Moeda Eletrônica do Banco Central: uma Introdução

Central Bank Digital Currency: an Introduction

Victor Augusto de Almeida Oliveira[a*]
Jefferson Donizeti Pereira Bertolai[a]

Resumo: O assunto criptomoedas tem recebido bastante atenção por parte da mídia, de organismos internacionais, de bancos centrais e do meio acadêmico. Em particular, tem sido discutido se é de interesse dos bancos centrais a emissão de uma criptomoeda ou de uma moeda digital soberana. A diferença entre essas duas formas de acesso ao balanço do banco central é a forma de transmissão de unidades monetárias entre os usuários. Enquanto a criptomoeda soberana possui transmissão por meio de um sistema descentralizado, a moeda digital soberana é transmitida em um sistema centralizado. Este trabalho busca mostrar que o principal ponto que distingue os sistemas centralizado e descentralizado é a necessidade de monitoramento dos intermediários. Ademais, conclui-se que o sistema permissionado pode ser considerado centralizado pela necessidade de monitoramento dos agentes. Por fim, este trabalho propõe-se a discorrer sobre outras questões que envolvem a emissão de uma moeda eletrônica do banco central, em particular sobre os benefícios que podem advir dessa inovação e sobre os efeitos que pode causar ao setor bancário.

Palavras-chave: moeda eletrônica do banco central; criptomoeda soberana; moeda digital soberana; monitoramento.

Abstract: Cryptocurrencies have received a lot of attention by media, international organizations, Central Banks and academics. It has been argued if it would be of interest of Central Banks to issue a cryptocurrency or an electronic money. The difference between these two ways to access the Central Bank balance sheet is the transmission of units from an user to another. While the Central Bank cryptocurrency changes hands through a decentralized system, the Central Bank electronic money is transferred through a centralized system. In this dissertation, we show that the main difference between centralized and decentralized systems is the need to monitor the intermediaries' actions. We conclude that the permissioned system may be regarded as a centralized system because it requires monitoring the intermediaries. We also study other questions related to the creation of a Central Bank digital currency (CBDC). Specially, we study the benefits that the issuance of a CBDC might have and the effects it may cause to the banking sector.

a Universidade de São Paulo (USP), Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto (FEARP), Departamento de Economia. Ribeirão Preto, São Paulo, Brasil.

* O autor agradece o apoio do CNPq no desenvolvimento deste trabalho, por meio da concessão de bolsa de mestrado.

Keywords: Central Bank digital currency; Central Bank cryptocurrency; Central Bank electronic money; Monitoring.

JEL Classification: E42

1 Introdução

Nota-se, atualmente, um crescente interesse com relação ao tópico moedas digitais descentralizadas[1] (criptomoedas), muito provavelmente motivado pela espetacular valorização, nos últimos dois anos,[2] da bitcoin, a primeira, mais conhecida e mais utilizada moeda digital descentralizada.

O assunto criptomoedas ganhou força em 2008 com a proposição e criação, no ano seguinte, da bitcoin. Em particular, considera-se a importância do sistema descentralizado de registros e legitimação de transações no qual ela é baseada. Esse sistema, denominado *blockchain*, é apontado[3] como a inovação fundamental da moeda digital descentralizada Bitcoin. Argumenta-se que o conceito *blockchain* possui potencial de aplicação muito mais abrangente que o gerenciamento de moedas digitais.

Embora o setor privado seja, atualmente, o principal centro desenvolvedor de tecnologias que utilizam a *blockchain*, esse tema tem sido objeto de vários estudos promovidos por bancos centrais. Como apontam Ketterer e Andrade (2016), países tão diversos como Islândia, Suíça, Equador, Inglaterra, China, Austrália, Canadá e Colômbia estão, de forma ativa, empreendendo esforços para antecipar os possíveis riscos e benefícios (e a viabilidade) da implementação de moedas eletrônicas controladas (emitidas) pelos respectivos bancos centrais.

Uma importante implicação da adoção de moedas digitais (quer sejam emitidas de forma privada, como a bitcoin, quer sejam emitidas por um banco central) é sua repercussão sobre o funcionamento do setor bancário. Por exemplo, ao enfrentar a concorrência do serviço de pagamentos provido por tais moedas, o sistema bancário teria mais dificuldade para atrair depositantes. No caso limite em que precisariam financiar seus empréstimos (ativos de maturação alta) sem a captação via depósitos à vista (passivo de maturação baixa), os bancos seriam incapazes de prover liquidez aos indivíduos por meio de seu papel de transformação de maturidade (reserva fracionária). Como consequência imediata, o sistema

1 Stevens (2017) define moeda digital como uma forma de dinheiro eletrônico gerenciada por um sistema de registros e pagamentos distribuído/descentralizado. Dinheiro eletrônico é o valor monetário mantido em um dispositivo eletrônico, o qual pode ser usado para realizar pagamentos. A fim de contrapor o conceito de moeda digital descentralizada ao conceito de moeda digital centralizada, Halaburda e Sarvary (2016) denominam o primeiro conceito como criptomoeda.

2 Para mais informações sobre cotação, consultar www.blockchain.info.

3 Por exemplo, ver Ali *et al*. (2014).

bancário seria estável, uma vez que o papel de transformação de maturidade está intrinsecamente relacionado à existência de corrida bancária, conforme estabelecido por Diamond e Dybvig (1983).

Para entender como a *blockchain* e outras tecnologias relacionadas podem afetar o sistema bancário, faz-se necessário primeiro estudar o funcionamento de tais tecnologias. Do ponto de vista da Teoria Monetária, Bertolai e Oliveira (2020, p. 228) concluem que as criptomoedas possuem como sua maior inovação "[...] a viabilização da geração de evidência confiável e flexível de produção de bens/serviços sem o uso de monitoramento das ações dos responsáveis por sua emissão e gerenciamento [...]". Considerando-se a Bitcoin em particular, é por meio da tecnologia *blockchain* e do conceito de *proof-of-work* que se possibilita a legitimação de transferências de saldos monetários eletrônicos sem a necessidade de um intermediário financeiro. A seção 2 deste artigo discute os possíveis tipos de gerenciamento de moeda digital: centralizado, descentralizado e permissionado. Dessa discussão, será extraído o importante conceito do que é uma criptomoeda.

Bertolai e Oliveira (2020) não descartam, no entanto, que o monitoramento pode ter um papel importante em parte do gerenciamento de uma criptomoeda, como no caso da política monetária. Um exemplo seria a possibilidade de que o setor público, na figura de um banco central, criasse uma moeda digital de tal forma que todos os depósitos seriam feitos diretamente no banco central, com registro por meio de uma *blockchain* criada pela instituição. A seção 2 discute os conceitos de moeda eletrônica do banco central (MEBC), criptomoeda soberana e moeda digital soberana, além da motivação para emissão de uma MEBC e as vantagens e desvantagens de cada tipo de gerenciamento de moeda digital.

Com a criação de uma MEBC, a opção de manter dinheiro nos bancos a título de depósito à vista passa a ser menos atraente, pois a opção ofertada pelo banco central é, teoricamente, mais segura (por exemplo, é livre da possibilidade de corridas bancárias por não haver transformação de maturidade). Isso dificultaria a atração de depósitos à vista pelos bancos. A seção 3 discute um modelo simples que analisa os efeitos que a emissão de uma MEBC pode ter sobre o sistema bancário. Após essa seção, este trabalho é concluído com as considerações finais.

2 Moedas Digitais

A criação das criptomoedas teve o objetivo inicial de possibilitar a troca de valores monetários sem demandar confiança entre as partes envolvidas e, ainda mais, sem que os indivíduos necessitem confiar em um intermediário para executar a troca. A primeira criptomoeda que obteve sucesso na solução do problema do gasto duplo teve origem no artigo de Nakamoto (2008), que a batizou bitcoin, há cerca de uma década. Até o momento, nenhuma outra criptomoeda atingiu

a popularidade nem o valor da Bitcoin, embora existam criptomoedas com propriedades "melhores".[4] Por isso, e assim como o fazem Bertolai e Oliveira (2020), considera-se a bitcoin como representante das criptomoedas. Na seção 2.1, será mostrado um breve resumo da história das criptomoedas. Na seção 2.2, serão discutidos os aspectos técnicos do funcionamento dos sistemas centralizado, descentralizado e permissionado de gerenciamento de moeda digital. Com relação ao sistema descentralizado, a bitcoin será utilizada para a explicação de seu funcionamento. Por fim, a seção é concluída com a discussão da inovação monetária fundamental das criptomoedas.

2.1 Dos Experimentos dos anos 1980 e 1990 à Moeda Eletrônica do Banco Central

David Chaum, ainda no começo da década de 1980, fez a primeira proposta séria de um "dinheiro digital" que mantinha o anonimato nas transações e evitava o gasto duplo, embora em um processo centralizado de verificação.[5] O artifício usado para tanto é chamado *blind signature*, que funciona da seguinte maneira: no ato de emissão do dinheiro digital, o emissor delega ao usuário o poder de escolher o número de série que sua nota possuirá; em seguida, o emissor assina a autorização para a emissão da moeda sem conhecer o número que foi escolhido; idealmente, o número de série escolhido por quem receberá a moeda digital deve ser grande e aleatório, de modo que ele não tenha sido escolhido anteriormente por outro usuário e que o resgate seja possível; o emissor, de forma centralizada, mantém o controle sobre os números de série que já foram resgatados; o resgate de um dado número de série pode ser feito somente uma vez de forma a evitar o gasto duplo.

No final da década, em conjunto com Amos Fiat e Moni Naor, David Chaum fez uma proposta para um "dinheiro digital *off-line*". A ideia é, ao invés de prevenir o gasto duplo, investir em sua detecção, como ocorre comumente com muitos meios de pagamentos (por exemplo, cheques). De forma simples, o truque é que cada indivíduo que deseja receber uma moeda emitida – por exemplo, Maria – codifica sua identidade de uma maneira que apenas ela própria conseguiria decodificá-la. Quando essa moeda fosse transmitida, o destinatário solicitaria que Maria decodificasse um subconjunto aleatório de sua identidade. Caso Maria transmitisse a mesma moeda para duas pessoas (gasto duplo) e elas fossem resgatar a moeda com o emissor, os dois pedaços da identidade de Maria que foram decodificados seriam, com grande probabilidade, suficientes para revelar sua identidade, permitindo que Maria fosse cobrada pelo gasto duplo. A cobrança poderia ocorrer,

4 Como exemplo, pode-se citar a litecoin, que conta com confirmações mais rápidas e com um mecanismo de escolha de blocos diferente, a ethereum, que permite contratos inteligentes mais sofisticados, e a dash e a monero, que oferecem maior anonimidade.

5 Esta seção baseia-se, em grande parte, em Narayanan *et al*. (2016).

inclusive, judicialmente se esse tipo de gasto duplo fosse reconhecido como crime por lei (assim como pessoas que emitem cheques sem fundos podem ser cobradas pelos credores).

Com essas ideias, Chaum abriu a empresa DigiCash, cuja moeda emitida era chamada ecash. O sistema de Chaum foi implementado por alguns bancos e tinha como característica o fato de que os consumidores (remetentes) eram anônimos para os bancos, enquanto os vendedores (destinatários da moeda) não, o que torna a rede indesejável para trocas *peer-to-peer* (em que tanto o remetente quanto o destinatário gostariam de se manter anônimos). O ecash era, portanto, extremamente dependente da adoção por parte de vendedores e bancos, o que acabou não acontecendo, levando a DigiCash à falência.

Na taxonomia de Bech e Garratt (2017), que será apresentada detalhadamente na seção 3.1, a ecash possuiria a mesma classificação que depósitos bancários, pois ambas as moedas digitais são emitidas de forma eletrônica, universalmente acessíveis, não são emitidas por um banco central e não possuem como característica a transferência *peer-to-peer* (descentralizada). A centralização dos primeiros experimentos de moedas digitais foi um dos fatores que contribuíram para seus fracassos.

O valor de uma moeda emitida pela DigiCash era determinado pelo pagamento da quantia ao banco associado. Algumas outras propostas pretendiam dar valor a suas moedas ao formar reservas, como no caso da e-Gold, que emitia dinheiro digital baseado na quantia de ouro armazenado, e da Digigold, que possuía apenas reservas parciais. Por ter sua emissão atrelada a uma determinada *commodity*, o valor da moeda acabava também a ela atrelado.

Nota-se que, para que a moeda tenha valor, é necessário que seja escassa.[6] Uma maneira de criar escassez artificialmente é impor a resolução de um *puzzle* para que a moeda seja criada, como é feito no caso da bitcoin. A ideia de impor o custo da resolução de um desafio para a criação de identidades, na verdade, teve origem como uma medida para evitar *spams* – cada *e-mail* enviado necessitaria também carregar consigo a resolução de seu *puzzle*, o que não causaria problemas para usuários comuns, apenas para *spammers*. Utilizando uma ideia similar a essa, Adam Back propôs o sistema Hashcash em 1997. Essa ideia foi utilizada de forma similar na *proof-of-work* do sistema bitcoin, como será mostrado na seção 2.2.2.

A cadeia de blocos que se autorreferencia formando uma ordenação parcial das transações é outro aspecto relevante da bitcoin. Essa ideia surgiu em 1991, com o intuito de manter a ordenação da existência de documentos digitais por meio da marcação do horário em que o servidor recebeu o pedido de cadastramento do documento. Cada documento cadastrado possuía uma indicação de seu antecessor. Posteriormente, surgiu a ideia de agrupar mais de um documento em

6 Para mais detalhes, ver Cavalcanti e Wallace (1999b).

um bloco, cada um apontando para o bloco antecessor. Isso diminui o número de checagens necessárias para verificar se um documento aparece em um ponto particular da cadeia de blocos.

Foram propostas duas ideias de criptomoedas mais simples que a bitcoin utilizando-se as ideias de imposição de um *puzzle* para regular a criação de moedas e de uma cadeia de blocos para seguramente marcar os horários das transações: a b-money, proposta por Wei Dai em 1998, e a bitgold, proposta por Nick Szabo, que começou a fazer postagens sobre sua ideia em 2005.

