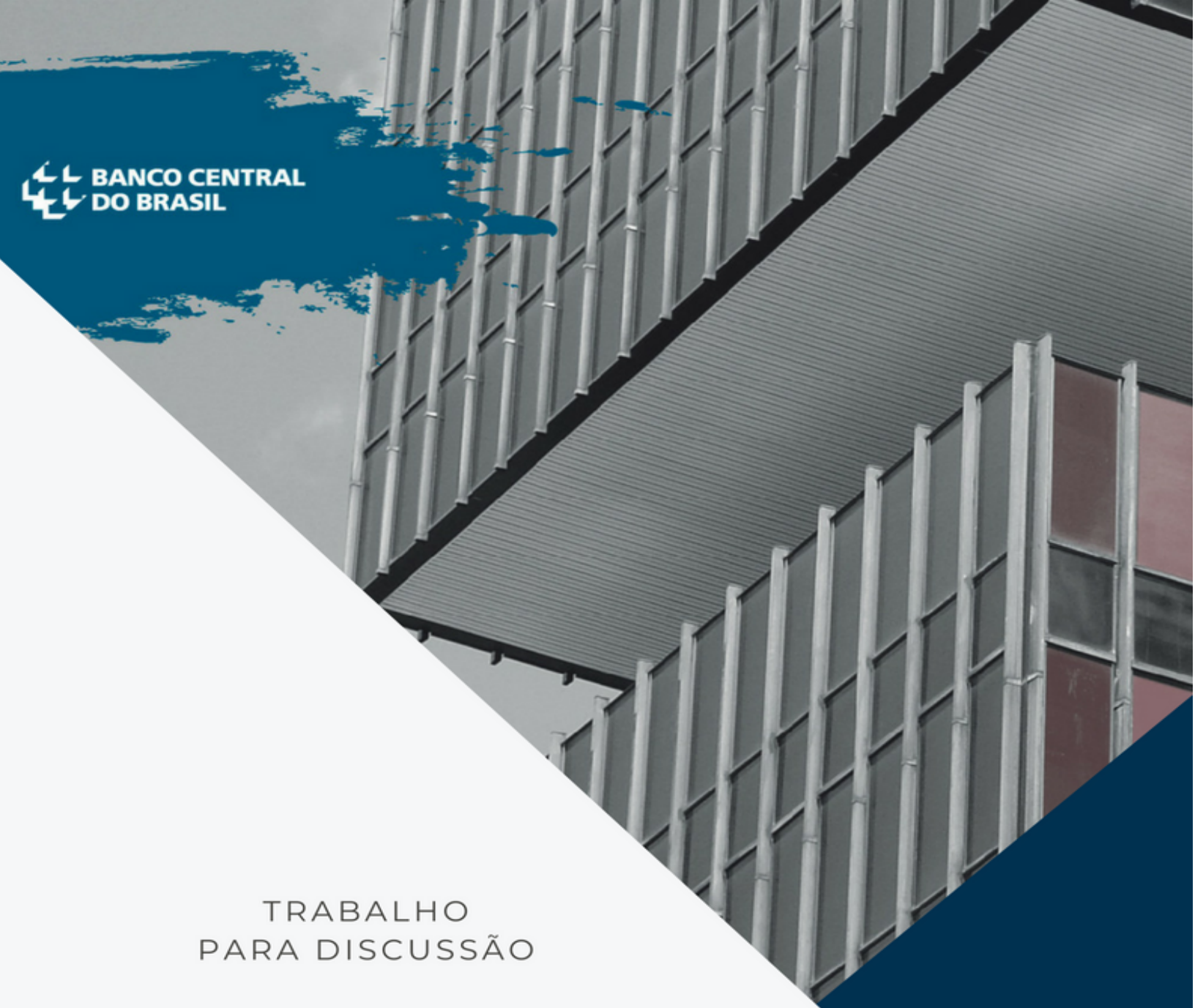


BANCO CENTRAL DO BRASIL

TRABALHO
PARA DISCUSSÃO

# O MEIO CIRCULANTE NA ERA DIGITAL

ALDÊNIO BURGOS & BRUNO BATAVIA

JULHO· 2018

**E-mails**
aldenio.burgos@bcb.gov.br
bruno.batavia@bcb.gov.br

**Autorizado pela: Diretora de Administração**
Carolina de Assis Barros



**Divisão de Atendimento ao Cidadão**
Banco Central do Brasil
Deati/Diate
SBS – Quadra 3 – Bloco B – Edifício-Sede – 2º subsolo
70074-900 Brasília – DF
DDG: 0800 9792345
Fax: (61) 3414-2553
Internet: http//www.bcb.gov.br/?FALECONOSCO

# Apresentação

Avanços tecnológicos notáveis têm rotineiramente impactado nosso mundo. A chamada transformação digital está redefinindo indústrias, tornando possíveis novos modelos de negócio e proporcionando oportunidades antes nunca imaginadas. Seu impacto, no entanto, não se limita aos negócios; já está mudando drasticamente como vivemos, trabalhamos e nos relacionamos um com o outro.

A digitalização tem o potencial de oferecer imensos benefícios para a sociedade e o meio ambiente, apresentando uma série de oportunidades e desafios para empresas e formuladores de políticas públicas.

Segundo estudo do Fórum Econômico Mundial [1], a digitalização tem o potencial de gerar, em termos financeiros, cerca de US$ 100 trilhões, na próxima década, para a indústria e a sociedade em geral. Entretanto, não há qualquer garantia de que seus benefícios serão capturados pela sociedade, pois diversas barreiras devem ainda ser superadas. Estas incluem arcabouços regulatórios desatualizados e complexos, lacunas de infraestrutura, falta de confiança pública em tecnologias e processos inovadores, bem como a carência de incentivos para a geração de valor social.

Neste espírito, sob a premissa de aporte à inovação, o presente estudo sobre desmaterialização do meio circulante pretende instigar a reflexão, ao analisar motivos e caminhos para uma eventual reinvenção do produto mais simbólico de um banco central: a sua moeda.

Quanto ao numerário em espécie, é forçoso reconhecer seus benefícios e imprescindibilidade na economia, em particular, para a população de mais baixa renda, para o qual o dinheiro emitido pelo Banco Central do Brasil é provavelmente o único meio de pagamento e reserva de valor que conseguem ter acesso.

Não obstante, o dinheiro físico tem sido alvo crescente de iniciativas que buscam redução do seu uso, em razão das conhecidas repercussões sobre seus custos e ônus para a sociedade - com segurança, bem como a preferência de uso para atividades criminosas de toda espécie, tais como: corrupção, lavagem de dinheiro e evasão fiscal. Ademais, quanto às moedas metálicas, estima-se que 30% deixem de circular por motivos diversos como perda, esquecimento e guarda por prazo indeterminado: o entesouramento.

Nesta conjuntura, em uma abordagem exploratória sobre a digitalização do papel-moeda, os autores procuram agregar valor, ao buscar soluções, trazendo ao conhecimento do leitor conceitos, arquiteturas, funcionalidades e tecnologias aplicáveis, bem como consolidando parte da experiência internacional no tema.

Assim, sob os auspícios de ambiente organizacional de saudável estímulo à reflexão e à inovação, trazemos ao conhecimento o presente estudo "Desmaterialização do Numerário", com o fito de contribuir com desenvolvimento do conhecimento e massa crítica sobre o assunto.

Rio de Janeiro e Brasília, 06 Julho de 2018.

Aldênio Burgos e Bruno Batavia

# 1 Introdução

A atual disponibilidade e onipresença de dispositivos eletrônicos e redes de alta velocidade motivou diversos bancos centrais e autoridades monetárias a explorar a possibilidade de emissão da moeda soberana em suporte digital (moeda fiat digital).

Assim como o numerário em espécie, o meio circulante digital poderia ser: (a) fixado em termos nominais; (b) universalmente acessível; e (c) válido como moeda com curso legal para todas as transações públicas e privadas. Consequentemente, uma moeda oficial desmaterializada é essencialmente diferente das moedas virtuais criadas por entidades privadas, como o Bitcoin, cujos preços de mercado têm flutuado acentuadamente nos últimos anos.

# 2 Objetivo

Como premissas do estudo, entendemos que a construção de um sistema capaz de dar amplo acesso à população à moeda soberana nacional em formato digital deveria, entre outras coisas, melhorar:

- a eficiência da função monetária e os processos e sistemas de pagamento subjacentes;
- o nível de inclusão financeira; e
- a experiência geral do usuário ("ux") - traduzida em menor "fricção" e maior proteção ao consumidor.

Sob estas condições, estudamos formas de emissão complementar da moeda fiduciária em formato digital (5), buscando minimizar incertezas e riscos, bem como aproveitar, até certo ponto, os atuais modelos de negócio e sistemas existentes, sem, no entanto, abrir mão de abordagens inovadoras, que tragam claros benefícios, em termos de eficiência e inclusão para o Sistema Financeiro Nacional.

# 3 Contexto

Nesta seção, exploraremos algumas das motivações que justificariam eventual criação de um novo suporte digital para a moeda brasileira.

Como mote central da análise, consideramos que somente uma moeda oficial digital, aceita de forma irrestrita pelo público, teria a vitalidade para desintermediar os mercados e realmente complementar ou até mesmo substituir, no longo prazo, o dinheiro físico tradicional.

## 3.1 Eficiência da função monetária

Uma moeda nacional "tokenizada" operada por um sistema de pagamentos distribuído, a depender de seu design, permitiria ao emissor o acesso do histórico transacional, se necessário, em tempo real. O meio circulante digital (MCD), portanto, forneceria mais dados aos formuladores de políticas econômicas e monetárias, incluindo a capacidade de observar a resposta da economia aos choques ou às mudanças de políticas quase que imediatamente e com maior precisão. Isso mostra-se útil para o gerenciamento da estabilidade macroeconômica.

Tal solução de pagamento permitiria a liquidação final diretamente entre o beneficiário e o pagador nas transações digitais, em nível varejo, em moeda de banco central. O risco de contraparte seria, portanto, totalmente evitado, de modo que qualquer tipo de garantia vinculada à operação

não se faria necessária. Assim, isso traduz-se na liberação de quantias significativas de capital colateralizado. Na medida em que há uma escassez de boa garantia no mercado financeiro, esta abordagem propõe importantes benefícios macroeconômicos e de estabilidade financeira.

O modelo em discussão, através da desintermediação da cadeia de pagamentos digitais e do aumento dos níveis de transparência, deve buscar a garantia de que suas taxas de transação reflitam com mais precisão o custo marginal de verificação - líquido de qualquer subsídio público, caso fornecido -, bem como permitir a adoção mais rápida de novas tecnologias que fiquem no topo de suas infraestrutura de pagamento, aumentando a oferta de serviços de transferência e pagamento digital e reduzindo (ou até mesmo evitando) os custos repassados ao usuário.

Neste sentindo, a arquitetura precisa ser flexível o bastante, para permitir a eventual entrada de novos atores, caso desejável, como, por exemplo, empresas de tecnologia financeira na área de pagamentos. Assim, instituições financeiras que venham a atuar como mantenedores/participantes da infraestrutura tecnológica da moeda digital poderiam prestar serviços de "Banco como Plataforma" ("Bank as a Platform - BaaP"), franqueando acesso ao sistema por terceiros, algo bem alinhado com recente e desejável agenda de "open banking".

Portanto, como um meio de troca de baixíssimo custo, a moeda digital aumentaria a eficiência geral do sistema de pagamentos. O numerário digital seria particularmente benéfico para as famílias de baixa renda, que tendem a depender muito do papel-moeda, e para pequenas empresas, que incorrem em altos custos para lidar com dinheiro físico ou altas taxas transacionais, quando realizam/recebem pagamentos com cartões. No nível macroeconômico, os ganhos de produtividade decorrentes da adoção do MCD seriam semelhantes aos de uma redução substancial de impostos distorcivos.

Quanto ao ciclo do numerário, no Brasil, uma pesquisa realizada em 2015 pela "Consultoria Tendências" a pedido da MasterCard com 610 comerciantes de grandes centros mostrou que 64% deles acreditam que as transações em dinheiro geram custos mais altos do que se pensava até recentemente. Entre as razões estão (i) a necessidade de ter um empregado de confiança, cuja função principal seja lidar com o dinheiro; (ii) tempo perdido para trazer os valores de/para o banco; e (iii) a constante ameaça de roubo. Além disso, um quarto dos entrevistados tem seguro contra roubo e 60% deles sabem que o custo do seguro seria menor se dependessem menos do papel-moeda [2].

Para combater tais crimes, os bancos brasileiros investem, anualmente, cerca de R$ 9 bilhões [3]. Esse valor supera a própria perda dos bancos para os ataques. "A perda financeira é desproporcional ao investimento feito pelos bancos", disse Murilo Portugal, presidente da Federação Brasileira de Bancos (Febraban). "Essa é uma das muitas causas de nossos 'spreads' serem maiores".

