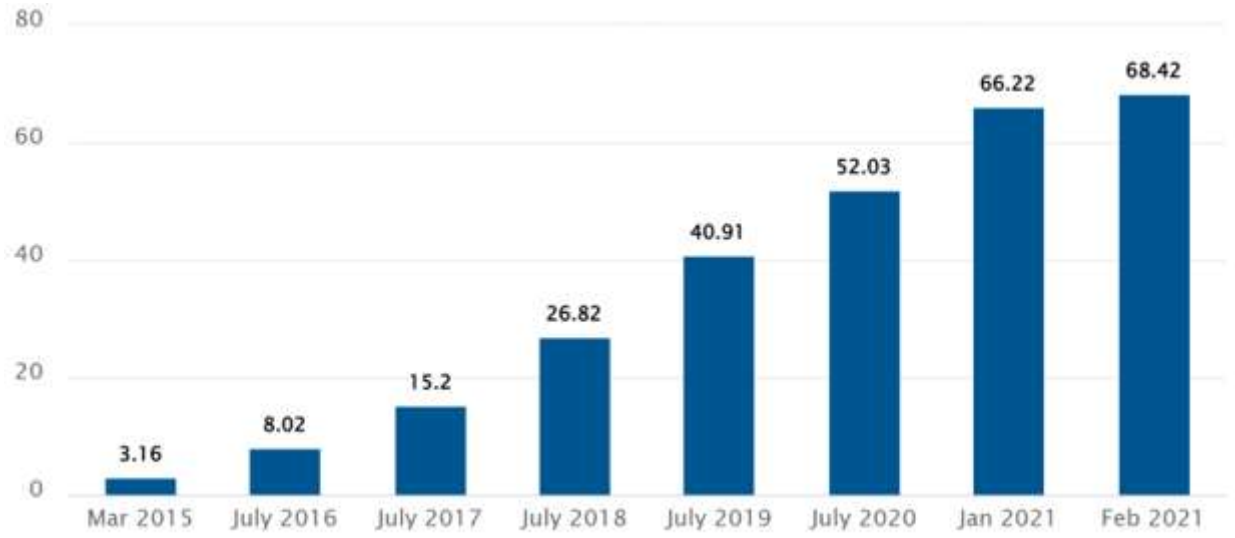


Figura 9: Evolução do número de endereços de carteiras existentes dentro das blockchains em milhões - 2015-2021
Fonte: Statista, 2021

Por não apresentarem curso forçado – isto é, serem garantidas por imposição estatal como moeda circulante, de ampla aceitação dentro de uma determinada economia – sua adoção depende da adesão voluntária por parte dos indivíduos ou empresas e demais instituições e vem demonstrando um massivo crescimento de usuários como demostrado na Figura 9 entre os anos 2015-2021. Outro passo para sua consolidação se deu com o recente processo de estudo e adesão de criptoativos como moedas oficiais de países. – Como El Salvador, que em 7 de setembro de 2021, se tornou o primeiro país a adotar a Bitcoin como moeda oficial. De acordo com levantamento do National Bureau of Economic Research – NBER – (2022), após um ano de adesão oficial do governo, a maioria da população El salvadorenha ainda não havia transacionado em criptomoedas.

> Metade das famílias do país baixou o aplicativo quando a lei da bitcoin entrou em vigor. Desde o início de 2022, no entanto, muito poucos agregados familiares aderiram aos pioneiros. Entre os primeiros usuários, mais de 60% não fizeram nenhuma transação depois de gastar a quantia gratuita em bitcoin que veio com a conta, e 20% ainda não gastaram o bônus. No entanto, um pequeno grupo de consumidores, a maioria dos quais bancários, instruídos, jovens e do sexo masculino, é muito ativo no aplicativo. Este grupo não era o alvo pretendido do lançamento do Bitcoin. (NBER, 2022. Tradução própria).

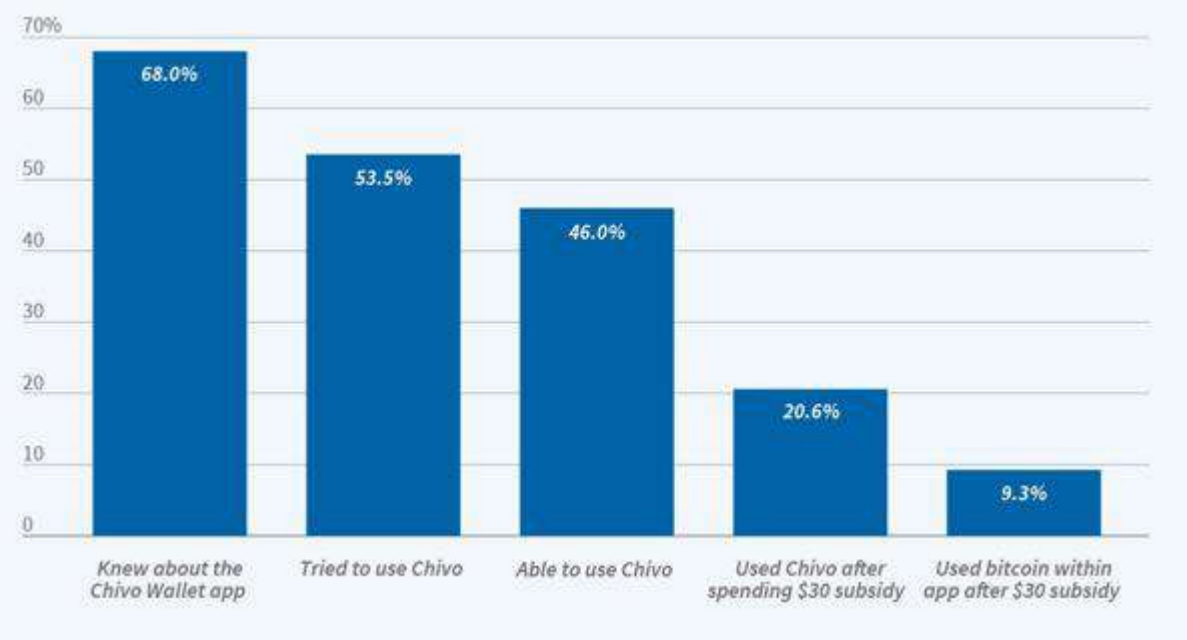


Figura 10: Medidas do uso do Bitcoin em El Salvador

Fonte: NBER, 2022

Um dos principais argumentos dos críticos sobre a não aceitação de criptoativos como moedas é sua alta volatilidade – se comparado aos ativos financeiros tradicionais –. De fato, a volatilidade dificulta o uso dos criptoativos como unidade de conta, pois os preços de bens e serviços cotados em criptoativos podem mudar drasticamente de um dia para o outro. De acordo com Wolla (2018), a volatilidade pode não parecer uma ameaça para a função de reserva de valor quando os ativos estão se valorizando, mas o cenário muda caso a variação no preço seja negativa. Como o autor descreve em *Bitcoin: Money or Financial Investment?* (2018):

> Como o dinheiro também serve como reserva de valor, a estabilidade desse valor é ainda mais importante. O valor do Bitcoin cresceu dramaticamente nos últimos anos. Agora, preços voláteis podem não parecer uma ameaça para a função de reserva de valor do dinheiro quando os preços estão subindo; mas quando os preços estão caindo, as pessoas são lembradas de que o valor estável é um aspecto importante da reserva de valor (Wolla, p.2 2018. Tradução própria).

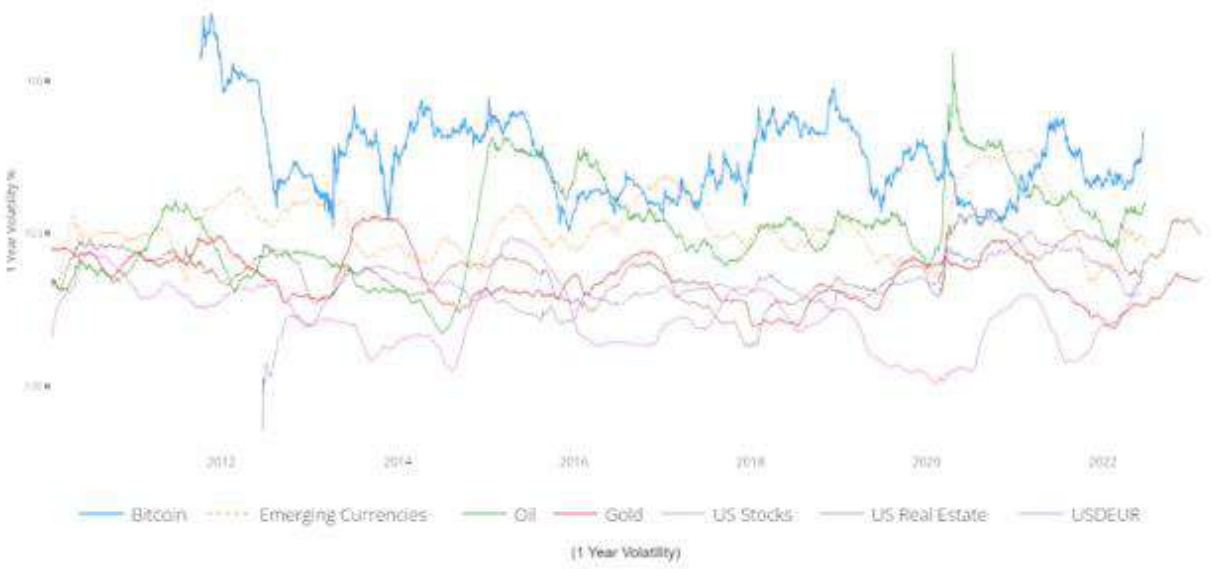


Gráfico 1: Volatilidade da Bitcoin comparado a outros ativos – 2012-2023

Legenda: Bitcoin – Azul; Moedas emergentes – Linha pontilhada; Verde - Petróleo; Lilás - Ações americanas; Marrom - Imóveis nos EUA; Vermelho – Par Dólar / Euro

Fonte: Willy Woo | Woobull, 2023

A volatilidade do preço da Bitcoin vem apresentando uma tendência de queda nos últimos anos, conforme observado no Gráfico 1. Tal redução na taxa de variação média no preço do ativo permitiu que, em 2020-21 – diante do choque de oferta causado pelo início da pandemia de COVID-19 -, a variação no preço do barril do petróleo superasse a volatilidade do Bitcoin, de acordo com dados do economista Willy Woo, em seu portal Woobull.