Uma diferença entre essas propostas e a bitcoin é que a resolução dos *puzzles* estava diretamente ligada à criação das moedas (a resolução do desafio em si é uma unidade de moeda), enquanto, na bitcoin, a ligação é apenas indireta (a resolução do desafio dá o direito de incluir um bloco na cadeia contendo uma transação que cria novas moedas e as aloca para o criador do bloco). Outra diferença é que essas propostas usavam as marcações de horários para controlar a criação e a transferência de moedas, enquanto a bitcoin depende apenas da ordenação parcial consistente da ordenação dos blocos na cadeia. Essas propostas já previam que cada nó possuiria seu próprio *ledger*. No caso de discordância entre os nós, depreende-se que o *ledger* correto seria escolhido pela maioria. No entanto, os sistemas b-money e bitgold não possuíam custo para a criação de identidades (nós), o que os torna suscetíveis a *Sybil attacks*. Nenhuma dessas moedas digitais chegou a ser implementada.

A bitcoin foi construída a partir de inúmeras ideias surgidas anteriormente, inclusive algumas que foram desenvolvidas para objetivos que não eram a criação de um sistema monetário. O artigo de Nakamoto (2008) busca a criação de um sistema monetário alternativo no qual não exista a necessidade de confiar em intermediários (instituições financeiras) para a realização de transações via internet, visto a não existência de um instrumento como dinheiro em espécie para realizar o pagamento *on-line*. Ademais, a existência de intermediários impossibilita a liquidação definitiva dos valores, já que há a possibilidade de o consumidor contestar o pagamento, o que, segundo o autor, acaba inviabilizando pagamentos de pequena monta. Na seção 2.2.2 será discutido de maneira breve o funcionamento desse sistema.

É notável que a bitcoin também possui defeitos. Em particular, Danezis e Meiklejohn (2015) e Koning (2016) citam a dificuldade de lidar com quantidades grandes de transações, além da impossibilidade de realização de política monetária ativa, que torna o preço da moeda volátil. Para resolver esses problemas, propõem a criação de uma moeda eletrônica do banco central, que contaria com um grau de centralização quanto à criação de moeda para atingir a estabilidade de preços.

2.2 Gerenciamento de Moedas Digitais

De maneira bastante simplificada, a tecnologia *blockchain* utilizada pelas criptomoedas é usada para manter um arquivo eletrônico que armazena a quantidade de moeda (virtual) de cada indivíduo cadastrado na rede de computadores da respectiva moeda digital, um livro-razão (*ledger*) que mantém devidamente atualizado o saldo monetário (virtual) de cada pessoa:

> Nesse sentido, essa tecnologia é bastante similar ao livro-razão utilizado pelo sistema bancário para manter atualizado o saldo monetário (eletrônico) de cada pessoa depositado no sistema. A inovação central da tecnologia de registros das criptomoedas é manter atualizado o saldo monetário das pessoas sem a necessidade de uma entidade central *monitorável* para verificar a autenticidade das informações registradas (BERTOLAI; OLIVEIRA, 2020, p. 201).

2.2.1 Sistema Centralizado

O sistema bancário mantém atualizado o saldo monetário (eletrônico) de cada pessoa cadastrada no sistema por meio de um livro-razão que registra todas as transações monetárias (eletrônicas) entre seus depositantes.[7]

A título de ilustração, suponha-se que João efetuou um depósito de 100 reais no sistema bancário e pretende liquidar uma dívida de 30 reais com José, que também possui conta no sistema bancário, embora ainda sem saldo. Uma forma de João liquidar sua dívida com José é enviar uma mensagem ao sistema bancário informando sobre tal liquidação. O sistema bancário, então, reduz o saldo de João em 30 unidades e eleva o saldo de José em 30 unidades. Após tal operação contábil, o sistema bancário deve 70 reais para João e 30 reais para José.

Em seguida, João gostaria de liquidar uma outra dívida, agora com Maria, no valor de 90 reais. Analogamente à liquidação anterior, João poderia enviar uma mensagem para o sistema bancário informando sobre tal liquidação. Obviamente, a liquidação com Maria seria negada, uma vez que João não possui saldo suficiente para tanto após o pagamento efetuado a José.

A obviedade da incapacidade de João gastar mais de uma vez a mesma unidade monetária (*double spending*) decorre da característica centralizada do controle contábil executado pelo sistema bancário.[8] Toda transação que requer o uso

7 Assim como as transações entre o sistema bancário e seus depositantes. Por exemplo, saques nos caixas eletrônicos.

8 Essa propriedade de centralização é preservada mesmo em sistemas bancários com mais de um banco. Para detalhes sobre isso, ver Brown (2013).

de uma unidade de moeda já gasta em uma transação anterior é automaticamente rejeitada pelo sistema bancário.

2.2.2 Sistema Descentralizado

A proposta de Nakamoto (2008) busca possibilitar transferências monetárias entre duas pessoas de forma direta sem depender de uma autoridade central (sistema bancário) para registrar e legitimar a transação.[9] O grande desafio computacional superado pela tecnologia da bitcoin, a *blockchain*, é o de evitar o gasto duplo[10] sem a necessidade de confiar em um intermediário, de forma descentralizada. Conforme observado por Bertolai e Oliveira (2020), essa é exatamente a inovação central da *blockchain*: a autenticidade dos registros das operações é garantida de forma descentralizada por todos os computadores conectados à rede da criptomoeda em substituição ao sistema bancário.

Utilizando a moeda digital descentralizada bitcoin, um pagamento de João a Maria no valor de um bitcoin, por exemplo, ocorreria da seguinte forma: João enviaria uma mensagem via internet para os computadores conectados à rede da moeda digital informando o pagamento a Maria. Essa mensagem é recebida, verificada e repassada por cada um dos computadores (nós) da rede.

Até aqui, o procedimento é bastante similar àquele executado centralizadamente pelo sistema bancário. A rede bitcoin, no entanto, não mantém registrado o saldo de cada pessoa. Ao invés disso, cada computador conectado à rede da criptomoeda armazena as transferências de cada unidade de moeda desde a sua emissão. Como a rede não guarda de forma explícita o saldo de João, ele precisará, em sua mensagem à rede, fazer referência a transferências já confirmadas pela rede nas quais ele tenha recebido unidades da criptomoeda cuja propriedade será transmitida a Maria.

Para que uma mensagem (transação) seja aceita como válida pela rede, deve atender a duas condições: a) o remetente deve ter saldo suficiente, isto é, deve ter recebido transações no passado ainda não gastas que somem no mínimo o valor monetário a ser enviado; e b) o remetente deve provar que os saldos monetários que deseja enviar realmente lhe pertencem. Portanto, João precisa ter recebido pelo menos um bitcoin que ainda não tenha sido gasto e precisa provar que detém o direito de gastar o saldo das transações referenciadas.

---

9 Esta seção baseia-se, em grande parte, em Bertolai e Oliveira (2020), cuja leitura é sugerida para maiores detalhes. Além disso, recomenda-se a leitura de Driscoll (2013), Narayanan *et al.* (2016) e Antonopoulos (2017).

10 De forma sucinta, o gasto duplo ocorre quando um indivíduo consegue gastar o mesmo saldo duas vezes. O sistema monetário atual, de forma centralizada, consegue facilmente resolver o problema, como ilustrado na seção 2.2.1. Basta delegar a função de conferir o saldo a um intermediário, no qual as duas partes necessitam confiar, ao qual dá-se o nome de sistema bancário. Para um exemplo hipotético de gasto duplo utilizando criptomoedas, ver Bertolai e Oliveira (2020).

A primeira condição é trivialmente verificada: basta somar o valor recebido por João nas transações por ele referenciadas. A segunda condição é atingida preservando o anonimato do remetente, por meio de uma assinatura digital feita pelo autor na mensagem enviada à rede. A assinatura digital é criada a partir da chave privada[11] do remetente, o que implica que ele é o único capaz de fazê-la (ou alguém em poder da chave privada do remetente). Tomando em conjunto a assinatura da transação, a mensagem enviada (transação) e a chave pública[12]do remetente, os computadores da rede conseguem verificar se a mensagem foi enviada pelo proprietário dos saldos monetários eletrônicos. Nota-se que a verdadeira identidade do remetente não precisou ser conhecida pela rede de computadores para a verificação da autenticidade da mensagem. Então, atendidas ambas as condições, a transação é aceita pela rede e adicionada ao histórico de transações mantido por ela.

Uma questão importante, neste ponto, é como a rede reagiria caso recebesse duas mensagens fazendo referência a uma mesma transação anterior. Caso todos os computadores recebessem as mensagens na mesma ordem, todos concordariam com relação à ordenação das transações de forma análoga ao que ocorre em um sistema centralizado. No entanto, em uma rede descentralizada como a bitcoin, o caminho de cada mensagem até chegar a todos os nós é diferente, o que implica que a ordenação das transações feita por diferentes nós seja potencialmente diferente.[13]

Para entender a relevância dessa falta de uniformidade de ordenação entre os nós, nota-se que João poderia enviar duas mensagens à rede quase simultaneamente. Em uma mensagem, ele informaria a transação com Maria e, na outra mensagem, informaria um pagamento a José, utilizando, em ambas, a mesma moeda (tentativa de gasto duplo). Parte da rede receberia primeiro a transação com Maria e a outra parte receberia primeiro a transação com José. Quando um computador é informado de duas transações que utilizam a mesma moeda, ele (por padrão) aceita como legítima a primeira mensagem recebida e descarta a segunda, considerando-a ilegítima (BERTOLAI; OLIVEIRA, 2020; ANTONOPOULOS, 2014).

Portanto, faz-se necessário decidir (eleger) qual nó possui a correta ordenação das transações recebidas. O nó eleito ganha o direito de criar um bloco de transações e comunicá-lo à rede, que o aceitará se todas as transações forem

11 De forma didática, Bertolai e Oliveira (2020) comparam a chave privada a uma senha que permite a utilização dos saldos monetários recebidos.

12 Novamente de maneira didática, Bertolai e Oliveira (2020) resumem a funcionalidade da chave pública como sendo o endereço eletrônico do remetente na rede.

13 Também importante para essa propriedade, conforme observado por Bertolai e Oliveira (2020), a rede de computadores (nós) não é interligada de forma serial. A rede de nós se organiza sem topologia ou estrutura fixa como forma de conferir robustez à rede (ANTONOPOULOS, 2014).

legítimas e se o nó realmente tiver sido eleito. Assim, a ordenação das transações será a mesma para todos os nós conectados à rede.

Tomando em conjunto a sequência de nós eleitos para a proposição de blocos, forma-se uma cadeia de blocos, denominada *blockchain*. A forma usada para a ordenação entre os blocos é uma referência, em cada bloco, ao seu anterior, formando uma corrente até o bloco inicial.

Para completar essa explicação introdutória sobre o funcionamento das criptomoedas, resta explicar como ocorre a eleição dos nós que propõem os blocos com transações. A eleição ocorre de maneira descentralizada, em um processo chamado mineração, pois o nó eleito precisa pagar um custo e possui o direito de emitir uma certa quantidade de novas moedas para si.

Para um dado nó ser eleito, precisa encontrar uma solução para um problema matemático baseado no bloco construído. Tal solução é denominada *proof-of-work*. Para minimizar a probabilidade de empate,[14] o problema matemático é desenhado de forma que suas soluções (*proof-of-work*) sejam encontradas apenas de forma aleatória e por tentativa e erro (força bruta).[15] O primeiro nó a encontrar uma solução para o bloco que construiu terá uma *proof-of-work* para seu bloco, que será a prova (frente aos demais nós) de que tem o direito de incluir o próximo bloco na cadeia de blocos (*blockchain*).

Como o processo para encontrar a solução é feito por tentativa e erro, nota-se que os nós que perderam a eleição realizaram esforço computacional e consumiram grande quantidade de eletricidade, que acabou sendo "desperdiçada". Porém, essa tarefa computacionalmente custosa possui uma função importante: prover confiança às informações registradas na *blockchain*, servindo como proteção contra fraudes.

Caso a eleição fosse realizada sem a necessidade de gasto energético para realização de esforço computacional, estaria sujeita a fraudes do tipo *Sybil attack*. Em uma rede anônima, como a bitcoin, se não houver nenhuma dificuldade para a criação de identidades, uma única pessoa pode criar vários perfis (nós). Como cada nó pode criar seu bloco candidato e, supondo-se que a rede ainda elegeria o nó de forma aleatória, uma pessoa que criasse muitos nós teria facilidade em fraudar a rede, pois a sua probabilidade de ser eleita é maior que a dos demais nós.

14 Um empate seria resultado, por exemplo, de dois nós distintos chegarem a uma solução para seus respectivos blocos ao mesmo tempo. No caso em que um nó eleito tenha recebido a transação com Maria primeiro e o outro nó tenha recebido a transação com José primeiro, os registros não estariam conciliados na rede. A uniformização da cadeia de blocos será atingida na próxima eleição em que não houver empate, quando uma cadeia passará a ser maior e, por padrão, será aceita por todos os nós. Nota-se que uma determinada transação poderia estar em apenas uma das cadeias e, sendo essa cadeia a perdedora após o empate, a transação voltaria a não estar confirmada por nenhum bloco. Portanto, uma baixa probabilidade de empate na eleição favorece a rapidez na confirmação de transações.

15 Para mais detalhes do processo de mineração, ver Antonopoulos (2017).

Assim, pode-se entender a necessidade da realização de esforço computacional "inútil" como um mecanismo que aumenta a dificuldade (custo) de criar um nó (identidade).

A proteção contra fraudes (em particular, *Sybil attacks*) é efetiva, pois, para fraudar um bloco na *blockchain*, é necessário substitui-lo por um outro diferente. Esse novo bloco deverá ser enviado à rede junto com sua *proof-of-work*, que só pode ser encontrada usando força bruta. No entanto, para a fraude em um determinado bloco ser efetivada, não é suficiente substitui-lo. Conforme apontam Narayanan *et al*. (2016), por padrão, cada nó sempre trabalha com a maior cadeia de blocos. Portanto, é necessário substituir tantos blocos quanto forem necessários para que a *blockchain* que contém o bloco fraudado tenha tamanho maior que a *blockchain* que está sendo fraudada.

Como conclusão, desenvolveu-se um sistema capaz de registrar de forma confiável a transmissão de propriedade das unidades de moeda, sem a necessidade de uma autoridade central digna de confiança para certificar a legitimidade destes registros. (BERTOLAI; OLIVEIRA, 2020).

2.2.3 Sistema Permissionado

O sistema do tipo permissionado para gerenciamento de moeda digital parece, do ponto de vista dos governos e de seus respectivos bancos centrais, uma opção mais aceitável (isto é, menos descentralizada) de implementação de uma moeda digital. Uma proposta cuja ênfase recai sobre os aspectos técnicos da moeda digital soberana com gerenciamento permissionado é a rscoin (DANEZIS; MEIKLEJOHN, 2015).

