Faculdade de Economia,
Administração e Contabilidade
de Ribeirão Preto
Universidade de São Paulo

Universidade de São Paulo

Texto para Discussão

Série Economia

TD-E 01 / 2018

CRIPTOMOEDAS E TEORIA MONETÁRIA: UMA INTRODUÇÃO

Jefferson Bertolai – Victor Oliveira

Av. Bandeirantes, 3900 - Monte Alegre - CEP: 14040-905 - Ribeirão Preto - SP
Fone |16| 3315.4961 - e-mail: apoiopq@fearp.usp.br site: www.fearp.usp.br

Universidade de São Paulo

Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto

Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto
Avenida dos Bandeirantes,3900
14040-905 Ribeirão Preto – SP

A série TEXTO PARA DISCUSSÃO tem como objetivo divulgar: i) resultados de trabalhos em desenvolvimento na FEA-RP/USP; ii) trabalhos de pesquisadores de outras instituições considerados de relevância dadas as linhas de pesquisa da instituição. Acesse a página eletrônica da Comissão de Pesquisa das FEA-RP/USP em https://www.fearp.usp.br/pesquisa. Informações: apoiopq@fearp.usp.br ou 55 16| 3315.4961.

Criptomoedas e Teoria Monetária: uma introdução*

Jefferson Bertolai† & Victor Oliveira
FEARP-USP

19 de Julho de 2018

Resumo

O tradicional conceito de moeda é limitado e insuficiente para estudar o fenômeno *"criptomoedas"*. Um conceito de moeda mais sofisticado é apresentado neste artigo como alternativa superior para estudar e analisar criptomoedas. Sua utilização permite concluir que a grande inovação monetária das criptomoedas foi viabilizar a geração de evidência *confiável* e *flexível* de produção de bens/serviços *sem* o uso de *monitoramento* de ações dos responsáveis por sua emissão e gerenciamento.

A principal contribuição deste artigo é disseminar (*i*) o conceito alternativo de moeda e (*ii*) o conceito fundamental de criptomoeda do ponto de vista da Teoria Econômica. Tal contribuição é especialmente importante para o meio acadêmico brasileiro, no qual estes conceitos são pouco conhecidos.

Classificação JEL: E42
Palavras-Chave: criptomoedas, moeda, monitoramento, bitcoin

*Agradecemos as críticas e sugestões de Milton Barossi Filho, Fernando Barros Jr., Ricardo Cavalcanti, Karina Justino, Aline Pinheiro e Julio M. Pires, assim como aquelas dos participantes dos seminários de pesquisa na FEARP/USP, FACE/UFMG e FCE/UFRGS. Eventuais erros e omissões ainda presentes no texto são de responsabilidade dos autores. Victor Oliveira agradece o financiamento via Bolsa de Mestrado do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq.

†Autor correspondente: jbertolai@fearp.usp.br.

Introdução

O recente surgimento de *criptomoedas*[1] estabelece um desafio para o conceito de moeda tradicionalmente encontrado em livros-texto de Macroeconomia e, em particular, de Economia Monetária:

> Como estudar o fenômeno "criptomoedas" utilizando a definição tradicional segundo a qual moeda é um objeto que cumpre as funções de (i) unidade de conta, (ii) meio de troca e (iii) reserva de valor?

É motivação e ponto de partida deste artigo que este conceito de moeda é limitado e insuficiente para esta tarefa. Ele é mais uma *descrição* das funções que a moeda desempenha do que uma *explicação* do que é moeda (Kocherlakota, 1998b).

Consistente com tal limitação, as tentativas de estudar criptomoedas utilizando este conceito se orientam pela discussão sobre o cumprimento ou não das três funções *"definidoras"* de moeda e, com base na grande volatilidade da evolução dos preços das criptomoedas até o momento, concluem equivocadamente que criptomoedas não são moedas. Ainda mais importante, esta orientação da análise não permite reconhecer com a devida atenção a importância da tecnologia de legitimação de transações desenvolvida e utilizada pelas criptomoedas (a *blockchain technology*).

Um conceito de moeda mais sofisticado e completo é apresentado como alternativa superior para estudar e analisar criptomoedas. Seguindo a abordagem de *Desenho de Mecanismos*, a moeda é entendida neste conceito alternativo como parte fundamental de uma instituição criada pela sociedade para resolver o *problema de dupla coincidência de interesses* e, assim, melhorar o bem estar dos indivíduos. No jogo implicado por esta instituição, o uso de um objeto como meio de troca viabiliza produção e consumo de bens e serviços em situações sem coincidência dupla de interesses.