Existem inúmeras razões que ajudam a explicar o processo de normalização da volatilidade da Bitcoin. Sendo possível destacar que o maior acesso ao mercado de corretoras de criptoativos e a crescente adoção da criptomoeda por instituições financeiras e investidores institucionais contribuem para um cenário de maior estabilidade do preço do criptoativo. Estes investidores tendem a possuir um horizonte de investimento mais longo e uma abordagem mais conservadora em relação ao risco, o que reduz a pressão por vendas massivas em períodos de volatilidade. De acordo com Robert J. Shiller (2017), a volatilidade de um ativo cai na medida em que novos mercados futuros são estabelecidos:

> A literatura acadêmica nos diz que a volatilidade de um ativo subjacente geralmente cai após o estabelecimento de novos mercados futuros para ele. Mas a capacidade de vender um ativo com mais facilidade não superará necessariamente o poder da empolgação do investidor (Shiller, 2017. Tradução própria).

Se por um lado faltam incentivos para transacionar de maneira cotidiana em criptomoedas,

pelo outro sobram razões para utilização de criptoativos como reserva de valor. O ouro, metal precioso utilizado como meio de assegurar riquezas ao longo do tempo, desde as civilizações indo-europeias mais antigas até hoje, vem perdendo espaço para moedas digitais como a Bitcoin.

Figura 12: Bitcoin vs. Ouro (Oz.) – 2010-2021.

Legenda: Amarelo pontilhado = $1 investidos em Ouro / Laranja = $1 investidos em Bitcoin / Roxo pontilhado = Bitcoin por onça de ouro

Fonte: charts.woobull.com

Por exemplo, é possível definir o valor do ouro como um resultado das suas propriedades. O ouro é escasso – isto é, não está suscetível a grandes choques de oferta, o que afetaria seu preço –, e não apresenta desgaste ao longo do tempo. Tais características fazem com que o ouro tenha sido usado como reserva de valor ao longo dos séculos. Por sua vez, a bitcoin se comporta cada vez mais como um ouro digital, igualmente escassa, apontada como reserva de valor e demandada por agentes financeiros em diferentes cenários, seja de especulação ou aversão ao risco, se comparado a moedas mais voláteis - ainda que este último seja mais comum em eventos onde uma determinada moeda estatal apresenta hiperinflação – definida por Phillip Cagan (1956) em *The Monetary Dynamics of Hyperinflation* como um episódio onde a taxa de inflação mensal excede 50%.

O processo de emissão da Bitcoin é demostrado de forma clara e objetiva através de seu *whitepaper*[7] em Nakamoto (2008). Seu limite máximo de moedas emitidas foi definido por seu

[7] Documento com aspectos técnicos e propostas de uma determinada plataforma blockchain ou moeda

criador, Satoshi Nakamoto em 21 milhões de unidades, e não pode ser alterado. Atualmente mais de 18 milhões de unidades de Bitcoin foram emitidas, e continuarão o processo de emissão via novos blocos dentro da sua blockchain em ritmo decrescente, através de um processo denominado de halving[8], que ocorre em aproximadamente 4 anos - ou a cada 210 mil blocos gerados. Tal processo, a ceteris paribus, leva a mitigação da inflação relativa do criptoativo.

Dada sua descentralização, refletida na ausência de uma autoridade central e única responsável pela manutenção da rede, o processo de perda do acesso a carteiras é apontado como outro fator que colabora para a escassez do ativo, através do mal armazenamento de senhas ou esquecimento pelos ex-detentores de carteiras digitais. De acordo com um relatório da Wallet Recovery Services (2021), uma empresa que atua no processo de recuperação das senhas das carteiras digitais de criptoativos, cerca de 20 por cento do montante em circulação do Bitcoin – isto é, quase 4 milhões de unidades – foram ou estão perdidas por seus ex-usuários. O baixo apelo inicial, e lento processo de adesão e valorização do ativo, fez com que muitos de seus *early-adopters* (pioneiros), acabassem por esquecer suas chaves privadas.

Dessa forma, a escassez torna-se uma das principais premissas da Bitcoin, favorecendo uma crença de valorização a longo prazo em caso. Apesar de facilmente criticável, o histórico recente (2019-2023) aponta para uma curva de valorização e com progressiva redução na volatidade de moedas já estabelecidas, como a Bitcoin e Ethereum, consolidadas como referências dentro da criptoeconomia. Como resultado, há a possibilidade da decisão de investimento se apoiar em um padrão histórico, que pode não se concretizar em realidade.

Tabela 2: Criptomoedas e número máximo de transações por segundo (TPS)

Criptomoeda	**TPS**
Solana (SOL)	50.000
Ripple (XRP)	1.500
Bitcoin Cash (BCH)	300
Monero (XMR)	até 1.000
Litecoin (LTC)	56
Digital Cash (DASH)	35
Zcash (ZEC)	27
Ether 1.0 (ETH)	25
Bitcoin (BTC)	7

Fonte: Newbery, E. (2021)

Um outro fator importante para a aceitação dos criptoativos como moedas é a sua liquidez

[8] Do inglês, ato de reduzir pela metade

– isto é, a capacidade de conversão de um determinado ativo em moeda corrente –. Ao longo dos anos, novos mercados foram abertos – tornando mais fácil a compra ou venda de criptoativos. No uso prático – a qual se refere majoritariamente a transação ponto-a-ponto (P2P) –, a capacidade de transações por segundo (TPS) afeta o número máximo de usuários ativos numa determinada rede *blockchain*, pois quanto maior o número de transações por segundo maior é a capacidade de uma rede ser utilizada em massa como meio de pagamento. De acordo com a Tabela 2, criptoativos como a Solana (SOL) e Ripple (XRP) apresentam maior desempenho no número de transações por segundo (TPS) do que a Bitcoin ou a Ether 1.0 (pré-transição para o Ether 2.0).

Em suma, criptoativos são capazes as três funções da moeda – meio de troca, reserva de valor e unidade de conta –, com a Bitcoin desempenhando um melhor papel de reserva de valor e outros projetos como a Solana ou Ripple tendo seu desenvolvimento inicial focado em desempenharem uma melhor função de meio de pagamento. Entretanto, ao compararmos com moedas estatais mais consolidadas, os criptoativos apresentam um pior desempenho no emprego das funções acima de forma generalizada e conjunta.

Por seu caráter privado e de uso voluntário, uma comparação mais acurada deve ser realizada em relação a moedas privadas pré-*blockchain*, onde as semelhanças com criptoativos são mais aparentes. A tendência é que ao decorrer do tempo, com maior número de usuários, novas tecnologias e regulamentações, os criptoativos se aproximem cada vez das moedas tradicionais, mas por enquanto, ainda há muitas incertezas em relação a esse assunto.

3.4 Stablecoins e CBDC: O início da era Criptofiduciária

Os criptoativos revolucionaram o sistema financeiro, garantindo a segurança das transações, com a adição da descentralização. Com a popularização destes – sobretudo a Bitcoin e o Ethereum -, formas garantidoras de reserva de valor em moedas fiduciárias ou de liquidez foram cada vez mais demandadas como mecanismos facilitadores do ato de compra/venda dos ativos digitais, surgindo as denominadas stablecoins – ativos digitais com paridade em moedas fiduciárias, como o dólar, com a tutela de uma instituição financeira privada, como a Dólar Tether (USDT) ou Binance Dólar (BUSD). O surgimento de ativos financeiros digitais criptografados levou posteriormente ao surgimento de moedas públicas digitais criptografas ou moeda digital de banco central (da sigla em língua inglesa CBDC, *Central Bank Digital Currency*).

As stablecoins inicialmente foram desenvolvidas como uma solução para o problema da alta volatilidade do preço das criptomoedas – se comparadas às moedas fiduciárias –, visando proporcionar maior estabilidade aos investidores e facilitar o processo de compra e venda de ativos digitais. Além disso, as stablecoins permitiram a entrada de investidores institucionais no

mercado de criptoativos, dado a maior aversão ao risco por parte dos agentes institucionais e fundos financeiros. Com o tempo, as stablecoins evoluíram e novas formas de garantir a paridade com moedas fiduciárias foram desenvolvidas, incluindo a adoção de tecnologias blockchain e a criação de reservas em moedas fiduciárias. Entretanto, as stablecoins ainda sofrem problemas como a falta de transparência por parte de seus agentes garantidores de conversibilidade, resultando em episódios de manipulação de mercado.

Nesse contexto, as CBDCs surgem como uma alternativa às stablecoins, dado que são emitidas e lastreadas pelos bancos centrais. As CBDCs têm como objetivo fornecer uma forma digital de moeda fiduciária emitida e controlada pelo banco central, oferecendo maior segurança e estabilidade do que as stablecoins emitidas por instituições privadas. Atualmente, o dinheiro digital do banco central já é empregado nas economias desenvolvidas. Segundo relatório da Federal Reserve, Money and Payments: *The U.S. Dollar in the Age of Digital Transformation* (2022):

> A moeda do banco central é um passivo do banco central. Nos EUA, o dinheiro do banco central vem na forma de moeda física emitida pelo FED e saldos digitais mantidos por bancos comerciais no FED; O dinheiro do banco comercial é a forma digital de dinheiro mais comumente usada pelo público. O dinheiro do banco comercial é mantido em contas em bancos comerciais; Dinheiro não bancário é dinheiro digital mantido como saldo em provedores de serviços financeiros não bancários. Essas empresas normalmente realizam transferências de saldo em seus próprios livros usando uma variedade de tecnologias, incluindo aplicativos móveis (Federal Reserve, 2022. p. 5. Tradução própria).