Segundo cálculos da Diebold, multinacional fabricante de caixas eletrônicos, um caixa eletrônico no Brasil é, em média, 60% a 70% mais caro do que em outras partes do mundo. Em grande parte, a diferença é explicada pelos dispositivos de segurança adicionais que as máquinas exigem aqui [4].

Neste contexto, o custo total anual do ciclo do dinheiro brasileiro é de aproximadamente R$ 90 bilhões, quando se considera a emissão, custódia, distribuição de atacado/varejo e os custos das tratativas com o dinheiro no comércio [5].

Por outro lado, entendemos que os cartões de crédito e débito não são uma solução completa, uma vez que estão fora do alcance do público desbancarizado e, não raro, impõem altas taxas de transação para os cidadãos bancarizados de baixa renda. Entre os brasileiros, os cartões pré-pagos vêm aos poucos ganhando força e, embora capazes de contribuir com o incremento dos níveis de inclusão financeira, estão ligados a uma indústria, em geral, bastante intermediada, o que reduz a oferta de taxas transacionais mais palatáveis.

Os depósitos – em geral, através de boletos – ainda são um dos principais meios pelo qual o público não bancarizado pode efetuar pagamentos na economia digital. Ademais, muitos dos serviços oferecidos por instituições de pagamentos - não necessariamente bancárias -, como dinheiro eletrônico/"carteiras digitais" (contas de pagamento), ainda que alvissareiros, enfrentam algumas barreiras para sua plena adoção.

Neste sentido, embora recentes inovações legais e regulatórias (Lei 12.865/2013, Resolução 4.282/13 e Circular 3.885/18 do Banco Central do Brasil), bem como a criação de grupo de trabalho sobre pagamentos instantâneos (GT-PI), busquem proporcionar um terreno mais fértil para o florescimento de novos atores e esquemas de pagamentos no país, ainda há barreiras técnicas, que dificultam a evolução de tais soluções.

Portanto, entendemos que uma nova infraestrutura de pagamento, com foco na interoperabilidade e que venha a permitir a emissão da moeda de banco central em formato digital para o varejo, poderia ser a interface ideal entre provedores de serviços de pagamento e transferência, acelerando a adoção de soluções de pagamento orientadas para dispositivos móveis - predominantes em diversos países, como China e Índia, mas ainda tímidos no Brasil. Nesse cenário, o numerário digital serviria como um "token" com potencial único para o incremento de liquidez deste ecossistema.

Supomos que a eventual disseminação do uso de uma moeda fiat digital, em paralelo à obsolescência do dinheiro em espécie, desencorajaria a evasão fiscal, a lavagem de dinheiro e outras atividades ilegais facilitadas pelo numerário físico - em especial, por notas de grande valor. Esse benefício é importante nas economias avançadas, sendo ainda mais pertinente nas economias em desenvolvimento, onde uma relevante fração da atividade econômica é informal e conduzida por meio do uso do dinheiro em espécie.

Finalmente, podemos destacar os possíveis benefícios socioambientais trazidos pela redução do fornecimento de dinheiro em espécie, tendo em vista a consequente diminuição do consumo de matérias primas e combustíveis fósseis, particularmente, nas etapas de produção e distribuição do numerário nacional. Quanto ao processo de saneamento do meio circulante, poderíamos evitar a geração de centenas de toneladas de resíduos. Neste sentido, para fins ilustrativos, registramos que, ao longo do exercício de 2017, foram geradas 1.189 toneladas de resíduos de cédulas derivados das atividades de destruição do numerário inservível no Brasil.

## 3.2 Incremento dos níveis de inclusão financeira

Os pagamentos digitais servem de porta de entrada para a cidadania financeira, posto que uma infinidade de serviços é advinda deste canal. Portanto, acreditamos que o potencial incremento dos níveis de inclusão financeira através da oferta de solução de numerário digital se destaca como um dos benefícios de maior relevância.

No país, de acordo com o Global Findex Report (2017) [6], 70% dos adultos têm conta bancária (idade: 15+). Quanto aos 30% não-bancarizados: (i) 32% afirmam não possuir contas, pois não há instituições financeiras próximas às suas residências; e (ii) 57% alegam não ter conta em razão dos altos custos dos serviços financeiros. Ainda, segundo a mesma pesquisa, apenas 58% da população brasileira adulta afirmou ter realizado ou recebido pagamentos digitais no ano passado.

Dados do Banco Mundial [5] retratam que 92% dos adultos brasileiros (idade: 15+) possuem acesso à telefonia celular ou à internet residencial, gerando, portanto, uma oportunidade de integrar em torno de 34% da população não atendida às soluções de pagamento digital, caso uma moeda fiat desmaterializada seja implementada com sucesso.

Ademais, é importante frisar que mesmo muitos dos cidadãos bancarizados no Brasil não podem

contar com canais eletônicos de transferência de recursos, posto que, por vezes, as instituições financeiras cobram taxas muito elevadas nestes tipos de operação (TED e DOC). Esta situação é agravada quando consideramos que os cidadãos de baixa renda geralmente apresentam 'tickets' médios reduzidos em suas transferências e essa tarifa é fixa - e não 'ad valorem'.

### 3.3 Melhoria da experiência do usuário ("ux")

No Brasil, uma grande desvantagem trazida por roubos recorrentes de caixas eletrônicos, bancos comerciais e bancos postais é o surgimento de "cidades sem dinheiro", tratando-se de pequenas cidades no interior do país sem qualquer canal para saque de numerário [7].

Quando pensamos em questões de segurança e possíveis danos à integridade física de clientes e funcionários no atual ciclo do numerário brasileiro, concluímos que eventuais 'trade-offs' ligados à exposição de riscos de segurança cibernética nos meios de pagamento digital parecem ser de fácil solução. Devemos também considerar os grandes avanços na maturidade das soluções de segurança para pagamentos digitais - como os novos padrões da indústria propostos nos últimos dois anos pela "FIDO Alliance" [8].

Há também de se ressaltar que, em geral, a experiência do usuário em relação às moedas metálicas é notoriamente ruim. Isto ocorre globalmente, tendo em vista os crescentes níveis de entesouramento, levando enormes quantidades de moedas metálicas para fora de circulação - em torno de 30%, no país [9]. Adicionalmente, ressaltamos os altos custos de produção e logísticos embutidos, em razão do material e peso deste item, frente ao seu baixo valor de face.

Por fim, salientamos que as novas tendências estão fazendo diversos países pensarem em digitalizar sua moeda, para engajar e facilitar novas formas de transação. Algumas delas são (i) "Finanças Invisíveis" (por exemplo, Uber e Amazon GO), que dependem de pagamentos móveis; (ii) a chamada "Internet das Coisas" (IoT), que se traduz em transações "máquina a máquina (M2M)" pela Internet; e (iii) "Contratos Inteligentes", que são codificados e podem movimentar dinheiro automaticamente, se algumas condições específicas forem implementadas.

## 4 Taxonomia do dinheiro

De acordo com os recentes estudos do 'Committee on Payments and Market Infrastructure' (CPMI) do 'Bank for International Settlements' (BIS) [10], existem dez propriedades básicas que distinguem os diferentes tipos de dinheiro. Tendo em mente o contexto brasileiro, listamos essas propriedades, bem como propomos a adição de um novo item à lista, que trata da função do numerário:

- **Forma**: O dinheiro pode ter suporte físico, como o papel-moeda; ou digital, como o saldo das contas correntes.
- **Emissão**: O dinheiro pode ser emitido por um banco central ou por outras entidades, como, por exemplo, no caso das criptomoedas que têm sua emissão realizada de forma descentralizada por mineradores.
- **Acessibilidade**: O dinheiro pode ser de acesso amplo à população como o papel-moeda, ou ser restrito a um grupo como é o caso das reservas bancárias do Sistema de Pagamentos Brasileiro (SPB).

- **Tecnologia**: Existem duas tecnologias básicas que dizem respeito a representação do valor. Nesse quesito, o dinheiro pode ser baseado em contas, como as reservas bancárias, ou, pode ser baseado em tokens que armazenam valor, como o papel-moeda.
- **Disponibilidade**: O numerário físico, tem disponibilidade completa, ou seja, pode ser movimentado 24 horas por dia todos os dias. Em sua forma digital, o dinheiro pode apresentar disponibilidade completa ou restrita, como, por exemplo, as reservas bancárias que somente estão disponíveis para movimentação durante o horário de operação do Sistema de Transferência de Reservas (STR).
- **Duração**: A duração é o tempo de vida do numerário, podendo ser indefinida como nas cédulas do papel-moeda, ou limitada, como, por exemplo, num dinheiro digital que fosse criado, emitido e resgatado diariamente.
- **Anonimato**: O anonimato diz respeito ao grau de privacidade em relação a posse e ao uso. O dinheiro físico é completamente anônimo. O dinheiro digital baseado em contas não é anônimo, uma vez que a instituição depositária tem acesso total às suas informações, podendo ou não garantir o sigilo de saldos e movimentações em relação a terceiros. No dinheiro digital baseado em tokens, em princípio é possível alcançar diferentes níveis de privacidade dependendo da arquitetura adotada.
- **Limites**: Essa propriedade está relacionada com a existência ou não de limites na quantidade monetária que pode ser transferida e armazenada em implementações de dinheiro digital.
- **Mecanismos de transferência**: Essa opção define como a operação de transferência do dinheiro ocorrerá. A movimentação pode ser realizada diretamente entre as partes, chamado ponto-a-ponto (no inglês, 'peer-to-peer'), ou utilizar um intermediário como um banco central ou outro participante do sistema financeiro.
- **Incidência de Juros**: Assim como nos saldos de reserva bancária, é possível ocorrer incidência de juros (inclusive negativos) no valor armazenado digitalmente. Essa decisão pode encorajar ou desencorajar a demanda por dinheiro digital.
- **Função**: O dinheiro, em formato físico ou digital, serve essencialmente como meio de troca, reserva de valor e unidade de conta. Recentes iniciativas, como ativos criptográficos emitidos por governos, ao se afastarem de ao menos uma destas funções, não devem ser confundidos com uma moeda fiat digital - tratando-se, em geral, apenas de mecanismos de captação de recursos e/ou de especulação.

# 5 Modelo

O modelo aqui estudado trata-se de um dinheiro digital emitido por banco central. Ele seria de acesso amplo à população, baseado em tokens, com disponibilidade completa, duração indefinida e sujeito aos limites estabelecidos pelo próprio BC. Seu mecanismo de transferência seria ponto-a-ponto, sem incidência de juros, com a privacidade de saldo e movimentações garantida pelo sigilo bancário. Apesar de seguir tais definições, a arquitetura que suporta o novo dinheiro digital é flexível o suficiente para permitir inúmeras diferentes configurações.

O sistema financeiro nacional já opera com representações digitais de valores monetários. No entanto, o papel-moeda continua sendo um dos principais meios de pagamento para operações no varejo do Brasil e seu ciclo de vida é bastante oneroso aos cofres públicos. Esse trabalho cuida do estudo de um novo dinheiro digital de banco central, com foco no varejo.

## 5.1 O token

O meio circulante digital seria formado por pequenos registros digitais assinados chamados tokens, capazes de representar a relação de propriedade entre uma pessoa física ou jurídica e um valor arbitrário na moeda nacional, vide figura 1. Tais registros digitais circulariam pelo sistema financeiro e pela sociedade por caminhos análogos aos do papel-moeda.

O token pode ser utilizado como reserva de valor, enquanto estiver armazenado em alguma mídia eletrônica não volátil, ou como instrumento de troca, quando transferidos entre as partes por meio do seu sistema. Esse registro digital pode ser entendido como um pequeno arquivo.

| Outros campos | Valor | Pertence a: | Assinatura do BC ou Validador: |
|---|---|---|---|
| ... | R$ 10,00 | 18WwqTVKLQNhL4eE14WmeqEEdwZcGsY1FM | aaadec456778sdf224d4s44ED787778901ad07s4 |

Figure 1: Modelo simplificado de um token.

Toda moeda digital para seu uso como meio de pagamento depende de uma infraestrutura mínima de energia elétrica e telecomunicações. Essa infraestrutura necessária já segue em um processo de expansão conduzido pela demanda crescente gerada pelas novas tecnologias.

Segundo dados do IBGE, as áreas urbanas brasileiras concentram 84,35% da sua população [11]. A Agência Nacional de Telecomunicações (Anatel) estabeleceu a regra de que a cobertura do serviço de telefonia móvel deve ser de pelo menos 80% da área urbana das sedes dos municípios brasileiros, para todas as operadoras. O cumprimento dessas obrigações pelas prestadoras é acompanhado periodicamente pela fiscalização da Agência [12]. Ainda segundo dados de janeiro de 2018 da Anatel, o Brasil tem hoje 236,2 milhões de linhas móveis, das quais mais de 217 milhões têm acesso a uma conexão de dados suficiente para a operação do meio circulante digital (MCD) [13].