A moeda emerge como um substituto para outros esquemas (instituições) de viabilização de trocas. Em economias minimamente especializadas, o problema de dupla coincidência de interesses não pode ser resolvido eficientemente via *escambo*: a especialização produtiva dos indivíduos torna a coordenação de interesses requerida pelo escambo um processo proibitivamente custoso. O problema tampouco pode ser resolvido eficientemente via *crédito*, dada a incapacidade dos indivíduos em se comprometer a cumprir

[1] O conceito de criptomoeda é frequentemente também referido como *moeda digital* ou *moeda virtual*. Seguindo Halaburda and Sarvary (2016), moedas digitais com gerenciamento *descentralizado* serão aqui denominadas criptomoedas. Adicionalmente, a `Bitcoin` (https://bitcoin.org) será considerada representativa das criptomoedas. Embora exista várias outras criptomoedas cujo protocolo (desenho) não coincide exatamente com o protocolo Bitcoin (Nakamoto, 2008), elas são essencialmente equivalentes do ponto de vista mais abstrato deste artigo. Ver Halaburda and Sarvary (2016), Antonopoulos (2014, 2017) e Narayanan et al. (2016) para discussões sobre diferenças entre as criptomoedas até então criadas.

promessas. Um esquema de crédito entre indivíduos sem comprometimento (*commitment*) requer uma *tecnologia de monitoramento* de ações individuais a fim de identificar, punir e, assim, inibir eventuais falhas de cumprimento de promessas. A não disponibilidade de ampla tecnologia de monitoramento inviabiliza o uso do crédito como alternativa social para induzir produção e consumo em toda a economia.

Ao substituir o crédito como instituição criada para induzir produção e consumo na economia, interpreta-se a

> "moeda como um substituto para tecnologias de registros (*record-keeping*)"[2].

Mais especificamente, a moeda cumpre o papel social de "registrar transações" ao servir de evidência *confiável* de produção (de bens e serviços) em situações nas quais não há tecnologia de monitoramento de ações individuais (*record-keeping*) para cumprir este papel. A posse de moeda é uma prova de produção no passado: ela substitui o histórico de transações do indivíduo utilizado no esquema de crédito.

A interpretação da moeda como evidência confiável de produção induz a análise de criptomoedas de forma natural e direta a reconhecê-las como moeda e a identificar como sua inovação fundamental a tecnologia de legitimação de transações na qual estas se baseiam.

Esta tecnologia de legitimação, baseada na tecnologia *blockchain* e no conceito de *proof-of-work* a ela associado, foi desenhada para tornar eventuais fraudes ao sistema contábil (de transmissão de propriedade) da criptomoeda um procedimento proibitivamente custoso. A inovação nesta estratégia de proteção contra fraudes é *não haver necessidade de monitorar* os indivíduos envolvidos no gerenciamento do sistema monetário ao mesmo tempo em que há enorme *flexibilidade* de formatação das criptomoedas, sendo possível otimizar propriedades importantes para o desempenho da função de moeda, como escassez, durabilidade e divisibilidade.

Esta inovação faz parte de um longo processo de aperfeiçoamento tecnológico dos meios de troca. Historicamente, a sociedade superou/minimizou as imperfeições físicas da moeda ao adotar meios de troca reproduzíveis e configuráveis. Inicialmente, os objetos utilizados como moeda eram mercadorias ou objetos (virtualmente) sem valor intrínseco cuja emissão e configuração de propriedades eram bastante custosas (se não impossíveis)[3]. Concomitantemente à sofisticação da divisão do trabalho (especialização produtiva), moedas mais flexíveis e de emissão mais barata foram adotadas. Certificados de dívida (em sua maioria certificados de depósitos) e papel moeda sem lastro se destacam nestes quesitos ao viabilizar (i) a configuração de propriedades como durabilidade e divisibilidade

[2]Conforme estabelecido por Kocherlakota (1998a) e discutido de forma mais didática por Kocherlakota (1998b).

[3]Halaburda and Sarvary (2016), por exemplo, destacam o uso de cevada, sal e conchas como moeda.

por meio da simples anotação de tais informações no meio de troca e (*ii*) a emissão de novas unidades de moeda por meio de uma simples assinatura no meio de troca.