Ao propor essa criptomoeda, os autores buscam, principalmente, resolver o problema da escalabilidade das criptomoedas.[16] Um segundo ponto em que se busca melhorias é quanto à descentralização da geração de moedas, que impossibilita a realização de política monetária ativa e torna o valor da criptomoeda bastante volátil.[17]

Para atingir esses objetivos, a rscoin busca separar as responsabilidades pela geração de novas moedas para o sistema e pela manutenção do *ledger* com as transações. As primeiras ficariam a cargo do banco central, enquanto a segunda, de entidades denominados *mintettes*, que seriam credenciadas (autorizadas)

16 A escalabilidade de um sistema se refere a sua capacidade de operação. No caso de moedas digitais, essa característica está relacionada à quantidade de transações que podem ser processadas em um determinado período de tempo. Segundo Danezis e Meiklejohn (2015), a bitcoin pode suportar apenas sete transações por segundo, enquanto grandes operadoras de cartões de crédito processam até sete mil.

17 Conforme a análise de Bertolai e Oliveira (2020), essa volatilidade característica das criptomoedas é a razão pela qual diversos autores concluem precipitadamente que as criptomoedas não são moedas.

pelo banco central para realizar o trabalho de verificar a validade das transações recebidas pelo sistema. Nota-se que essa é uma enorme diferença com relação ao sistema descentralizado, no qual os mineradores não são identificados e, por isso, impunha-se um custo (*proof-of-work*) para a criação de uma identidade a fim de evitar fraudes (por exemplo, *Sybil attacks*). Como os *mintettes* são conhecidos e puníveis por condutas inadequadas, não é necessária a imposição de tal custo.

Os *mintettes*, como responsáveis pela manutenção do *ledger*, serão encarregados de receber as transações dos usuários do sistema e checar se são válidas, isto é, se os *inputs* da transação ainda não foram gastos e se o remetente é o proprietário dos saldos que deseja enviar.[18] Cada *mintette* definirá um período de tempo que levará para formar cada um de seus blocos. Danezis e Meiklejohn (2015) chamam esse período de *epoch*. Por exemplo, o banco central poderia determinar que os *mintettes* escolhessem formar seus blocos a cada dois, cinco ou dez minutos e que, a cada 30 minutos, os blocos criados pelos *mintettes* fossem enviados para o banco central, que ficará responsável por produzir um bloco que unifique todos os blocos recebidos dos *mintettes*. Esse período de 30 minutos após o qual os blocos de nível inferior devem ser enviados ao banco central foi denominado *period*.

É importante frisar que os *mintettes* não possuem todo o *ledger*, mas apenas conhecimento da cadeia de blocos principal, que contém os blocos criados pelo banco central e é aberta a todos, e dos blocos criados por si mesmo. Os *mintettes* serão responsáveis pela prevenção de gasto duplo dos *outputs* das transações registradas nos blocos que eles próprios criaram.

Dessa forma, ao criar seus blocos de nível inferior, os *mintettes* precisam consultar (indiretamente, por meio dos usuários) os demais para verificar a validade das transações que recebem. Isso ocorre porque os *inputs* da transação recebida por um *mintette* podem estar (e provavelmente estarão) registrados como *outputs* em um bloco de nível inferior produzido por outro *mintette*. O conjunto de *mintettes* é responsável por produzir um *ledger* consistente e, para tanto, pode optar pela criação de blocos de nível inferior que referenciem outros blocos dos demais *mintettes*.

A estrutura permissionada para gerenciamento de moeda digital se assemelha à disposição do sistema bancário atual. De fato, nota-se que, assim como na estrutura bancária, os *mintettes* não possuem acesso a toda contabilidade. Cada entidade conhece apenas seus próprios registros e as informações fornecidas pelo banco central. Enquanto os bancos são responsáveis pela prevenção do gasto duplo de seus depositantes, cada *mintette* é responsável pela prevenção do gasto duplo dos *outputs* das transações que, de forma randômica, foram encaminhadas para que ele as registrasse em sua própria contabilidade.

18 Assim como os mineradores checam tais condições ao validarem uma transação, conforme visto na seção 2.2.2.

Além disso, é importante notar que tanto os bancos quanto os *mintettes* são entidades que precisam de autorização do banco central para atuação como mantenedor dos registros eletrônicos. Por serem entidades conhecidas do regulador, não necessitam de um processo computacionalmente custoso (*proof-of-work*) para o registro no *ledger*. Por serem instituições conhecidas, podem ser monitoradas pelo ente regulador da moeda digital.[19] Por toda essa semelhança entre as instituições bancárias do modelo centralizado (seção 2.2.1) e os *mintettes*, estes podem ser também considerados intermediários no processo de gerenciamento de uma moeda digital.

Como diferença entre o sistema centralizado com mais de um banco e o sistema permissionado, é possível citar que o conjunto de bancos não possui conhecimento comum de uma parte de transações (como os blocos de nível superior criados pelo banco central) nem utilizam a tecnologia *blockchain* para confirmar as transações.

2.2.4 Criptomoeda

Criptomoedas costumam ser classificadas, primeiramente, como um sistema que se utiliza da criptografia para prover um sistema (monetário) seguro com relação à manutenção do *ledger* e à criação de novas moedas.[20] No entanto, a utilização de criptografia é apenas um meio para atingir o objetivo de prover um sistema monetário seguro de forma descentralizada. Veja que o sistema monetário controlado pelo banco central também tem o objetivo de ser seguro com relação a esses dois pontos (manutenção do *ledger* e criação de novas moedas), porém de forma centralizada com a utilização de monitoramento.

Conforme observado por Bertolai e Oliveira (2020), a disponibilidade da tecnologia de monitoramento altera a escolha da sociedade quanto ao meio de troca utilizado para indução de trocas. No caso de monitoramento perfeito, não há necessidade de um instrumento que as induza. A capacidade de monitoramento e punição pelo não cumprimento de promessas é suficiente para que os indivíduos produzam/consumam baseando-se em um esquema de crédito.

A utilização de um meio de troca surge como um substituto (imperfeito) para o crédito nos casos em que a disponibilidade da tecnologia de monitoramento seja parcial ou inexistente. No primeiro caso, o setor monitorável, denominado setor bancário, é capaz de produzir certificados de dívida como meio de troca. No segundo caso, a evidência de produção de bens/serviços por meio de uma moeda fiduciária (objeto sem valor intrínseco) é capaz de viabilizar trocas.

19 Nesse sentido, para que os *mintettes* sejam devidamente monitorados e puníveis por suas condutas, Danezis e Meiklejohn (2015) apontam duas características importantes que o sistema rscoin deve apresentar: a) ser transparente; e b) permitir que o *ledger* possa ser auditado para verificar sua integridade e o comportamento dos *mintettes*.

20 Por exemplo, ver Narayanan *et al.* (2016) e a página sobre criptomoedas no *site Investopedia*.

A inovação das criptomoedas é que o desenho do protocolo torna elevada a dificuldade de se fraudar o sistema monetário, conforme explanado na seção 2.2.2. Por isso, as criptomoedas têm a possibilidade de usar uma tecnologia contábil eletrônica como a utilizada pelo sistema bancário, mas sem a necessidade de monitoramento. A inovação das criptomoedas pode ser resumida na proposição a seguir:

> Do ponto de vista conceitual (da Teoria Econômica), a grande inovação das criptomoedas foi viabilizar a geração de evidência confiável e flexível de produção (de bens/serviços) sem o uso de tecnologia de monitoramento das ações dos responsáveis por seu gerenciamento (BERTOLAI; OLIVEIRA, 2020, p. 228).

É importante notar que, considerando-se a proposição, não é possível defender que uma moeda digital emitida utilizando o sistema permissionado de gerenciamento (seção 2.2.3) seja uma criptomoeda. Apesar disso, o artigo propõe que a rscoin seja nomeada de *centrally banked cryptocurrencies* (DANEZIS; MEIKLEJOHN, 2015). Evidentemente, ainda é possível classificar a proposta como sendo de uma moeda eletrônica do banco central, termo que será definido na seção 3.1.

3 Moeda Eletrônica do Banco Central

Considerando-se a perspectiva histórica da criação dos bancos centrais apresentada por Barossi-Filho e Sztajn (2015), nota-se que essa instituição foi criada com a principal função de monitorar a emissão de moeda feita pelos bancos comerciais. Do ponto de vista da Teoria Econômica, Cavalcanti *et al.* (1999) e Cavalcanti e Wallace (1999a, 1999b) mostram que é exatamente a existência de monitoramento de (ao menos) uma parte dos indivíduos, os bancos, que disciplina os responsáveis pela emissão de moeda a administrar sua escassez.

Barossi-Filho e Sztajn (2015) pontuam, no entanto, que, na qualidade de emissor de papel-moeda, o banco central não atua como "[...] moderador das assimetrias de informação [...]". Isto é, ao exercer a função de emissor de papel-moeda, os bancos centrais muitas vezes optam pela discricionariedade na execução da política monetária na tentativa de estimular a economia.

De forma geral, as criptomoedas surgiram, em parte, pela insatisfação quanto ao gerenciamento da política monetária realizado pelos bancos centrais (LO; WANG, 2014). Como resposta a essa ingerência, as criptomoedas foram criadas com regras de política monetária explicitamente programadas no desenho da moeda. Em muitos casos, como no desenho da bitcoin, a política monetária foi definida de modo que o estoque de moedas fosse, em algum momento, fixo. Com uma

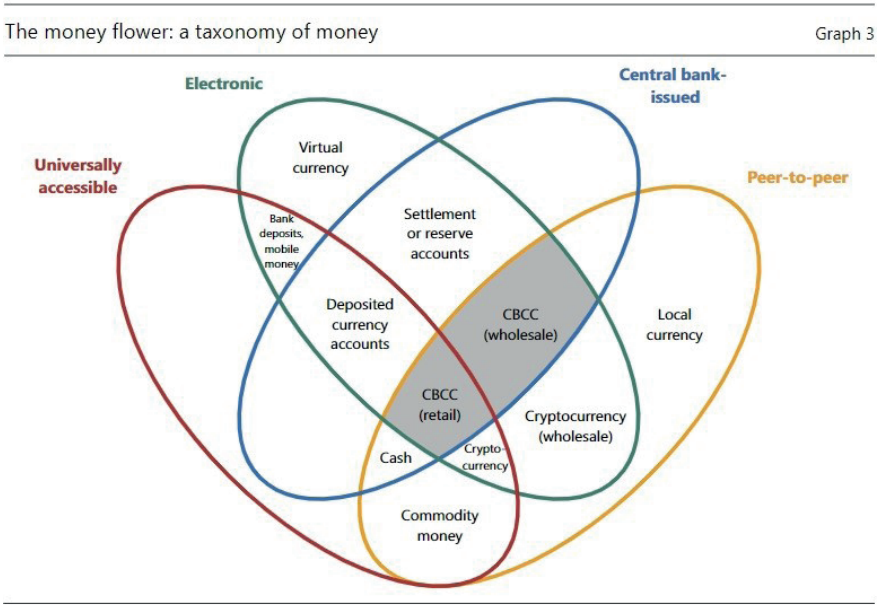
política monetária que não responde às variações na demanda por moeda, tem-se por resultado que o preço da criptomoeda possui uma elevada variação.[21]

As propostas de moeda eletrônica do banco central surgem da insatisfação com relação à instabilidade de preços que atinge as criptomoedas de emissão privada. Busca-se diminuir a descentralização existente no desenho das criptomoedas e reintroduzir um ponto central de controle: a possibilidade de um banco central definir a oferta de moedas.

3.1 O que são Moedas Eletrônicas do Banco Central

Bech e Garratt (2017) apresentam uma taxonomia para classificar os diferentes tipos de dinheiro. Essa taxonomia é baseada em quatro características: a) se o acesso é universal ou não; b) se a emissão é eletrônica ou física; c) se a emissão é realizada pelo banco central ou não; d) se a transmissão é feita diretamente entre os usuários (*peer-to-peer*) ou se é controlada por intermediários. A classificação taxonômica relativa a diferentes tipos de moeda pode ser vista na Figura 1.

Figura 1 – Taxonomia do dinheiro



Fonte: Bech e Garratt (2017).

21 Existem algumas exceções, como as criptomoedas bitUSD e tether, que foram desenhadas com o objetivo de manter uma cotação constante em relação ao dólar americano. No entanto, considerando-se a análise de Andolfatto (2015a), é provável que essas criptomoedas acabem por não conseguir manter essa cotação.

Com relação à característica de transmissão *peer-to-peer*, Bech e Garratt (2017, p. 56) a definem dizendo que "[...] a transação ocorre diretamente entre o remetente e o beneficiário sem a necessidade de um intermediário central [...]". Completam dizendo que "Em uma rede de computadores, o conceito P2P significa que as transações podem ser processadas sem a necessidade de um servidor central [...]".

Esse conceito precisa de uma definição mais clara, em especial com relação ao que significa ser um intermediário. Nota-se que, se for considerado que "[...] o conceito P2P significa que as transações podem ser processadas sem a necessidade de um servidor central [...]" (BECH; GARRATT, 2017, p. 56), é possível classificar tanto o sistema descentralizado de gerenciamento de moeda digital (seção 2.2.2), quanto o sistema permissionado (seção 2.2.3) como possuindo a característica *peer-to-peer*.[22] Ainda mais, seria possível classificar até o sistema centralizado (seção 2.2.1) com mais de um banco como possuidor da característica *peer-to-peer*, já que cada banco é um servidor diferente.

Por outro lado, se for considerada a definição de transação *peer-to-peer* como sendo aquela que "[...] ocorre diretamente entre o remetente e o beneficiário sem a necessidade de um intermediário central [...]" (BECH; GARRATT, 2017, p. 56), talvez nem o sistema descentralizado seria considerado *peer-to-peer*, a depender do entendimento do que é um intermediário central. Logo, no sistema descentralizado, a transação depende de um tipo de intermediário para ser concretizada – os mineradores.

O que difere, então, os três sistemas (centralizado, permissionado e descentralizado)? Uma boa definição seria a de que um intermediário central é aquele que precisa ser monitorado para que as suas ações não se desviem do protocolo. Com essa definição, é possível enquadrar os sistemas centralizado e permissionado como não sendo possuidores da característica de transferência *peer-to-peer*, ao contrário do sistema descentralizado.