Na hipótese de uma indisponibilidade na infraestrutura de telecomunicações em uma área específica ou por um tempo curto espaço de tempo, a solução proposta ainda poderá ser utilizada porém em modo sub-ótimo (item A.4.3). Os usuários que não possuem smartphones, poderiam utilizar a moeda digital em seus computadores, em celulares compartilhados, ou através de serviços de carteira digital fornecidos por terceiros. Numa circunstância extrema, o usuário poderia fazer uso do papel-moeda como meio alternativo. A implantação do numerário digital não determinaria a extinção imediata do papel-moeda, trata-se apenas de um passo em direção ao futuro. Uma longa fase de transição deve ser realizada até que a infraestrutura necessária para sua operação plena esteja inequivocamente atendida em toda a extensão do país.

## 5.2 Funcionamento

O numerário digital funcionaria como um grande sistema computacional distribuído onde vários atores executam diferentes papéis para garantir uma movimentação fluida, correta e tempestiva dos valores desmaterializados. A interação entre os atores acontece por meio de diversos softwares, por

diferentes tipos de conexões, inclusive pela internet, todos de acordo com as regras e protocolos definidos pela autoridade monetária.

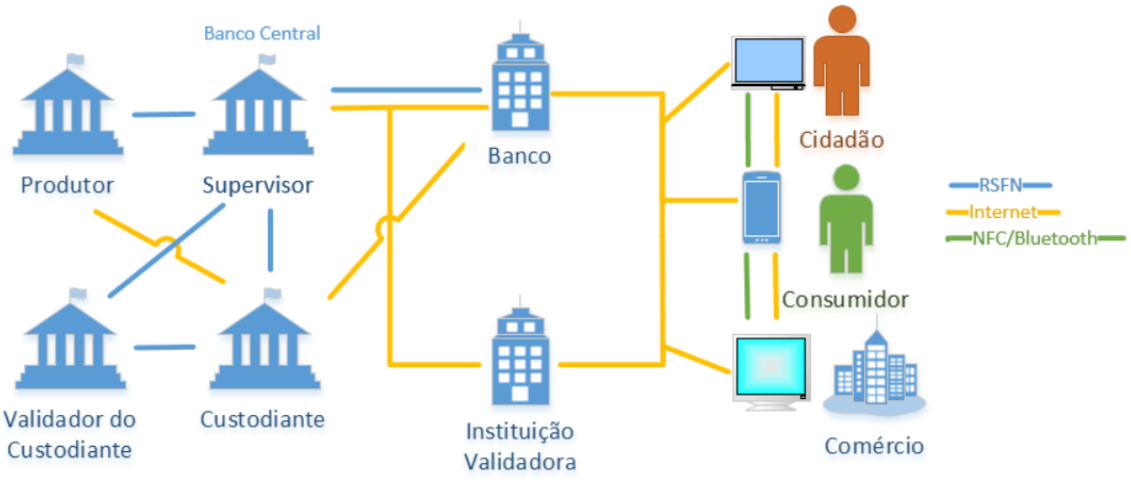



Figure 2: Ecossistema do numerário digital.

Na figura 2 pode-se ver os principais papéis do sistema MCD. As linhas entre os atores representam os canais de comunicação que podem ser estabelecidos durante a operação do sistema. Não existe ligação direta entre o BC e os não participantes do SFN: toda relação entre o BC e a sociedade segue intermediada pelas instituições financeiras, assim como ocorre com o numerário físico. Os papéis fundamentais do BC e a organização em camadas do sistema financeiro permanecem preservados.

Vale destacar a presença das instituições validadoras na Figura 2. Esse é um papel novo e crucial neste modelo de moeda digital, pois ele é responsável pela garantia e finalidade de cada transação realizada. A atuação dos participantes do SFN no papel de instituição validadora é opcional, sendo tecnicamente possível que o próprio BC exerça exclusivamente este papel. No entanto, quanto mais softwares de validação forem implantados e quanto mais distribuídos estiverem em diferentes centros de dados (data-centers), maior será a resiliência e a performance da moeda digital como sistema de pagamentos.

No token (figura 1), como é chamado registro digital do numerário, o proprietário do valor declarado é definido por uma identidade criptográfica. Neste caso, é a chave pública de um certificado digital de sua posse. Para ser considerado válido, o token precisa atender a um conjunto de regras técnicas que fogem ao escopo deste documento e não pode ter sido utilizado em qualquer outra transação do sistema. A validade do token é garantida, em última instância, por meio da assinatura digital de uma instituição validadora, seja ele o BC ou outra instituição, em seu nome. Enquanto operado segundo as definições do modelo proposto, tais tokens têm funções e características muito próximas às de uma moeda soberana física.

### 5.2.1 Emissão

O controle da emissão do numerário digital é exclusivo do BC. De acordo com suas políticas, o BC poderia determinar em que quantidades e valores o Meio Circulante Digital (MCD) deve ser

produzido.

A escolha da instituição responsável pela execução do software específico de produção de novas moedas digitais é uma decisão política, sendo tecnicamente possível que o próprio BC execute este papel. O produtor, no entanto, teria que manter em segurança os novos tokens e o certificado digital com o qual assina digitalmente todos eles.

Esse passo do fluxo do numerário digital tem seu paralelo na produção do numerário físico.

### 5.2.2 Custódia

Os valores digitais nascem vinculados a uma identidade criptográfica. Tal identidade deve pertencer à instituição escolhida para exercer o papel de custodiante do novo numerário. Novamente, a escolha de tal instituição é uma decisão política, sendo tecnicamente viável que o próprio BC acumule este papel.

O custodiante recebe do BC, ou diretamente do produtor, o numerário recém produzido, e deverá então validá-lo e garantir sua segurança. Seria de sua responsabilidade a segurança do certificado digital de custodiante.

O tokens em custódia seguem armazenados por software específico até que um saque seja solicitado por algum banco e autorizado pelo BC. Podemos perceber uma relação direta desta etapa com a logística demandada pelo papel-moeda até sua estocagem pelo custodiante, conforme apresentado na figura 3.

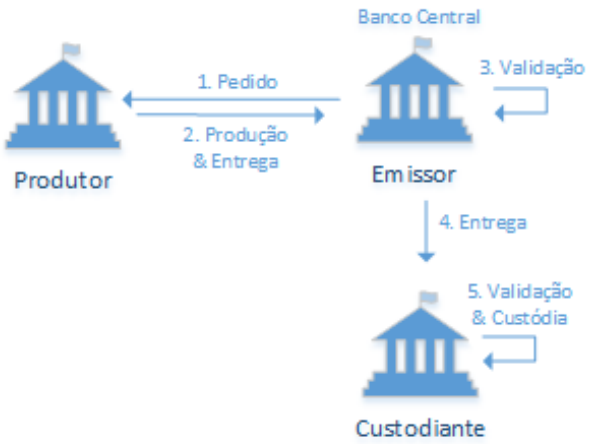



Figure 3: Esquema simplificado da emissão.

### 5.2.3 Abertura de conta de numerário digital

O equivalente às contas bancárias, no sistema do meio circulante digital, são as chaves públicas dos certificados digitais escolhidos pelos bancos para representar as identidades criptográficas de seus estoques de numerário digital. Os bancos deverão realizar o registro de suas contas em um sistema do BC destinado ao gerenciamento de todas as contas, ou identidades criptográficas, do novo

dinheiro digital. Uma vez registrados e autorizados pelo BC, os bancos poderão operar, recebendo e mantendo vinculado a essas contas o numerário digital necessário para atender seus clientes.

Os valores armazenados nas contas bancárias digitais seguem regras e controles análogos aos aplicados ao numerário físico de posse dos Bancos em seus cofres e caixas eletrônicos.

### 5.2.4 Saque contra reserva bancária

O banco que desejar fazer um saque em dinheiro digital, deve acionar o BC, através de mensagem específica do Sistema de Pagamentos Brasileiro (SPB), informando, dentre outras coisas, sua conta de numerário digital (seção 5.2.3) de destino do saque. Os tokens referentes ao valor sacado de sua reserva poderão ser transferidos para o banco sacador também via mensagem específica do SPB. As referidas mensagens ainda não foram implementadas, suas definições farão parte da fase de estudos aprofundados.

Quando acionado por um banco, o banco central em questão deve efetuar o respectivo débito na conta reserva bancária e acionar o custodiante, solicitando-o a transferência do valor digital demandado para o banco sacador. O custodiante deverá criar uma transação de saque contra reserva bancária utilizando-se dos tokens em sua custódia, de acordo com as instruções da seção 5.2.11. Tal transação, além da assinatura digital do próprio custodiante, seria reconhecida pela instituição ocupante do papel de Validador do Custodiante, conforme instruções na seção 5.2.12.

A atribuição do papel de Validador do Custodiante trata-se de uma escolha política, contudo, é interessante que este papel seja executado pelo próprio BC. Todos os validadores do sistema devem garantir a segurança do certificado digital que lhes concede tal poder.

O valor digital transferido para o banco ficaria em sua posse, vinculado à sua conta de MCD (seção 5.2.3), armazenado pelo seu software de carteira digital, assim como o papel-moeda quando encontra-se em seus cofres e caixas eletrônicos, até que um novo processo de saque ocorra, agora entre um cliente e o banco abastecido.

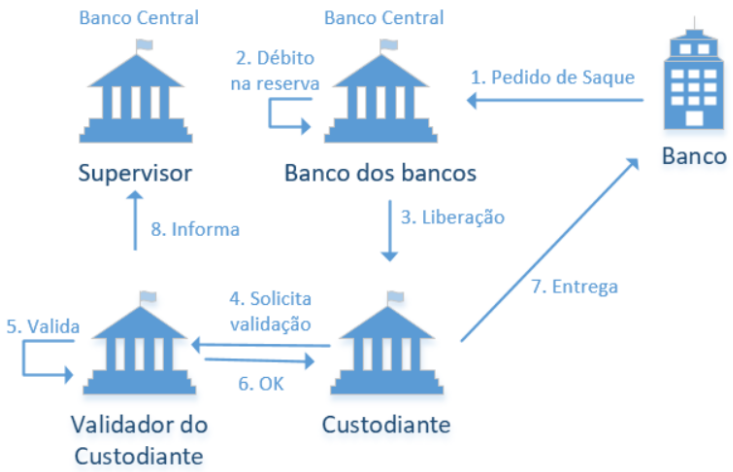



Figure 4: Esquema simplificado de saque contra reserva bancária.

### 5.2.5 Abertura de conta corrente digital

Assim como nas contas bancárias digitais da seção 5.2.3, as contas correntes digitais também são as chaves públicas dos certificados digitais escolhidos, agora pelos clientes, para representar uma de suas identidades criptográficas no sistema de moeda digital. No item 5.3.10 discutimos com alguma profundidade as questões relativas à privacidade e ao anonimato. O procedimento descrito abaixo foi o que apresentou a melhor relação custo X benefício dentre as possibilidades já estudadas.

As chaves públicas de certificados digitais, utilizadas na definição de propriedade dos tokens deverão ser registradas no sistema de suporte ao MCD para que estejam autorizadas a operar no sistema. Os registros de chave pública das carteiras digitais bancárias são realizados diretamente pelo BC. Os registros de chave pública das outras carteiras digitais são realizados pelos Bancos autorizados. A operação de registro de uma nova chave pública estará vinculada aos procedimentos de **KYC** (*Know Your Customer*), porém a identidade real do proprietário de cada certificado digital registrado será mantida pelo banco de sua escolha e estará protegida pelo sigilo bancário.

### 5.2.6 Saque digital contra conta corrente

O saque em moeda digital pode ser realizado presencialmente nos pontos de atendimento dos bancos assim como ocorre com o papel-moeda. No dinheiro digital também é possível realizar saques remotamente, no próprio celular do cliente, via aplicativo de 'mobile banking', não dependendo da presença física do cliente em uma agência bancária ou caixa eletrônico. Para tanto, bastaria que o aplicativo de mobile banking interaja com o aplicativo de carteira digital pessoal, ou simplesmente receba as informações necessárias para executar o saque, e que o cliente tenha uma conexão com a internet.

Quando um saque for solicitado, o banco deve criar uma transação transferindo para o cliente a propriedade do valor solicitado. Essa transação será construída segundo as instruções do item 5.2.11. Em seguida, será ratificada pela instituição validadora, segundo as instruções do item 5.2.12. Uma vez validada, a transação é transferida pelo banco, para o aparelho do cliente, onde será novamente validada e posteriormente armazenada pelo seu aplicativo de carteira digital pessoal.