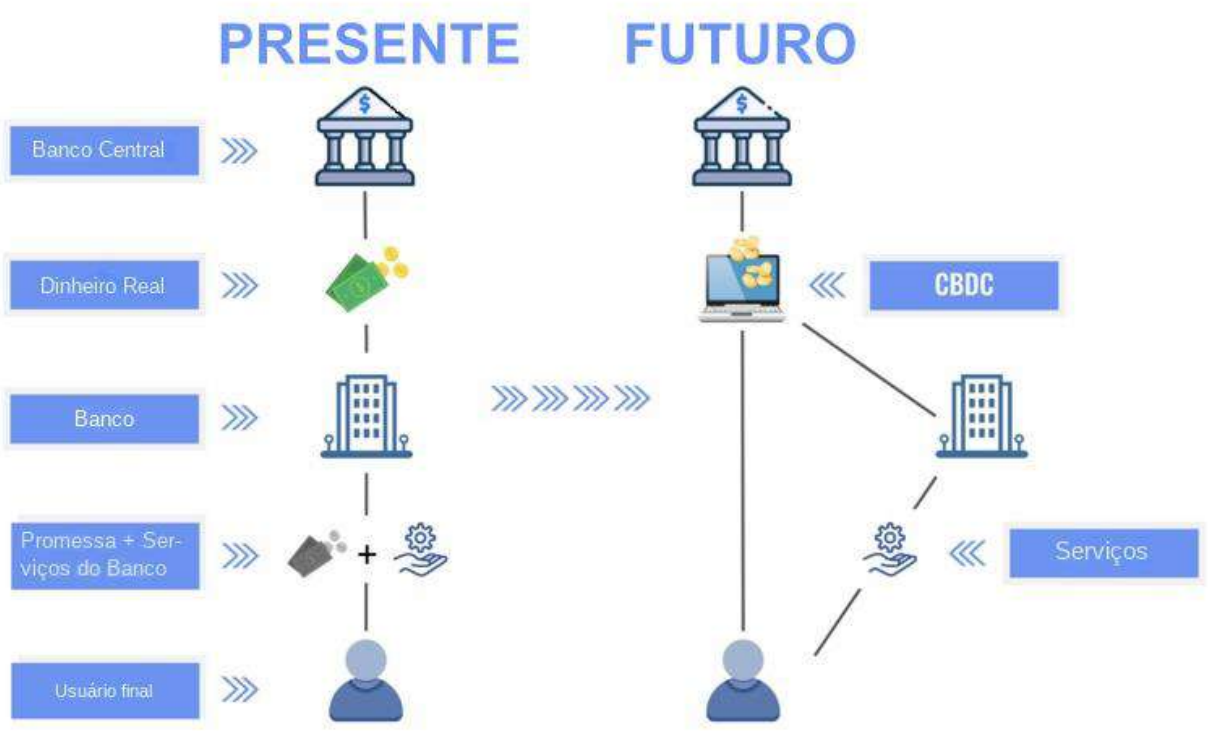


Figura 13: Ilustração de como o modelo de CBDCs pode remover o risco dos usuários e permitir que os bancos se concentrem nos serviços.
Fonte: Darko Pilav (2020) / DigitalAsset.com . Tradução Própria

Segundo Darko Pilav (2020), dado que a CBDC criará um canal direto entre os bancos centrais e os cidadãos detentores de moeda, o papel futuro dos bancos será mais focado na prestação de serviços relacionados ao uso desse dinheiro digital.

As stablecoins representam um tipo especial de criptoativo devido a representarem paridade a moedas estatais "comuns", feito obtido através da vinculação destes ativos a ativos fiduciários - isto é, moedas estatais como o dólar ou euro – commodities ou outros instrumentos financeiros em caso de stablecoins de tutela privada como o Dólar-Tether (USDT) ou o Dólar-Binance (BUSD). Já em stablecoins estatais, a paridade para moeda fiduciária é estabelecida e garantida diretamente pela autoridade monetária - desta forma fornecendo maior segurança aos agentes detentores destes ativos.

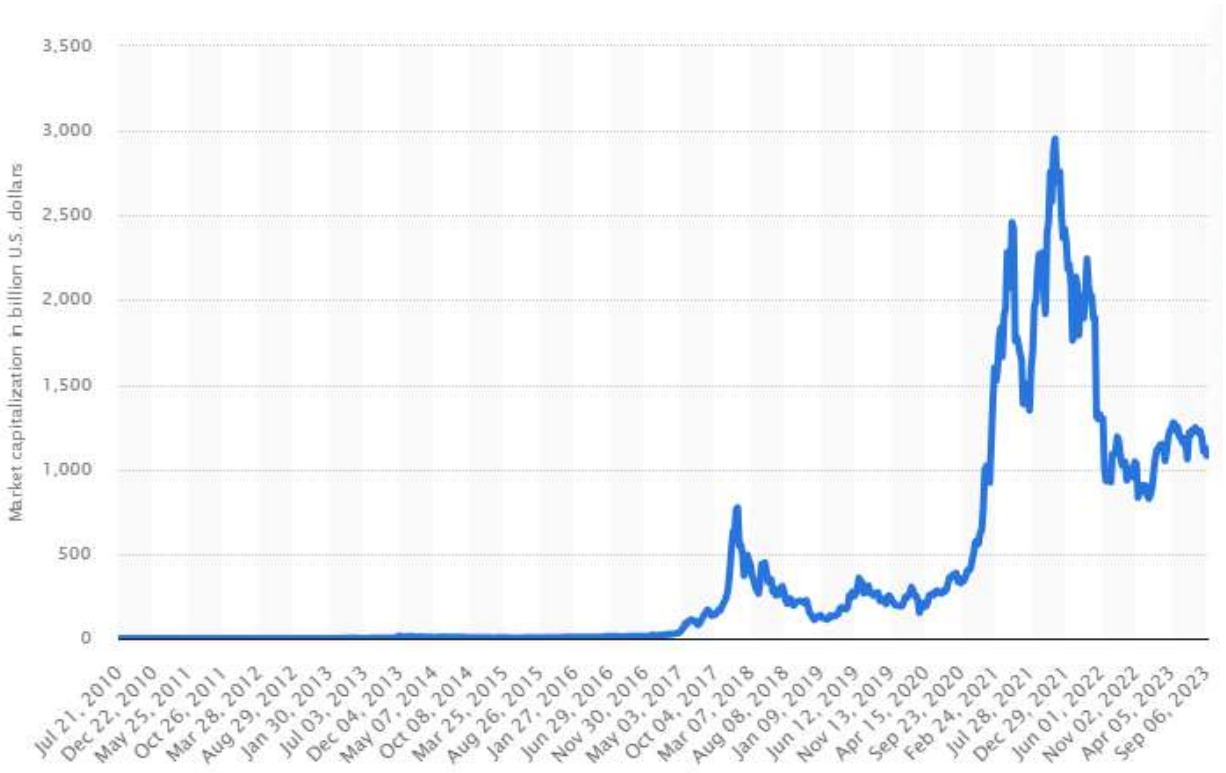
Em suma, a evolução das stablecoins até o surgimento das CBDCs mostra a constante busca por soluções que garantam maior estabilidade e segurança no mercado de criptoativos oferecendo uma alternativa mais segura e confiável para a moeda digital. Sendo assim, a consolidação das stablecoins de tutela estatal (CBDCs) é um feito relevante para a adesão do *proof-of-stake* (PoS) - dada a natureza de seu uso – que exige um maior volume de transações abrindo mão de outras propriedades, como a centralização, tal qual demonstrado anteriormente no Trilema da Escalabilidade (Figura 2) proposto por Vitalik (2021). Desta forma, na medida em

que blockchains se tornam cada vez mais populares, há uma preocupação crescente com seu consumo de energia, especialmente a respeito das redes blockchains que utilizam o algoritmo de consenso *proof-of-work* (PoW), com a adesão das stablecoins – sobretudo as CBDCs - ao PoS essa preocupação é reduzida nas mesmas propoções da redução de consumo energético da nova modalidade – Segundo a Ethereum Foundation Blog (2021), a migração do Ethereum para o PoS reduziria o consumo elétrico da rede em até 99,95%, tornando o sistema de validação PoS uma escolha natural não só para as stablecoins privadas (USDT, BUSD e outras) quanto para as CBDCs.

Capítulo 4 - CRIPTOATIVOS E ENERGIA

As criptomoedas surgiram como uma força disruptiva no cenário financeiro global, transformando transações e sistemas financeiros tradicionais. Com a Bitcoin sendo a pioneira e outros criptoativos surgindo posteriormente, o mercado de criptomoedas cresceu exponencialmente nos últimos anos, como podemos ver no gráfico 2. No entanto, o aumento da popularidade das criptomoedas levantou preocupações sobre seu consumo de energia e impacto ambiental, levando o tema ao debate público, conforme demonstrado na Figura 14, onde é possível notar a dimensão do consumo energético da validação de transações da rede Bitcoin se comparado ao consumo de países inteiros.

Gráfico 2 – Capitalização geral do mercado de criptomoedas por semana, de julho de 2010 a setembro de 2023 em bilhões de dólares



Fonte: Statista (2023)

A adoção generalizada de criptomoedas aumentou a demanda por eletricidade devido ao processo de validação de sua tecnologia blockchain. A mineração de criptomoedas – isto é, o processo de registro e monitoramento de transações nas blockchains – é uma tarefa computacionalmente intensiva, consumindo uma quantidade significativa de energia o que torna esse tema importante, especialmente para os formuladores de políticas energéticas e ambientais.

A crescente intensidade da indústria de criptomineração levantou preocupações sobre o impacto que esta pode gerar na rede elétrica existente. Segundo levantamento realizado pelo

Digiconomist (2023), a rede Bitcoin consome 107.21 TWh, isto é, aproximadamente 92% do consumo elétrico dos Países Baixos. Na Figura 14, é possível notar que o consumo elétrico da rede blockchain da Bitcoin é superior a uma parcela significativa de países, sobretudo países em desenvolvimento e alguns países desenvolvidos, como Portugal e Bélgica.

Figura 14 – Consumo elétrico da rede BTC em abril de 2023 com 100 TWh em relação ao consumo dos demais países do mundo. Em cinza claro, estão os países que consomem menos energia do que a rede digital.

Fontes: Digiconomist e PowerCompare. 2023.

Além do gasto global de energia, a escala das operações geográficas de mineração agrava ainda mais as preocupações ambientais. Como os custos de energia desempenham um papel importante na determinação da lucratividade da mineração, a indústria de criptomineração acaba por se concentrar em regiões geográficas onde o custo de energia é baixo e as regulamentações são favoráveis à essa atividade, ou pelo menos não proibitivas. Neste capítulo, iremos abordar a trajetória da evolução da mineração como atividade econômica, tal qual o seu impacto no sistema elétrico ao redor do mundo. Ademais, iremos apresentar as novas tecnologias que visam aumentar a eficiência energética das redes blockchains visando a sustentabilidade do sistema.

4.1 A mineração de criptomoedas como atividade econômica: A evolução dos hardwares e ganhos de escala

Segundo Michael B. Taylor (2017), inicialmente, a embrionária rede de computadores que alimentava as transações da rede Bitcoin era formada por CPUs (*Central Processing Uni*t ou Unidades de processamento central, também conhecidas como processadores) comuns, que com o passar do tempo, se mostraram menos rentáveis do que placas de processamento gráfico

dedicadas (GPUs), que posteriormente foram ultrapassadas por FPGAs[9] (da sigla em inglês, arranjo de portas programáveis em campo), ainda que estes equipamentos tivessem um reinado muito curto na mineração de Bitcoin. Hoje em dia, a maior parte do processamento é feito através de equipamentos mais sofisticados chamados de ASIC (*Application-specific Integrated Circuit* ou Circuito integrado de aplicação específica), um tipo de hardware especialmente desenvolvido para esta função que facilita a escala industrial do segmento, como demonstrado na Figura 15.

