Moedas digitais – que dinheiro é esse?

Por **GLAUCIA CAMPREGHER***

Considerações sobre as moedas digitais; como funcionam e quais as suas possibilidades

Da moeda como registro de informação e do dinheiro como instituição social que a veicula

Primeiramente é importante que se diga que o dinheiro nasceu virtual antes que real. Isso quer dizer que nasceu registro de débitos e créditos em "livros" de líderes religiosos ou comunitários que centralizavam o poder antes que os registros ganhassem vida em pedaços de madeira, pedra ou metal que circulavam generalizadamente. Registros de débito/crédito podiam ser centralizados se grande parte das trocas se dava dentro dos limites das comunidades onde todos se conheciam.

Foi o crescimento das cidades, e depois das nações e dos impérios, com a ampliação concomitante dos espaços de trocas e a maior regularidade do comércio com "estrangeiros", que estimulou a monetização que tornava os registros algo impessoal e fungível, podendo servir para realizar até mesmo transações únicas e com quem não se conhecia.[i] O dinheiro amoedado foi assim fundamental para passarmos das "sociedades humanas" (como as chama David Graeber) – onde seu papel era marcar o que não podia ser resolvido com ele -, para as "sociedades mercantis" – onde o dinheiro chama a si todo tipo de relação.

Um equívoco que há que ser esclarecido é que o comércio e os agentes privados (o Mercado) têm a ver com a moeda impessoal, mercadoria, enquanto os registros de débito/crédito têm a ver com o poder centralizado (o Estado). De fato, no passado como também no presente, Mercado e Estado são instituições complexas que regulam, em acordos mais ou menos tácitos, as formas de produção e circulação monetária. Tanto pequenos comerciantes árabes criavam as suas "cadernetas" usando como unidade de conta símbolos comunais, quanto grandes comerciantes italianos criavam as suas letras de câmbio.

O que ocorre é que quando o Estado se organiza territorialmente de forma imperial (Lídia, Índia e China, mais ou menos ao mesmo tempo, em torno do século VI a.c) colocando exércitos e escravos a caminhar longas distâncias, o dinheiro amoedado passa a ser produzido em larga escala (nos metais preciosos que passam a ser buscados para essa função). Ao longo da história, à medida que o Estado vai fincando suas raízes não apenas na organização da vida econômica mas na regulação da vida social como um todo, o que vai se passando é que as moedas produzidas privadamente vão se referenciando cada vez mais na moeda pública até que os bancos nos nossos dias se tornem "meros" concessionários do poder público. Meros entre aspas, dado a instrumentalização que fazem desse poder, a ponto de não sabermos mais se o cachorro balança o rabo ou o rabo ao cachorro...

Mas voltando à questão da informação que é passada nos registros – sejam eles feitos nos livros sob a guarda de um poder central ou amoedados e carregados nos bolsos por qualquer um – o fato é que a informação é a mesma e todo dinheiro significa tão somente um título de dívida. A mensagem grafada no livro ou gravada na moeda é – você tem direito a um crédito de um tanto de x (y, z, etc). O que são os bens x, y, z e quanto deles você pode ter acesso é uma outra questão. Não à toa a economia política teve de teorizar o "valor" das coisas em separado de seus preços monetários. Entrar nesse tema faria esta reflexão tomar outro ramo, mas não tenho como não alertar que ao mesmo tempo que o "regime monetário" (a

moeda e o sistema inteiro que as produz, troca, amarra numa aposta ou num investimento) tem alguma autonomia em relação à economia real (disputando inclusive com ela como diria Keynes) isso não nos pode levar a pensar que esse mundo real está absolutamente separado do mundo monetário, onde a moeda reina distante e neutra como querem os neoclássicos.[ii]

Mas o fundamental a ressaltar é que o dinheiro é uma instituição social e um dos motivos do Estado vir a se tornar a instituição-mor das sociedades mercantis é justamente ter sido capaz de tornar a moeda estatal o dinheiro mais usado. A história do dinheiro está assim umbilicalmente ligada à história dos Estados. A credibilidade na moeda estatal se confunde com a credibilidade/legitimidade do Estado mesmo. Talvez poucos saibam, mas as pesquisas históricas sobre o passado mostram que a cobrança de impostos foi a maneira que os governantes acharam para garantir isso. Ao aceitarem o pagamento de impostos nas moedas que eles próprios criam, os governantes não estão se financiando com o público, mas tornando esse público cativo da sua moeda.

Se a moeda é uma criação do Estado, é pois política por natureza. E isso não significa só que ela nasce política, mas o seu desenvolvimento é político. Todo o desenho institucional que cuida da contínua produção, distribuição, regulação, e até indexação e substituição (se necessário, temporariamente, pois senão é o fim da moeda nacional), envolve interesses e fóruns que os administrem. Essa dimensão política da moeda é muito mais que a política monetária de dado governo em dado momento. Esta concerne à atuação do Estado junto aos mercados, bancos principalmente – concessionários que são da moeda estatal pois criam moeda própria (direitos de crédito) mas denominados na moeda pública – no controle da liquidez da economia.

O que não se faz controlando a quantidade de moeda em circulação (impossível dada a criação monetária bancária) mas as taxas de juros do sistema via controle das taxas dos títulos públicos com risco zero, dada a improbabilidade do desaparecimento da nação mesma. A dimensão política da moeda diz respeito assim a todo o edifício que a mantém viva e funcionante; e, portanto, ao conjunto de regulações auto-impostas que afetam os gastos públicos (ou a política fiscal) e a gestão da dívida pública (e diferentes modos de operá-la beneficiam diferentes grupos sociais), e o poder de compra da moeda nacional interna e externamente (inflação e câmbio).