Para os objetivos deste trabalho, será denominada MEBC a moeda que possuir acesso universal e emissão eletrônica realizada pelo banco central. Essa definição, portanto, independe da característica de transmissão *peer-to-peer* da moeda. Assim, pode-se distinguir dois tipos de MEBC: a criptomoeda soberana (de varejo), que possui transmissão *peer-to-peer* entre os usuários (sistema descentralizado), e a moeda digital soberana, cuja transmissão não é feita de forma direta entre os usuários (necessidade de intermediário monitorável).

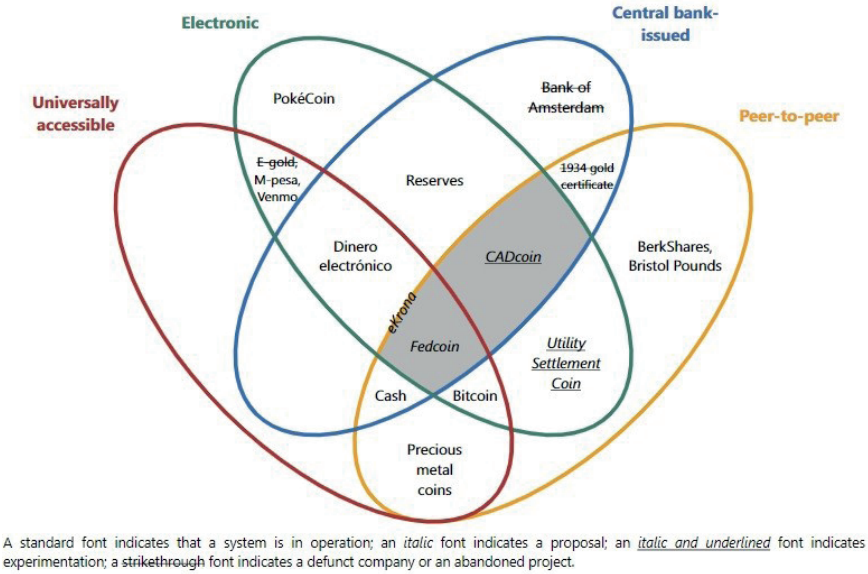
Na Figura 1, são identificados dois tipos de criptomoeda soberana: uma destinada ao uso pelo público em geral (operações de varejo) e outra com destinação específica (operações de atacado). Em comum, esses dois tipos possuem como característica emissão eletrônica realizada pelo banco central e transmissão feita

22 Para isso, no sistema permissionado, cada transação é processada por um *mintette* diferente e, portanto, por um servidor diferente.

diretamente entre os usuários. Elas se diferem em relação ao seu objetivo: enquanto a primeira possui acesso universal e é voltada para operações pequenas, a segunda tem como objetivo a movimentação das reservas bancárias mantidas no banco central, com acesso limitado às instituições bancárias que já possuem autorização para manter reservas no banco central.

Na Figura 2, são mostradas as classificações de diferentes moedas (atuais e históricas).

Figura 2 – Taxonomia do dinheiro: exemplos



Fonte: Bech e Garratt (2017).

Como exemplos, conforme mostrado na Figura 2, cita-se, para a moeda universal, a fedcoin (KONING, 2016) e, para a de acesso restrito, a CADcoin (CHAPMAN *et al.*, 2017). Uma ressalva é que Koning (2016) aponta que a fedcoin poderia ser implementada por meio de um sistema permissionado de gerenciamento de moeda digital ao citar o trabalho de Danezis e Meiklejohn (2015). É importante frisar que a utilização desse tipo de gerenciamento possui, como característica, transferência de moeda não *peer-to-peer*, não se tratando, nesse caso, de criptomoeda soberana, mas sim de moeda digital soberana. O acesso ao Central Bank Money (CBM) para operações de varejo na forma eletrônica pode, também, ser feito de forma centralizada (ou seja, transmissão não *peer-to-peer*). Seria, então, uma moeda eletrônica, emitida pelo banco central, universalmente acessível e com transmissão

centralizada. Conforme mostrado na Figura 1, Bech e Garratt (2017) identificam essa moeda como a proposta de *deposited currency accounts* (TOBIN, 1985). Além de sistemas centralizados de gerenciamento de moeda digital, os sistemas do tipo permissionado também se encaixam nessa classificação. Neste trabalho, define-se uma moeda com tais características como uma moeda digital soberana.

Atualmente, a única forma de o público em geral possuir acesso ao CBM é por meio de dinheiro em espécie, que possui acesso universal, emissão física realizada pelo banco central e transmissão feita de forma *peer-to-peer*. A única diferença entre a classificação do dinheiro em espécie e a definição de criptomoeda soberana para varejo é quanto à emissão ser feita de forma eletrônica ou não.

3.2 Razões pelas quais um Governo Gostaria de Emitir uma Moeda Eletrônica do Banco Central

Na seção 3.1, foi observado que, nos termos da classificação feita por Bech e Garratt (2017), a única diferença entre uma criptomoeda soberana (gerenciamento descentralizado) e o dinheiro em espécie é que este possui representação física, enquanto aquela possui apenas representação eletrônica. Tal diferença que, a princípio, não parece ser de extrema relevância, traz o questionamento de quais seriam as motivações para a criação de uma criptomoeda (ou, até mesmo, uma moeda digital) soberana. Isto é, quais potenciais benefícios (e potenciais prejuízos) devem ser considerados para a criação de uma MEBC?

Conforme pontuado por Bertolai e Oliveira (2020), as criptomoedas possuem uma flexibilidade de configuração muito grande. Isso vale não apenas para a definição da política monetária da criptomoeda, relacionada à característica de escassez, mas, inclusive, para as características de durabilidade e divisibilidade. A flexibilidade quanto à escassez permite a determinação, por parte do banco central, da quantidade de moeda emitida, seja por regras (como no caso da bitcoin), seja discricionariamente. Portanto, um aspecto positivo possuído pela criptomoeda soberana é a flexibilidade na definição de suas características. Nota-se que a moeda digital soberana também possui bastante flexibilidade, assim como a moeda digital controlada pelo sistema bancário.

Com relação à flexibilidade no controle de sua escassez, ressalta-se ainda que uma criptomoeda soberana permite que a regra da política monetária seja programada diretamente no desenho da moeda, possibilidade que "[...] pode ser vista como o limite máximo de Independência do Banco Central [...]" (BERTOLAI; OLIVEIRA, 2020, p. 231).

A despeito da possibilidade de usar a MEBC como possível instrumento de política monetária, o banco central poderia escolher pagar nenhum juro nominal aos possuidores da moeda (como ocorre com a moeda em espécie, resultando

em um pagamento de juros reais negativos se a inflação for positiva). Poderia, também, optar por uma regra de apenas corrigir o valor da moeda pela inflação (pagando um juro nominal igual à inflação apurada para que os juros reais sejam iguais a zero).

No primeiro caso, a moeda digital seria, assim como o dinheiro em espécie, uma barreira ao pagamento de taxa de juros nominais negativas. A moeda seria uma saída acessível e segura em tempos de crise, nos quais o banco central potencialmente gostaria de praticar taxas de juros nominais negativas. No segundo caso, a moeda digital seria uma barreira contra o pagamento de taxas de juros reais negativas, pois a moeda seria uma opção segura de proteção contra a inflação. Isso restringe ainda mais o campo de ação da política monetária. No caso anterior, o banco central poderia pagar uma taxa de juros real negativa ao adotar uma taxa de juros nominal positiva, porém menor que a inflação (supondo que esta seja, também, positiva).

Bordo e Levin (2017), portanto, concluem que a utilização de uma MEBC como instrumento primário da política monetária seria benéfica, diminuindo a necessidade de utilização de políticas alternativas como *quantitative easing* e intervenções fiscais. O interesse em usar uma MEBC como instrumento de política monetária surge de uma vantagem que independe de a política monetária da moeda ser definida por regras ou de modo discricionário: a possibilidade de ser paga uma taxa de juros nominal negativa aos possuidores da moeda eletrônica (KONING, 2016), assim como já ocorre com a remuneração das reservas bancárias.

Uma eventual coexistência da MEBC com o dinheiro em espécie seria prejudicial ao objetivo de pagamento de taxa de juros nominal negativa, já que seria possível escapar da taxa de juros nominal negativa da MEBC ao trocá-la pela moeda em espécie. Stevens (2017) aponta que, no caso de haver a substituição da moeda em espécie pela sua versão eletrônica, seria possível superar o "limite inferior negativo" enfrentado pela política monetária, além de também possibilitar aos domicílios e às empresas o acesso ao CBM. No entanto, Stevens (2017) destaca a existência de estudos questionando se o "limite inferior negativo" realmente reduz a efetividade da política monetária.

A emissão de uma MEBC poderia ser uma maneira de prover serviços financeiros para uma maior parcela da população, além de aumentar a eficiência das trocas (KETTERER; ANDRADE, 2016; YANAGAWA; YAMAOKA, 2019). Além disso, conforme pontuado por Berentsen e Schär (2018), pode vir a atender uma necessidade da população por acesso a um dinheiro digital que não ofereça de risco de contraparte. Como consequência, se todos optassem por manter seu dinheiro na forma de MEBC, os bancos não exerceriam sua função de transformação de maturidade, o que potencialmente diminuiria o risco do sistema financeiro como um todo. Essas questões são analisadas por Andolfatto (2018) e discutidas na seção 3.

3.3 Gerenciamento Descentralizado, Centralizado ou Permissionado?

Embora a ideia de criar uma MEBC tenha sido estimulada após a criação da bitcoin e da tecnologia *blockchain* (SCORER, 2017), não é necessário utilizar essa tecnologia para que o acesso ao CBM seja permitido a um grupo maior de agentes.

Por exemplo, Kumhof e Noone (2018), ao estudar as implicações causadas no balanço de um banco central pela possibilidade de acesso ao CBM pelo público, e Andolfatto (2018), ao estudar o efeito causado no setor bancário, não assumem que o acesso será feito usando-se a tecnologia *blockchain*, mas sim no esquema de *deposited currency accounts*[23] proposto por Tobin (1985), denominado, neste trabalho, moeda digital soberana.

As três maneiras de implementar uma MEBC (gerenciamento centralizado, descentralizado e permissionado) possuem características distintas que devem ser analisadas antes da escolha de como implementar a moeda digital.

3.3.1 Sistema Descentralizado

Berentsen e Schär (2018) apresentam argumentos contrários à emissão de uma criptomoeda soberana (gerenciamento descentralizado). Argumentam que nenhum banco central respeitável teria incentivos para emitir uma criptomoeda soberana devido à anonimidade existente em um sistema descentralizado de legitimação de transações. Segundo os autores, instituições como bancos, que são obrigadas a seguir políticas como *know your costumer* (KYC) e *anti-money laundering* (AML), questionariam por que a autoridade monetária está emitindo uma moeda digital anônima em vez de expandir o acesso ao CBM de forma centralizada (e com menor anonimidade).

Em contraposição a esse argumento, observa-se que a moeda amplamente oferecida atualmente pelos bancos centrais, a moeda em espécie, é totalmente anônima, sendo bastante difícil (se é que possível) implementar um sistema centralizado que monitore as transações realizadas por esse meio com vistas a atender políticas do tipo KYC e AML. Nesse sentido, um banco central que emitisse uma criptomoeda soberana, mesmo que fosse tão anônima quanto o dinheiro físico, não poderia, necessariamente, ser censurado por facilitar a vida de criminosos.

Andolfatto (2015a) argumenta no mesmo sentido, notando ainda que a criptomoeda soberana produz ao menos um rastro digital, enquanto o dinheiro físico produz rastro nenhum. Andolfatto (2015b) acrescenta que, enquanto o livro-razão que mantém uma criptomoeda é visível e mantido pelos nós da rede, o livro-razão

23 O Equador já ofereceu a seus residentes esse tipo de acesso ao CBM, chamado *dinero electrónico* (BECH; GARRATT, 2017).

que mostra a distribuição do dinheiro em espécie é invisível para todos, elevando o grau de anonimidade.

Outros argumentos contrários à implementação de uma MEBC por meio de um sistema descentralizado são o alto gasto energético da mineração, a demora da confirmação dos pagamentos no sistema e a dificuldade de o sistema atingir uma grande escala.

Além disso, outra característica que deve ser considerada com relação à criptomoeda soberana é o fato de as transações serem visíveis a todos, o que potencialmente violaria leis direcionadas a bancos e colocaria algumas partes em situação de desvantagem (CHAPMAN *et al.*, 2017). Apesar de no sistema bitcoin apenas a chave pública ser visível a todos, é certo que através de algoritmos ou até mesmo por um erro do usuário é possível descobrir a real identidade por trás da chave pública (característica pseudônima da rede) (NARAYANAN *et al.*, 2016).

Uma característica do sistema descentralizado que pode influenciar a escolha de um banco central por esse sistema é a possibilidade de manter seus usuários anônimos, embora não completamente. Essa característica aproxima a criptomoeda soberana ao dinheiro em espécie. Além disso, o sistema descentralizado é mais resiliente a ataques, já que não existe um ponto único que, se atacado, faz o sistema não funcionar. Por fim, conforme observado por Bertolai e Oliveira (2020), o sistema descentralizado prescinde da utilização de monitoramento.

3.3.2 Sistema Centralizado

Berentsen e Schär (2018) defendem que o acesso ao CBM seja feito de forma centralizada por meio de contas – como as que os bancos mantêm suas reservas depositadas. Uma crítica a esse modelo é que os bancos centrais não possuem vantagem comparativa em oferecer esse tipo de serviço (KAHN, RIVADENEYRA; WONG, 2018). Há uma divergência com relação à força dessa crítica: enquanto Kahn, Rivadeneyra e Wong (2018) concluem que é pouco provável que um banco central forneça acesso ao CBM por meio de contas, Berentsen e Schär (2018) concluem que o acesso poderia se dar por meio dos bancos comerciais, que seriam obrigados a fornecer uma conta com acesso direto ao CBM, cujos registros financeiros seriam distintos dos registros do próprio banco. Kahn, Rivadeneyra e Wong (2018) não consideram a possibilidade de os bancos comerciais operacionalizarem o acesso ao CBM.