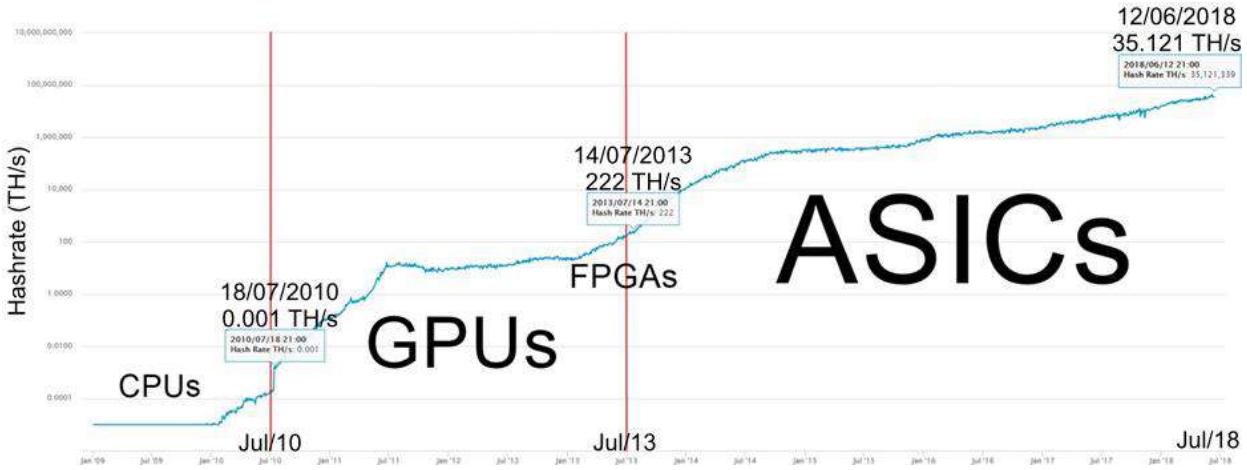


Figura 15 - Evolução do poder de processamento, em escala logarítmica, destacando a evolução dos *hardwares*, da Bitcoin desde sua criação até junho de 2018.

Adaptado de Blockchain.info com base nas eras destacadas por Taylor (2017).

A transição entre as diferentes fases de hardwares mostra a evolução da mineração desde uma simples contribuição entusiástica, em meados de 2009, para uma atividade comercial de grande magnitude conforme vista na atualidade. Devido a aversão ao risco do grande capital, não é estranho pensar que, no ocidente, as grandes mineradoras foram inicialmente fundadas por entusiastas que aproveitaram os primeiros-passos da rede para acumular um significativo montante em criptoativos, sobretudo Bitcoin, e reinvestir em máquinas destinadas à mineração de criptomoedas.

[9] Ainda que as FPGAs tenham tido um impacto mais tímido na evolução do *hash rate* da rede, Michael B. Taylor, não menospreza sua participação neste processo. Para Taylor (2017), os FPGAs enfrentaram problemas ao competir comas GPUs de alto volume no custo de GH/s (frequência de *hashs* minerados por segundo) que já contavam com uma boa penetração no varejo. O Autor destaca que as FPGAs chegavam a consumir até cinco vezes menos do que as GPUs para uma mesmo montante de capacidade computacional, porém seu reinado teve curta duração devido a entrada das ASICs no mercado, um componente eletrônico desenvolvido especialmente para a mineração que, devido seus ganhos de escala, possibilitou menores custos devido e melhorias de eficiência energética.

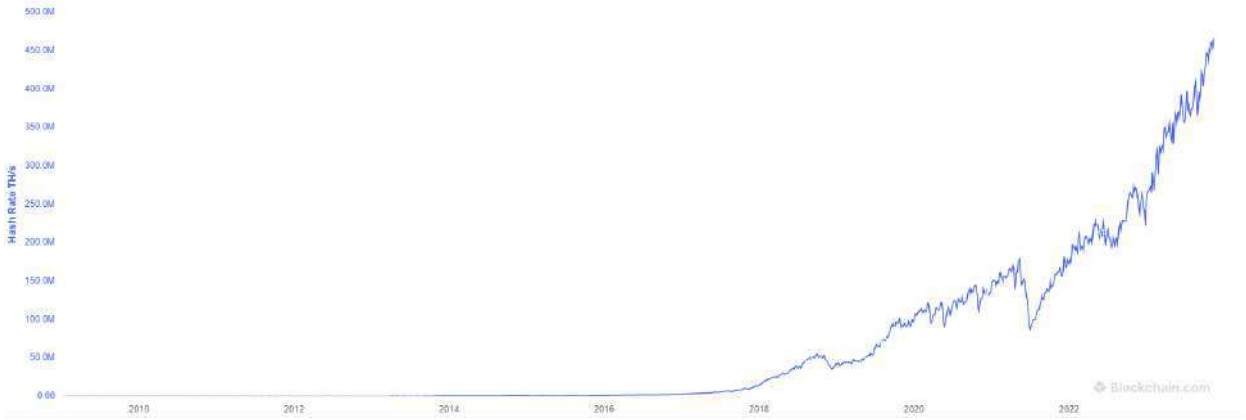


Figura 16 – Evolução do poder de processamento da rede Bitcoin desde sua criação - em EH/s (10^18 ou quintilhão de *hashes*) – 2009-2023. Escala linear, médias móveis de 7 dias.

Fonte: Blockchain.com

É inevitável a comparação do crescimento do poder de processamento das redes *blockchains* com a valorização das criptomoedas, conforme observado na figura 16, já que a sua valorização torna, no curto-prazo, a mineração uma atividade economicamente rentável. Porém, é perceptível que os investimentos em mineração se dão em razão da valorização ou da expectativa de valorização do ativo. De modo geral, para a melhor funcionalidade da rede, é necessário um maior poder computacional empregado.

Durante o último trimestre de 2017 até início de fevereiro de 2018, houve uma valorização muito maior do preço do ativo diante da capacidade transacional do sistema. O que resultou em um aumento nas taxas de transferências, o que contribuiu para a migração de uma parte significativa do *marketcap* da Bitcoin para outras moedas com transações energeticamente otimizadas e, consequentemente menores custos operacionais e taxas.

A necessidade de processamento da rede cresce na medida em que a mesma se torna mais utilizada. Nakamoto[4] (2008) explica que para compensar o aumento da velocidade de processamento devido a evoluções tecnológicas, a dificuldade do *proof-of-work* aumenta seguindo sua média móvel. Se os números de blocos gerados por hora aumentarem muito rápido, cresce a dificuldade na mineração. Isto é, as altas taxas de transação funcionaram como um incentivo a entrada de um maior poder de mineração, que foi generosamente recompensado por um curto intervalo de tempo, e que agora encontra-se em uma situação menos favorável.

Figura 17 – Evolução do consumo estimado da rede Bitcoin em TWh – 2017-2023.

Fonte: BitcoinEnergyConsumption.com / Digiconomist

4.2 A equação de lucratividade da mineração de criptomoedas

Nas redes blockchains baseadas em *proof-of-work* (PoW), quanto maior o poderio computacional de um agente validador, maior é a probabilidade de este ser o validador das transações e obter a recompensa das mesmas. Desta forma, os mineradores tendem a agir em prol do interesse próprio, investindo e aumentando o seu poder computacional, o que no agregado, resulta no aumento do grau de dificuldade da rede, e por tanto, numa menor probabilidade de obter a recompensa de um bloco ou fração do mesmo, caso este opere em um pool de mineração[10].

Os rendimentos da mineração são um resultado do grau de dificuldade da rede – que reflete a competitividade entre os mineradores –, da parcela de comissão paga na criptomoeda minerada e do preço dessa criptomoeda em moeda fiduciária. Dessa forma, obtemos a seguinte Equação dos Rendimentos da Mineração[11]:

R.M = G.Dif x C.Cripto x P.Cripto/fiat.

Onde: R.M = Rendimentos da Mineração; G.Dif = Grau de dificuldade da rede; C.Cripto = Comissão paga aos mineradores (em cripto) x P.Cripto/fiat = Preço da criptomoeda sobre moeda fiduciária.

Assumindo como verdadeira a premissa de que o grau de dificuldade da rede tende a

[10] Associação de mineradores que visa a repartição do montante total encontrado, dando maior previsibilidade a receita da mineração.

[11] Elaboração própria, com base na massa de taxa de transações pagas aos mineradores retirada da Blockchain.info e grau de dificuldade da rede.

aumentar ao longo do tempo, devido ao comportamento egoísta dos agentes mineradores, a trajetória real de rendimentos da mineração depende da relação entre a comissão paga aos mineradores e o preço da criptomoeda minerada em uma determinada moeda fiduciária, sendo geralmente pareada em dólar.

Se por um lado o aumento do preço geral dos criptoativos – sobretudo da Bitcoin – leva ao aumento do consumo elétrico da rede, o movimento contrário da queda de demanda elétrica decorrente da depreciação dos ativos digitais também pode ser verificado, ainda que de forma temporária. Com a queda dos preços, uma parcela dos agentes optará por não operar mais seus maquinários, dado o resultado contábil final da sua função lucro. Sendo a função do Custo da Mineração dividida entre custos fixos, sobretudo de maquinário, e variáveis, sobretudo do custo elétrico operacional. Desta forma, obtemos de forma resumida, a seguinte Equação de Custos da Mineração:

$$\mathbf{C.M = CFm + CVm}$$

Onde: C.M = Custos da Mineração; CFm = Custo Fixo: Maquinário (Mineradoras), Transformadores, Infraestrutura de forma geral; CVm: Eletricidade, manutenção dos equipamentos e salários.

Desta forma, obtemos de forma resumida, a seguinte Equação de Lucros da Mineração:

$$\mathbf{L.M = R.M - C.M}$$

Onde: L.M = Lucros da Mineração; R.M = Rendimentos da Mineração; C.M = Custos da Mineração

Por fim, obtemos a forma expandida da Equação de Lucros da Mineração:

$$\mathbf{L.M = [G.Dif \times C.Cripto \times P.Cripto/fiat] - [CFm + CVm]}$$

Onde: R.M = Rendimentos da Mineração; G.Dif = Grau de dificuldade da rede; C.Cripto = Comissão paga aos mineradores (em cripto) x P.Cripto/fiat = Preço da criptomoeda sobre moeda fiduciária. / C.M = Custos da Mineração; CFm = Custo Fixo: Maquinário (Mineradoras), Transformadores, Infraestrutura de forma geral; CVm: Eletricidade, manutenção dos equipamentos e salários.

Analisando de forma mais profunda o problema do crescente aumento sistêmico de consumo de energia do *proof-of-work* (PoW), obtemos um cenário de *tragedy of the commons* (tragédia dos comuns), definido pelo economista britânico William Forster Lloyd em *Two Lectures on the Checks to Population*, como um cenário onde os agentes optam por ações egoístas, afetando diretamente seus pares, até que se esgotem os recursos comuns – no modelo PoW, tais recursos são as taxas de transações pagas aos validadores da rede.