### 5.2.7 Conversão físico X digital

A conversão entre os suportes do numerário dependerá, devido a tangibilidade do papel-moeda, da presença física do interessado junto a um ponto de atendimento de um participante do sistema financeiro nacional.

A conversão do dinheiro digital para físico poderá ser realizada de forma automática por caixas eletrônicos de bancos independente de existir ou não uma relação entre o cliente e o banco proprietário do caixa eletrônico. O cliente deve se aproximar do ponto de auto-atendimento de sua escolha, selecionar a opção de conversão desejada. Na sequência, o caixa eletrônico apresentará um QRCode com sua identidade criptográfica, o valor solicitado e o endereço de envio da transação. A carteira digital do cliente prepara a transação corretamente, enviando-a para o endereço informado pelo terminal, em seguida.

O banco, por sua vez, enviará a transação para ratificação pelo validador, segundo as instruções do item 5.2.12. Uma vez validada a transação, o banco poderá disponibilizar o valor acordado em papel-moeda para o cliente. Todo esse procedimento não deverá levar mais que alguns poucos segundos.

A troca do dinheiro físico pelo digital poderia ter um fluxo semelhante, na direção oposta, porém depende da confirmação da veracidade do papel-moeda entregue, função costumeiramente realizada por humanos (caixa) ou sensores (ATMs).

### 5.2.8 Transferência

Com o dinheiro digital armazenado em sua carteira digital, o usuário do MCD pode realizar pagamentos, transferências e depósitos. A transferência do numerário digital entre usuários do dinheiro digital não depende da localização geográfica dos envolvidos. Vários canais de comunicação de dados podem ser usados para transferir os tokens ao favorecido, por exemplo, e-mail, sistemas de mensagem instantâneas como o WhatsApp, ou até outro protocolo de conexão direta entre os aplicativos de carteira digital pessoal.

Na transferência, um QRCode seria oferecido pelo favorecido contendo uma de suas contas digitais. O mesmo QRCode poderá ainda informar o valor a ser transferido, seu validador de preferência e um endereço eletrônico para entrega. De posse dessas informações, a carteira digital do cliente produziria novos tokens a partir dos tokens de sua posse, como descrito no item 5.2.6. Em seguida, o cliente transfere a transação para o favorecido, que deve submetê-la à instituição validadora. Caso o favorecido não consiga, ou não queira, conectar-se com o validador, por qualquer motivo, ele pode solicitar ao cliente que ratificação junto à instituição validadora antes de entregá-lo os novos tokens. Nada impede, porém, que os dois solicitem a validação da mesma transação ao validador: a requisição que chegar em segundo lugar consumirá poucos recursos, sendo confirmada instantaneamente. Na figura 5 podemos ver um esquema desses caminhos alternativos.


Figure 5: Caminhos alternativos de validação.

A transferência de valores entre dois usuários do sistema de numerário digital ocorre de forma distribuída e ponto-a-ponto entre as partes envolvidas. Porém, ao menos um dos participantes precisa conectar-se com o validador definido no token, para solicitar-lhe a invalidação dos tokens consumidos e a validação dos novos tokens.

Para que haja confiança no sistema, as identidades criptográficas dos validadores oficiais devem ser amplamente divulgadas pelo BC. Devem também ser armazenadas junto com seus endereços eletrônicos nos aplicativos de carteira digital antes que este possa operar com tais validadores. O usuário favorecido poderá considerar a transação confirmada e finalizada, quando encontrar nela a assinatura válida do validador oficial definido no próprio token. A lista dos validadores e seus

endereços deve ser atualizada pelas carteiras digitais junto a um serviço oficial criado para este fim, com uma periodicidade que será definida estudos futuros.

### 5.2.9 Pagamento

A transação de pagamento é muito parecida com a transação de transferência, descrita no item 5.2.8, com as seguintes diferenças:

- A carteira favorecida poderá ser do tipo carteira comercial (item 5.3.13).
- Novos campos poderão ser adicionados para referenciar, por exemplo, o número do cliente, no caso de pagamento de boletos.
- Uma taxa, ou a coleta de impostos, poderão ser automatizadas.
- Limites específicos poderão ser atribuídos.

### 5.2.10 Depósitos

A operação de depósito em conta corrente pode ser realizada presencialmente, num ponto de atendimento do banco escolhido, ou remotamente, via integração entre o aplicativo de carteira digital pessoal e o aplicativo de mobile banking, dispensando nessa opção o deslocamento requerido na primeira.

O funcionamento de um depósito não difere do funcionamento de uma transferência (item 5.2.8) onde a conta digital debitada pertence ao cliente depositante e a conta digital creditada pertence a o banco depositado. A operação de depósito, assim como a de pagamento (item 5.2.9), admite a inclusão de campos auxiliares que, no caso do depósito, permitam a identificação da conta corrente ou conta poupança do favorecido.

Um banco, por sua vez, pode encontrar-se sobre-abastecido de numerário digital. Para realizar o depósito em sua conta reserva bancária, ele deve seguir procedimento semelhante, com o detalhe de que a transação validada deverá ser enviada para o BC por meio de mensagem específica do SPB, para este fim.

### 5.2.11 União e desmembramento de tokens

Toda transação em moeda digital envolve a transferência de valores entre duas contas, a conta de origem e a conta de destino. O tipo da transação define que tipos de contas podem estar presente nessas duas extremidades.

Cada nova transação gerada, independente do seu tipo, irá consumir um ou mais tokens da conta de origem. Esses são os tokens de entrada da transação, que serão somados e do resultado serão gerados um ou dois novos tokens, chamados de tokens de saída. Um dos tokens de saída apresentará sempre o valor a ser entregue à conta de destino. O outro, opcional, apresentará o saldo restante da soma dos tokens de entrada, ou seja, o troco, e será vinculado à conta de origem.

A soma dos valores dos tokens gerados deverá ser igual à soma dos valores dos tokens consumidos, não sendo permitida a criação ou destruição do numerário digital por meio do seu uso. Embora sejam possíveis outras combinações, neste modelo, propomos limitar em 255 o número máximo de tokens de entrada e em até dois o número de tokens de saída numa transação.

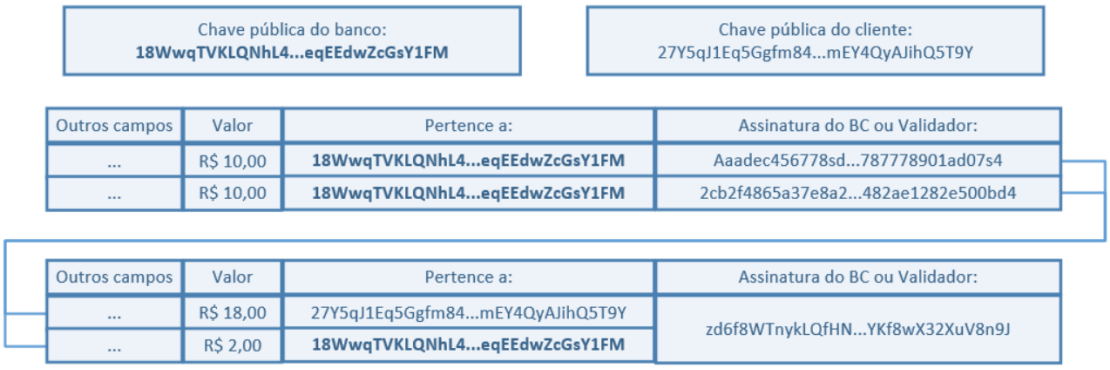



Figure 6: Modelo simplificado da união e desmembramento de tokens.

### 5.2.12 Validação da transação

Para que haja confiança no sistema, por parte do favorecido, as transações são assinadas tanto pelo seu originador quanto pelo seu validador. Os validadores executam o papel de um terceiro neutro, que assinará a transação garantindo que esteja válida. Quando a transação é considerada correta pelo validador, os tokens originais serão consumidos, pelo validador, tornando-se impróprios para nova utilização. Caso seja rejeitada, a transação é considerada sem efeito para todos os fins. Os validadores são os responsáveis pela resistência do sistema às falsificações. Antes de assinar a transação reconhecendo-a como efetivada, o validador realiza dentre outras, as verificações abaixo:

- Eu sou o validador dessa transação?
- Os tokens de entrada pertencem ao proponente da transação?
- A soma dos tokens gerados é igual a soma dos tokens consumidos?
- Os tokens de entrada estão sendo utilizados pela primeira vez?
- Os valores estão dentro dos limites determinados pela autoridade monetária para este tipo de transação?
- As contas envolvidas na transação são do tipo permitido para esse tipo de transação?
- As contas envolvidas na transação estão todas válidas, ativas e desbloqueadas?
- Há uma assinatura digital válida do proponente da transação?

Ao receber o token sacado, a carteira digital do favorecido realiza algumas validações simples, antes de armazenar os valores recebidos:

- O token de saída está vinculado a uma de minhas contas digitais?
- O valor deste token coincide com o valor esperado?
- O validador que validou a transferência está na minha lista de validadores de confiança?
- Há uma assinatura digital válida do validador?

### 5.2.13 Migração de validador

A migração de tokens entre os validadores permite uma melhor distribuição da responsabilidade da validação do dinheiro digital entre os validadores ativos. A decisão de permitir ou não a livre escolha dessa migração deve ser tomada numa futura etapa de estudos. Contudo, é tecnicamente possível criar uma transação especial que tem por finalidade a simples troca do validador dos tokens ativos, ou simplesmente permitir que, em qualquer tipo de transação, todo novo token especifique seu validador livremente.

A transação de migração de validador teria sempre um ou mais tokens de entrada e um único token de saída cujo valor seria igual à soma dos tokens de entrada. Todos os tokens, tanto os de entrada, quanto os de saída, pertencerão à mesma conta digital, porém, o token de saída apresentará um validador diferente do validador dos tokens de entrada.

Se a migração de validador for permitida em todas as transações, cada token da moeda digital possuirá, dentro de si, a identidade criptográfica de seu validador. Como os tokens são assinados digitalmente desde sua origem, não haverá como alterar a identidade do validador sem invalidar a assinatura digital e o token por consequência. Todavia, a cada nova transação haverá sempre tokens consumidos e novos tokens criados. Cada um desses novos tokens poderá ser vinculado a um validador diferente, independentemente do validador dos tokens de origem.

### 5.2.14 Supervisão do sistema

O banco central, no papel de supervisor, receberia tempestivamente de cada validador uma cópia de cada transação por este validada. Assim, o BC teria acesso a uma cópia de todos os tokens ativos e válidos e também de todos os tokens já consumidos. Esse passo no processo do numerário digital não encontra-se em seu caminho crítico, ou seja, caso o BC estivesse fora do ar, os validadores não cessariam seus trabalhos. Eles poderão enviar ao banco central as transações validadas, assim que o BC estivesse online novamente.

Com tal mecanismo de comunicação entre os validadores e o BC, este teria instrumentos para:

- Monitorar a economia em tempo quase-real.
- Supervisionar e fiscalizar o comportamento dos validadores.
- Substituir um validador em caso de falha sistêmica ou catástrofe no data-center do validador.
- Para reconstruir a base de dados de um validador e entregá-lo de volta a sua operação.
- Calcular algum tipo de remuneração para os serviços prestados pelos validadores com base em alguma regra sobre as transações validadas.
- Fornecer aos bancos um serviço de recuperação de dinheiro perdido de seus clientes.
- Fornecer aos bancos um serviço de recuperação de conta pessoal dos seus clientes que perderam a chave privada de suas contas digitais.
- Operar no combate a ilícitos financeiros, lavagem de dinheiro e financiamento ao terrorismo.

Mesmo tendo uma visão privilegiada do numerário digital, o BC não teria acesso à identidade real de nenhum usuário do dinheiro virtual. O BC só deteria acesso ao nome do banco que registrou e ativou a conta de seu usuário no sistema de gerenciamento de contas do MCD. A privacidade do

usuário e de sua movimentação financeira seguem protegidas pelos mesmos instrumentos que temos hoje para a garantia do sigilo bancário. Todavia, a quebra do sigilo bancário mostraria-se possível com a moeda digital, como ocorre hoje com as contas bancárias. O BC não precisará aumentar seus quadros para realizar atendimentos à população referentes a operação com o dinheiro digital.

## 5.3 Detalhamento do modelo em estudo

A moeda digital nacional apresentaria as seguintes características:

### 5.3.1 Disponibilidade

O uso do numerário digital pela população garantiria uma disponibilidade 24/7/365 - independente da atuação direta do BC. A validação de transações, única operação que realmente precisa funcionar ininterruptamente, pode ser realizada pelo BC ou delegada a uma ou mais instituições. O BC ocupando o papel de emissor e supervisor pode manter sua rotina atual de funcionamento, sem que sua ausência cause qualquer impacto na performance do MCD. As movimentações entre Bancos e BC, por sua vez, continuarão ocorrendo dentro da grade horária normal do Sistema de Pagamentos Brasileiro (SPB).