O dinheiro é político também porque o Estado que o produz tem por função principal a de gerir as desigualdades entre os membros das sociedades, cujas dívidas tornadas dinheiro (e transitáveis com máxima liberdade no tempo e no espaço) podem agravar. Não à toa, as idas e vindas do dinheiro de crédito e do dinheiro amoedado ao longo da história coincidem com processos de sobre-endividamento dos mais pobres para com os mais ricos que abalam as bases da reprodução social levando, muitas das vezes, ao colapso. Desse modo, cabe ao Estado, seja ele qual for, definir que direitos e deveres são permitidos a quem e em que circunstâncias. Por exemplo, pode haver escravização por não pagamento? E cobrança de juros? E que tipo de proteção pública deve haver contra cobranças extorsivas?

Esse poder do Estado mantinha desde antes do capitalismo, mas também neste, a estabilidade e a longevidade do arranjo social básico. O incômodo com isso por parte dos agentes privados me parece contudo maior no capitalismo que em épocas passadas. Os liberais por isso inventaram que a moeda ideal deveria ser não política, não do Estado mas "da sociedade de indivíduos livres e iguais" (como se isso existisse). Essa moeda neutra, acima de todos, não poderia ser emitida a mais por "perdulários" (quando gastam com o povo, óbvio). Para tanto as regras de sua emissão deveriam ser amarradas a algo fixo acima de todos – o ouro como defendiam os liberais do passado e os algoritmos matemáticos como defendem os libertários do presente. Trata-se de raciocínio ingênuo e profundamente equivocado, mesmo quando bem intencionado.[iii]

Ao desconsiderar a realidade não se tornam transformadores dela, mas reforçadores de seus piores aspectos. Não por outra razão, os nerds criadores do Bitcoin em vez de criarem a moeda nova do novo mundo criaram apenas mais um ativo especulativo no velho. Ainda assim, fizeram uma revolução sobre o modo de passagem da informação adiante. Eles tornaram os registros eletrônicos, que já existiam, de tal modo amarrados uns aos outros numa corrente (daí o nome *blockchain* da tecnologia usada), com a informação seguindo adiante com uma espécie de assinatura eletrônica (os hashes) em cada elo. Isso torna os registros de operações não apenas checáveis, mas rápidos e seguros[iv]. Ou seja, transações monetárias de todo tipo, envolvendo agentes dispersos no espaço mais distante, podem ser feitas quase simultaneamente. O dinheiro volta assim a ser o que já era lá atrás, um mero signo num livro de registros. Apenas agora o livro mesmo é tão imaginário como o signo usado em seu interior. Ainda assim, faz o que tem de fazer, mobilizar a riqueza real no tempo e no

espaço.

Das moedas fiduciárias como signos virtuais da riqueza real que dispensa o lastro mercantil

O dinheiro com o qual operamos ao longo de quase todo o século XX e início do XXI é a moeda fiduciária nacional. Os pedacinhos de papel coloridos com imagens e números impressos são títulos de dívida, diferem dos títulos negociados em mercado com prazos diversos apenas porque estes nos pagam juros para os mantemos conosco por algum tempo. A credibilidade na moeda dispensa qualquer lastro em ouro ou qualquer outra mercadoria com valor próprio. O que há por trás de uma moeda forte é apenas a força de sua economia – a capacidade interna de gerar riqueza e externa de gerar respeito (da diplomacia às armas).

A moeda nacional é a única com poder legal para cumprir as funções de dinheiro e mesmo que inflação interna ou ameaças especulativas externas possam desvalorizar a moeda nacional apenas um colapso institucional que ameace a existência mesma da nação pode lhe tirar essa prerrogativa. Por fim, a estabilidade do valor da moeda tem pouco a ver com rigidez das regras de emissão de moeda e títulos e muito a ver com a adequação da liquidez conforme as fases do ciclo capitalista. Se há capacidade ociosa e desemprego na economia a moeda pública deve empregá-los para que mais riqueza seja gerada e seu valor seja mantido.

Os registros informacionais contidos no papel remetem a símbolos nacionais. Por isso, frequentemente encontramos desenhados símbolos universais (cifrão e números) e símbolos nacionais fortes – que vão desde paisagens e animais, a heróis nacionais e a lembrança de que todos ali acreditam em algo maior (podendo ser o “In God we trust” do dólar, o “Deus seja louvado” do real, ou o “Moeda do povo” do yuan). O significante numérico, remete às particularidades das coisas – ou melhor dizendo do que está sendo contabilizado (para ser trocado, guardado, apostado) -, e os significantes linguísticos R$ ou E$ remetem ao universal que é a nação a qual aquela moeda é referida. Aqui, de nada importam as coisas, mas as pessoas que mantêm entre si um contrato maior que os meramente econômicos, o de se reconhecerem pertencentes à mesma unidade nacional, sob jugo do mesmo Estado.

A necessidade da presença de uma “relíquia bárbara” (como Keynes chamava o ouro) nos cofres nacionais para que o povo de cada nação acreditasse em suas moedas foi uma convenção política de época; como é hoje uma convenção política acreditar que o “Estado não deve gastar mais que arrecada”. Estas convenções são tão vazias em si e por si como as mensagens acima citadas grafadas nas moedas. Se valem algo é por conta do contexto todo ao seu redor. Do mesmo modo como enfiar uma aliança no dedo é só enfiar uma aliança no dedo, mas de frente ao padre, aos familiares, depois de tanto esforço e tempo empregado na construção de um relacionamento, de tanto trabalho e riqueza mobilizado para a festa, é de se esperar que a aliança signifique uma promessa, e que ela seja cumprida!

Carregar valores no tempo foi desde sempre o papel principal do dinheiro, ainda que apenas ao longo dos milênios a questão de ao que o valor se refere tenha se estabelecendo de modo mais racional e universal. Mas no passado a produção de riqueza futura jamais seria muito diferente da passada. No capitalismo, a coisa é diferente, e então as moedas, e suas taxas de juros, são usadas para trazerem informação sobre o futuro, informação esta com usos variados, incluindo o de municiar apostas. Isso é complicado de explicar, mas é algo como se as moedas espelhassem, e servissem de critério de comparação, para as avaliações que se fazem no presente de quanto vai haver de outras tantas riquezas no futuro[v]. Segurar o dinheiro, em vez de fazê-lo circular, passa a valer algo, ou conferir um prêmio, isso é básico para a especulação.