Com o aumento da competitividade dos agentes mineradores via maiores rodadas de investimentos em maquinários destinados à mineração, há o consequente aumento na demanda energética da criptomineração, devido à sua característica sistêmica, oriunda da tragédia dos comuns. De acordo com Bentov et. Al (2014) em *Proof of Activity: Extending Bitcoin's Proof of*

Work via Proof of Stake:

> Sem limitações impostas pelo protocolo sobre o que pode entrar em um bloco, um minerador racional preferirá incluir todas as transações que pagam taxas, mesmo que a taxa seja muito baixa, porque o custo marginal de incluir uma transação é trivial. Se os mineradores aceitarem transações com taxas baixas, os usuários não terão motivos para pagar taxas significativas e as taxas totais que podem ser coletadas pelos mineradores não serão suficientes para cobrir o custo da mineração PoW (Bentov et al., 2014, p.2 Tradução própria).

Moedas digitais com sistema de validação PoW com um montante máximo limitado, como a Bitcoin, estão mais suscetíveis ao esgotamento dos rendimentos da mineração – dado que parte dos ganhos dos mineradores são oriundos das novas moedas geradas. O halving, fenômeno programado de diminuição da expansão monetária da Bitcoin, contribui para o afunilamento das taxas pagas aos mineradores. Assim, a ceteris paribus, uma menor expansão no número de moedas entrando em circulação faz com que a recompensa geral da mineração diminua.

Entretanto, o resultado é definido pela equação de rendimentos da mineração, que leva em consideração as taxas transacionais e o preço do criptoativo em moeda fiduciária. Desta forma, os mineradores são estimulados a competirem agressivamente por maquinários mais eficazes – isto é, com maior poder de processamento e menor consumo elétrico – de modo a continuarem operando. Sendo assim:

> É provável que a mineração PoW se torne significativamente menos lucrativa quando o subsídio de recompensa em bloco se tornar insignificante e a recompensa consistir quase inteiramente em taxas de transação. […] É do interesse de cada usuário de Bitcoin que as taxas sejam pagas pelas transações, para incentivar os mineradores a fornecerem à rede um nível suficiente de segurança; no entanto, cada usuário preferirá que outros paguem taxas, enquanto ele não paga nenhuma taxa e ainda usufrui da segurança da rede [...] A solução está no poder que os mineradores têm de rejeitar transações se a taxa paga não for alta o suficiente (Bentov et al., 2014, p.1-2 Tradução própria).

Por apresentar um sistema de validação competitivo de esforço computacional, o modelo PoW é alvo de críticas por causa do dispêndio de recursos, sobretudo eletricidade. No *Proof-of-Work*, "[...] as taxas de transação são pagas apenas ao minerador que criou o bloco, enquanto o custo de propagação, verificação e armazenamento das transações é compartilhado por todos os nós da rede" (Bentov et al,. 2014, p.3 Tradução própria).

Outro aspecto criticável é a existência de um número limitado de transações permitidas por bloco, definido pela rede. De acordo com Bentov (2014), a existência de um limite

determinado de transações por blocos é uma medida que visa a proteção dos próprios agentes validadores (mineradores) contra eles mesmos. Segundo o autor:

> [...] Manter uma rede saudável requer algumas regras impostas por protocolo que protegem os mineradores, como um grupo, deles mesmos - como um limite no valor total transferido em transações em cada bloco. Se o limite for escolhido corretamente, os mineradores realmente ganharão mais com esse tipo de limite - tornando o espaço em bloco um recurso escasso, seu preço sobe; as transações terão que competir com outras para admissão e pagar altas taxas pelo privilégio. Um minerador individual não pode quebrar o mercado aceitando transações com taxas baixas, pois ele só pode colocar algumas no bloco (Bentov et al., 2014, p.4 Tradução própria).

Em suma, a mineração de criptomoedas é uma atividade econômica que envolve o fator incerteza, dada a grande variabilidade no preço das criptomoedas, componente fundamental na *equação de rendimentos da mineração*. Outro fator a ser considerado é o aumento no grau de dificuldade da mineração, dado que os agentes continuam aumentando seus poderes computacionais até o ponto em que os recursos – sob a forma das taxas pagas aos mineradores – não justifiquem mais o processo de reinvestimento, isto é, dada a relação risco-retorno, comparando a mineração com demais atividades da economia.

4.3) PoW vs PoS: Eficiência energética e regulamentação podem decidir futuro dos criptoativos

A ineficiência energética do *proof-of-work* tem sido apontada como um problema outrora latente, mas cada vez mais preocupante na medida em que o aumento da popularidade de criptoativos financeiros e projetos de *blockchain,* de uma forma geral, crescem. É notado que a quantidade de energia consumida pelo processo de mineração está diretamente relacionada ao aumento da popularidade dos projetos digitais, o que evidencia uma correlação relativa entre a energia consumida pelo sistema e o uso efetivo da rede – isto é, em transações reais ponto-a-ponto *(peer-to-peer)* e não sob a face especulativa –. Desta forma, o eventual cenário onde há a adesão generalizada de projetos *blockchains* esbarra na adequação dos mesmos às demandas regulatórias das autoridades governamentais, sobretudo se levarmos em consideração o alto consumo energético. Neste contexto, torna-se necessário explorar soluções e alternativas técnicas para elevar o grau de eficiência energética no processo de validação de transações das *blockchains*.

Devido sua descentralização, a demanda por energia do processo de mineração de criptoativos apenas foi notada a partir de 2015, quando essa atividade começou a ganhar volume. A estimativa de consumo de energia da atividade de mineração ultrapassou 107 TWh em meados

de 2023, segundo levantamento realizado pelo Digiconomist (2023). A fim de ilustrar a ineficiência do sistema é importante ressaltar que a transação de um único bloco de bitcoin, onde são realizadas aproximadamente 2 mil transações, consome o mesmo montante de energia que o necessário para realizar 596.787 transações na rede VISA. Ou seja, a rede *blockchain* da Bitcoin é 298 vezes menos eficiente[6] do que o sistema de pagamentos da rede VISA, de acordo com a Figura 18.

Figura 18 – Consumo elétrico e pegada de carbono da rede bitcoin em comparação ao sistema VISA.
Fontes: Bitcoin Energy Consumption / Digiconomist. 2023. Tradução Própria.

Se acrescentarmos o impacto ecológico oriundo da emissão de carbono produzida para alimentar as redes BTC e VISA obtemos uma disparidade ainda maior, sendo uma única transação na rede Bitcoin emitindo o equivalente em carbono a 1,1 milhões de transações na rede VISA, de acordo com o *Bitcoin Energy Consumption* (2022).

Dado o perfil histórico de alocação da atividade de mineração em regiões com uso massivo de energia fóssil, o impacto ecológico da mineração de Bitcoin é um outro fator a ser levado em consideração em um mundo cada vez mais focado na eficiência energética e no ambientalismo. Segundo De Vries, A. (2022), economista e fundador do Digiconomist, mineradores "não possuem incentivo para se importar com energia limpa" e irão migrar para onde a eletricidade for mais barata e com fornecimento estável. Desta forma, agentes mineradores no modelo PoW comumente se concentram em países ou regiões específicas dentro de países que apresentem vantagens comparativas, sobretudo em estados nos EUA e províncias no Canadá, com baixo custo elétrico, regulamentações favoráveis e excedentes de fornecimento de energia.

4.3.1 Concentração da Mineração: Como vantagens comparativas afetam a indústria da mineração de criptoativos e o sistema elétrico de países

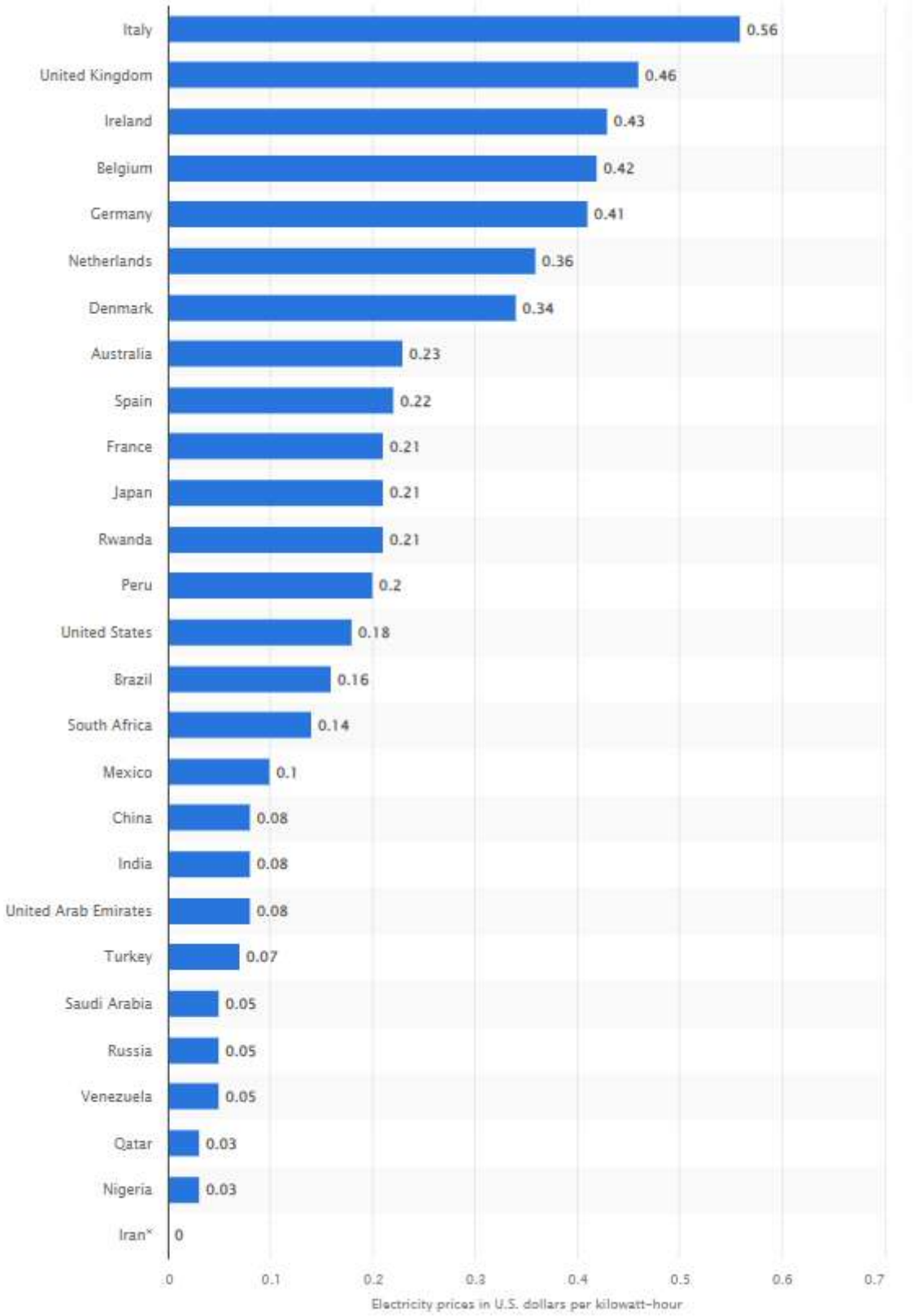
Conforme abordado anteriormente neste estudo, a mineração de criptoativos – sobretudo

a mineração da Bitcoin – é uma atividade econômica que pode ser realizada teoricamente de qualquer lugar do mundo. Na prática, é possível observar a concentração de maquinário (ASICs) em um pequeno grupo de países – China, Estados Unidos, Canadá, Cazaquistão, Malásia e Alemanha. Tal fenômeno de concentração evidenciado pelo Gráfico 3 abaixo pode ser explicado através das vantagens relativas destes países em relação às demais localidades, sejam elas um menor custo elétrico, maior facilidade para aquisição ou importação do maquinário e um cenário regulatório mais favorável ou inexistente que não ameace a atividade da mineração.