### 5.3.2 Duração

O token do MCD, por ser digital, tem duração indeterminada. Porém, sua validade, assim como a do papel-moeda será determinada pela legislação vigente.

Caso ocorra a necessidade de substituição ou atualização completa do numerário, a exemplo da mudança do Cruzeiro Real para o Real, em 1994, o modelo proposto permitiria a aplicação de procedimentos automáticos de baixo custo, o que facilitaria o processo.

### 5.3.3 Formato e Mecanismo de transferência

O MCD possuiria o formato de token digital. Sua transferência seria realizada de forma distribuída, ponto-a-ponto, em 2 passos que não possuem ordem definida.

### 5.3.4 Liquidação

A liquidação no MCD seria instantânea, irrevogável e irrefutável, sendo efetuada com finalidade no ato da validação pelo validador. Ou seja, após validação pelo validador, o novo token já pertence ao favorecido, mesmo que não lhe seja entregue, o favorecido pode, assim, entrar em contato com seu banco e solicitar a recuperação de tokens, como descrito no item A.3.3.

### 5.3.5 Monitorado

Todas as operações relativas ao numerário digital, sensibilizam em tempo real, ou com algum atraso (dentro de padrões aceitáveis), os sistemas de monitoramento do BC. Todos os validadores comunicam as transações validadas ao BC tempestivamente para fins de monitoramento e fiscalização. Essa comunicação deve ser assíncrona, com garantia de entrega, por algum sistema de mensageria onde o BC teria um papel passivo, não tornando-se um ponto de falha, ou de retenção, caso esteja fora do ar.

### 5.3.6 Público alvo

O MCD teria seu foco nas operações de varejo. Porém, a sua arquitetura é flexível o suficiente para atender o mercado interbancário ou até os dois simultaneamente.

### 5.3.7 Emissão

A emissão do numerário digital seria exclusiva do BC. Contudo, sua produção pode ser realizada de forma similar a emissão do papel-moeda.

### 5.3.8 Remuneração do uso

O MCD não prevê nenhum tipo de remuneração ou juros.

### 5.3.9 Remuneração do validador

O MCD traduziria-se em um sistema computacional de baixo custo de produção e operação, quando comparado à outros do SFN e ao próprio papel-moeda. Entretanto, o sistema consumiria recursos das partes envolvidas, com um custo de sustentação que poderá estar sujeito a ressarcimento.

Esse ressarcimento pode, por exemplo, ser feito por meio da cobrança de uma tarifa de operação ao token, a ser paga pelo usuário final. Entretanto, esta abordagem distancia-se da experiência do usuário com o dinheiro físico. Também seria possível custear toda a operação do novo sistema com a economia no manejo do papel-moeda por ele substituído, mediante subsídio, ou através de novo arranjo acordado em eventual Parceria Público-Privada. Em uma terceira proposta, os custos seriam arcados na sua totalidade pelos próprios validadores, caso haja benefícios indiretos que possam ser auferidos - tais como eventual abertura de novos canais de relacionamento e a oferta de serviços aos usuários atendidos.

### 5.3.10 Privacidade e anonimato

É tecnicamente possível permitir que identidades criptográficas anônimas operem com o MCD. O grau de privacidade nesse caso, seria ainda maior do que o do Bitcoin, pois o banco de dados que armazena todo o histórico das transações realizadas no MCD, seria privativo do BC, e não de conhecimento público como o da cripto-moeda mencionada. Por outro lado, também é possível garantir que só as contas digitais devidamente identificadas pelo BC possam usar o dinheiro digital.

Na primeira situação, o BC, apesar de ainda possuir a rastreabilidade do numerário digital, não teria a capacidade de identificar os proprietários do meio circulante. As ações de combate à lavagem de dinheiro e financiamento ao terrorismo seriam prejudicadas. Não haveria meios práticos de impedir que estrangeiros utilizassem a moeda nacional e inviabilizaria a aplicação de limites sobre o uso da moeda.

Na situação onde o BC teria todo o conhecimento sobre o cidadão usuário da moeda digital, os riscos apresentados acima seriam mitigados por regras e validações do sistema. Porém, a concentração de tamanha informação numa única instituição do governo poderia comprometer a privacidade do cidadão. A coexistência de contas anônimas e contas reconhecidas é possível, podendo-se inclusive determinar limites diferenciados entre elas.

A abordagem desse estudo objetiva encontrar um equilíbrio entre o anonimato e a total falta de privacidade no uso do MCD. Para tanto, o usuário deve identificar-se junto a instituição financeira

de sua preferência para ter sua conta digital ativa. Entretanto, sua identidade seguirá protegida pelo sigilo bancário.

### 5.3.11 Segurança

Para a utilização de um token é necessária a posse do mesmo e da chave privada do certificado que o token declara como proprietário do montante nele descrito. Sem um desses elementos é impossível a utilização ou o furto do numerário digitalizado. Além desse critério, pelo senso comum, o simples fato dos tokens serem rastreáveis já desincentiva a prática de delitos a ele relacionados.

### 5.3.12 Limites definidos pelo BC

Com diferentes tipos de conta e de transação, seria possível definir diversos limites específicos como, por exemplo, limites nos valores de saques, depósitos ou transferências, com valores diferentes para cada tipo de conta. É possível também, colocar limites no número de saques, depósitos ou transferências por período, com valores diferentes para cada tipo de conta.

A colocação de um limite no saldo total da conta digital é possível, porém existe uma situação específica em que, apesar dos melhores esforços, dada a arquitetura atual do sistema, a conta poder exceder um limite estabelecido. Essa situação poderia ocorrer caso houvessem transferências simultâneas para a mesma conta, validadas por validadores diferentes que não estejam em sincronia, cujo valor somado ao saldo pre-existente da conta digital creditada exceda o limite definido. Apesar de ser uma situação limite e pouco frequente, ela é possível. Contudo vale a pena considerar se a própria existência de um limite no saldo de dinheiro digital seria algo desejável para o sistema, uma vez que outros limites e controles podem levar aos mesmos resultados.

Também é possível impor limites no número de contas digitais por cliente bancário. O registro da conta digital proposto seria de responsabilidade dos bancos e a identidade de seu usuário não seria compartilhada com o BC, nem com os outros bancos. Se implementado dessa forma, a fiscalização quanto ao cumprimento desse limite terá que ser feita in loco nos bancos.

### 5.3.13 Diferentes tipos de Contas Digitais

Alguns tipos de conta de dinheiro digital podem ser criados, abaixo segue a descrição de três tipos considerados importantes para o funcionamento do MCD:

- Conta Digital Bancária: Faria parte dos cálculos do compulsório, deverá ser tratada como o equivalente digital ao saldo de moeda física disponível nos bancos. Servem só para atender às operações de saque e depósito da população, na posição de sacado ou depositário, respectivamente. O BC só envia moeda digital para esse tipo de conta. O BC só recebe moeda digital desse tipo de conta. Não pode realizar operações de transferência nem pagamentos. Caso o banco queira operar com o MCD, terá que criar uma carteira de PJ e usá-la para realizar transferências e pagamentos.

- Conta Digital Comercial (Ponto de venda (PDV)): Não está sujeita ao compulsório e deve ser tratada como o equivalente digital ao dinheiro vivo na gaveta das caixas registradoras. Tem como finalidade principal viabilizar o troco digital de pagamento em dinheiro físico nos pontos de venda, pois os pagamentos digitais não necessitam de troco.

- Conta Digital Pessoal (Física ou Jurídica): Não incide compulsório e deve ser tratada como o equivalente digital ao dinheiro físico de posse do cidadão ou empresa. Terá como finalidade principal o uso do numerário digital como guarda de valor e meio de pagamento. Realizará saques, depósitos, transferências e pagamentos dentro dos limites determinados pelo BC.

#### 5.3.14 Combate a lavagem de dinheiro e financiamento ao terrorismo

Caso o sigilo bancário do suspeito seja quebrado por ordem judicial, seria possível rastrear sua movimentação financeira em dinheiro digital. Caso seja necessário, também por ordem judicial, a conta digital pode ser bloqueada impedindo o uso do numerário eletrônico como meio de pagamento. Outros instrumentos de investigação poderão ser utilizados para combater os ilícitos, como por exemplo, a adição de um marcador especial na conta digital que indicará aos validadores não o bloqueio da conta, mas a coleta e envio de todas as informações disponíveis para a localização e monitoramento do criminoso.

#### 5.3.15 Recuperação de conta

Segundo as características do modelo tratado, seria possível prover serviços à população de recuperação de tokens e de contas digitais. Esses serviços seriam realizados pelo sistema bancário à população, utilizando-se para tanto de um sistema disponibilizado pelo BC aos bancos. Os procedimentos relativos a recuperação estão descritos nos itens A.3.3, A.3.4 e A.3.5.

#### 5.3.16 Todo serviço é fornecido em camadas

Todos os serviços prestados pelo BC seriam consumidos pela sociedade por meio do sistema bancário.

### 5.4 Vantagens

- Reduz custos do sistema financeiro nacional.
- Permite o monitoramento em tempo real.
- Aumenta a eficiência e a resiliência do sistema de pagamentos.
- Aumenta a rastreabilidade e permite uma maior eficácia no combate à corrupção.
- Desconcentra os sistemas de pagamentos.
- Responde ao avanço das criptomoedas.
- Potencial aumento da inclusão digital e cidadania financeira.
- Não utiliza tecnologias imaturas.
- Não provoca desintermediação bancária.
- Não impacta significativamente as corridas bancárias.
- Não compete com títulos remunerados nem acordos de recompra.
- Não implica em aumento no balanço patrimonial do banco central.

- Não implica em aumento na demanda por prestação, pelo Banco Central, de atendimento pessoal à população.
- Não altera os papéis fundamentais de banco central.

## 5.5 Riscos de sistema

- **Falsificação e Gasto Duplo**: Todo dinheiro baseado em token se apoia na capacidade do favorecido em verificar a validade do objeto de pagamento. Com o papel-moeda, a preocupação está na falsificação das notas físicas, no mundo digital a preocupação está em verificar se o token é genuíno ou não (falsificação eletrônica) e se ainda não foi gasto em uma transação anterior.

  O Gasto Duplo é um problema em potencial dos tokens digitais, pois há o risco do pagador usar o mesmo token em diferentes transações. Contudo, para evitar esse problema seria necessária a participação de um software validador a cada movimentação, para garantir ao favorecido que esse esteja realmente recebendo o valor apresentado no artefato digital e não uma cópia inválida do valor. Tal sistema de validação poderia ser operado pelo BC ou por instituições financeiras autorizadas e é chamado de validador neste documento.

  Há outras soluções que mitigam o risco de gasto duplo (falsificações) de valores digitais sem a participação de um terceiro a cada transação. Os sistemas de cartões inteligentes (smartcards) recarregáveis, como os usados em bilhetagem de transporte público, são exemplos disso. Esses sistemas, porém, apresentam-se inviáveis para a aplicação de uma moeda digital soberana por diversos fatores:

  - Sua implantação com alcance nacional exigiria vultosos investimentos similares aos já realizados pela indústria de cartões de crédito e débito, pois utiliza-se de hardware específico construído unicamente para este fim.
  - A quebra da segurança segurança física do cartão inteligente é possível, apesar do custo elevado.
  - O descobrimento tardio de uma falha de segurança no hardware poderia exigir a substituição de todos os equipamentos já implantados.

  Em sistemas como o de bilhetagem de transporte público, onde o saldo médio dos cartões inteligentes é baixo, a quebra de sua segurança física é desestimulada. A combinação entre os sistemas de cartões inteligentes e o modelo proposto demandaria uma abordagem específica, em fase de aprofundamento de estudos.

- **Ataque cibernético - furto de numerário**: Como o Banco Central assumiria o papel de supervisor da rede e o sistema teria grande importância no Sistema Financeiro Nacional, ele se tornará ainda mais atraente para ataques cibernéticos. Entretanto é de conhecimento público a capacidade do Banco Central do Brasil em atuar na segurança de seus sistemas, não havendo sofrido qualquer tipo de invasão apesar de ser alvo constante de inúmeros ataques cibernéticos.

  Todavia, caso ocorra uma invasão cibernética bem sucedida, com furto de numerário digital, ou seja, dos tokens armazenados no BCB, o hacker não seria beneficiado pois não possuirá as chaves privadas necessária para a utilização de tais tokens como meio de pagamento. A chave

privada de cada token é de posse e conhecimento apenas do seu proprietário, não estando armazenada no BC ou em qualquer outro participante do SFN.