Na linha de Berentsen e Schär (2018), Bordo e Levin (2017) também defendem o acesso ao CBM por meio de contas, sejam fornecidas diretamente pelo banco central ou por bancos comerciais parceiros. Como vantagem desse tipo de acesso, citam que os pagamentos seriam realizados de forma instantânea e praticamente sem custos. Seria como o sistema centralizado discutido na seção 2.2.1,

em que existe apenas um banco. No caso do sistema bancário, para a liquidação de uma dívida entre dois agentes é necessária somente a mudança do credor do banco (depositante).[24] Bordo e Levin (2017) acreditam que, com a capacidade de armazenamento de dados e a velocidade de transmissão de dados pela internet atuais, seria possível que o próprio banco central fornecesse as contas ao público.

O sistema centralizado para gerenciamento de moeda digital soberana é, do ponto de vista da Teoria Econômica, bastante parecido com o sistema bancário atual. Desse modo, esse sistema precisa ser monitorado e, por não possuir a anonimidade como característica, permite a implementação de políticas do tipo KYC e AML. Outras características incluem a inexistência da necessidade de custos com a mineração, pagamento praticamente instantâneo e a existência de um sistema que suporta grande número de transações por segundo.

3.3.3 Sistema Permissionado

Comparando-se os métodos descentralizado e permissionado para gerenciamento, nota-se que o primeiro possui como pontos positivos maior anonimidade, pois mesmo os nós têm sua identidade desconhecida, e maior resistência à censura, características que o tornam mais próximo ao dinheiro em espécie. Por outro lado, o sistema permissionado é superior na quantidade de transações que pode processar, a confirmação da transação é mais rápida e sua liquidação é definitiva (KONING, 2016).

O conhecimento dos *mintettes*, a princípio, diminui a anonimidade da rede. A proposta de Danezis e Meiklejohn (2015) garante a (pseudo) anonimidade dos usuários, já que as transações ocorrem por meio de sua chave pública. Koning (2016) argumenta quanto à diminuição da resistência à censura do sistema permissionado, pois governos e outros atores poderiam compelir os nós, que são conhecidos, a não registrar determinadas transações. No entanto, considerando-se a natureza pseudônima dos usuários, não parece que essa ameaça deva ser considerada, afinal um usuário que tenha suas transações por meio de uma chave pública negada possui a faculdade de criar uma nova, desconhecida das autoridades.

As diferenças entre as características dos sistemas descentralizado, centralizado e permissionado estão resumidas no Quadro 1.

Quadro 1 – Aspectos dos sistemas de gerenciamento de moeda digital

Característica	**Descentralizado**	**Centralizado**	**Permissionado**
Anonimidade	Pseudo	Não	Pseudo
Evita ponto único de falha	Sim	Não	Sim
Requer monitoramento	Não	Sim	Sim

Continua...

24 No caso de uma moeda digital soberana, assim como ocorre com a moeda em espécie, a moeda não é uma dívida, portanto não há que se falar no termo credor. No entanto, a liquidação da transferência entre os usuários ocorreria da mesma forma.

Conclusão.

Implementação de políticas KYC e AML	Não	Sim	Não
Custos de mineração	Sim	Não	Não
Pagamento praticamente instantâneo	Não	Sim	Sim
Escalabilidade do sistema	Baixa	Alta	Alta

Fonte: Elaboração dos autores.

Ao emitir uma MEBC, existe um *trade-off* entre dificultar operações de lavagem de dinheiro e manter a anonimidade da moeda *outside* fornecida pelo banco central, conforme é possível observar no Quadro 1. Enquanto os sistemas descentralizado e permissionado de gerenciamento possibilitam que o usuário desfrute de uma pseudoanonimidade e, portanto, impedem a implementação de políticas de KYC e AML, o sistema centralizado possibilita tais políticas em detrimento de qualquer anonimidade dos usuários.

Em comparação à moeda *outside* atualmente fornecida pelo banco central, nota-se que o dinheiro em espécie, por um lado, é anônimo apenas de forma incidental e não por escolha de seu emissor. No caso da emissão de uma MEBC, por outro lado, a característica de anonimidade seria optada conscientemente pelo banco central (BECH; GARRATT, 2017) caso escolhesse realizar a emissão pelo sistema descentralizado ou permissionado de gerenciamento. Este trabalho não busca avaliar qual opção seria mais adequada. Conforme argumentado anteriormente, pontua-se que a emissão de uma criptomoeda soberana, por si só, não necessariamente prejudica políticas de prevenção de lavagem de dinheiro.

4 Efeitos de uma Moeda Eletrônica do Banco Central no Setor Bancário

Os efeitos provocados pela emissão de uma MEBC sobre o setor bancário não são completamente conhecidos pela Teoria Econômica. Nota-se que dois atrativos dos bancos para os depositantes são a manutenção segura de suas posses e a possibilidade de transmitir seus fundos para outros usuários do sistema. Tais objetivos também podem ser atingidos ao manter seu dinheiro aplicado em MEBC em vez de depósitos bancários. Portanto, é possível que exista um fluxo de depósitos à vista para aplicação em MEBC, especialmente se ela possuir a faculdade de remunerar, por meio de pagamento de juros, quem a possui.

Stevens (2017) aponta que a retirada de fundos do sistema bancário tradicional, que é construído com base em reservas fracionárias, poderia tanto criar um sistema mais seguro, com menor necessidade de garantia de depósitos e da função de prestamista de última instância, quanto poderia diminuir a oferta de crédito.

Quatro cenários possíveis são apontados por Stevens (2017). O primeiro é o caso em que os bancos, ao perderem depósitos bancários como fonte de financiamento, conseguem se financiar por meio de instrumentos de longo prazo como dí-

vida de longo prazo e/ou capital próprio por meio de ações. Nesse caso, os bancos se tornariam *narrow banks*, pois as maturidades de seus ativos e passivos seriam próximas. No entanto, é possível que os bancos não consigam se capitalizar de outras maneiras, o que caracteriza o segundo cenário. Com menor capital disponível, a capacidade de empréstimo dos bancos diminuiria, o que poderia prejudicar a atividade econômica.

Um terceiro cenário possível seria um no qual, supondo-se que os bancos não consigam se financiar por um meio que não seja depósitos à vista, o banco central assume o papel de conceder empréstimos. Com relação ao governo, esse cenário apresenta um possível aumento dos ganhos de senhoriagem e maior controle por parte do banco central sobre as condições financeiras, o que facilitaria a manutenção da estabilidade macroeconômica. Por outro lado, o balanço inflado do banco central seria uma ameaça a sua independência, diminuindo a confiança de que o banco central está, de fato, perseguindo os objetivos a ele delegados.

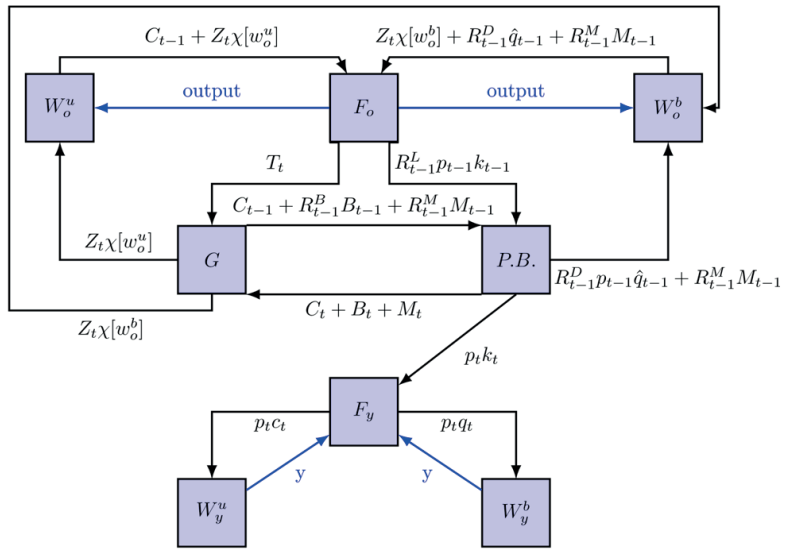
Por fim, o quarto cenário salienta que a substituição de depósitos à vista pela MEBC pode, na realidade, aumentar a instabilidade financeira. A existência de um ativo seguro (MEBC) facilmente adquirível pode diminuir ainda mais os recursos depositados nos bancos em tempos de estresse financeiro, o que tornaria a oferta de crédito volátil.[25] Outra alternativa possível é que o setor privado, ao se deparar com a insuficiência de fundos causada pela MEBC, buscaria substituir as atividades bancárias por atividades de *shadow banking*. Isso ocorreria, por exemplo, se houvesse uma demanda da sociedade por transformação de maturidade. Essa demanda pode ser motivada pela necessidade de provisão de liquidez (DIAMOND; DYBVIG, 1983) ou pela necessidade de disciplinar banqueiros oportunistas (DIAMOND; RAJAN, 2001).

4.1 MEBC em um Modelo de Gerações Sobrepostas

Andolfatto (2018) estuda o impacto da implantação de uma moeda digital (centralizada, por meio de contas) do banco central sobre os bancos privados utilizando uma abordagem de equilíbrio estacionário, em uma economia em que o setor bancário possui poder de mercado (monopólio). Para explicar os fluxos (de dinheiro, bens e trabalho), foram elaboradas as Figuras 3 e 4, que, respectivamente, mostram os fluxos nos períodos t e $t + 1$.

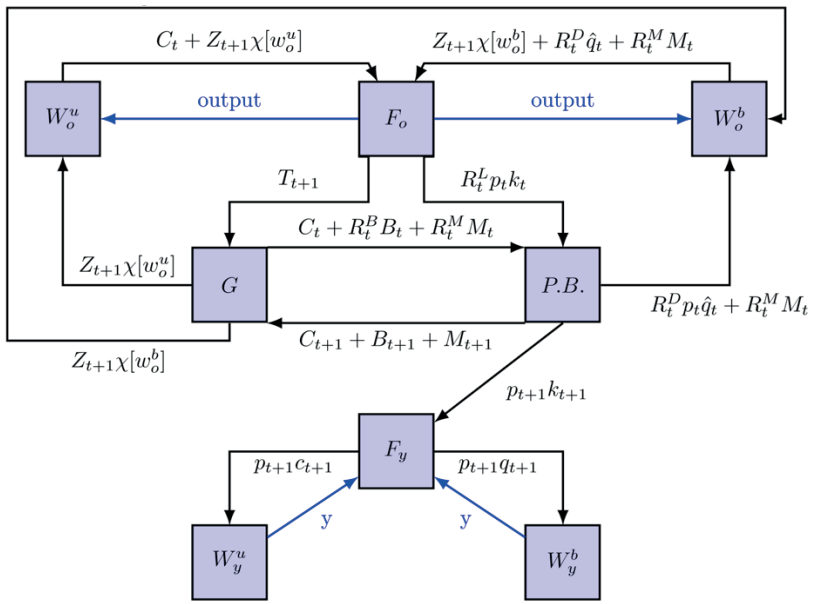
25 Uma qualificação desse argumento é que ele somente é válido se a troca entre MEBC e dinheiro/depósitos bancários for, garantidamente, realizada a uma taxa fixa. Caso o valor da troca possa ser decidido pela oferta e demanda dos bens, o mercado se equilibraria sem que todo o dinheiro fluísse para a MEBC (YANAGAWA; YAMAOKA, 2019).

Figura 3 – Fluxo de moeda e de bens no período t



Fonte: Elaboração dos autores, com base em Aldolfatto (2018).

Figura 4 – Fluxo de moedas e de bens no período $t + 1$



Fonte: Elaboração dos autores, com base em Aldolfatto (2018).

O modelo apresenta gerações sobrepostas e tanto jovens quanto idosos se dividem entre trabalhadores e firmas. Nas Figuras 3 e 4, os trabalhadores jovens são denotados W_y e os velhos são denominados W_o. Da mesma maneira, as firmas jovens são denotadas F_y e as velhas, F_o. Os trabalhadores jovens são dotados de uma unidade de tempo, na qual produzem y>0 unidades de bem,[26] sendo que y é heterogêneo dentro da população, obedecendo uma função distribuição acumulada exógena $G(a) \equiv Pr[y \leq a]$. As firmas jovens são dotadas de um projeto de investimento que requer K_t unidades de bem em t, que são transformadas em F(k_t) unidades de bem em $t + 1$, sendo F uma função que satisfaz as condições de Inada e é tal que F''<0<F'.

A dívida do governo (nas Figuras 3 e 4, denominado G) D_t se divide em três componentes: dinheiro em espécie (C_t), títulos de dívida (B_t) e moeda digital soberana (M_t). Portanto, a dívida do governo em um determinado período t pode ser escrita como $D_t = C_t + B_t + M_t$. Esses três componentes possuem taxas nominais de remuneração $R_t^C = 1$ para todo período t, que indica que a moeda em espécie não é remunerada, R_t^B e R_t^M, que são, respectivamente, as taxas nominais de retorno dos títulos do governo e da moeda digital soberana. As taxas dos títulos e da moeda digital soberana são os instrumentos de política monetária que o governo possui.

O governo necessita obedecer a seguinte restrição orçamentária intertemporal:

$$Z_t + (R_{t-1}^B - 1)B_{t-1} + (R_{t-1}^M - 1)M_{t-1} = T_t + (D_t - D_{t-1}) \quad (1)$$

em que Z_t são as transferências de renda aos trabalhadores e T_t são os impostos pagos pelas firmas, ambos configurando a política fiscal do governo. O lado esquerdo da equação 1 pode ser reescrito como:

$$Z_t + R_{t-1}^B B_{t-1} + R_{t-1}^M M_{t-1} - B_{t-1} - M_{t-1} \quad (2)$$

e o lado direito pode ser reescrito como:

$$T_t + (C_t + B_t + M_t - C_{t-1} - B_{t-1} - M_{t-1}) \quad (3)$$

Portanto, a equação 1 pode ser reescrita da seguinte forma:

26 Nota-se que y é a produtividade do trabalhador, de modo que será também seu salário real. Como os trabalhadores valorizam consumo apenas quando velhos, y será também sua poupança realizada quando jovens.

$$Z_t + R_{t-1}^B B_{t-1} + R_{t-1}^M M_{t-1} = T_t + (C_t + B_t + M_t - C_{t-1}) \quad (4)$$

Percebe-se que essa restrição é representada pelo fluxo apresentado na Figura 3. De fato, os fluxos de saída do governo, na Figura 3, são as transferências $Z_t\chi[W_o^b]$ e $Z_t\chi[W_o^u]$ para os trabalhadores[27] com e sem acesso ao sistema bancário, respectivamente, além do pagamento $R_{t-1}^B B_{t-1} + R_{t-1}^M M_{t-1} + C_{t-1}$ ao banco. Por outro lado, como receitas, o governo recebe T_t das firmas velhas e $C_t + B_t + M_t$ do banco (o banco está comprando a dívida do governo do período *t*).