Além desse potencial especulativo que circula em torno de todas as moedas roubando-as da circulação, fazê-las circular não é algo tão fácil. Não se cria uma moeda e se lhe confere credibilidade do nada! E não adianta que ela seja crível e desejável num seleto grupo de apoiadores. Isso acontece frequentemente também com as moedas sociais, que podem até circular bastante numa região limitada (um bairro, uma favela, ou município até) mas se não ganham escala jamais chegam e não podem também alavancar, a partir de um certo limite, os negócios locais. Mas o mais interessante da experiência do Bitcoin ficou, e cresceu… Trata-se da tecnologia *blockchain* que substitui a checagem pessoal presencial das transações efetuadas com base na informação impressa no dinheiro por uma checagem automática. Como é isso?

Bem, algo nada a ver com verificação de cheques, com autorização de débitos e créditos com assinatura do caixa, ou de transferências de valores com o aval do gerente. E sequer se trata dessas checagens por meio de máquinas, operação por operação. Não se trata aqui de nos assegurarmos do que exatamente a primeira criança disse a segunda na brincadeira do telefone sem fio. Na tecnologia blockchain quando a informação segue adiante ela carrega já um "carimbo", uma assinatura, que garante a exatidão.

As moedas digitais privadas, o que pode a tecnologia sem política

A moeda de papel já é algo um tanto "virtual", pois a informação que está escrita e desenhada remete à ordem do simbólico que por sua vez ilustra que há por trás do dinheiro toda uma institucionalidade que impõe regras para sua produção e circulação. Mas o que ocorre quando, lá pelas tantas na história da humanidade, toda a informação pode ser digitalizada (passada para linguagem de máquina, 0 e 1, presença e ausência de corrente elétrica)? O que acontece é que a informação sobre a combinação social que está por trás do dinheiro não precisa mais de um papel para ser impressa, de um desenho que apele à cultura do povo, e de um carimbo e uma marca d'água sofisticadas que atestem o poder dos órgãos de controle do Estado Nacional. Ou seja, a informação será passada apenas por registros numéricos *on line*.

Na corrida pela digitalização de todo tipo de informação – seja ligada a produções nossas (linguagem falada e escrita, matemática, música, imagens, etc), seja ligada à natureza onde o que fazemos é apenas buscar traduzi-las (o sequenciamento genético dos seres, a composição química dos elementos, etc) – Estado e Mercados, mais uma vez, convivem, cooperam, mas também disputam. No caso da informação econômica das transações monetárias, os agentes privados deram um enorme salto quando criaram o Bitcoin (BTC), uma moeda completamente digital que circulava num ambiente próprio fora da jurisdição dos Bancos Centrais. O BTC é assim, como as moedas antigas, um sistema inteiro.

Nesse caso, o sistema é composto do registro de uma operação primária que caminha na rede de computadores interligados (que rodam o mesmo programa) que ao passarem adiante as informações (os pacotes ou *blocs)* por cada elo da cadeia (daí o *chain*) vão certificando-as. Os vários computadores dessa rede descentralizada vão armazenando estas informações no espaço virtual chamado *banco de dados distribuídos*, ao mesmo tempo que vão certificando a veracidade dos registros através de uma assinatura criptografada, chamada *hash*.

A tecnologia que descreve esse caminho da informação amarrada em pacotes e indo adiante numa cadeia sendo certificada pelos nós da rede é chamada de *blockchain*. O poder operacional das máquinas confere a seus donos um papel mais significativo nessa checagem descentralizada e premia seus operadores com novas unidades informacionais, ou *tokens,* que são a própria moeda da rede. Quando se diz que o BTC é *minerado*, o que se está dizendo é que quem fica trabalhando nesse processo de registro/checagem das transações vai recebendo em troca unidades transacionais. Daí muita gente sem recursos ter dedicado a sua pobre maquininha a esse esforço, enquanto outros com muitos recursos construíram prédios inteiros com computadores para fazê-lo.

Os criadores (mais provável que um criador) do BTC, pensaram que sua moeda estaria fora dos vis interesses políticos (há que lembrar que o *White Paper* do BTC foi lançado no ano do estouro da bolha americana em 2008) porque transitava por um sistema apartado do sistema Banco Central/bancos privados. Contudo, parecem ter ignorado que, se tudo desse certo – o BTC não sendo uma moeda oficial não mercantil sem valor ela mesma –, seria uma moeda mercadoria, cotada na moeda oficial hegemônica, mais cara ou mais barata conforme sua demanda, e demandada mais por motivos especulativos que transacionais. Ignoraram o óbvio, que qualquer mercadoria no capitalismo pode funcionar como moeda.

Cigarros podem ser moeda nos presídios, petróleo pode ser moeda nos mercados internacionais, etc. Mas nenhuma mercadoria é absoluta na tarefa de ser o dinheiro ideal, mais estável porque mais escasso, e por isso mais desejável. Já o dinheiro fiduciário que não é mercadoria, que não é retirado da terra com furatrizes, nem dos computadores com matemática avançada (e muita energia elétrica), pode ser estável se quisermos que seja, e melhor ainda quando queremos que ele não seja meramente estável mais adequável. Ao fim e ao cabo o BTC tornou-se uma opção a mais para quem tem riqueza sobrando, e apenas o sonho da vez para quem não a tem.

Mas enquanto o BTC fracassava como moeda, transações nele se limitando a poucos mercados, ora ilegais, ora temporários (como países em crise com suas moedas, e, nesse caso, o BTC era meio que um dólar disfarçado) e se tornava um mero

ativo especulativo, a tecnologia *blockchain* ganhava espaço. Isso ocorre porque ela funciona com um sistema de rastreamento que pode ser usado não só por transações financeiras mas por todo tipo de informação que queremos ver chegar no destinatário e também ser armazenada de forma segura.