Desta lista de componentes de vantagens comparativas para a mineração, a China reunia todos os requisitos para a consolidação do setor de criptomineração em escala industrial - traduzido em energia e equipamentos baratos. De acordo com o *Cambridge Electricity Consumption Index* (2022), a China concentrava cerca de 70% do poder computacional da rede BTC até final de 2020.

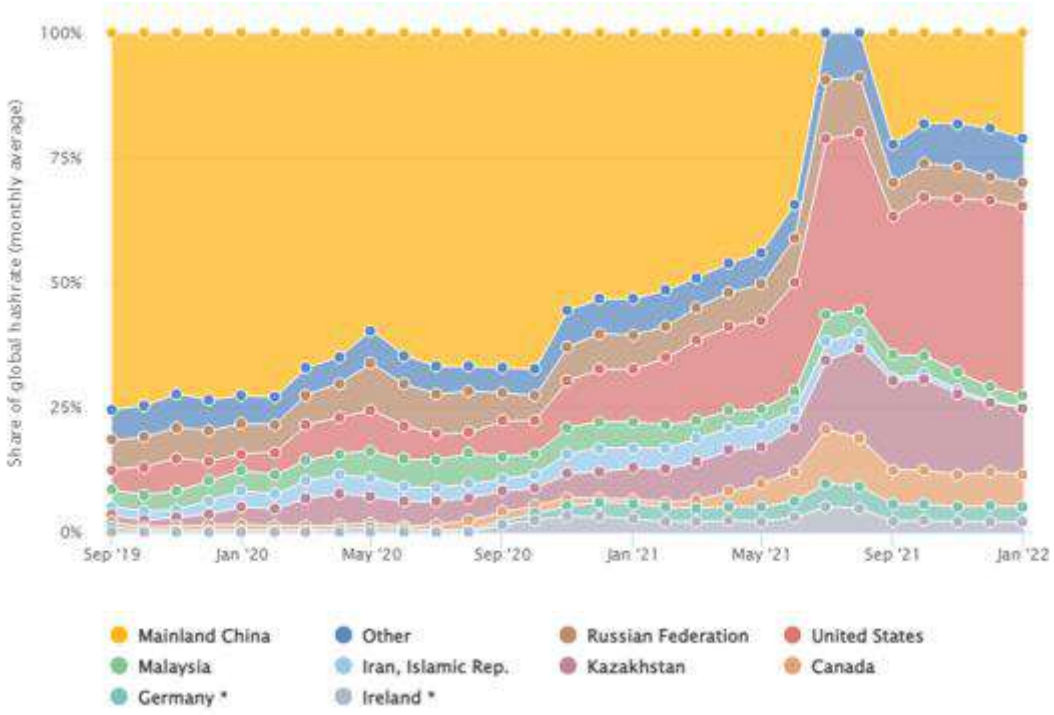
O Brasil, como visto no gráfico abaixo, apresenta um custo elétrico médio relativamente baixo quando comparado a outros países. Porém, a alíquota elevada sobre componentes eletrônicos importados e a burocracia estatal são fatores que diminuem a atração do país para as mineradoras. Países com condições mais favoráveis a mineração, como o caso do Canadá, Paraguai e de determinadas regiões dos Estados Unidos, por outro lado, vêm sendo o principal destino para os investidores em mineração.

Gráfico 3 – Custo do kWh em países selecionados em março de 2023, preços em USD.



Fonte: Statista (2023).

Gráfico 4 – Distribuição do poder de processamento da rede Bitcoin por país (2019-2022)



Fonte: University of Cambridge / Cambridge Bitcoin Electricity Consumption Index. 2022

A criptomineração tem como característica a concentração de suas atividades em países que apresentam vantagens comparativas, proporcionando desde a viabilidade operacional até maiores margens de lucros, alimentando um ciclo de investimento como observado na seção 4.2. É devido a essas características que a atividade de mineração se concentrou sobretudo em países como a China e EUA.

No entanto, desde 2021, o governo chinês vem aumentando as restrições a atividade de mineração de criptomoedas em seu território. De acordo com levantamento do *Tony Blair Institute for Global Change (2022)*, o efeito total do êxodo da criptomineração da China demorou para ser notado, devido ao fato de uma parcela considerável dos agentes mineradores ter conectado suas operações à fontes produtoras *off grid.* O incremento na demanda elétrica da mineração de bitcoin, em decorrência ao êxodo chinês, sobrecarregou as redes dos EUA e aumentou a emissão de carbono norte-americana, uma vez que a produção de eletricidade nos EUA tem como característica a alta participação de fontes fósseis de energia.

De acordo com o *Cambridge Bitcoin Electricity Consumption Index* (2022), os EUA receberam a maior parte do êxodo chinês da indústria da criptomineração, resultante das vantagens comparativas relacionadas ao custo energético e regulatórios de alguns estados. Por se tratar de um modelo federativo, os EUA são encarados como um país com maior margem regulatória, onde os agentes podem facilmente migrar seus maquinários internamente dentro do

país para estados com leis mais favoráveis à mineração de criptoativos, desde que estes possuam vantagens comparativas referentes ao custo energético.

Os Estados Unidos, porém, acompanham a tendência regulatória de outras regiões. Em março de 2022, o governo norte-americano assinou o "executive order" número 14.067, garantindo o desenvolvimento futuro responsável dos ativos digitais, que entre outros objetivos, visa a melhor eficiência energética das blockchains, reduzindo o impacto ambiental da tecnologia. Tal dispositivo jurídico tem como objetivo fornecer um relatório sobre o panorama do setor e seus impactos ambientais, onde:

> (...) O relatório também deve abordar o efeito dos mecanismos de consenso das criptomoedas sobre o uso de energia, incluindo a pesquisa sobre potenciais medidas de mitigação e mecanismos alternativos de consenso e as compensações de design que isso pode implicar. O relatório deve abordar especificamente: (A) usos potenciais do blockchain que poderiam apoiar tecnologias de monitoramento ou mitigação dos impactos climáticos, como a troca de passivos por emissões de gases de efeito estufa, água e outros ativos naturais ou ambientais; e (B) implicações para a política energética, incluindo no que diz respeito à gestão e fiabilidade da rede, incentivos e normas de eficiência energética e fontes de fornecimento de energia. (14067 *Executive Order – Ensuring Rensnsible Development of Digital Assets*. US Presidencial Document. 2022. Tradução Própria)

A proibição efetiva da criptomineração em território chinês em meados de 2021 modificou drasticamente o rumo da indústria da mineração, o que provocou um êxodo do poder de processamento e o aumento da demanda energética em países como os EUA, Canadá, Cazaquistão e Rússia. A dimensão do problema do êxodo da criptomineração chinesa pode ser vista analisando o consumo da rede em comparação ao consumo dos países que receberam o fluxo de investimentos do setor. De acordo com o *Cambridge Electricity Consumption Index* (2022), o consumo atual de 107 TWh da rede blockchain representava 1,3% da demanda elétrica chinesa de 8.090 TWh em 2022. Este mesmo valor absoluto representa uma inserção de 18,5% no consumo anual canadense (577 TWh).

O impacto da criptomineração no setor elétrico dos países que receberam os fluxos principais de investimentos chineses (implicações ambientais negativas e ameaça à segurança energética e ao crescimento econômico) tem levado os governos desses países a reverem suas políticas para o setor. Dessa forma, é possível destacar que os governos dos países hospedeiros – como a China e os EUA – caminham para um cenário convergente de adoção de uma abordagem mais proativa em relação ao licenciamento, tributação, regulamentação. No caso da China, a solução encontrada pelos mineradores que resistiram às proibições foram o uso de sistemas

eólicos ou solares off-grid ou até a clandestinidade[12], com a ocultação das minerações perante os olhos do estado chinês.

4.3.2 PoW vs PoS: Ethereum 2.0 no debate da transição tecnológica

Com o aumento da popularidade dos criptoativos, o debate acerca do dispendioso consumo elétrico causando pelas redes blockchains baseadas em *proof-of-work* (PoW) ganha destaque na medida em que um maior número de usuários e novas aplicações surgem dentro da rede Blockchain. Nesse contexto, a adesão a outros modelos de mineração menos intensivos em energia, como o *proof-of-stake* (PoS), vem se intensificando.

Concomitantemente a disputa tecnológica entre PoW e PoS, novas gerações de criptoativos vem surgindo. A popularização dos *utility tokens* – ativos utilizados para pagamento ou acesso a serviços – como a BNB, criado pela Binance, a maior corretora de criptoativos do mundo, evidencia essa tendência.

A exemplo da própria BNB, que surge como um *token* dentro da rede nativa da Ethereum (ERC-20) e posteriormente assume identidade e rede blockchain própria, a Binance Smart Chain (BSC) vem atraindo projetos utilitários, isto é, projetos com aplicações práticas, como *tokens* de pagamento ou contratos inteligentes. Dessa forma, a BNP vem ganhando participação de mercado frente à própria rede Ethereum. De acordo com um artigo publicado pela Binance Academy (2020):

> A Binance Smart Chain (BSC) é mais bem descrita como uma blockchain que é executada de forma paralela à Binance Chain. Ao contrário da Binance Chain, a BSC possui funcionalidade de contrato inteligente e compatibilidade com a Ethereum Virtual Machines (EVM). O objetivo da Binance Smart Chain foi introduzir contratos inteligentes em seu ecossistema [...] Como a BSC é compatível com a EVM, ela foi lançada com suporte para o vasto universo de ferramentas e Apps da Ethereum. Em tese, isso facilita que desenvolvedores migrem seus projetos da Ethereum (Binance Academy, 2020).