Por hipótese, o governo segue as políticas de usar os impostos apenas para pagar o serviço da dívida e de usar as novas emissões de dívida para pagar as transferências aos trabalhadores. Portanto, o governo deve respeitar as restrições:

$$T_t = (R_{t-1}^B - 1)B_{t-1} + (R_{t-1}^M - 1)M_{t-1} \quad (5)$$

e

$$Z_t = D_t - D_{t-1} \quad (6)$$

Com essa especificação, apenas o gasto do governo com transferências pode causar inflação. Ainda, por hipótese, $Z_t = (\mu - 1)D_{t-1}$, de modo que $D_t = \mu D_{t-1}$.

As firmas jovens, em um dado período , escolhem para maximizar sua riqueza no período subsequente:

$$\hat{w}_{t+1} = F(k_t) - \frac{R_t^L k_t}{\Pi_{t+1}} - \tau_{t+1} \quad (7)$$

em que R_t^L é a taxa de juros nominal cobrada pelo banco para o empréstimo de k_t, p_t é o nível de preços em *t*, $\Pi_{t+1} \equiv \frac{p_{t+1}}{p_t}$ é a taxa de inflação em $t + 1$ e $\tau_t \equiv \frac{T_t}{p_t}$. A demanda por capital, $k_t = k\left(\frac{R_t^L}{\Pi_{t+1}}\right)$, é caracterizada por:

$$F'(k_t) = \frac{R_t^L}{\Pi_{t+1}} \quad (8)$$

27 $\chi[W_o^b]$ representa a medida de trabalhadores velhos com acesso ao sistema bancário e $\chi[W_o^u]$ representa a medida de trabalhadores velhos sem acesso ao sistema bancário. Essas transferências devem ser tais que $Z_t\chi[W_o^b] + Z_t\chi[W_o^u] = Z_t$. O acesso ao sistema bancário pelos trabalhadores será discutido a seguir.

Como , $F''(k_t) < 0, F'(k_t)$ é uma função decrescente em k_t e, portanto, a demanda por capital das firmas é decrescente em relação à taxa de juros real do empréstimo bancário, $r_t^L \equiv \frac{R_t^L}{\Pi_{t+1}}$.

Na Figura 3, a firma jovem F_y recebe $p_t k_t$ do banco para financiar seu projeto. Esse dinheiro é pago aos trabalhadores jovens em troca de produção de bens (y). A firma paga os trabalhadores com acesso ao sistema bancário depositando um total de $p_t q_t$ em suas contas bancárias e paga aos trabalhadores sem acesso um total de $p_t c_t$ via dinheiro em espécie.

No período seguinte (Figura 4), as firmas vendem sua produção para os trabalhadores que agora estão velhos e gastam tanto as transferências governamentais quanto suas economias do período anterior nos bens. Com esse dinheiro, a firma paga tributos para o governo (T_{t+1}) e repaga o empréstimo ao banco ($R_t^L p_t k_t$). Esse fluxo pode ser observado na equação 7 ao se multiplicar essa equação por p_{t+1}. O primeiro termo do lado direito da equação multiplicada, $p_{t+1}F(k_t)$, será igual ao valor pago pelos consumidores às firmas devido à condição de *market-clearing* no mercado de bens.

Ao contrário das firmas, que são todas bancarizadas por hipótese, um trabalhador jovem com habilidade y, em um período t, deve optar por abrir ou não uma conta no sistema bancário. Se optar por não ter acesso ao sistema bancário, o trabalhador incorre em um custo de $(1-\theta)y$, em que $0 \leq \theta < 1$, de esforço para manter a salvo y unidades reais de dinheiro em espécie. O *pay-off* esperado do trabalhador, caso opte por não entrar no sistema bancário, é:

$$w_{t+1}^u = \frac{y}{\Pi_{t+1}} - \frac{(1-\theta)y}{\Pi_{t+1}} + z_{t+1} = \frac{\theta y}{\Pi_{t+1}} + z_{t+1} \tag{9}$$

em que $z_t \equiv \frac{Z_t}{p_t}$.

Para abrir uma conta, o trabalhador incorre em um custo ϕ, que pode, por exemplo, representar o tempo perdido para abrir a conta. O acesso ao sistema bancário permite ao trabalhador ser remunerado por seus depósitos. Caso os mantenha no sistema bancário privado, será remunerado pela taxa R_t^D , e caso os mantenha no banco central (na forma de moeda digital soberana), será remunerado pela taxa R_t^M . A decisão entre onde manter seu dinheiro eletrônico depende exclusivamente da competição entre as taxas de remuneração. Portanto, o trabalhador optará pelo sistema que oferecer maior remuneração. O *pay-off* esperado do trabalhador, caso opte por entrar no sistema bancário, é:

$$w_{t+1}^{b} = \frac{R_t y}{\Pi_{t+1}} - \frac{\phi}{\Pi_{t+1}} + z_{t+1} = \frac{R_t y - \phi}{\Pi_{t+1}} + z_{t+1} \tag{10}$$

em que $R_t \equiv max\{R_t^D, R_t^M\}$.

Haverá um trabalhador tipo $\hat{y}$ indiferente entre abrir uma conta no sistema bancário ou não se $\theta\hat{y} = R_t\hat{y} - \phi$. É simples notar que, para uma dada taxa R_t, é possível calcular o tipo indiferente:

$$\hat{y}(R_t) = \frac{\phi}{R_t - \theta} \tag{11}$$

Para R_t fixo, um trabalhador com habilidade $y \geq \hat{y} = \frac{\phi}{R_t - \theta}$ optará por acessar o sistema financeiro, pois $y \geq \frac{\phi}{R_t - \theta} \rightarrow R_t y - \phi \geq \theta y$ e, portanto:

$$w_{t+1}^{b} = \frac{R_t y - \phi}{\Pi_{t+1}} + z_{t+1} \geq \frac{\theta y}{\Pi_{t+1}} + z_{t+1} = w_{t+1}^{u} \tag{12}$$

Além disso, nota-se que $\hat{y}$ é decrescente com relação a R_t e, portanto, quanto maior for a remuneração recebida pelo acesso ao sistema bancário, maior será a população bancarizada.

Os tipos $y<\hat{y}$, por outro lado, optarão por não acessar o sistema bancário. A demanda por encaixes reais de moeda em espécie, nessa economia, será:

$$c(R_t) = \int_0^{\hat{y}(R_t)} y dG(y) \tag{13}$$

Essa demanda não depende da inflação e é decrescente em R_t, pois um aumento na remuneração obtida ao acessar o sistema bancário implica diminuição do intervalo de integração $[0, \hat{y}(R_t)]$.

A demanda de encaixes reais de depósito pelos tipos $y \geq \hat{y}$ é dada por:

$$q(R_t) = \int_{\hat{y}(R_t)}^{\infty} y dG(y) \tag{14}$$

que é crescente em e não depende da inflação. Seja $y \equiv \int_0^{\infty} y dG(y)$ a demanda total por poupança nessa economia. Nota-se que $\boldsymbol{y} = c(R_t) + q(R_t)$ não é afetada por nenhuma taxa de juros. A taxa de juros obtida ao acessar o sistema bancário, R_t, simplesmente altera a distribuição de **y** entre depósitos bancários e moeda em espécie, mas não a poupança total.

No período *t* (Figura 3), os trabalhadores jovens sem acesso ao sistema bancário recebem, em termos nominais, $p_t c_t = C_t$ como pagamento por seu trabalho (*y*). No período seguinte (Figura 4), quando estão velhos, levam consigo essa quantidade de dinheiro e a utilizam, em conjunto com as transferências governamentais recebidas no período, para comprar bens da firma velha. Desse modo, sua utilidade é o valor de seu consumo, $\frac{y}{\Pi_{t+1}} + z_{t+1}$, menos o esforço para manter a posse de sua moeda, $\frac{(1-\theta)y}{\Pi_{t+1}}$.

Os trabalhadores jovens que optam por ter acesso ao sistema bancário, por sua vez, recebem, em termos nominais, $p_t q_t$ pelo seu trabalho no período *t*. Por terem acesso ao sistema bancário (via moeda digital soberana ou depósitos bancários), seu dinheiro é remunerado. Portanto, em $t + 1$, possuem, além das transferências governamentais, $R_t^D \hat{q}_t + R_t^M M_t$ para comprar bens da firma, em que $\hat{q}_t$ é a quantidade de moeda mantida na forma de depósitos bancários e M_t, a quantidade de moeda mantida na forma de moeda digital soberana. Novamente, sua utilidade é dada por quanto consomem, $\frac{R_t y}{\Pi_{t+1}} + z_{t+1}$, menos o custo para abrir a conta bancária, $\frac{\phi}{\Pi_{t+1}}$.

O setor bancário, no modelo, é caracterizado por ser um monopólio. O balanço patrimonial do banco possui reservas bancárias e empréstimos como ativos e os depósitos como passivo. Essa estrutura, portanto, impõe a restrição de que:

$$B_t + p_t k_t = p_t \hat{q}_t \tag{15}$$

isto é, que os ativos igualam o passivo. Uma dada estrutura de balanço patrimonial leva o banco a ter, como lucro esperado:

$$V_{t+1} = R_t^B B_t + R_t^L p_t k_t - R_t^D p_t \hat{q}_t \tag{16}$$

No período *t* (Figura 3), o banco (*P.B.*) empresta $p_t k_t$ à firma jovem e recebe o pagamento $R_t^L p_t k_t$ no período posterior. O trabalhador jovem com acesso ao sistema bancário optará entre manter seu dinheiro em depósitos bancários (remuneração $R_t^D p_t \hat{q}_t$ em $t + 1$) ou em moeda digital soberana (remuneração $R_t^M M_t$). A remuneração da moeda digital soberana, caso exista, é transferida do governo para o banco e deste para os trabalhadores, de modo que essa remuneração se cancela no fluxo da Figura 4 e tais valores não entram no lucro do banco.

A descrição da interação entre o banco privado e o governo é relativamente trabalhosa. Nota-se que, em *t*, o banco comprou toda a dívida governamental $C_t + B_t + M_t$. No período seguinte, o governo recomprará toda essa dívida, pagando inclusive os juros, totalizando $C_t + R_t^B B_t + R_t^M M_t$. Percebe-se que o dinheiro em espécie se cancela, de forma que não afeta o lucro do banco. Com relação

aos títulos, apenas o pagamento de juros afeta o banco, de modo que o lucro esperado é dado por suas receitas, $R_t^L p_t k_t + R_t^B B_t$, menos suas despesas, $R_t^D p_t \hat{q}_t$.

Combinando-se as equações 15 e 16, é possível caracterizar o lucro esperado do banco como:

$$V_{t+1} = R_t^B p_t \hat{q}_t - R_t^D p_t \hat{q}_t + R_t^L p_t k_t - R_t^B p_t k_t \tag{17}$$

É possível interpretar a equação 17 da seguinte forma: os dois primeiros termos mostram qual seria o lucro do banco caso atuasse com 100% de reservas; os dois últimos termos mostram o lucro adicional que o banco recebe por não atuar com 100% de reservas, ou seja, retirando uma parte $p_t k_t$ das reservas mantidas junto ao banco central e emprestando-a para as firmas.

Ainda, é possível reescrever o lucro esperado como:

$$V_{t+1} = [R_t^L - R_t^B] p_t k \left(\frac{R_t^L}{\Pi_{t+1}} \right) + [R_t^B - R_t^D] p_t \hat{q}(R_t^D) \tag{18}$$

em que fica explícito o fato de a demanda por capital ser determinada pela firma por meio da função $k_t = k\left(\frac{R_t^L}{\Pi_{t+1}}\right)$, caracterizada pela equação 8, e o fato de a demanda por depósitos depender da taxa de juros paga aos depositantes. Essa dependência é da seguinte forma:

$$\hat{q}(R_t^D) = \begin{cases} q(R_t^D), R_t^D \geq R_t^M \\ 0, caso\ contrário \end{cases} \tag{19}$$

em que $q(R_t^D)$ é dado pela equação 14. As variáveis que o banco escolhe para otimizar seu lucro são a taxa de empréstimo R_t^L e a taxa paga pelos depósitos R_t^D. A política monetária do governo (R_t^B e R_t^M) e o comportamento dos depositantes definido pela equação 19 são considerados dados para o banco. Nota-se que não há interação entre as taxas R_t^L e R_t^D na equação 18. Isso implica que a definição das taxas ocorrerá de forma independente.

Suponha-se que a remuneração da moeda digital soberana, R_t^M, seja tal que não afete a decisão ótima do banco. Em um caso limite, pode-se supor a não existência da moeda digital soberana. Defina-se X_t como a taxa de remuneração dos depósitos que maximiza o lucro do banco. Nesse caso, partindo-se da equação 18 e derivando-a com relação à taxa de remuneração do depósito bancário, X_t deve satisfazer:

$$[R_t^B - X_t] q'(X_t) = q(X_t) \tag{20}$$

Ou seja, ao escolher X_t, o banco maximiza seu lucro no ponto em que a diminuição do lucro causada por um aumento incremental da taxa, $q(X_t)$, é igual ao aumento da receita $[R_t^B - X_t]q'(X_t)$, em que $q'(X_t)$ é o aumento na quantidade de depósitos e $R_t^B - X_t$ é o *spread* de taxas que remunera o banco ao captar mais depósitos e guardá-los no banco central. A taxa de remuneração dos depósitos que maximiza o lucro, X_t, definida pela equação 20, pode ser reescrita como:

$$X_t = \left[\frac{\eta(X_t)}{1+\eta(X_t)}\right] R_t^B \tag{21}$$

em que $\eta(X_t) \equiv X_t \dfrac{q'(X_t)}{q(X_t)}$.

Caracterizada a escolha ótima da taxa de remuneração dos depósitos à vista, suponha-se agora que o banco central implemente uma moeda digital soberana. No caso em que a política monetária do governo seja tal que $X_t > R_t^M$, a escolha ótima do banco será $R_t^D = X_t < R_t^B$. Nota-se que, nesse caso, a criação da moeda digital soberana não impactou nenhuma escolha na economia.