N outras moedas digitais privadas foram criadas com adaptações tecnológicas, com menos gasto de energia, com maior participação social na sua elaboração, etc. Uma das mais interessantes é o Ethereum que se apresenta como uma plataforma descentralizada capaz de executar contratos inteligentes – dado que são imutáveis, ou não passíveis de alterações. No principal, o Ethereum é como o BTC um modo de registrar as transações numa espécie de livro aberto, ou planilha pública, dita distribuída, o que não diminui mas aumenta a segurança, pois as informações são garantidas não por pessoas mas por uma assinatura criptografada pela máquina que atestou o registro. O *Ethereum* tem a pretensão de ser como um grande computador passível de ser utilizado por todos e em qualquer parte para registrar em Ether todas as transações que possam ser codificadas.

O que tudo isso significa? Ao meu ver significa que, ao nível mundial, do ponto de vista tecnológico já podemos ter uma moeda para as transações internacionais que não seja a do país hegemônico, que tem vantagens excepcionais por isso. A demanda por essa moeda/registro poderia ser mais facilmente restringida ao seu uso como meio de pagamento, desestimulando seu entesouramento por motivo especulativo. Mas já podíamos ter isso (desde 1944 quando Keynes o propôs em Bretton Woods) muito antes da tecnologia *blockchain*; se não o fizemos foi porque não conseguimos um acordo político para tanto. Seria mais trabalhoso, mais sujeito a falhas? Sim, mas não é porque hoje essa questão técnica esteja superada que o é a questão política.

Internamente aos países ocorre algo similar. Já podemos eliminar os bancos como intermediários, senão das operações de crédito, do sistema de pagamentos. Mas a questão é tanto mais política quanto tecnológica. Tanto assim que é mais provável que os bancos se apropriem dessa tecnologia (para melhorarem a segurança do seus sistemas e reduzirem custos, aumentando lucros) do que nós nos apropriemos delas e os dispensemos. Por suposto, bancos comerciais privados preferem o arranjo em vigor, onde a moeda que eles próprios criam é chancelada pelo Estado. Preferem claro que usemos a sua moeda, tanto que fazem (junto com a mídia e a academia a seus serviços) todo um discurso anti "gastança" dos governos (que colocaria moeda em circulação automaticamente) e anti dívida pública. Nesse caso, a cantilena se dirige a aumentar os juros que o Estado lhes paga, eles que são os maiores compradores dos títulos públicos.

Mas se os poderes privados são fracos – mesmo o de *nerds* brilhantes – frente aos poderes consorciados de grandes empresas e bancos, uma participação mais efetiva das massas organizadas no Estado pode obter mais êxito...

Moedas digitais estatais, ou o que pode a tecnologia com política.

Nos anos recentes a digitalização de informações ganhou não apenas empresas em todos os ramos mas também bancos, e mesmo Bancos Centrais mundo afora. Essa digitalização, no que diz respeito às moedas e bancos, começa por substituir processos em papel (como por exemplo para abrir uma conta), passa pela facilitação de pagamentos usando a internet (por exemplo o Paypal ou o Pix) e chega na criação de crypto moedas privadas (como visto acima) e agora também cripto Estatais.[vi] O ganho econômico (redução de custos) e social (democratização bancária) é evidente.

Como o demonstra a experiência de diversos países africanos onde companhias telefônicas transformaram créditos de ligação em moeda. Ou seja, dado o fácil acesso a telefones celulares e internet as pessoas podiam dispensar o acesso aos bancos para realizar pagamentos, transferências, poupança e empréstimos. Os créditos telefônicos passaram a funcionar como *tokens* carregadores de informação pra lá pra cá com custo irrisório e, ainda assim, bastante seguro. Isso significou, e significa, a possibilidade de monetizar trocas nos recônditos mais atrasados do planeta e fazer o que via de regra a presença do dinheiro faz – estimula o trabalho a produzir riqueza.

Mas uma coisa é usar créditos de telefone, ou tickets de ônibus, ou o que mais a população convencione (incluindo a moeda bancária de papel ou eletrônica), como dinheiro no lugar da moeda nacional – o que só é possível porque todos estes se referem àquela –-, e outra é a moeda nacional mesma passar a ser digital. O que significa isso? Significa o fim da moeda física para todos os usos. Mas significa também a construção de todo um outro sistema – ou ecossistema (pois

envolve diversos “seres” e “ambientes”) onde esta deverá circular. Isso ultrapassa um mero sistema de pagamentos digital, como o Pix por exemplo.

Como sabemos, o Pix não é uma moeda digital mas apenas uma alternativa às formas existentes (doc, ted, boleto, cartão) para fazermos pagamentos e transferências – verdade que tomará o lugar de todas as demais porque é seguro, instantâneo e sem custo. Mas o fato é que a moeda que opera os pagamentos/transferências dentro do sistema Pix é o Real, e a construção desse sistema não precisou operar uma revolução tecnológica ou institucional. Ele não exige um aplicativo ou plataforma especial (cada banco usa os seus próprios apps e caixas eletrônicos) e não usa tecnologia *blockchain*.

Além disso, o Pix é gerido e operado centralizadamente pelo Banco Central, que construiu um Sistema de Pagamentos Instantâneos (SPI) ao qual estão conectados os bancos e outras entidades financeiras. Mesmo que o sistema garanta rastreabilidade plena (segundo o site do Banco Central) esta só o é por uma estrutura centralizada (uma Diretoria dentro do BC) através de uma tecnologia *mensageira* utilizada para integrar diferentes sistemas de diferentes instituições.[vii] Mas então, o que seria e o que poderia uma cripto moeda estatal, ou uma Moeda Digital do Banco Central (CBDC da sigla em inglês)? Seria algo também baseado em tecnologia *blockchain* e de operação descentralizada?