A flexibilização da emissão e configuração do meio de troca permitiu otimizar suas propriedades e administrar sua escassez. Esta última atividade, no entanto, demandou o uso da escassa tecnologia de *record-keeping* da sociedade para monitorar os responsáveis pela emissão e gerenciamento da moeda[4] — um subgrupo de indivíduos denominados *bancos* (dentre eles o Banco Central). Sem a coordenação de atividades proporcionada por este monitoramento, a ação descentralizada destes indivíduos inviabilizaria a moeda por meio da excessiva emissão monetária (endividamento) e da escassa destruição de moeda (resgate de dívidas).

O desenvolvimento das criptomoedas é mais um passo neste aprimoramento histórico dos meios de troca, no sentido de que seu desenho permite otimizar propriedades da moeda e administrar sua escassez sem a necessidade de monitorar os responsáveis pelo seu gerenciamento. A flexibilidade de configuração decorre diretamente de sua natureza eletrônica e a dispensabilidade de monitoramento é possível devido ao alto custo computacional que, por construção, é requerido para fraudar o sistema monetário.

Além desta introdução e das considerações finais, este artigo se divide em 3 seções. A seção 1 discute a tecnologia de legitimação de transações na qual se baseiam as principais criptomoedas: a tecnologia *blockchain* e o conceito de *proof-of-work*. Na seção 2 são apresentadas de forma mais detalhada o conceito alternativo de moeda, sua interpretação como substituto para tecnologias de *record-keeping* e a importância da tecnologia de monitoramento para o sistema monetário. Em ambas as seções, a sofisticação conceitual é introduzida de maneira gradual a fim de suavizar a exposição — embora esta estratégia implique em um texto mais longo. A tecnologia de legitimação apresentada na seção 1 e o conceito de moeda apresentado na seção 2 são utilizados na seção 3 para discutir em detalhes a limitação/insuficiência do tradicional conceito de moeda e a inovação monetária fundamental das criptomoedas.

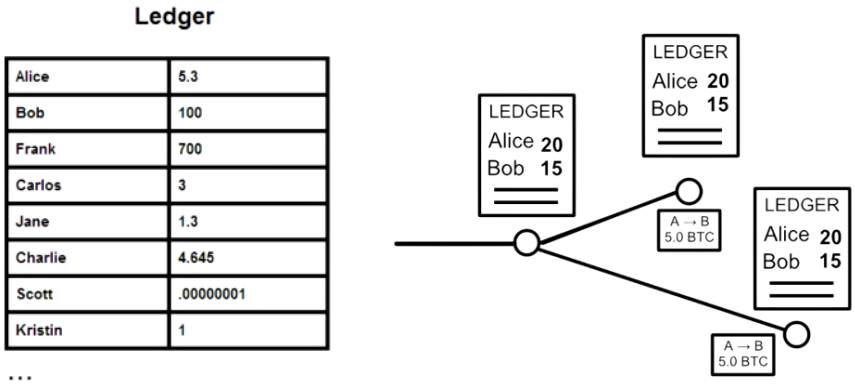
1 A tecnologia de legitimação das criptomoedas

De maneira bastante simplificada e conceitual, a tecnologia contábil utilizada pelas criptomoedas é um arquivo eletrônico que armazena a quantidade de moeda (digital/virtual) de cada pessoa cadastrada na rede de computadores da respectiva criptomoeda[5]. Ou seja, a tecnologia é um livro-razão (*ledger*) que mantém atualizado o saldo monetário (virtual) de cada pessoa. A Figura 1a ilustra esta definição simplificada com um exemplo de in-

[4]Ver Cavalcanti et al. (1999) e Cavalcanti and Wallace (1999a,b).

[5]Esta seção é baseada em grande parte em Driscoll (2013) e Antonopoulos (2014, 2017).

formação armazenada no livro-razão (*ledger*). Neste exemplo, `Alice` possui atualmente 5,3 unidades de moeda, `Bob` possui 100 moedas, Frank 700 moedas e assim por diante.



(a) Livro-razão (*ledger*) (b) Atualização dos *ledgers*

Figura 1: Ilustração simples da tecnologia de *record-keeping* (Driscoll, 2013).