Por outro lado, se a política monetária for tal que $R_t^B > R_t^M > X_t$, o banco escolherá $R_t^D = R_t^M < R_t^B$. Para ver isso, nota-se que, na equação 18, enquanto $R_t^B > R_t^D$, aumentar a taxa de remuneração dos depósitos é de interesse do banco se isso implicar também em aumento do número de depositantes. Pela equação 19, se $R_t^D < R_t^M$, $q(R_t^D) = 0$, o que zera o segundo termo da equação 18. No entanto, se $R_t^D = R_t^M < R_t^B$, $q(R_t^D) = q(R_t^D) > 0$, o que torna o segundo termo da equação 18 positivo, já que $R_t^B - R_t^D > 0$.

Logo, nesse caso a criação da moeda digital soberana afetou a tomada de decisões na economia. Embora os trabalhadores ainda optem por manter seus depósitos no banco, a taxa R_t^D escolhida pelo banco foi mais alta, o que implicará que uma maior parcela da população acessará o sistema bancário, conforme mostrado na equação 11.

Agora, suponha-se que a política monetária seja tal que $R_t^M > R_t^B$. Como o custo para captação de depósitos R_t^D deve ser maior ou igual a R_t^M para que o banco capte recursos via depósito à vista, ele optará por não captar depósitos com essa configuração de política monetária. Como $R_t^B - R_t^D < 0$, o segundo termo da equação 18 seria negativo e o lucro do banco diminuiria se houvesse a captação. Uma hipótese importante para esse resultado é que o banco não pode investir a moeda captada via depósito à vista em moeda digital soberana. Isto é, o banco atua apenas como um intermediário entre o banco central e os depositantes com relação à moeda digital soberana, e o único meio pelo qual ele consegue acessar o balanço do banco central de forma eletrônica é adquirindo títulos públicos (reserva bancária).

A outra variável de escolha do banco é a taxa de juros cobrada pelo empréstimo, R_t^L. A partir da equação 18, a escolha dessa taxa que maximiza o lucro do banco satisfaz:

$$\frac{-[R_t^L - R_t^B]}{\Pi_{t+1}} k'\left(\frac{R_t^L}{\Pi_{t+1}}\right) = k\left(\frac{R_t^L}{\Pi_{t+1}}\right) \tag{22}$$

Definindo-se que $r_t^L \equiv \frac{R_t^L}{\Pi_{t+1}}$ e $r_t^B \equiv \frac{R_t^B}{\Pi_{t+1}}$, é possível reescrever essa condição em termos das taxas reais:

$$-[r_t^L - r_t^B]k'(r_t^L) = k(r_t^L) \tag{23}$$

Essa condição deve ser interpretada da mesma forma que a equação 20. Isto é, a taxa real de empréstimo r_t^L que maximiza o lucro do banco é tal que, dado um incremento marginal dessa taxa, o aumento no lucro, dado pelo nível dos empréstimos $k(r_t^L)$, compensa a diminuição nos lucros causada pela queda no nível dos empréstimos, de magnitude $k'(r_t^L)$, sobre a qual o banco lucra com a diferença das taxas $r_t^L - r_t^B$.

Sem perda de generalidade, considera-se a classe de funções de retornos de investimentos que satisfazem $F'(k)k = \alpha F(k)$ com $0 < \alpha < 1$. Isso implica que:

$$r_t^L = \frac{1}{\alpha} r_t^B \tag{24}$$

isto é, a taxa de juros real (nominal) dos empréstimos obedece a uma regra de *markup* com relação à taxa real (nominal) de remuneração dos títulos públicos.[28]

4.1.1 Equilíbrio Estacionário sem Moeda Digital Soberana

O conceito de equilíbrio adotado por Andolfatto (2018) é o de equilíbrio estacionário, no qual todas as variáveis reais, razões e taxas permanecem constantes. É assumida a existência, unicidade e estabilidade desse equilíbrio.[29]

Será considerada, inicialmente, a não existência de uma moeda digital soberana (ou, de forma equivalente, $R_t^B > X_t > R_t^M$). Define-se $d_t \equiv \frac{D_t}{p_t}$, o valor real da dívida governamental. No equilíbrio estacionário, $d_t = d$. Desse modo:

---

28 Para ver isso, basta derivar $F'(k)k = \alpha F(k)$ e $F'(k_t) = \frac{R_t^L}{\Pi_{t+1}}$ com relação a r_t^L e substituir a segunda na primeira.

29 Conforme Andolfatto (2018), a existência normalmente é fácil de ser atingida, enquanto a unicidade e a estabilidade são mostradas por Andolfatto e Martin (2018) em um ambiente similar ao apresentado.

$$\frac{D_t}{p_t} = d_t = d_{t+1} = \frac{D_{t+1}}{p_{t+1}} \tag{25}$$

Como $D_{t+1} = \mu D_t$, segue que:

$$\Pi_{t+1} = \frac{p_{t+1}}{p_t} = \mu, \forall t \tag{26}$$

ou seja, a inflação no equilíbrio estacionário é igual à taxa de crescimento da dívida nominal do governo.

A taxa de juros nominal cobrada pelo empréstimo será dada por $R^L = \frac{1}{\alpha} R^B$. Ela é crescente com relação à taxa de remuneração dos títulos governamentais, o que implica que o nível de investimento é decrescente em relação a R^B. A taxa de juros real será, por sua vez, $r^L = \frac{R^L}{\mu}$. Isto é, a política fiscal (em particular, a definição das transferências aos trabalhadores velhos, Z_t) influencia a taxa de juros real, mas não a nominal. Nota-se que um aumento na meta de inflação μ diminui a taxa de juros real r^L, portanto o nível de investimento é crescente com relação à taxa de inflação.

Para uma dada taxa real de empréstimo, r^L, as firmas desejam tomar emprestado, em termos reais, $k(r^L)$ e, em termos nominais, $p_t k(r^L)$, que é o total de *inside money* existente na economia. A oferta monetária total é dada por $C_t + B_t + p_t k(r^L) = D_t + p_t k(r^L)$, em que a dívida total do governo, D_t, corresponde à base monetária. Para todo período t, deve valer a condição de *market-clearing*:

$$D_t + p_t k(r^L) = p_t \boldsymbol{y} \tag{27}$$

em que $\boldsymbol{y} \equiv \int_0^\infty y dG(y)$ é a produção total de bens. O nível de preços em um determinado período t pode ser escrito, a partir da equação 27, como:

$$p_t = \left[\frac{1}{\boldsymbol{y} - k(r^L)}\right] D_t \tag{28}$$

Portanto, o nível de preços em um período t depende do nível da dívida governamental, D_t, e da demanda por encaixes reais de moeda *outside*, $d(r^L) = \boldsymbol{y} - k(r^L)$.

Um aumento da taxa de remuneração nominal dos títulos públicos, R^B, possui efeito deflacionário. De fato, um aumento em R^B eleva a taxa real de remuneração dos títulos públicos, r^B, aumentando a taxa de juros real dos empréstimos, r^L, o que diminui o nível dos empréstimos, $k(r^L)$, provocando uma diminuição no nível dos preços.

Ainda, um aumento em R^B provoca um aumento na taxa de remuneração dos depósitos bancários, R^D, conforme pode ser notado pela equação 21. Por sua vez, esse aumento causa uma expansão dos depósitos bancários em detrimento da manutenção da poupança em moeda em espécie. Ou seja, o acesso dos trabalhadores ao sistema bancário será maior.

Seja que $v_{t+1} \equiv \frac{V_{t+1}}{p_{t+1}}$ é o lucro real do banco no período $t + 1$. A partir da equação 18, é possível escrevê-lo como:

$$v(R^B, \mu) = \left[\frac{R^L - R^B}{\mu}\right] k\left(\frac{R^L}{\mu}\right) + \left[\frac{R^B - R^D}{\mu}\right] q(R^D) \tag{29}$$

Fica explícita a dependência de R^L e de R^D com relação a R^B. Seja $b_t \equiv \frac{B_t}{p_t}$ o valor real das reservas bancárias. Pelo teorema do envelope, o efeito no lucro do banco causado por um aumento em R^B depende do sinal de $b(R^B, \mu) = q(R^D) - k\left(\frac{R^L}{\mu}\right)$. Portanto, se as reservas bancárias são positivas, um aumento em R^B aumenta o lucro do banco. Por outro lado, se as reservas bancárias são negativas (isto é, o banco toma emprestado do banco central), um aumento em R^B diminui o lucro do banco.

Para cobrir o serviço da dívida, o governo precisará coletar impostos no montante real de:

$$\tau = \frac{(R^B - 1)b(R^B, \mu)}{\mu} \tag{30}$$

Com isso, o bem-estar das firmas no estado estacionário, a partir da equação 7, é:

$$\hat{w} = F(k) - \frac{R^L k}{\mu} - \tau = (1 - \alpha)F(k) - \tau \tag{31}$$

usando-se $r^L = F'(k)$ e $\alpha F(k) = F'(k)k$.

Lembrando-se que $z_t \equiv \frac{Z_t}{p_t}$, partindo-se da equação 6 e considerando-se a equação 27, tem-se que:

$$z_t = \frac{D_t - D_{t-1}}{p_t} = \frac{D_t}{p_t} - \frac{D_{t-1}}{\mu p_{t-1}} = d(r_t^L) - \frac{d_{t-1}(r_{t-1}^L)}{\mu} \tag{32}$$

No equilíbrio estacionário,

$$z = \left[1 - \frac{1}{\mu}\right] d(r^L) \tag{33}$$

Portanto, o bem-estar no estado estacionário dos trabalhadores sem acesso ao sistema bancário é:

$$w^u(y) = \frac{\theta y}{\mu} + z \tag{34}$$

enquanto o dos trabalhadores com acesso ao sistema bancário é:

$$w^b(y) = \left[r^D y - \frac{\phi}{\mu}\right] + z \tag{35}$$

4.1.2 Equilíbrio Estacionário com Moeda Digital Soberana

A emissão de uma moeda digital soberana apenas afetará as escolhas nessa economia se $R_t^M > X_t$, ou seja, se a taxa de remuneração da moeda digital for maior que a taxa de juros dos depósitos que otimiza o lucro do banco. A taxa de remuneração da moeda digital pode ser maior ou menor que a taxa de remuneração dos títulos públicos, o que traz diferentes consequências à economia.

No caso em que $R^M < R^B$, a escolha ótima do banco com relação à taxa de remuneração dos depósitos é igualá-la à taxa de remuneração da moeda digital soberana, $R^D = R^M$. Nota-se que a diferença positiva entre R^B e R^D torna lucrativo para o banco captar depósitos e mantê-los como reserva bancária. Como a quantidade de moeda digital soberana nas mãos do público será M_t=0 para todo t, não há implicações orçamentárias para o governo por causa dessa nova moeda.

Com o aumento da taxa de remuneração dos depósitos, R^D, a quantidade de trabalhadores com acesso ao sistema bancário aumentará, assim como o bem-estar desses trabalhadores, pois o seu dinheiro depositado renderá mais, possibilitando maior consumo quando forem velhos. O bem-estar dos trabalhadores que continuam sem acesso ao sistema bancário não será alterado.

Como consequência, uma maior parte da dívida governamental, $D_t = C_t + B_t + M_t$, será alocada aos títulos governamentais em detrimento do dinheiro em espécie. Isso aumentará a necessidade de tributação para pagar o serviço da dívida, o que diminuirá o bem-estar das empresas. Além disso, o banco verá o seu lucro diminuir, já que a margem de lucro nos depósitos, $R^B - R^D$, será menor e não será compensada pelo aumento na quantidade de depósitos, pois o banco não escolherá $R^D = X_t$.

A taxa de juros dos empréstimos, R^L, não é afetada por R^M, como pode ser visto pela equação 24. Portanto, o nível de empréstimo demandado pelas firmas não será alterado. Como conclusão, tem-se que o nível de intermediação bancária aumenta, já que há aumento dos depósitos e manutenção dos empréstimos.

O nível de preços não é alterado, como pode ser observado a partir da equação 28. O nível de preços depende apenas da diferença entre poupança e empréstimos (demanda por encaixes reais de moeda "*outside*") e do nível da dívida governamental, e nenhuma dessas variáveis será alterada em relação ao caso sem moeda digital soberana.

Agora, considerando-se o segundo caso, $R^M > R^B$, percebe-se que, para o banco, não faz sentido atrair depósitos oferecendo $R^D = R^M > R^B$, pois isso diminuiria seu lucro, como pode ser observado na equação 18. Portanto, todos os trabalhadores que optarem por acessar o sistema bancário o farão via moeda digital soberana, o que implica que $M_t = p_t q(R^M)$.

Como as taxas R^D e R^M não afetam a taxa de empréstimo, o banco continua a emprestar $p_t k(r^L)$ para as firmas. Pela restrição imposta ao balanço patrimonial do banco, conforme a equação 15, a quantidade de títulos públicos em seu balanço deve ser $B_t = -p_t k(r^L)$, ou seja, o banco toma emprestado do banco central à taxa de R^B. O empréstimo às firmas jovens sairá do banco ao final do período e fluirá para os trabalhadores sem acesso ao sistema bancário via dinheiro em espécie e, para os com acesso, via depósito em moeda digital soberana.

A dívida governamental pode ser reescrita como:

$$D_t = C_t + M_t + B_t = p_t c(R^M) + p_t q(R^M) - p_t k(r^L) \tag{36}$$

Essa expressão pode ser reescrita como $D_t + p_t k(r^L) = p_t \boldsymbol{y}$, isto é, a condição de *market-clearing* mostrada na equação 27. Um aumento na remuneração da moeda digital soberana, portanto, afeta a razão entre moeda digital soberana e dinheiro em espécie, mas não afeta a habilidade do banco em emprestar caso ele possa tomar emprestado do banco central pagando, como remuneração, R^B. Isso afetará o governo em sua política fiscal. A partir da equação 5, e considerando-se as quantidades de títulos e de moeda digital soberana existentes no balanço do banco central, o imposto real a ser cobrado das (ou repassado para as) empresas será:

$$\tau = \frac{1}{\mu}\left[(R^B - 1)\left(-k\left(\frac{R^L}{\mu}\right)\right) + (R^M - 1)q(R^M)\right] \tag{37}$$

No entanto, a hipótese de que o banco pode tomar emprestado à taxa R^B pode ser forte. Caso o banco não possa tomar emprestado via reserva no banco central, é restrito por $B_t \geq 0$.