É válido destacar que os *utility tokens* dependem da arquitetura PoS para serem utilizados em larga escala, devido a desempenharem um papel transacional em maior escala se comparado aos criptoativos utilizados primariamente como reserva de valor – como a Bitcoin. Desta forma, a equipe desenvolvedora da BNB criou uma rede alternativa, a Binance Smart Chain (BSC), de modo a criar um ambiente mais atrativo para os contratos inteligentes.

[12] De acordo com reportagem da CNBC, 2021.

Figura 18: O Ethereum 2.0 no centro do Trilema da Escalabilidade proposto pelo seu cofundador, Vitalik.

Fonte: Ethereum Foundation. (2022)

Do ponto de vista prático, o método de validação de uma rede blockchain impacta em quão descentralizada ela é ou em quantas transações ela é capaz de realizar por segundo, de acordo com o Trilema da Escalabilidade de Vitalik (2021) citado anteriormente neste estudo. Segundo De Vries (2023, p.2), independentemente da validação PoW ou PoS estar sendo utilizada, as blockchains são cadeias literais de blocos de dados. Segundo o autor, a diferença técnica entre os sistemas de validação PoW e PoS torna-se relevante no que diz respeito a como os diferentes métodos alinham o processo de adicionar novos blocos ao conjunto atual de blocos existentes em uma blockchain. Desta forma:

> Quando uma rede emprega PoW (...) novos blocos podem ser adicionados ao blockchain apenas uma vez que um PoW válido foi obtido (...), permitindo que o vencedor sortudo para o adicionar ao blockchain e obter a recompensa associada por fazê-lo. (...) Em contraste, uma rede que usa PoS não incentiva os participantes a competirem em poder computacional para criar novos blocos para o blockchain. Em vez disso, o processo de

> seleção de quais computadores criam o próximo bloco para o blockchain é principalmente baseada na riqueza. (...) O software então seleciona aleatoriamente um ‘‘*staker*” (acumulador) para produzir o próximo bloco para a cadeia de blocos (...) (De Vries, 2023, p.2).

É justamente neste contexto da pressão que os *utility tokens* exerceram no mercado no final da década de 2010 que novas redes *blockchains* capazes de suportarem um elevado número de transações simultâneas ganharam popularidade, entre elas a própria rede BSC, a rede Solana e a própria atualização da rede Ethereum, denominada de *merge* (fusão) ou Ethereum 2.0. Anteriormente, os contratos inteligentes utilizavam majoritariamente a rede ERC-20 da Ethereum. Com limitações decorrentes do sistema PoW, como altas taxas, novos protocolos, sobretudo PoS, atraíram projetos utilitários devido às vantagens representadas por menores taxas transacionais e maior escalabilidade do número e velocidade de transações.

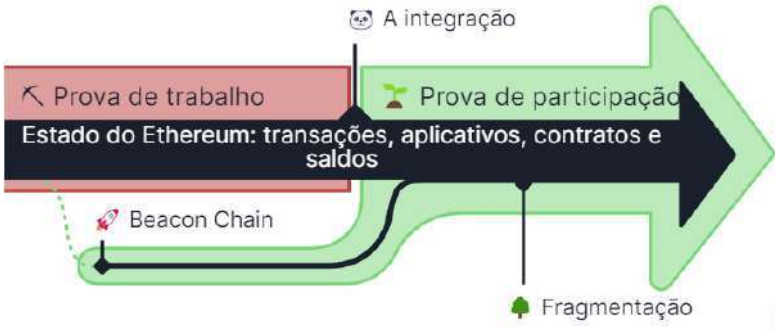


Figura 19: Processo de fusão (*merge*) das redes Ethereum, com a fusão das redes ERC-20 (rede principal) e rede Beacon Chain.

Fonte: Ethereum Foundation Blog (2023).

O processo de fusão da rede Ethereum demorou alguns anos e foi realizado em diversas etapas de modo a mitigar riscos técnicos de colapso da rede, sendo realizado com sucesso em setembro de 2022. De acordo com a *Ethereum Foundation*, o processo de fusão consistiu na coexistência de uma rede principal (ERC-20, operada via PoW) e uma rede secundária, a Beacon Chain, operada através do PoS. De acordo descrito através do blog *The Merge* da *Ethereum Foundation Blog*:

> Inicialmente, a Beacon Chain foi enviada separadamente da *Mainnet*. A rede principal da Ethereum - com todas as suas contas, saldos, contratos inteligentes e estado da cadeia de blocos - continuou a ser protegida pela prova de trabalho, mesmo enquanto a Beacon Chain funcionava em paralelo usando a prova de participação. A Fusão foi quando esses

> dois sistemas finalmente se uniram, e a prova de trabalho foi permanentemente substituída pela prova de participação (Ethereum Foundation, 2023).

A coexistência das duas redes dentro da plataforma Ethereum (ERC-20 e Beacon Chain) antes da fusão foi possível através de um mecanismo de sincronização. De acordo com o Ethereum Foundation Blog (2023), antes do *merge* a rede Beacon Chain não processava as transações da rede principal. Ao invés disso, a Beacon Chain estava chegando ao consenso sobre seu próprio estado ao concordar com validadores ativos e seus saldos de conta. Após o *merge*, a Beacon Chain tomou o lugar da rede principal, se tornando o mecanismo de consenso para todos os dados da rede, incluindo transações da camada de execução e saldos de contas. Através do PoS, os agentes validadores do Ethereum deixaram de ser os mineradores e se tornaram os *stakers*, detentores de quantidades de ETH operando de forma autônoma ou em grupos através dos fundos de *staking* de corretoras de criptoativos.

Tabela 4: Comparação da banda maior e menor da estimativa de demanda energética do Ethereum antes e após o Merge

Cenário de Demanda de Energia	Demanda de Energia (kW)	Redução em comparação ao PoW (banda inferior)	Redução em comparação ao PoW, banda superior
Ethereum PoS banda inferior	36	-99,9914%	-99,9996%
Ethereum PoS banda superior	675	-99,8385%	-99,9927%

Fonte: De Vries, A. (2022)

Antes do *merge* – fusão das redes da Ethereum –, sobretudo a partir de 2017, o mecanismo de consenso PoW da rede Ethereum foi alvo de críticas pelo seu alto consumo de energia, fenômeno explicado pelo modelo sistêmico de competitividade entre poderio computacional de agentes (mineradores) cada vez mais crescente, com consumo estimado em 93 TWh[13], que seria reduzido em até 99,99% com a atualização da rede Ethereum. De acordo com De Vries (2022, p.3), a natureza semi-descentralizada da estrutura PoS, composta por *node* – termo em inglês para

[13] De acordo com dados do *Ethereum Energy Consumption* do Digiconomist

nó, um sistema que possui uma cópia primária do protocolo original da rede, funcionando como ponto de conexão – da rede Ethereum 2.0 e as variedade nos hardwares utilizados para a manutenção dos nós dificulta uma estimativa precisa no consumo da rede. Conforme De Vries (2022) aponta em seu estudo, os requisitos de hardware também dependem da combinação de cliente de consenso e execução que está sendo utilizada para operar um. O autor sugere que um dispositivo simples, como o Raspberry Pi 4gb – um mini-computador de baixo custo, com consumo de 8 W –, pudesse ser capaz de rodar um *node* da rede PoS do Ethereum, embora não fosse recomendado. Em um cenário extremamente otimista, onde os aproximadamente 4.500 *nodes* existentes nos dias posteriores ao *merge* do Ethereum fossem rodados por esses dispositivos, o consumo aproximado da rede Ethereum PoS seria de apenas 36kW. Em um cenário mais realista, com uso de servidores empresariais, com consumo estimado em 100-150 W, De Vries (2022) calcula a demanda total de energia da rede Ethereum PoS em 675 kW. Segundo o autor:

> No entanto, devido à natureza descentralizada da rede Ethereum, não há uma visão centralizada de todos os nós conectados. (...) parece provável que a rede Ethereum tenha reduzido sua demanda de energia em pelo menos 99,84% (banda maior) ao fazer a transição de PoW para PoS (Tabela 4). Na melhor das hipóteses, a redução total na demanda de energia poderia chegar a até 99,9996% (banda menor). De qualquer forma, é muito provável que o Merge tenha realizado uma diminuição significativa na demanda total de energia da rede Ethereum, uma vez que o Ethereum em PoW exigia de 619 a 255.833 vezes mais energia elétrica do que o Ethereum em PoS. Em termos absolutos, a redução na demanda de energia poderia ser equivalente ao requisito de energia elétrica de um país como a Irlanda ou até mesmo a Áustria (De Vries, 2022, p. 3. Tradução própria).

Embora tenha solucionado o problema do alto consumo de energia da rede, a fusão (*merge*) da rede Ethereum não solucionou de imediato problemas da rede como a escalabilidade – isto é, a limitação no número de transações validadas por segundo –, fundamental para o futuro dos contratos inteligentes. De acordo com artigo *Danksharding* (2023) publicado na *Ethereum Foundation*, o *merge* foi uma etapa fundamental para uma série de atualizações que visam resolver os problemas sistêmicos da rede. Segundo os desenvolvedores, a rede Ethereum adotará uma atualização denominada de *Danksharding* iniciada em testes com a EIP-4844. Segundo eles, a atualização propõe otimizar o processo de agrupar transações de forma eficaz, conhecido como *rollups*, ao utilizar bolhas de camada 2 (L2):

> O Proto-Danksharding, também conhecido como EIP-4844, é uma forma para *rollups* adicionarem dados mais baratos aos blocos. O nome vem dos dois pesquisadores que

> propuseram a ideia: Protolambda e Dankrad Feist. No momento, os rollups têm limitações em quão econômicas podem tornar as transações de usuários devido ao fato de que eles enviam suas transações em CALLDATA. Isso é caro porque é processado por todos os nós Ethereum e permanece na cadeia para sempre, mesmo que os rollups precisem dos dados por um curto período de tempo. O Proto-Danksharding introduz "bolhas de dados" que podem ser enviados e anexados aos blocos. Os dados nessas "bolhas" não são acessíveis ao EVM e são automaticamente excluídos após um período de tempo fixo (de 1 a 3 meses). Isso significa que os *rollups* podem enviar seus dados de forma muito mais barata e repassar as economias aos usuários finais na forma de transações mais baratas (Ethereum Foundation, 2023. Tradução Própria).