- **Ataque cibernético - negação de serviço**: Os ataques de negação de serviço, ou DoS (Denial of Service, na sigla em inglês), interrompem a disponibilidade do sistema ao cidadão. Um ataque DoS direcionado ao BC não poderia causar qualquer tipo de interrupção no funcionamento do dinheiro digital. Contudo, dirigido a um validador desprotegido, poderia impactar o fornecimento do serviço de validação dos tokens associados a esse validador. Contudo, há diversas técnicas já empregadas hoje pelos bancos em seus serviços de internet banking e mobile banking, que poderiam ser aplicadas com sucesso para mitigar esse tipo de ataque.

  Além dos mecanismos já utilizados no combate ao DoS, mostra-se possível a implantação de validadores compostos, ou seja, a união de mais de uma instituição no mesmo papel de validador. Essa opção aumentaria a resistência a ataques e a resiliência geral do sistema, porém adicionaria uma latência marginal ao processamento das validações. Se mesmo com a aplicação desses mecanismos houver um ataque DoS bem sucedido, o BC ainda poderá optar por substituir temporariamente o validador desabilitado, seguindo procedimentos de recuperação de desastres a serem definidos na fase de implementação.

- **Falha futura de protocolos**: A abordagem proposta está apoiada em protocolos de criptografia de domínio público de ampla utilização. Eventualmente são descobertas novas técnicas de criptoanálise que podem enfraquecer a sua segurança. Caso algum algoritmo utilizado pelo sistema tenha sido comprometido, sua substituição por uma versão mais segura será realizada tempestivamente pelo BC. O mesmo ocorrerá com todos os sistemas de pagamento e bancários apoiados nas mesmas tecnologias.

## 5.6 Outros riscos

Há fatores que podem interferir no interesse do cidadão pelo dinheiro digital. Dentre eles, destacamos os itens abaixo:

- **Baixa demanda - Concorrência**: Grandes empresas de tecnologia como o Google e o Facebook estão investindo em sistemas de transferências eletrônicas instantâneas. Na Índia, por exemplo, a entrada em operação do Google Tez, em setembro de 2017, contribuiu para o aumento na quantidade de transações instantâneas utilizando a Interface Unificada de Pagamentos (UNI - Unified Payment Interface). O número de transações utilizando esse protocolo passou de aproximadamente 17 milhões/mês para quase 145 milhões/mês de agosto a dezembro de 2017 [14]. Até a data da produção deste estudo, foi divulgada pelo menos uma iniciativa de construção de sistema similar por bancos brasileiros.

  A movimentação de atores privados, nacionais e internacionais, na direção da construção de sistemas de pagamento com características semelhantes ao dinheiro digital apresentado é um indicativo de demanda da população. A presença de uma solução de governo nesse mercado, através da disponibilização de uma nova infraestrutura, bem como a adoção da moeda fiduciária em formato digital, como token transacional, evitaria a concentração dos meios de pagamento nas mãos de poucas instituições privadas e estimularia a manutenção das taxas de operação em valores competitivos, além de permitir, em tempo real, o monitoramento aprofundado dos pagamentos digitais realizados no varejo - mesmo pela economia informal.

- **Baixa demanda - Dificuldade de uso**: É de conhecimento comum que uma fatia da população tem dificuldades na absorção e utilização das novas tecnologias. A dificuldade no manuseio dos celulares pode ser uma barreira na adoção da solução proposta por esse grupo.

  Possíveis ações para mitigação:

  - Realizar ampla divulgação sobre o que é e como funciona o dinheiro digital;
  - Incluir a moeda digital em programas de educação financeira;
  - Realizar um estudo de usabilidade e interface de usuário no manuseio de aplicativos em celular pelo público em geral;
  - Criar concursos, ou Hackathons [15], para incentivar o desenvolvimento de aplicativos de carteira digital pessoal seguros e intuitivos.

- **Baixa demanda - Falta de confiança**: Apesar de supostamente reduzida, uma parcela da demanda por papel-moeda advém da desconfiança no governo e sistema financeiro nacional, principalmente na classe de pessoas que sofreram as ações do confisco de recursos em planos econômicos passados (plano Collor - 1990). É razoável supor que, nesse grupo de usuários, a mesma desconfiança ocorreria com uma moeda fiat digital, uma vez que o sistema permitiria o bloqueio dos valores sem o consentimento do cidadão e não garantiria o anonimato absoluto tal qual o papel-moeda. No mesmo sentido, a solução não se apresentaria atrativa para os criminosos, que tem preferência pelo uso de numerário físico e até moedas virtuais anárquicas.

## 5.7 Questões em aberto

Durante as pesquisas iniciais, houve levantamento (não exaustivo) de uma série de questões, que poderiam ser tratadas de forma mais detida, em fase de estudos aprofundados:

- Quais seriam todas as oportunidades para a política monetária? Quais são os riscos?
- Existe a necessidade de adaptação do arcabouço legal? Quais adaptações deverão ser feitas?
- Quais são os impactos na eficiência econômica e no PIB?
- Como conciliar eventuais concorrências do dinheiro digital com outros meios de pagamento?
- Teremos limitações na infraestrutura de telefonia? Como superar?
- Como promover o uso e disseminar o conhecimento?
- Qual é o melhor caminho para a implantação?
- Até que ponto a digitalização do dinheiro aumentaria a suscetibilidade do sistema financeiro aos crimes cibernéticos?
- Como combater os crimes cibernéticos?
- Como lidar com validadores mal comportados?
- Como lidar com perda/vazamento de chaves privadas?
- Como evitar a criação de contas falsas, contas de “laranjas”?

- Existe risco do dinheiro digital competir com títulos do tesouro como ativos de baixo risco?
- Em um cenário de instabilidade no sistema financeiro, o risco de aceleração de corrida bancária está mitigado?
- Quais seriam as melhores abordagens para facilitar o acesso e incrementar os níveis de inclusão financeira digital?

# 6 Conclusão

As decisões de "design" do meio circulante digital podem acarretar diversas mudanças na forma como o sistema financeiro atual funciona - alterando atores, processos, instrumentos de política econômica e monetária, bem como mecanismos de estabilidade. Esta é a principal razão do modelo tratado adotar uma abordagem pragmática, minimizando os entraves e mitigando incertezas, ao evitar a desintermediação bancária e preservar os papéis fundamentais do Banco Central do Brasil.

Asseveramos, no entanto, que esta abordagem traz consigo uma série de inovações e potencialidades, que poderiam implicar em notável incremento dos níveis de eficiência e inclusão para o Sistema Financeiro Nacional.

Por fim, ressaltamos que o presente documento trate-se apenas de ensaio acadêmico, no sentido de consolidar e aprofundar a compreensão sobre o tema.

# Anexo A: Perguntas Frequentes

## A.1 Sobre o manejo das chaves privadas

### A.1.1 Onde as pessoas vão guardar suas chaves privadas?

Entendemos que ser comum manter a chave privada da conta digital criptografada e armazenada no aparelho celular. Essa será a cópia de uso diário e deverá ser protegida criptograficamente por uma senha local. É aconselhável que os aplicativos de carteira digital peçam ao usuário que defina uma senha (de 4, 6 ou 8 números, por exemplo) para desbloquear os dados armazenados.

### A.1.2 Seria possível fazer cópias de segurança das chave privada?

Seria possível manter um backup da chave privada em outro dispositivo de memória, um pendrive, por exemplo. Na nuvem, se for do interesse do usuário. Será possível até fazer um outro backup em papel da mesma chave, através do registro de doze palavras sorteadas aleatoriamente.

## A.2 Sobre o manejo das contas digitais

### A.2.1 Como bloquear temporariamente uma conta digital?

Cabe ao usuário ligar para seu banco de relacionamento e solicitar o bloqueio temporário de sua conta digital. Caso o cliente não tenha uma relação próxima com seu banco, outras alternativas podem ser oferecidas, por exemplo, ele poderá buscar o backup de sua chave privada, onde estiver armazenado. Inseri-la na carteira digital de outro aparelho de celular ou computador pessoal. Em seguida, solicitar a um validador qualquer o bloqueio temporário de sua conta, através de um comando específico que será criado para este fim.

### A.2.2 Como desbloquear uma conta digital?

Caso deseje desbloquear a conta digital, o cidadão deve apresentar-se ao banco onde abriu sua conta digital e solicitar o desbloqueio pessoalmente.

### A.2.3 Como cancelar definitivamente uma conta digital?

O cancelamento de uma conta digital, bloqueada ou não, seria realizado exclusivamente pelo banco responsável por sua abertura na presença do cliente solicitante. No ato do cancelamento, o banco pode solicitar a criação de nova conta substituta e a transferência dos recursos da conta cancelada para a conta recém criada.

## A.3 Sobre a segurança da solução

### A.3.1 O que fazer se alguém copiar os tokens do cidadão?

O dinheiro continua sendo do cidadão. Pois não há como utilizá-lo sem a chave privada da conta digital a qual pertence o token. Assim que o cidadão fizer uma transação, os tokens copiados serão

consumidos não tendo mais serventia para quem os copiou.

### A.3.2 O que fazer se alguém copiar a chave privada do cidadão?

Só com a chave privada não é possível utilizar o dinheiro digital. É necessário ter também os tokens válidos. Porém, a chave privada é o principal instrumento de segurança do sistema. Assim que possível o cidadão deve seguir os procedimentos de bloqueio temporário de conta digital (item A.2.1). Após o bloqueio realizado o cidadão pode optar pelos procedimentos de desbloqueio (item A.2.2) ou de cancelamento de conta (item A.2.3).

### A.3.3 O que fazer se o cidadão perder seus tokens?

De posse da sua chave privada, o cidadão poderia se dirigir ao banco que abriu sua conta digital e solicitar a recarga dos seus tokens na sua carteira digital. O banco irá acessar o serviço de recuperação de tokens do banco central.

### A.3.4 O que fazer se o cidadão perder sua chave privada?

Deve seguir os procedimentos de bloqueio temporário de conta digital (item A.2.1). Após o bloqueio realizado o cidadão pode optar pelos procedimentos de desbloqueio (item A.2.2) ou de cancelamento de conta (item A.2.3).

### A.3.5 E se o cidadão perder os tokens e a chave privada?

O cidadão deve seguir os procedimentos de bloqueio temporário de conta digital (item A.2.1). Após o bloqueio realizado, o cidadão pode optar pelos procedimentos de desbloqueio (item A.2.2) ou de cancelamento de conta (item A.2.3).

### A.3.6 O que fazer se o cidadão tiver seu celular roubado?

Furtando o celular de um cidadão, o indivíduo que subtraiu o aparelho móvel provavelmente terá acesso a uma cópia criptografada dos tokens válidos e da chave privada do cidadão. Nesse caso, teremos um procedimento similar ao furto de cartões de crédito, conforme descrito no item A.3.5. Em eventual êxito na descriptografia da chave privada do usuário, através de procedimento, em regra, altamente complexo e demorado, a conta digital já estará bloqueada, inutilizando-lhe todos os esforços.

Além desse procedimento, alguns fabricantes de celular já consideraram a possibilidade de implantar uma função de auto-destruição remota do aparelho junto com seus dados. Essa função poderá ser útil no caso de furto de celulares abastecidos com dinheiro digital. Além disso, os fabricantes já estão começando a oferecer soluções de hardware para o armazenamento de chaves privadas em telefones móveis como um mecanismo adicional de segurança.

### A.3.7 E se o criminoso conseguir usar o dinheiro do cidadão antes do bloqueio temporário da conta digital?

Diferentemente do cartão de crédito, onde o banco ressarce o cliente e repassa ao lojista o prejuízo ("charge back"), e do dinheiro físico, que, por não ser rastreável, é de improvável recuperação, com o dinheiro digital, o cidadão poderia seguir o procedimento do item A.3.8.

### A.3.8 O que fazer se o cidadão for vitima de "sequestro relâmpago?"

O cidadão pode solicitar à autoridade policial a instauração do devido inquérito criminal. Este procedimento, mediante autorização judicial, poderá levar à quebra de sigilo da conta digital do próprio cliente e ao rastreamento da conta digital para onde o valor subtraído foi transferido.

### A.3.9 Qual é o mais seguro: o dinheiro físico ou o dinheiro digital?

A segurança do dinheiro físico está na manutenção de sua posse. Uma vez extraviado, por não ser rastreável, é muito difícil reavê-lo. O furto do dinheiro digital exige a subtração dos tokens ativos e a chave privada da respectiva conta digital. Além disso, é preciso também que se transfira o valor furtado para outra carteira digital, ou que use-o na compra de algum produto, antes que a conta seja bloqueada. Como o dinheiro digital é rastreável, a pedido do particular, o sigilo bancário de sua conta poderá ser quebrado, fornecendo os insumos necessários para uma investigação policial.

Os aplicativos de mobile banking, responsáveis hoje pela maior fatia das transações bancárias, são bons exemplos de aplicativos seguros. Mecanismos de segurança semelhantes serão utilizados na construção das carteiras digitais pessoais.