De imediato, o fato é que enquanto os Estados gozarem da confiança da população em geral, e das classes dominantes em particular, as suas moedas (de ouro, papel ou dígitos eletrônicos) serão demandadas para o pagamento dos impostos a estes Estados. Os Estados que criam moeda apenas ao gastar (e a destroem na medida que recolhem os impostos) tornam a população carente de suas moedas, e forçam assim a sua circulação. Que as moedas estatais (e as privadas nelas denominadas) possam faltar à circulação quando agentes de peso (capitalistas cujo gasto é que emprega a massa de trabalhadores) preferem manter sua riqueza em moeda, é algo que pode ser contrabalançado pelo Estado de modo bastante fácil (ainda que exija convencimento político) sem que nenhuma equação matemática complexa precise ser resolvida ao custo de muita energia mental e elétrica.

Isso tem menos a ver com a moeda e mais com a irracionalidade capitalista que pode transformar tudo o que signifique dinheiro em objeto de especulação. Mas, por isso mesmo, a gestão pública da moeda é tão importante, pois só o Estado pode “desencorajar” esse tipo de especulação contra o futuro. Como também pode diminuir a circulação monetária (gastando menos) e desencorajar o gasto privado nas fases de *boom*. A forma eletrônica da moeda não muda nada o princípio geral – os Estados criam moeda ao gastar, e obrigam sua aceitação e circulação ao taxar os cidadãos; nem a necessidade de um órgão central regular a liquidez de tudo o que possa funcionar como dinheiro, visando fazer com que os recursos disponíveis na economia – trabalho, máquinas, capacidade produtiva em geral – não fiquem desocupados.

Mas como seria a gestão da liquidez num mundo de moeda digital? Ou como e quem controlaria a criação dessas moedas? Uma cripto estatal acabaria na prática (ou na lei) com as criptos privadas – sejam elas de instituições não bancárias (do *Bitcoin* à Libra do Facebook), sejam dos bancos já agora se reposicionando a respeito? Bem, os cenários estão todos muito em aberto ainda[viii], mas já sabemos que isso do descontrole total não existe. Mesmo que as cripto privadas alardeiem que, dada a sua natureza descentralizada, ninguém controla a sua criação, bem sabemos que se não for o Estado a controlá-las quem o fará são os grandões privados (afinal os detentores de poder energético, dos conhecimentos tecnológicos, das empresas de exchange, etc não somos todos nós...).

Acho interessante pensar sobre esse controle a partir do que já ocorre hoje com os bancos, afinal eles também gozam de autonomia na criação de moeda privada, mas sempre sob um certo acordo político-institucional. Acordo este que pode variar desde a regulação draconiana (pensemos nos EUA de Roosevelt, das regulações Glass Steagall e outras) até a liberalização geral (dos 80 pra cá, ainda que com algum recuo depois de 2008). Talvez o diferente aqui seja a possibilidade de uma super democratização da criação de moeda (com mais e mais empresas podendo criar seus *tokens* próprios) mas todos referidos – como hoje o é a moeda bancária – à moeda nacional, que é acima de tudo mais um nome a zelar que um pedaço de papel ou um dígito eletrônico.

Essa questão de poder político é tão relevante que talvez toda essa história de criptomoedas não dê em nada, ou melhor, dê em que Estados e bancos peguem o que quiserem (a tecnologia por exemplo) e refaçam seus pactos. Acredito contudo que se o Estado (espaço por excelência da criação de todas as regras) está plenamente a salvo, o mesmo não se pode dizer dos bancos. Estes estão duplamente ameaçados, de um lado pelas empresas não financeiras que hoje operam serviços de pagamento e transferências mas já começam a esbarrar na função crédito.[ix] Por outro lado, a sua função como caixas e

gestores de depósitos é ameaçada também se todos os cidadãos passarem a ter contas digitais nos Bancos Centrais de seus países. O fato é que a facilidade e o baixíssimo custo na obtenção e operação da moeda digital parece colocar em xeque o pacto de poder que vinha funcionando até aqui entre empresas não financeiras (mas que foram se financeirizado ao longo do século passado mas só agora ameaçam o monopólio bancário na criação de moeda), bancos e governos.

Nesse ponto, é interessante pensar na tentativa, frustrada, do Facebook de criar a "sua" própria moeda digital[x] e nas respostas do Estado norte-americano e chinês na sequência. A ideia de Mark Zuckerberg era organizar uma espécie de consórcio de empresas e lançar a Libra uma cripto moeda que pudesse superar as demais criptos e plataformas de pagamentos privadas. Mas, entendeu o poder público norte-americano, também poderia ameaçar a força do dólar, ou pelo menos a engenharia estabelecida entre governo e bancos na sua gestão. Assim é que, três dias depois do anúncio de Zuckerberg, o presidente Trump usou seu canal oficial de comunicação, o Twitter, para mandar um recado – o de que moeda mesmo só o bom e velho dólar.[xi] A reação do governo motivou uma audiência pública com o dono do Facebook no Congresso onde este assegurou que o projeto só seria lançado se e quando o aprovassem os reguladores. Mas Zuckerberg também vaticinou – se a Libra não sair, em breve os americanos estarão usando uma moeda virtual chinesa. Talvez ele já soubesse dos planos chineses, planos que ficaram evidentes no dia seguinte à fala de Zuckerberg, quando Xi Jinping anunciou que a China deveria ser liderança no processo de criação de uma cripto pública que funcionasse "na vida cotidiana das pessoas".

Ao que o BC chinês dá mais detalhes, explicando que o *yuan digital* substituirá toda a base monetária em papel e usará a tecnologia *blockchain* por sua rastreabilidade e confiabilidade. Bem, de fato não sabemos ainda como a tecnologia *blockchain* pode ser adaptada para uma gestão centralizada; mas sabemos que uma coisa é o desaparecimento dos bancos privados (que provavelmente não desaparecerão mas se revinventarão, ou se fundirão plenamente às empresas) e outra o desaparecimento do Banco Central, ou da moeda estatal como instituição mais importante do Estado Nacional. Sendo assim, só nos resta pensar que a política vai desenvolver a tecnologia que lhe convém.