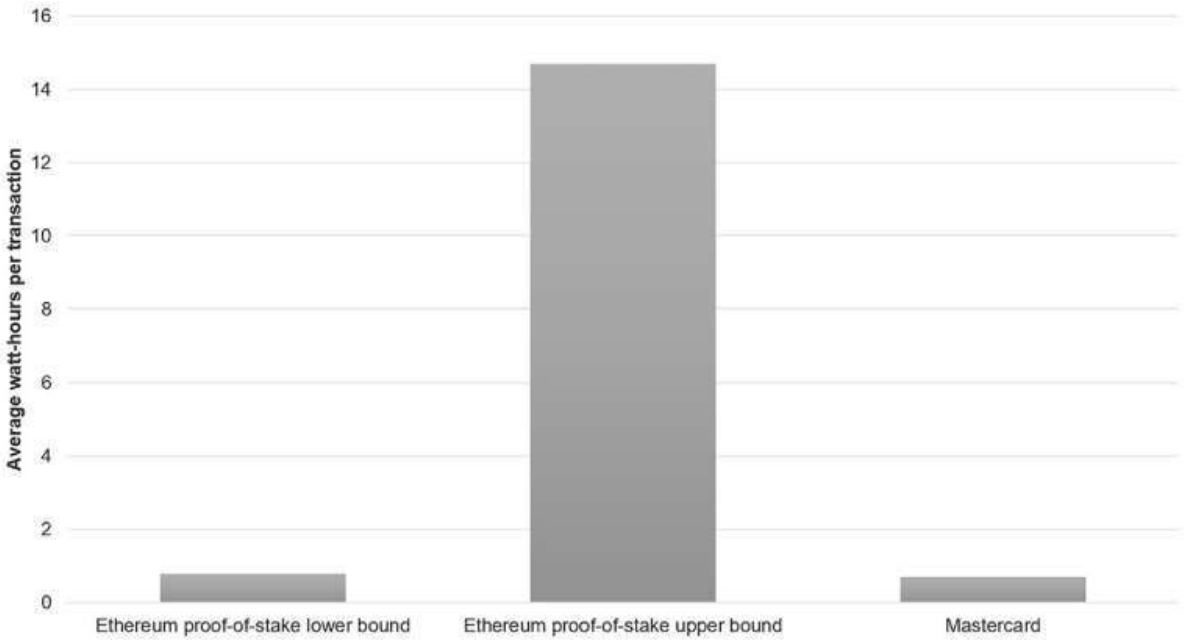


Figura 20: Comparação entre a eficiência energética do PoS do Ethereum 2.0 em relação a transação na rede Mastercard.

Fonte: De Vries, A. (2022)

A atualização do Ethereum de *proof-of-work* (PoW) para *proof-of-stake* (PoS) no evento popularmente denominado de *merge* soluciona permanentemente o problema da sustentabilidade da rede, a tornando até 99,99%[14] energeticamente mais eficaz, a equiparando com o consumo da rede Mastercard, como demonstrado na Figura 20, em projeções mais otimistas. Além disso, essa transição vai de acordo com as diretrizes regulatórias rumo a uma economia mais sustentável a nível global.

Entretanto, o Ethereum 2.0 ainda possui uma longa trajetória repleta de desafios técnicos, sobretudo relacionados à problemas de escalabilidade. Caso as atualizações da rede funcionem

[14] De acordo com projeção realizada por DE VRIES (2022)

sem comprometer a segurança do sistema, o Ethereum pode pavimentar o caminho dos criptoativos rumo a um futuro sustentável. O obstáculo para esse futuro "verde" dessa vez consiste no Bitcoin, cuja rede consome estimados 107.60 TWh (DIGICONOMIST, 2023). Ao contrário do Ethereum, que possui uma centralização na tomada de decisão, a Bitcoin não possui nenhuma autoridade centralizada ou entidade organizadora, recebendo suas atualizações de protocolo através do voto das *pools* de mineração. Outro fator que dificultaria uma migração da rede Bitcoin ao PoS é a baixa demanda transacional da mesma, que através do seu processo de financeirização, a consolidou como uma espécie de ouro virtual.

5 CONCLUSÃO

O desenvolvimento do presente estudo buscou investigar e aprofundar a questão da eficiência energética em redes *blockchain*, examinando em detalhes as propriedades da atividade e os consequentes desafios e oportunidades que esta tecnologia apresenta em termos de gestão de energia e formulação de políticas públicas visando a mitigação dos impactos desta tecnologia à luz do crescente foco global nas emissões de carbono e no meio ambiente.

O estudo confirma que as redes *blockchain*, sobretudo aquelas que usam mecanismos de *proof-of-work* (PoW), em destaque a Bitcoin e o Ethereum 1.0, resultam em um maior consumo de energia. Sobretudo, o estudo reconhece que as características do setor resultam em uma concentração da criptomineração em determinadas regiões com vantagens comparativas referentes ao custo elétrico e ausência de proibição da atividade, gerando externalidades negativas nessas mesmas regiões. Em alternativa, o protocolo de *proof-of-stake* (PoS) e algoritmos de consentimento de baixa energia, demonstram a capacidade de resolver gargalos técnicos e alcançar a eficiência energética.

Além disso, fatores exógenos como as respostas regulatórias ao avanço do impacto das blockchains validadas via mecanismos PoW e o surgimento de *utility tokens*, que visam um alto número de transações simultâneas, aceleram a necessidade de implementação de protocolos mais eficazes, capazes de suprir as necessidades, sociais e de mercado, de uma nova economia.

Essencialmente, essa análise destaca que a eficiência energética em redes *blockchain* é um objeto de esforço de pesquisa e desenvolvimento multidisciplinar. Embora as preocupações sobre o elevado e crescente consumo de energia pelas redes blockchains seja legítimo, é um problema possível de ser solucionado. Os avanços tecnológicos, tanto faceados em melhorias referentes à eficiência energética dos componentes utilizados no PoW, quanto representados por uma maior participação de sistemas *off grid* que utilizem fontes de energia sustentáveis e mudanças regulatórias serão capazes de guiar as redes blockchains rumo a um futuro sustentável.

Referências

BEEKHUIZEN, Carl. Ethereum's energy usage will soon decrease by ~99,95%. In: Carl Beekhuizen. **Ethereum Foundation Blog**, Bern, 2021. Disponível em: https://blog.ethereum.org/2021/05/18/country-power-no-more. Acesso em 18 mar. 2022.

BENTOV, Ido et al. Proof of activity: extending bitcoin's proof of work via proof of stake [extended abstract]. **Association for Computing Machinery,** New York, v. 42, n. 3, p. 34-37, Dec. 2014. Disponível em: https://doi.org/10.1145/2695533.2695545. Acesso em: 14 fev. 2022.

Bitcoin Energy Consumption Index. **Digiconomist,** 2023. Disponível em https://digiconomist.net/bitcoin-energy-consumption. Acesso em: 16 jun. 2023.

Cambridge bitcoin electricity consumption. **University of Cambridge**, 2023. Disponível em: https://ccaf.io/cbeci/index. Acesso em: 05 abr. 2023.

CAGAN, Phillip. The Monetary Dynamics of Hyperinflation. 1956. In: Adriana Navarro. **Academia.edu.** Disponível em: https://www.academia.edu/4690826/Cagan_The_monetary_dynamics_of_hyperinflation. Acesso em: 14 fev. 2022.

DE VRIES, Alex. Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. **Perspective**, v. 4, n. 1, p. 1-5, Dec. 2022. Disponível em: https://doi.org/10.1016/j.patter.2022.100633. Acesso em: 03 abr. 2022.

DERKS, Jona; GORDIJN, Jaap; SIEGMANN, Arjen. From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016. In: Jona Derks, Jaap Gordijn, Arjen Siegmann. **Springer.** Berlin, 2018. Disponível em: https://link.springer.com/article/10.1007/s12525-018-0308-3. Acesso em: 26 ago. 2022.

DI PIERRO, Massimo. What is the Blockchain? Computing in Science & Engineering, v. 19, n. 5, p. 92-95, Sep/Oct, 2017. **IEEE Computer Society**. Washington, DC. Disponível em: https://cse.sc.edu/~mgv/csce190f19/diPierro_mcs2017050092.pdf. Acesso em 30 abr. 2022.

DWORK, Cynthia, NAOR, Moni. Pricing via Processing or Combatting Junk Mail. In: Brickell, E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. **Springer**. Berlin, 2001. Disponível em: https://link.springer.com/chapter/10.1007/3-540-48071-4_10. Acesso em: 23 jan. 2022.

Energy Efficiency 2022. **IEA**, 2022. Disponível em: https://www.iea.org/reports/energy-efficiency-2022. Acesso em: 16 mar. 2023.

Estimate of the number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from january 2015 to october 2022. **Statista,** 2022. Disponível em: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/. Acesso em: 06 abr. 2023.

Ethereum average gas price. **Ychart**. Disponível em: https://ycharts.com/indicators/ethereum_average_gas_price. Acesso em: 30 jul. 2023.

Ethereum energy consumption index. **Digiconomist**, 2023. Disponível em: https://digiconomist.net/ethereum-energy-consumption. Acesso em: 16 jun. 2023.

Ethereum's energy expenditure. **Ethereum Foundation Blog**, 2023. Disponível em: https://ethereum.org/en/energy-consumption/. Acesso em: 30 jul. 2023.

FUNG, Ben; HENDRY, Scott; WEBER, Warren E. **Swedish Riksbank Notes and Enskilda Bank Note**: Lessons for Digital Currencies. Bank of Canada. Ottawa, 2018. Disponível em: https://www.bankofcanada.ca/2018/06/staff-working-paper-2018-27/. Acesso em: 29 ago. 2022.

Global energy efficiency progress is accelerating, signalling a potential turning point after years of slow improvement. **IEA**, 2022. Disponível em: https://www.iea.org/news/global-energy-efficiency-progress-is-accelerating-signalling-a-potential-turning-point-after-years-of-slow-improvement. Acesso em: 16 mar. 2023.

HAYEK, Friedrich August; BARBOSA, Heloisa G. **Desestatização do dinheiro**: uma análise da teoria e prática das moedas simultâneas. 2ª ed. São Paulo: Instituto Von Mises Brasil, 2011. Disponível em: https://rothbardbrasil.com/wp-content/uploads/arquivos/dinheiro.pdf. Acesso em 13 mar. 2022.

LIAO, Kevin at al. **Behind closed doors**: measurement and analysis of cryptolocker ransoms in bitcoin. Arizona: **Arizona State University**. Arizona, 2016. Disponível em: https://www.researchgate.net/publication/301612942_Behind_Closed_Doors_Measurement_and_Analysis_of_CryptoLocker_Ransoms_in_Bitcoin. Acesso em: 13 mar. 2022.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. Bitcoin.org, 2008, p. 1-9. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 13 mar. 2022.

UNITED STATES OF AMERICA. Ensuring Responsible Development of Digital Assets. Executive Order n° 14067, of March 9, 2022. Executive Office of the President. 2022 Mar 14. **Federal Register.** v. 87, n° 49, p. 14143-14152, Mar. 2022. Washington, D.C. Disponível em: https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets. Acesso em: 23 de outubro de 2023.

Understanding and Unleashing the Power of Blockchain**. Columbia Business School, 2023.** Disponível em: https://leading.business.columbia.edu/main-podcasts/21st-century-finance/understanding-blockchain. Acesso em: 01 set. 2023.