Os sistemas operacionais dos celulares atuais não permitem que um aplicativo acesse dados de outro aplicativo, não sendo possível a um aplicativo mal intencionado furtar os dados da carteira digital sem a autorização expressa do usuário. Mesmo que essa autorização ocorra, os dados da carteira digital armazenados no celular estarão protegidos por uma senha escolhida pelo usuário.

## A.4 Sobre os aparelhos e a conexão

### A.4.1 Quais os requisitos mínimos para um celular operar o dinheiro digital?

Como referência, acreditamos que o aplicativo de carteira digital pessoal iria requerer dos celulares menos recursos que o popular aplicativo 'WhatsApp', que, em maio de 2017, já contava com mais de 120 milhões de usuários ativos no Brasil [16]. Com base nesses dados e tendo em vista a velocidade exponencial dos avanços tecnológicos, fica fácil concluir que a moeda digital brasileira não encontrará na capacidade dos aparelhos de telefonia móvel uma barreira para sua adoção na data de sua implantação.

### A.4.2 Quem poderia desenvolver e distribuir o aplicativo de carteira digital pessoal?

Este aplicativo poderia ser desenvolvido exclusivamente pelo BC ou pelo mercado em geral. Acreditamos que pode existir uma carteira digital pessoal de referência, construída e distribuída pelo BC. Porém, entendemos ser benéfico para a população, e inevitável, que o mercado construa opções, provavelmente mais atrativas que a do BC. Contudo, para garantir a segurança dos usuários do MCD, o BC poderia exercer o papel de homologador dos aplicativos privados, bem como delegar este serviço, dando conhecimento à sociedade dos aplicativos seguros: possivelmente, listando-os em página específica sobre o dinheiro digital no próprio site BC.

### A.4.3 O que fazer se não houver conexão com a internet?

Se uma das partes dispuser de algum tipo de conexão com a internet, ainda que se trate de conexão "discada", ela poderá ser a responsável pela validação da transação, sem prejuízos para o funcionamento do sistema. Se nenhuma das partes tiver qualquer tipo de conexão com a internet, o

pagamento poderá ser realizado normalmente, ficando o creditado como responsável pela realização da validação em momento posterior, quando sua conexão estiver disponível. Nesse momento, se sua transação for rejeitada por duplo gasto, caberá a execução de processos semelhantes aos do recebimento de cheques sem fundo. Em qualquer circunstância, o papel-moeda poderá ser utilizado alternativamente, dado que coexistirá com a solução proposta.

## A.5 Sobre os bits e bytes

### A.5.1 Qual o tamanho dos tokens?

Um token tem 72 bytes, mas o que circulará entre as partes do sistema na verdade são as transações.

### A.5.2 Qual é o tamanho das transações?

O tamanho das transações varia por diversos fatores: o número de tokens consumidos (de 1 a 255 tokens), o número de tokens gerados (1 ou 2), o tipo da transação (saque, depósito, pagamento e etc), os campos auxiliares, que por ventura sejam necessários (número do cliente, para o pagamento de boletos bancários). Para ilustrar, uma transferência simples entre duas pessoas físicas, quando finalizada, poderá ter entre 211 bytes e 8737 bytes (8,5 kilobytes). Contudo, a transação completa só será transferida entre as carteiras digitais. No entanto, entre as carteiras e os validadores, a carga útil transferida é diferenciada.

### A.5.3 Finalmente, quantos bytes trafegam pela rede?

A carga útil transferida depende do tamanho da transação (item A.5.2) e do trecho referente à etapa do processo. Considerando a transação exemplificada no item A.5.2, teremos os seguintes cenários.

- Do usuário para o validador: de 171 bytes a 8697 bytes (8,5 kilobytes).
- Do validador para o usuário, em caso de sucesso: 48 bytes.
- Do validador para o usuário, em caso de erro: 8 bytes.
- Do debitado para o creditado: de 211 bytes a 8737 bytes (8,5 kilobytes).

### A.5.4 Onde ficam esses tokens do dinheiro digital?

Cada transação consome e cria novos tokens. Os tokens criados ficam dentro da própria transação. Só quem tem acesso aos dados de uma transação são as carteiras digitais envolvidas, a instituição validadora e o supervisor do sistema. As transações só devem ficar armazenadas nas carteiras digitais dos donos dos tokens por ela gerados e no supervisor (BC).

### A.5.5 Esse sistema usa a tecnologia Blockchain?

A arquitetura é inspirada no conceito de "Directed Acyclic Graph - DAG", mediante validação distribuída. No entanto, ao contrário da tecnologia Blockchain tradicional, nesta não há blocos, nem cadeias de blocos, não há consenso, nem prova de trabalho, não há mineração, nem 'broadcasts'. O sistema do Meio Circulante Digital só utilizaria tecnologias maduras, comprovadas em batalha

e já utilizadas pelos sistemas financeiros no mundo inteiro há vários anos, como assinaturas e certificados digitais.

### A.5.6 Quanto à performance desse sistema, quantas transações por segundo ele consegue atender?

O número exato de transações por segundo que um notário poderá processar não é conhecido até o momento, posto que o sistema não foi prototipado. Porém, por sua característica de validação distribuída, o aumento do número de transações por segundo do sistema é diretamente proporcional ao número de validadores instalados (escalabilidade horizontal). Cada instituição validadora poderá e deverá operar vários programas validadores simultaneamente. Como não há limites para o número de programas validadores que podem operar em paralelo, dessa forma também não há limites para o número de transações por segundo que o sistema poderá alcançar. Além disso, devido às características minimalistas e paralelas do serviço executado pelo programa validador, podemos estimar, com base em premissas teóricas, o atendimento de um número bastante elevado de transações por segundo, que mostra-se adequado para uma solução de pagamento digital concebida para o varejo, e com baixo custo de investimento em hardware.

## A.6 Sobre câmbio e uso por estrangeiros

### A.6.1 Seria possível fazer câmbio com a moeda digital?

Sim. A corretora de câmbio teria que abrir uma conta digital para o fim específico junto a uma instituição financeira autorizada. A partir desse momento, ela poderá receber e entregar os Reais tanto em papel-moeda quando em formato digital.

### A.6.2 Seria possível para um estrangeiro usar o dinheiro digital brasileiro?

O procedimento de abertura de contas de dinheiro digital sugerido neste trabalho seria através das instituições financeiras. O regulamento para a abertura de contas é que vai definir se será possível para um estrangeiro ter conta em dinheiro digital ou não. Um segundo controle pode ser feito pelos validadores através da região geográfica vinculada ao endereço IP do usuário que está solicitando a validação.

## A.7 Sobre a governança do sistema

### A.7.1 A implantação desse sistema implicaria no fim do papel-moeda?

Não. Ainda que o objetivo principal seja a redução gradual da demanda por dinheiro em espécie, a coexistência dos dois tipos de numerário é esperada por vários anos. No longo prazo, o banco central em questão poderia decidir pela eventual descontinuação da oferta de dinheiro em espécie, caso entenda que a solução em formato digital e sua infraestrutura necessária atingiram um grau de maturidade suficiente para que tal decisão não implique em prejuízos para a sociedade.

### A.7.2 Como seriam feitas as atualizações no sistema do dinheiro digital?

Uma vez em circulação, o dinheiro digital estaria presente em inúmeros aparelhos celulares e computadores pessoais. Porém, o numerário digital possui uma versão, ou família, embutida no

cabeçalho de todos os tokens em circulação. Esse cabeçalho será utilizado para viabilizar a atualização do numerário de forma automática durante sua operação normal.

Com relação ao numerário armazenado em mídias não voláteis para uso como reserva de valor, será utilizado um procedimento semelhante ao das trocas da moeda soberana nacional.

### A.7.3 Qual a relação entre o dinheiro digital de atacado e o dinheiro digital de varejo?

Como o modelo foi idealizado para lidar com transações de varejo desde o início, tratando-se de um caso de uso mais complexo, o sistema teoricamente poderia ser adaptado em algum momento para lidar com transações interbancária - as principais diferenças seriam os tipos de transação, os atores, bem como os limites de transação permitidos. No entanto, poderia ser dispensável no caso do Brasil, já que o país conta com um sistema LBTR bastante funcional.

### A.7.4 Por que existem vários tipos de transação e de contas se todas funcionam do mesmo jeito?

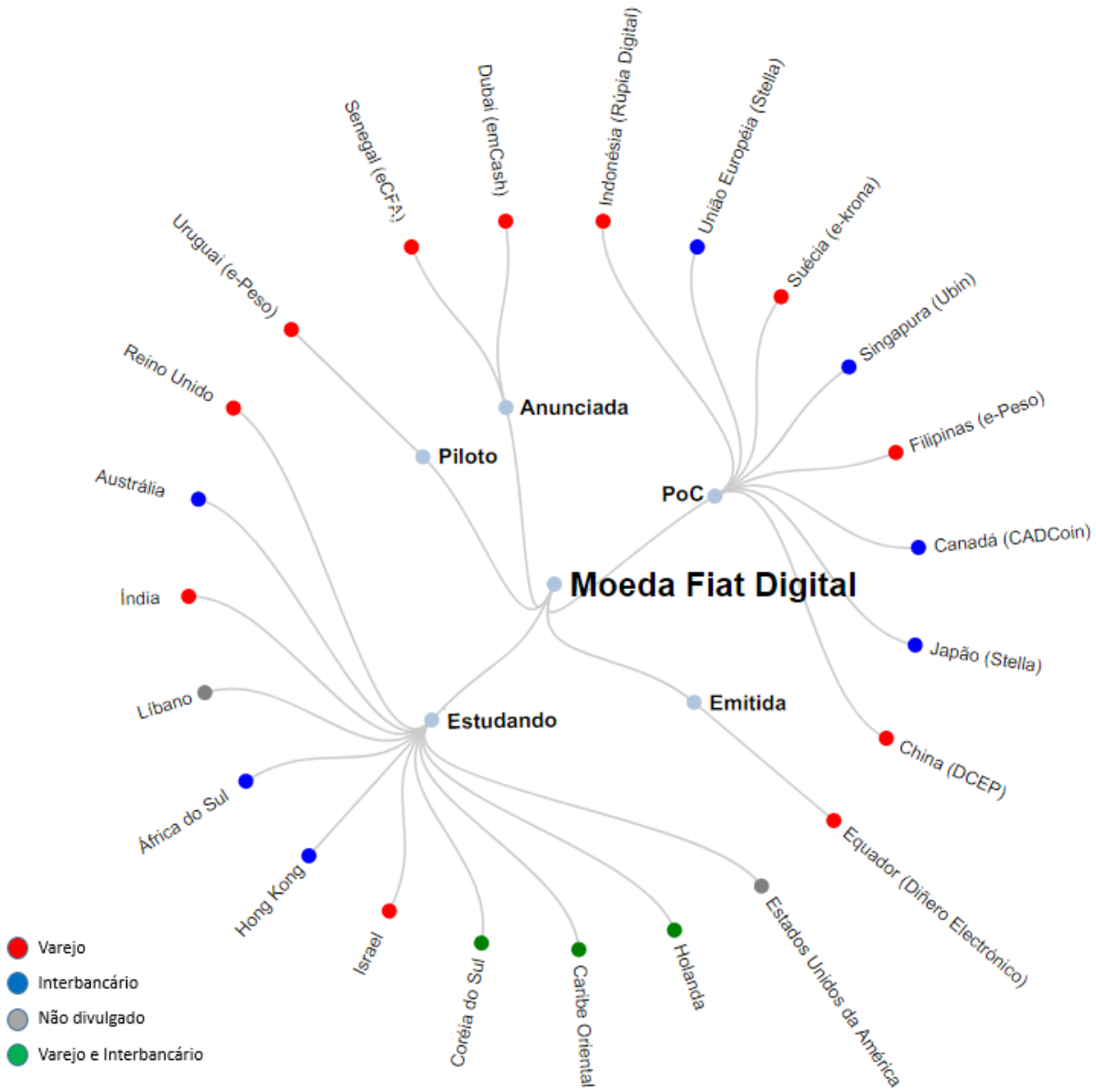
Os diferentes tipos de transação e de contas, listados abaixo, foram criados para permitir um maior controle sobre funcionamento do dinheiro digital. Essa listagem não é final e entendemos ser natural sua atualização, na medida que forem aprofundadas as definições do sistema a ser implantado.

- Tipos de transação:
  - Saque contra reserva bancária,
  - Saque contra conta corrente,
  - Transferência,
  - Transferência interbancária,
  - Pagamento a vista,
  - Pagamento de boleto,
  - Depósito em conta corrente,
  - Depósito em reserva.
- Tipos de contas:
  - Conta de custodia,
  - Conta bancária,
  - Conta comercial,
  - Conta pessoal.