Isso forçará o banco a captar depósitos $(p_t \hat{q}_t)$ em quantidade maior ou igual à quantidade de empréstimos que concedem, $p_t k(r^L)$, para obedecer a restrição imposta ao seu balanço patrimonial pela equação 15. Para isso, é necessário que o

banco remunere os depósitos com a mesma taxa da moeda digital soberana, isto é, $R^D = R^M > R^B$. O lucro do banco será, nesse caso específico:

$$V_{t+1} = [R^L - R^M]p_t k\left(\frac{R_t^L}{\mu}\right) \tag{38}$$

É importante ressaltar que, somente nesse caso, a taxa de juros dos empréstimos dependerá da taxa de remuneração da moeda digital soberana.

4.1.3 Conclusões a partir do Modelo

Com o modelo apresentado por Andolfatto (2018) é possível analisar diversas afirmações a respeito da implementação de uma MEBC.

Muitos autores como Cecchetti e Schoenholtz (2017) e Ricks, Crawford e Menand (2018) afirmam que a emissão de uma MEBC levará a uma expansão do balanço do banco central. No entanto, caso $R^B > R^M > X_t$, a MEBC não seria demandada e, portanto, não haveria expansão do balanço, embora provocaria uma alteração nas taxas de remuneração dos depósitos à vista. Entende-se que o banco, ao aumentar a taxa de remuneração, não permitirá um grande fluxo de depósitos à vista para a MEBC, de modo que não haverá, nesse caso, desintermediação financeira, conforme apontado por Cecchetti e Schoenholtz (2017).

Outro argumento é que a emissão de uma MEBC poderia aumentar os custos dos bancos privados e diminuir seus ganhos de monopólio (CECCHETTI; SCHOENHOLTZ, 2017). No entanto, o modelo desenvolvido mostra que a concessão de empréstimos é um negócio separado da captação de depósitos à vista. Desse modo, supondo-se que o banco possa tomar emprestado via reservas bancárias, ele continuará com a possibilidade de emprestar e a taxa de juros dos empréstimos não será alterada, pois depende apenas da taxa de juros dos títulos públicos. Por outro lado, é possível afirmar, baseando-se no modelo, que os lucros de monopólio do banco diminuirão.

4.2 MEBC no Modelo de Lagos e Wright (2005)

Keister e Sanches (2018) estudam os efeitos da existência de uma MEBC usando o modelo de Lagos e Wright (2005), um dos modelos cujo uso é bastante disseminado na literatura de economia monetária. Os autores apresentam resultados sobre como a emissão de uma MEBC pode afetar o sistema bancário.

É considerada a criação de três tipos de MEBC: a) se a moeda só pode ser usada em trocas que requerem uso de moeda em espécie (busca por anonimidade); b) se a moeda só pode ser usada em trocas que requerem uso de depósitos à

vista (quando comprador e vendedor não estão fisicamente no mesmo local, por exemplo, mas não se importam com anonimidade); e c) se a MEBC pode ser usada nas duas situações descritas anteriormente.[30]

A emissão de uma moeda em que os usuários podem utilizar pseudônimos em busca de privacidade não apresenta efeito algum caso sua taxa de remuneração seja não positiva. No caso em que é positiva, aumentará a quantidade de transações que antes poderiam ser realizadas somente com moeda em espécie e também o bem-estar, mas não afetará o nível de investimentos.

Uma MEBC que pode ser utilizada em substituição aos depósitos bancários será demandada somente se a sua taxa de remuneração for pelo menos igual à taxa de remuneração dos depósitos bancários que será praticada em equilíbrio no modelo sem moeda digital. Como efeitos dessa utilização, é possível citar o aumento de produção dos bens que podem ser trocados por depósitos à vista e o aumento da taxa real de remuneração dos depósitos, além da desintermediação dos bancos (queda na quantidade de dinheiro depositada, que leva à diminuição do investimento).

Por fim, a MEBC que pode ser utilizada nos dois tipos terá o mesmo efeito que a moeda que substitui apenas depósitos à vista se a sua remuneração for menor ou igual a zero. Se a remuneração for maior que a dos depósitos e maior que zero, ela será utilizada para os dois tipos de troca e o bem-estar será superior ao caso em que a moeda pode ser utilizada apenas para substituir depósitos.

Conforme o resultado geral do estudo de Keister e Sanches (2018), a introdução de uma MEBC não pode diminuir o bem-estar, já que a sua remuneração pode ser ajustada de modo que o seu uso seja mínimo, não afetando o bem-estar. Além disso, nota-se a existência de um *trade-off* a ser balanceado pela escolha da taxa de remuneração da MEBC. Se, por um lado, a moeda aumenta a eficiência das trocas, por outro retira depósitos do sistema bancário, aumentando o custo de financiamento dos bancos.

Comparando-se os efeitos apresentados pela introdução de uma moeda que substitui depósitos à vista com o resultado apresentado por Andolfatto (2018), é possível notar que se diferenciam em alguns pontos. No modelo de Keister e Sanches (2018), é possível a coexistência de saldos em depósito à vista e na MEBC. Embora a taxa de remuneração dos depósitos reaja à concorrência da MEBC, o aumento na taxa não é suficiente para que não ocorra desintermediação financeira. Para Andolfatto (2018), por outro lado, haverá apenas saldos em depósitos à vista ou em MEBC. A reação do banco de aumentar a taxa de depósito é suficiente para que não haja desintermediação financeira, mas somente se a taxa de remuneração da MEBC for menor que a taxa de juros dos títulos públicos.

30 Os autores admitem que o terceiro tipo de MEBC pode ser inviável, porém testam a hipótese no modelo para descobrir os efeitos.

5 Considerações Finais

Este trabalho buscou definir, de maneira clara, que uma criptomoeda é uma moeda digital que prescinde da utilização de monitoramento. Ou seja, embora existam agentes que contribuam para a transmissão da moeda entre os usuários (por exemplo, mineradores), o protocolo da moeda é desenhado de modo que não haja a necessidade de monitoramento dos agentes. Por isso, eles não são considerados intermediários no processo de manutenção do *ledger* da criptomoeda (transmissão de valores).

Definindo-se de forma clara os termos criptomoeda e intermediários, conclui-se que têm sido utilizados de maneira equivocada. Em particular, a aplicação do sistema permissionado de gerenciamento de moeda digital é incompatível com a utilização do termo criptomoeda, haja vista a necessidade de monitoramento dos intermediários responsáveis pela manutenção do *ledger* nesse tipo de sistema.

Além disso, denominou-se criptomoeda soberana uma moeda eletrônica, de acesso universal, emitida pelo banco central e com transmissão descentralizada (*peer-to-peer*, sem necessidade de monitoramento). Em contraposição a esse termo, denominou-se moeda digital soberana uma moeda eletrônica, de acesso universal, emitida pelo banco central, porém com transmissão centralizada (com necessidade de monitoramento). A união desses dois conceitos foi denominada MEBC.

Por fim, foi discutido um modelo simples no qual há a inclusão de uma moeda digital soberana em uma economia na qual o setor bancário possui poder de monopólio. No modelo, a moeda digital soberana afeta as decisões na economia apenas se sua taxa de remuneração for maior que a taxa ótima de remuneração dos depósitos bancários.

No caso em que a taxa da moeda digital é menor que a taxa de remuneração dos títulos públicos, o banco competirá com a moeda digital soberana, igualando a taxa de depósitos à taxa da MEBC. Desse modo, não há desintermediação bancária, como é previsto na literatura, a qual não considera a capacidade do banco de aumentar suas taxas em resposta à política monetária do banco central. Como consequência desse aumento, mais pessoas optarão pela abertura de contas, o que diminui a população sem acesso a serviços bancários.

No caso em que a taxa da moeda digital é maior que a taxa de remuneração dos títulos públicos, o banco privado não receberá depósitos, pois isso diminuiria seu lucro. Portanto, o acesso ao sistema bancário se dará apenas por meio da moeda digital soberana. O banco poderá manter a concessão de empréstimo às firmas caso tenha a possibilidade de se financiar com reservas bancárias. Portanto, o efeito que a emissão de uma moeda digital soberana causará ao sistema bancário depende da relação entre as taxas de remuneração dos depósitos bancários, dos títulos públicos e da moeda digital soberana.

Referências

ALI, R.; BARRDEAR, J.; CLEWS, R.; SOUTHGATE, J. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, v. 54, n. 3, p. 262–275, 2014.

ANDOLFATTO, D. Assessing the impact of central bank digital currency on private banks. *FRB St. Louis Working Paper*, v. 2018, n. 25, 2018.

ANDOLFATTO, D. Fedcoin: on the desirability of a government cryptocurrency. *MacroMania*, 2015a. Disponível em: http://andolfatto.blogspot.com/2015/02/ fedcoin-on-desirability-of-government.html. Acesso em: 05 abr. 2018.

ANDOLFATTO, D. Money and payments, or how we move marbles. *MacroMania*, 2015b. Disponível em: http://andolfatto.blogspot.com/2015/02/money-and-payments-or-how-we-move. html. Acesso em: 08 abr. 2018.

ANDOLFATTO, D.; MARTIN, F. M. Monetary policy and liquid government debt. *Journal of Economic Dynamics and Control*, v. 89, p. 183–199, 2018.

ANTONOPOULOS, A. M. *Mastering Bitcoin:* unlocking digital cryptocurrencies. Massachusetts: O'Reilly Media Inc., 2014.

ANTONOPOULOS, A. M. *Mastering Bitcoin: programming the open blockchain*. Massachusetts: O'Reilly Media Inc., 2017.

BAROSSI FILHO, M.; SZTAJN, R. Natureza jurídica da moeda e desafios da moeda virtual.

Revista Jurídica Luso-Brasileira, p. 1669–1690, 2015.

BECH, M. L.; GARRATT, R. Central bank cryptocurrencies. *BIS Quarterly Review*, 2017.

BERENTSEN, A.; SCHAR, F. The case for central bank electronic money and the non-case for central bank cryptocurrencies. *Federal Reserve Bank of St. Louis Review*, v. 100, n. 2, p. 97–106, 2018.

BERTOLAI, J. D.; OLIVEIRA, V. A. A. Criptomoedas e teoria monetária: uma introdução. *Revista Análise Econômica,* v.38, n. 76, p. 197-236, 2020.

BORDO, M. D.; LEVIN, A. T. Central bank digital currency and the future of monetary policy. Technical report, *National Bureau of Economic Research*, 2017.

BROWN, R. G. A simple explanation of how money moves around the banking system. *Thoughts on the future of finance*, 2013. Disponível em: https://gendal.me/2013/11/24/ a-simple-explanation-of-how-money-moves-around-the-banking-system/. Acesso em: 18 maio 2017.

CAVALCANTI, R. D. O.; WALLACE, N. Inside and outside money as alternative media of exchange. *Journal of Money, Credit and Banking*, pages 443–457, 1999a.

CAVALCANTI, R. D. O.; WALLACE, N. A model of private bank-note issue. *Review of Economic Dynamics*, v. 2, n. 1, p. 104–136, 1999b.

CAVALCANTI, R. D. O.; EROSA, A.; TEMZELIDES, T. Private money and reserve managementin a random-matching model. *Journal of Political Economy*, v. 107, n. 5, p. 929–945, 1999.

CECCHETTI, R. G.; SCHOENHOLTZ, K. L. Fintech, central banking and digital currency. *Money and Banking Blog*, 2017. Disponível em: https://www.moneyandbanking.com/commentary/2017/ 6/11/fintech-central-banking-and-digital-currency. Acesso em: 23 ago. 2018.

CHAPMAN, J.; GARRATT, R.; HENDRY, S.; McCORMACK, A.; McMAHON, W. Project jasper: are distributed wholesale payment systems feasible yet? *Financial System*, p. 59, 2017.

DANEZIS, G.; MEIKLEJOHN, S. Centrally banked cryptocurrencies. *arXiv preprint arXiv,* v. 1505.06895, 2015.

DIAMOND, D. W.; DYBVIG, P. H. Bank runs, deposit insurance, and liquidity. *Journal of Political Economy*, v. 91, n. 3, p. 401–419, 1983.

DIAMOND, D. W.; RAJAN, R. G. Liquidity risk, liquidity creation, and financial fragility: a theory of banking. *Journal of Political Economy*, v. 109, n. 2, p. 287-327, 2001.

DRISCOLL, S. How bitcoin works under the hood. *Imponderable things,* 2013. Disponível em: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood. html. Acesso em:12 jul. 2017.

HALABURDA, H.; SARVARY, M. *Beyond Bitcoin:* the economics of digital currencies. California: Palgrave Macmillan US, 2016. ISBN 9781137506429.

KAHN, C. M.; RIVADENEYRA, F.; WONG, R. Should the central bank issue e-money? Bank of Canada, 2018. SSRN 3271654.

KEISTER, T.; SANCHES, D. Should central banks issue digital currency? *Rutgers University* (Manuscript), 2018.

KETTERER, J. A.; ANDRADE, G. Digital central bank money and the unbundling of the banking function. Technical report, *Inter-American Development Bank*, 2016.

KONING, J. Fedcoin: a central bank-issued cryptocurrency. *R3 Report*, v. 15, 2016.

KUMHOF, M.; NOONE, C. Central bank digital currencies-design principles and balance sheet implications. *Working Paper*, 2018.

LAGOS, R.; WRIGHT, R. A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, v. 113, n.3, p. 463-484, 2005.

LO, S.; WANG, J. C. Bitcoin as money? *Current Policy Perspectives - Federal Reserve Bank of Boston*, 2014.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em 25 jul. 2017.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and cryptocurrency technologies:* a comprehensive introduction. New Jersey: Princeton University Press, 2016.

RICKS, M.; CRAWFORD, J.; MENAND, L. A public option for bank accounts (or central banking for all). *Vanderbilt Law Research Paper,* p. 18-33, 2018.

SCORER, S. Central bank digital currency: Dlt, or not dlt? that is the question. 2017. Disponível em: https://bankunderground.co.uk/2017/06/05/ central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/. Acesso em: 02 fev. 2018

STEVENS, A. Digital currencies: threats and opportunities for monetary policy. *Economic Review - National Bank of Belgium*, n. i, p. 79-92, jun. 2017.

TOBIN, J. Financial innovation and deregulation in perspective. *Bank of Japan Monetary and Economic Studies*, v. 3, n. 2, p. 19-29, 1985.

YANAGAWA, N.; YAMAOKA, H. Digital innovation, data revolution and central bank digital currency. Technical report, *Bank of Japan*, 2019.

Autor correspondente:

Jefferson Donizeti Pereira Bertolai
E-mail: jbertolai@fearp.usp.br

Recebido em: 25/04/2019.
Aceito em: 15/02/2021.