Mas justo no campo da política há algo importante em jogo aqui, pois se os Estados devem lançar suas Moedas Digitais dos Bancos Centrais (ou CDBC na sigla em inglês para *Central Bank Digital Currency*) para manter essa importante instituição pública nas mãos do público, é verdade também que "será quase impossível", como diz Izabella Kaminska, que estas moedas possam ser lançadas fora de "um sistema nacional abrangente de gerenciamento de identidade digital". Ou seja, é bem provável que estas moedas precisem estar vinculadas a contas pessoais e que todos os dados dos indivíduos acabem por ficar à plena disposição de um organismo central.[xii] Por suposto isso é perigoso, como também o é a propriedade privada e secreta de nossas informações por empresas privadas.

Dá pra ter um moeda digital baseada em tecnologia blockchain estatal e centralizada e ela ser mais democrática que a moeda fiduciária atual e as criptos privadas?

Acredito que sim. Se pensarmos que não é verdade que as cripto privadas funcionem sem nenhum grau de centralização, e que não é verdade que o Estado centralize totalmente a gestão da moeda fiduciária atual (uma vez que confere algum, por vezes grande, poder aos bancos), podemos pensar que arranjos políticos estão sempre em jogo e a tecnologia pode ser pensada para se adequar. Mas vejamos um pouco mais de perto porque acredito em alguma centralização na gestão das cripto privadas, e isso sem entrar nos aspectos ligados à compra e venda destas e todo o universo dos corretores (que de início eram um tanto independentes mas foram se tornando cada vez mais ligados ao sistema financeiro tradicional, ele mesmo bastante concentrado e centralizado). A intenção aqui é focar apenas na questão tecnológica e ver se é impossível mesmo haver centralização de poder na, por definição, descentralizada *blockchain*.

Como já comentado, a tecnologia *blockchain* tem entre seus aspectos fundantes a ideia de uma checagem das operações descentralizada, ou distribuída na rede de usuários, feita por diferentes máquinas de diferentes proprietários. Isso porque, como vimos, ela se dá por um processo em que, conforme a informação anda, uma assinatura criptografada (o tal *hash*) a

vai acompanhando como um rabo que não para de crescer. Isso significa que se alguém manipula uma transação esse rabo vai aparecer diferente em diferentes máquinas indicando não apenas que algo está errado mas a partir de quando o algo errado apareceu. Uma fraude só seria possível se se pudesse manipular todos os "valores de *hash*" que são produzidos automaticamente e sem qualquer interação humana. Isso não significa que as fraudes não sejam possíveis, mas são pouco prováveis na medida em que extremamente caras[xiii]. Mas a questão central é, a capacidade de checagem é realmente a mesma entre todos os participantes da rede?

São duas as principais maneiras de checagem, ou protocolos de busca de consenso, que operam dentro do blockchain, conhecidos também como algoritmos de prova.[xiv] O primeiro e original protocolo é o da "prova de trabalho", ou *proof of work* (também conhecido como PoW). O PoW é a solução mais antiga e generalizada (usada pelo Bitcoin, Etherium e a maioria das cripto) e é a base mesma da tecnologia blockchain – os checadores são os mineradores que ao resolverem as equações matemáticas correspondentes às transações criptografadas numa competição aberta e generalizada são recompensados com o recebimento da moeda interna à rede. Não há uma determinação prévia de quem está capacitado para realizar as provas. O problema evidente desse protocolo é o custo energético que cresce com o crescimento do número de transações e a necessidade de resolver equações cada vez mais complexas. Por suposto, quem tem maior capacidade computacional e disponibilidade de energia tem maior chance de minerar com sucesso, o que significa que há aí alguma centralização de poder.

O segundo protocolo que foi sendo desenvolvido para diminuir o tempo e o custo dessa checagem é o protocolo chamado de "prova de participação" (*proof of stake*, na sigla PoS). Neste, há uma determinação prévia de quem está capacitado a realizar as provas que é a participação na rede. De fato, a seleção é aleatória, mas leva em consideração a participação do usuário na rede (ou seja, a quantidade da cripto que ele dispõe). Muitos defensores da PoS dizem que ela, além de mais segura e eficiente energeticamente, apresenta também menores riscos de centralização; contudo, é evidente que a centralização é um pressuposto mesmo do protocolo e não há um limite para a quantidade de operações que um único validador pode realizar. Afinal, como diz a pesquisadora Catherine Mulligan, "você está selecionando apenas validadores que têm mais dinheiro".[xv]

Não disponho do conhecimento técnico adequado para ter uma opinião sobre qual sistema comporta maiores riscos de centralização, mas creio poder derivar dessa diversidade de sistemas de checagem nas cripto privadas descentralizadas que, se em ambos há possibilidade de centralização (que premia com poder de criar/obter moeda), uma cripto estatal, a princípio centralizadora da emissão e checagem, pode dividir com a sociedade essa tarefa e a premiar com moeda, não?!

Do mesmo modo imagino que se em ambos os mecanismos de prova há um incentivo econômico para os checadores – aqueles que vão ser capazes de adicionar um bloco contendo sua assinatura (hash) – que competem uns com outros, e não necessariamente em igualdade de condições, isto também tem algum paralelo com o sistema vigente da moeda fiduciária estatal e os incentivos dados aos bancos privados para cogerirem o sistema. Como explicam os entendidos, a "prova de participação envolve uma competição para ver qual novo bloco tem mais criptomoedas apostadas a seu favor, a prova de trabalho envolve uma competição para ver qual novo bloco tem mais trabalho computacional realizado a seu favor"[xvi].

Pois então, não há também um incentivo econômico aos bancos que participam igualmente da criação de moeda e checagem de transações nas moedas nacionais? E os bancos também não competem entre si, e não sem alguma concentração, e têm um peso maior na checagem como na criação de moeda? Desta reflexão extraio mais uma vez que a tecnologia pode ser adequada, e a política é quem orienta a adequação.