**Anexo B: Moedas Digitais Governamentais – Levantamento**

## B.1 Moeda Fiat Digital

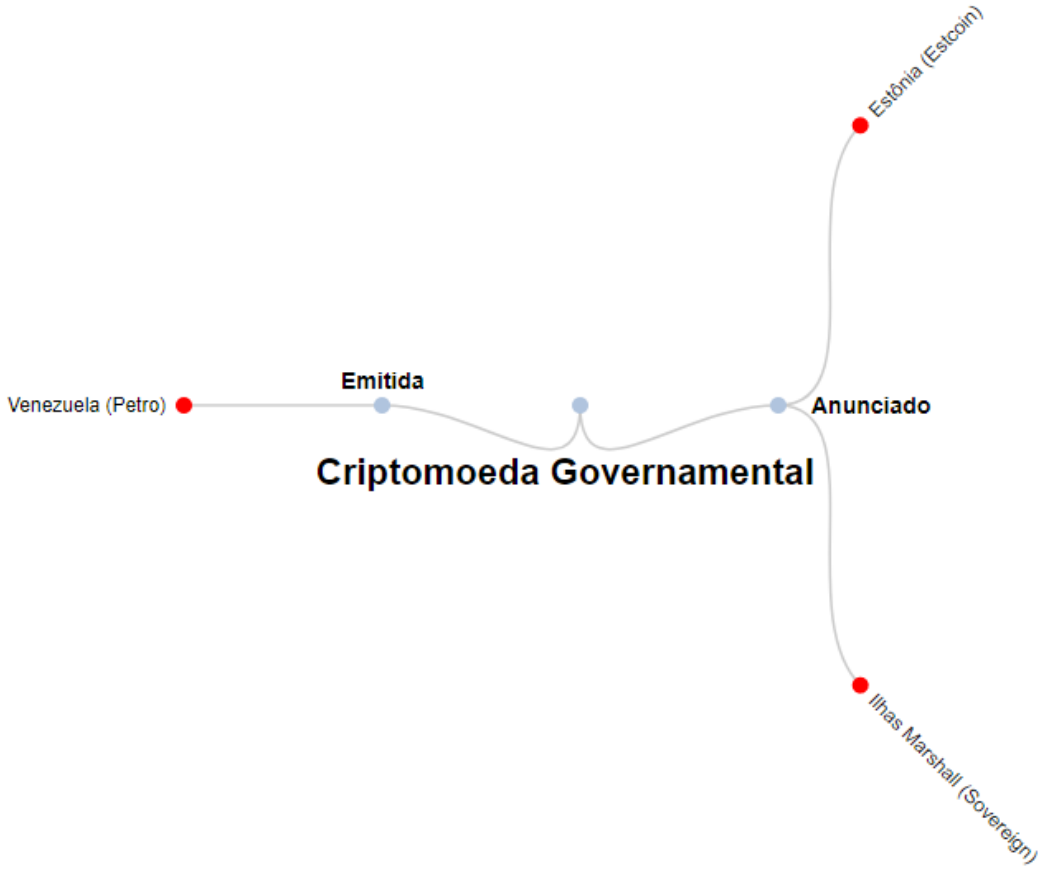
Diversos países estão avaliando ou buscando opções para a desmaterialização de suas moedas. Em alguns casos, o foco se limita à criação ou modernização de sistema de pagamento interbancário - problema resolvido pelo SPB há cerca de 16 anos, no Brasil -, em outros, estudos e testes voltam suas atenções às aplicações destinadas ao varejo, com o fito de complementar ou até substituir o numerário físico. O gráfico abaixo busca resumir e classificar estas experiências, com base em informações e dados públicos.




Referências: Equador [17] [18] Uruguai [19] [20] Dubai [21] [22] Senegal [23] [24] EUA [25] [26] China [27] [28] [29] [30]. Japão [31] [32] União Européia [33] França [34] Canadá [35] Reino Unido [36] Austrália [37]. África do Sul [38] Singapura [39] Hong Kong [40] Suécia [41] Filipinas [42] Indonésia [43] [44] Índia [45]. Libano [46] Caribe Oriental [47] Coreia do Sul [48] Israel [49] Holanda [50]

## B.2 “Criptomoeda” Governamental

As iniciativas listadas nesta seção diferem-se notoriamente da proposta de desmaterialização do numerário. Trata-se, em regra, de mecanismo de financiamento estatal, similar ao adotado por “criptomoedas” privadas - denominado de “Initial Coin Offer (ICO)”. Neste sentido, não são consideradas como uma representação digital de moeda fiduciária, mas apenas uma classe independente de “criptoativos”, com foco especulativo e/ou funcionalidades restritas, quando existentes - em geral, atreladas a um ecossistema específico.




Referências: Venezuela [51] [52] [53] Estônia [54] [55] Ilhas Marshall [56] [57]

# References


[1] World Economic Forum. Unlocking digital value to society: A new framework for growth. http://www.ciab.org.br/download/researches/research-2017_en.pdf. [Online; accessed 3-june-2018].

[2] http://www.abecs.org.br/revista/22/Revista_Abecs_22. [Online; accessed 23-april-2018].

[3] Febraban. Ra 2017 - pg. 51. https://relatorioanual2015.febraban.org.br/pt/download/Febraban-RAO-2015.pdf. [Online; accessed 23-march-2018].

[4] http://www.cnf.org.br/noticia/-/blogs/bancos-investem-ate-r-9-bi-para-proteger-caixas-e-agencias. [Online; accessed 23-april-2018].

[5] http://datatopics.worldbank.org/financialinclusion. [Online; accessed 23-april-2018].

[6] WBG. Global findex report 2017. https://globalfindex.worldbank.org. [Online; accessed 3-june-2018].

[7] http://g1.globo.com/fantastico/edicoes/2017/03/12.html!v/5719023. [Online; accessed 23-april-2018].

[8] https://fidoalliance.org/participate/members-bringing-together-ecosystem. [Online; accessed 23-april-2018].

[9] Banco Central do Brasil. https://bit.ly/2L7OkMg. [Online; accessed 23-march-2018].

[10] Klaus Löber and Aerdt Houben. Committee on payments and market infrastructures markets committee. 2018.

[11] IBGE. http://www.brasil.gov.br/governo/2011/02/demografia. [Online; accessed 23-march-2018].

[12] Agência Nacional de Telecomunicaçoes. http://www.anatel.gov.br/consumidor/telefonia-celular/direitos/cobertura-e-zona-de-sombra. [Online; accessed 23-march-2018].

[13] Agência Nacional de Telecomunicaçoes. http://www.anatel.gov.br/dados/destaque-1/283-brasil-tem-236-2-milhoes-de-linhas-moveis-em-janeiro-de-2018. [Online; accessed 23-march-2018].

[14] https://qz.com/1216715/googles-tez-not-modis-bhim-is-winning-the-upi-payments-race/. [Online; accessed 29-march-2018].

[15] Wikipedia. https://pt.wikipedia.org/wiki/Hackathon. [Online; accessed 29-march-2018].

[16] Estadão. http://link.estadao.com.br/noticias/empresas,whatsapp-chega-a-120-milhoes-de-usuarios-no-brasil,70001817647. [Online; accessed 23-march-2018].

[17] https://www.bis.org/publ/qtrpdf/r_qt1709f.htm. [Online; accessed 23-april-2018].

[18] https://seekingalpha.com/article/4159982-worlds-first-central-bank-electronic-money-come-gone-ecuador-2014minus-2018. [Online; accessed 23-april-2018].

[19] http://www.bcu.gub.uy/Comunicaciones/Conferencias/20171103_BCU_Billete_Digital.pdf. [Online; accessed 23-april-2018].

[20] https://negocios.elpais.com.uy/noticias/funcionan-billetes-digitales-hoy-lanzaron-plan-piloto.html. [Online; accessed 23-april-2018].

[21] http://www.dubaided.ae/English/MediaCenter/Pages/PressReleasesDetails.aspx?ItemId=233. [Online; accessed 23-april-2018].

[22] https://www.khaleejtimes.com/news/government/uae-strategy-to-cash-in-on-blockchain-. [Online; accessed 23-april-2018].

[23] https://qz.com/872876/fintech-senegal-is-launched-the-ecfa-digital-currency. [Online; accessed 23-april-2018].

[24] https://www.ecurrency.net/static/news/201611/press_release_BRM_translated.pdf. [Online; accessed 23-april-2018].

[25] https://www.wsj.com/articles/dudley-says-fed-has-started-thinking-about-official-digital-currency-1511968465. [Online; accessed 23-april-2018].

[26] https://cointelegraph.com/news/us-federal-reserve-has-no-plans-to-introduce-digital-currencies-says-san-francisco-fed-president. [Online; accessed 23-april-2018].

[27] https://www.coindesk.com/chinas-central-bank-opens-new-digital-currency-research-institute/. [Online; accessed 23-april-2018].

[28] https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency. [Online; accessed 23-april-2018].

[29] https://www.ethnews.com/pboc-governor-digital-currency-could-replace-cash-in-china. [Online; accessed 23-april-2018].

[30] http://news.ifeng.com/a/20180309/56592674_0.shtml. [Online; accessed 23-april-2018].

[31] https://www.bloomberg.com/news/articles/2018-04-04/banks-rush-to-turn-japan-cashless-ahead-of-looming-tech-rivals. [Online; accessed 23-april-2018].

[32] https://www.bloomberg.com/news/articles/2018-01-28/japanese-don-t-need-digital-currency-as-they-love-cash-boj-says. [Online; accessed 23-april-2018].

[33] https://www.boj.or.jp/en/announcements/release_2017/data/rel170906a1.pdf. [Online; accessed 23-april-2018].

[34] Morten L Bech and Rodney Garratt. Central bank cryptocurrencies. 2017.

[35] Carolyn Wilkins. Canada explores digital currency.

[36] https://www.bankofengland.co.uk/research/digital-currencies. [Online; accessed 23-april-2018].

[37] http://www.rba.gov.au/speeches/2017/pdf/sp-gov-2017-12-13.pdf. [Online; accessed 23-april-2018].

[38] https://www.coindesk.com/south-africas-central-bank-eyes-jpmorgan-blockchain-tech/. [Online; accessed 23-april-2018].

[39] Monetary Authority of Singapore. Project ubin. http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx. [Online; accessed 3-june-2018].

[40] http://www.legco.gov.hk/yr16-17/english/panels/fa/papers/fa20170418cb1-777-3-e.pdf. [Online; accessed 23-april-2018].

[41] http://www.riksbank.se/en/Financial-stability/Payments/Does-Sweden-need-the-e-krona/Reports. [Online; accessed 23-april-2018].

[42] http://congress.gov.ph/press/details.php?pressid=8212. [Online; accessed 23-april-2018].

[43] https://www.businesswire.com/news/home/20171018006021/en/Indonesia-Takes-Steps-Digital-Fiat-Currency-Solution. [Online; accessed 23-april-2018].

[44] http://www.thejakartapost.com/news/2018/01/29/bank-indonesia-considers-issuing-digital-rupiah.html. [Online; accessed 23-april-2018].

[45] https://www.coindesk.com/indian-central-bank-studies-fiat-cryptocurrency-for-digital-rupee/. [Online; accessed 23-april-2018].

[46] https://themerkle.com/lebanon-to-issue-its-own-digital-currency/. [Online; accessed 23-april-2018].

[47] https://www.coindesk.com/eastern-caribbean-central-bank-pilot-bitt-blockchain-tech/. [Online; accessed 23-april-2018].

[48] https://www.coindesk.com/koreas-central-bank-forms-task-force-to-study-cryptocurrency-impact/. [Online; accessed 23-april-2018].

[49] https://www.reuters.com/article/us-israel-cenbank-currency/israel-central-bank-mulls-issuing-digital-currency-for-faster-payments-idUSKBN1EI0D5. [Online; accessed 23-april-2018].

[50] Ron Berndsen. If blockchain is the answer, what is the question? In *Speech delivered at the Dutch Blockchain Conference, De Nederlandsche Bank*, volume 20, 2016.

[51] http://www.elpetro.gob.ve/index-en.htmlabout. [Online; accessed 26-april-2018].

[52] https://www.bloomberg.com/news/articles/2018-04-12/venezuela-says-government-bodies-must-soon-accept-cryptocurrency. [Online; accessed 26-april-2018].

[53] https://oilprice.com/Latest-Energy-News/World-News/Venezuelan-Parliament-Finally-Approves-Oil-Backed-Cryptocurrency.html. [Online; accessed 26-april-2018].

[54] https://qz.com/1072740/mario-draghi-of-the-ecb-dashes-estonias-plan-for-an-estcoin-cryptocurrency-backed-by-the-government. [Online; accessed 26-april-2018].

[55] https://e-estonia.com/were-planning-launch-estcoin-only-start. [Online; accessed 26-april-2018].

[56] https://www.sov.global. [Online; accessed 26-april-2018].

[57] https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD. [Online; accessed 26-april-2018].