Por último, um comentário sobre as criptos que não visam ser plataformas criadoras de moedas mas ambientes de realização/registro de contratos, onde quaisquer moedas possam operar. Este é o caso do *Ethereum*, cuja ambição é desde sua criação em 2015 ser "o computador mundial", ou o único livro-razão a conter todas as informações referentes a todos os contratos. A sua plataforma também é descentralizada e usa a tecnologia *blockchain*, mas em vez de registrar as transações monetárias mesmas, o que se registra é a mudança de propriedade.

Se no *Bitcoin* os blocos carregam informações de transações (que são checadas por inúmeros computadores que assinam criptograficamente em novos blocos informativos, etc), no *Ethereum* as informações relevantes são variadas e mais complexas. Diz-se que essa plataforma cria uma "interface padrão" para rodar diferentes tipos de *tokens* – sendo *tokens*

"unidades de valor que organizações ou projetos baseados em *blockchain* desenvolvem em cima de redes *blockchain* existentes"[xvii]. Mas todos estes *tokens,* ao fim e ao cabo, carregam uma informação que permite a mudança de titularidade/propriedade de ativos; o que os nós verificadores (os mineradores) na rede *Etherium* fazem é verificar se tudo foi feito corretamente nesta troca de ativos em conformidade com os contratos.

"Os pares não precisam consultar bancos de dados externos; eles não precisam seguir protocolos no topo do Ethereum para combinar valores ou trilhar transações. Eles só precisam verificar o estado, como eles fazem com qualquer outra transação padrão. É por isso que a integração do token ERC [20 em carteiras é fácil e perfeita]".[xviii] [xix]

Este uso da tecnologia *blockchain*, dos "contratos inteligentes" como veio a ser chamado, nos interessa aqui porque sua flexibilidade é um dado do programa, feito para receber sempre novos *tokens* e fazê-los dialogar com a plataforma já operante. Me parece em linha com a operação de uma moeda digital estatal, que poderia operar como gestora central de um grande livro-razão que também é distribuído, consultado, mexido (toda vez que uma troca/contrato for realizada) mas a moeda em si continua uma criação exclusiva sua. Afinal, a moeda é uma instituição social, criada pelo Estado em conformidade com objetivos de Estado (aqui e ali atrapalhados pelos objetivos egoístas dos mercados), e por isso jamais poderia ser algo criado por um algoritmo matemático com o objetivo equivocado de ser escasso (porque, afinal, para esse raciocínio esquiso-liberal, os homens não são confiáveis, ainda mais quando muitos são ouvidos!).

A moeda não deve ser escassa ou difícil em algumas circunstâncias (economia funcionando longe do pleno emprego dos recursos de trabalho e capital disponíveis) ainda que o deva ser em outras (indisponibilidade de recursos); saber reconhecê-las é fundamental, para depois saber gerir a liquidez em ambos os momentos. Mas essa moeda poderia operar contratos inteligentes em nível nacional, de maneira mais rápida, segura, e, em última instância, democrática.

***Glaucia Campregher** *é professora de economia na Universidade Federal da Bahia (UFBA).*

Notas

---

[i] As pesquisas de historiadores, arqueólogos e antropólogos, mostram que as primeiras formas de dinheiro nasceram dentro das comunidades mais que em suas franjas (onde uma comunidade se relaciona com outra) e por isso eram mais ligadas aos registros de dívida que a algo comercializado. As provas mais cabais remetem à civilização Suméria em torno de 3500 a.C. A prata física era utilizada, mas como unidade a qual se conferia um equivalente em produto (um "siclo de prata equivalia a um *bushel* de cevada") e seu valor não emergia de transações comerciais entre os sumérios todos em livres mercados, mas da necessidade da burocracia (sacerdotes, oficiais, administradores de templos e palácios) de "rastrear os recursos e transferir itens entre departamentos". Essa prata não era cunhada e pouco circulava, sendo a maioria das transações meramente registradas, e canceladas.

[ii] De fato, moeda e produção estão tão intimamente ligados no capitalismo que Keynes o chamava "economia monetária da produção", dado que o fundamental do sistema é a prerrogativa dos capitalistas de decidirem onde vão colocar sua riqueza – se irão preferir a liquidez do dinheiro, abrir mão desta por um ganho (juro) financeiro ou investir produtivamente (na expectativa de um lucro).

[iii] Esse raciocínio cola na população que pensa o Estado e os políticos como a serviço de si mesmos, dados a desviar para si um dinheiro que é dela (enquanto que dela é o trabalho que o dinheiro faz movimentar), ou a criar um dinheiro/dívida que empobrecerá as pessoas no futuro. Igualmente não imaginam que os bancos também criam dinheiro do nada. E, nesse caso, a busca da vantagem privada é mesmo a lógica e não um desvio. Bancos criam dinheiro nas contas a quem concedem crédito buscando lucros e o enfrentamento da concorrência. Isso significa que tendem a parir mais dinheiro quanto mais os outros parem e menos quanto menos os demais. Ou seja, são cuidadosos demais em dar crédito quando a economia mais precisa e descuidados demais quando ela está por demais aquecida. Ainda hoje, por mais que o dinheiro de papel circule cada vez menos, a população entende que empréstimos vêm de depósitos; que, quando um banco empresta demais e seus clientes o descobrem pode haver uma corrida bancária e que se caminhões de dinheiro não aparecerem rapidamente todos vão quebrar. Não desconfiam que na época das moedas sinaizinhos elétricos as reservas dos bancos podem ser mobilizadas

de um banco para outro em minutos. Desse modo, estão longe de entender também que grande parte da dívida pública objetiva justamente regular a liquidez da economia no sentido contrário ao do ciclo.

[iv] Uma explicação bastante didática enocntra-se aqui – https://blog.nubank.com.br/o-que-e-blockchain/

[v] O que se faz comparando as taxas de juros do dinheiro (algo sobre o que as autoridades monetárias têm o poder de definir, ainda que frequentemente abram mão de exercê-lo) com as taxas de juros que todos os bens possuem "em termos de si mesmos" (como diria Keynes no capítulo 17 de sua Teoria Geral), o que seria algo como se pudéssemos medir quantos chinelos faremos daqui há 5 anos com os chinelos que fazemos hoje. Ou seja, supondo que faremos mais desenvolvimentos tecnológicos e tornaremos o trabalho na produção de chinelos mais produtivo, podemos dizer que haveria uma taxa positiva aí, se a produtividade dobrar, ela seria 100%.

[vi] Balanço sobre as várias experiências a respeito do site moneytimes.com.br indica que dez países já lançaram sua moeda digital: Bahamas, Antígua e Barbuda, Granada, Santa Lúcia, São Cristóvão e Névis, Monteserrat, São Vicente e Granadinas, República Dominicana, Venezuela e Nigéria. Bahamas lançou o "Sand Dollar", versão digital do dólar bahamense (BSD) em outubro de 2020. Na fase "teste piloto", encontram-se 14 países, espalhados pela maioria dos continentes: Anguila, Jamaica, África do Sul, Arábia Saudita, Emirados Árabes Unidos, Ucrânia, Suécia, Lituânia, China, Hong Kong, Coreia do Sul, Tailândia, Cingapura e Malásia. A China tendo se destacado em 2021 com o yuan digital (ou "e-CNY"). Em agosto de 21, a capital Pequim havia integrado a moeda digital totalmente no sistema de pagamentos do metrô da cidade, e em novembro a quantidade de cidadãos chineses que aderiram ao yuan digital em quatro meses aumentou mais de seis vezes. Estima-se que hoje mais de 140 milhões de chineses (10% da população) já usem e-CNY. No grupo dos países que estão desenvolvendo projetos estão: Canadá, Brasil, Haiti, Ilhas Maurício, Bahrein, Austrália, Palau, Camboja, Japão, Rússia, Turquia, Líbano, Israel, Suíça e a União Europeia, com o euro digital. Segundo a Agência Senado, o Banco Central planeja lançar o real digital até 2024, mas a primeira versão da moeda poderá ser lançada no ano que vem.

[vii] Vide a respeito diversas notas no site do BCB, por exemplo https://www.bcb.gov.br/estabilidadefinanceira/pix. Trata-se, aliás, da mesma tecnologia usada hoje no sistema de pagamentos internacionais SWIFT, do qual os bancos russos foram banidos recentemente. Banimento é algo que só acontece quando há centralização do controle.

[viii] Vide o estudo "The rise of digital money"do FMI. In https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097

[ix] Como as Sociedades de Crédito Direto (SCDs) autorizadas pelo Banco Central do Brasil em 2013. Estas são empresas – em geral startups que cresceram rapidamente – que não são autorizadas a se tornarem financeiras, e, por isso, não podem captar recursos de terceiros, mas podem usar os seus próprios para emprestar através de suas plataformas digitais.

[x]As aspas se justificam porque o projeto lançado por Zuckerberg propunha ser a Libra uma moeda de um conjunto de empresas americanas organizadas na Libra Association. Aqui um bom resumo, https://techcrunch.com/2019/06/18/facebook-libra/

[xi] Conteúdo do tweet de Trump: *"I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behaviour, including drug trade and other illegal activity... Similarly, Facebook Libra's 'virtual currency' will have little standing or dependability. If Facebook and other companies want to become a bank, they must seek a new Banking Charter and become subject to all Banking Regulations, just like other Banks, both National... and International. We have only one real currency in the USA, and it is stronger than ever, both dependable and reliable. It is by far the most dominant currency anywhere in the World, and it will always stay that way. It is called the United States Dollar!"*

[xii] Em matéria do Financial Times aqui disponível. https://www.ft.com/content/88f47c48-97fe-4df3-854e-0d404a3a5f9a

[xiii] Embora muitos analistas considerem apenas hipotéticamente tais ataques – que resulta da ação de um grupo de mineradores que controlam mais de 50% de poder computacional/responsabilidade pela checagem – esse tipo de ataque já aconteceu. Segundo, Leonardo Kovacs atualmente esse risco é bem baixo "pois as redes de criptomoedas tem alcançado

números gigantescos de usuários, principalmente o *bitcoin*. Porém, a possibilidade nunca é zero. A redução de mineradores é uma característica verídica, logo após os movimentos de *halving* da rede *bitcoin*, o que aumenta a possibilidade de ocorrer o ataque, mesmo que seja pequena. Embora seja muito difícil alguém obter mais poder computacional do que o resto da rede *bitcoin*, não podemos dizer o mesmo se tratando de criptomoedas menores. Quando comparadas às principais, as menores têm pouco poder computacional protegendo suas *blockchains*. A situação poderia possibilitar um ataque de 51% (como já foram registrados). Alguns exemplos de vítimas dessa modalidade de ataque incluem: *Monacoin*, *Bitcoin Gold* e *ZenCash*." In https://tecnoblog.net/responde/o-que-e-o-ataque-51-em-criptomoedas/

[xiv] Uma boa apresentação e comparação de ambos os sistemas está disponível aqui – https://kriptobr.com/o-que-e-proof-of-stake/

[xv] https://www.businessinsider.com/personal-finance/proof-of-stake-vs-proof-of-work

[xvi] Idem

[xvii] https://webitcoin.com.br/por-que-o-protocolo-erc20-do-ethereum-e-base-da-maioria-das-ico-out-21/

[xviii] Idem

[xix] Para maiores aprofndamentos sobre a ECR20, ver https://academy.bit2me.com/pt/que-es-erc-20-token/#:~:text=Un%20token%20O%20ERC%2D20,de%20cria%C3%A7%C3%A3o%20para%20os%20desenvolvedores.