Neste sentido, esta tecnologia é bastante similar ao livro-razão utilizado pelo sistema bancário para manter atualizado o saldo monetário (eletrônico) de cada pessoa depositado no sistema[6]. A inovação central da tecnologia contábil 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. Enquanto no sistema bancário, a autenticidade das informações é garantida de forma *"centralizada"* pelos bancos (e pelo Banco Central), na tecnologia das criptomoedas ela é garantida de forma *"descentralizada"* pelos computadores conectados à rede da criptomoeda.

Cada computador conectado à rede da criptomoeda mantém uma cópia do livro-razão. Atualiza sua cópia ao receber mensagens de transação monetária e as repassa para outros computadores da rede[7]. A Figura 1b ilustra a comunicação entre computadores da rede de uma *transação* monetária entre `Alice` e `Bob`, na qual é informado que `Alice` pagou 5 unidades de criptomoeda (Bitcoin - BTC) para `Bob`. Neste caso, `Alice` comunica toda a rede de computadores sobre esta transação e, após receber tal mensagem, cada um dos computadores atualiza sua cópia do livro-razão reduzindo o saldo monetário de `Alice` em 5 unidades e elevando o saldo de `Bob` em 5 unidades[8]. A legitimidade da transação é garantida por meio da verificação de que `Alice` possui saldo suficiente para ser enviado para `Bob` e de que foi de fato `Alice` quem enviou a mensagem.

[6]Para uma descrição didática e introdutória sobre os detalhes da movimentação monetária no sistema bancário, ver Brown (2013).

[7]Segue desta característica a denominação *Distributed Ledger Technology* - DLT. Na verdade, nem todos os computadores conectados a rede se comportam exatamente desta forma. Para o propósito deste artigo, no entanto, este detalhe será omitido. Ver Antonopoulos (2014, 2017) e Narayanan et al. (2016).

[8]Uma transação verdadeira/real comunicada à rede às 16:15hs (horário de Brasília) do dia 10 de março de 2018 pode ser visualizada neste link.

1.1 A legitimidade da transação e o anonimato

A autoria da mensagem de `Alice` na ilustração da figura 1b é *criptografada* antes de ser enviada à rede a fim de preservar o anonimato de `Alice` nesta transação. A "autoria da mensagem" é verificável por meio de uma *assinatura digital* que `Alice` faz na transação utilizando sua *chave privada*[9], uma assinatura que somente `Alice` (ou alguém em poder da chave privada de `Alice`) é capaz de fazer. Os computadores da rede conferem se a assinatura de fato foi gerada pela chave privada de `Alice` por meio de uma função matemática. Esta função utiliza como insumos a assinatura na transação, o conteúdo da mensagem (transação) e a *chave pública*[10] de `Alice`. Ela gera resultado 1 (positivo) se de fato a assinatura foi feita com a chave privada de `Alice` e gera resultado 0 (falso) caso contrário[11]. Dessa forma, a verificação de "autoria" revela que a assinatura foi produzida com a chave privada de `Alice`, sem revelar sua identidade.

A disponibilidade de saldo monetário de `Alice` não é verificada simplesmente consultando o livro-razão, uma vez que a rede de computadores *não literalmente* armazena os saldos monetários de cada pessoa. Na verdade, a rede armazena as transações de cada unidade de moeda, desde sua emissão. Ou seja, são armazenadas somente as transferências de propriedade de cada unidade de moeda. No exemplo da figura 1b, a informação armazenada é a transação (mensagem) enviada por `Alice` à rede de computadores e não exatamente os saldos dos usuários.

Como então é possível verificar se `Alice` possui saldo monetário suficiente para transferir a quantia especificada na transação para `Bob`?

Para tornar possível tal verificação, `Alice` informa na mensagem (transação) que envia à rede de computadores transações prévias, nas quais ela recebeu as moedas que quer gastar na transação atual. Na figura 1b a transação foi apresentada de forma simplificada: ela continha apenas informação sobre a origem e destino do pagamento e a quantia transferida. Na realidade, a transação tem como insumos referências às transações nas quais `Alice` recebeu as moedas que quer gastar, conforme ilustrado na figura 2 (na qual, a sigla `txn` denota transação).

[9] Uma espécie de senha que permite abrir a conta (desbloquear o saldo) de `Alice` e gastar seu saldo.

[10] Para o propósito deste artigo, esta chave pública pode ser entendida como o endereço eletrônico de `Alice` na rede. Na figura 1b a chave pública de `Alice` é a letra A e a chave pública de `Bob` é a letra B. Para entender a diferença entre chave pública e endereço na rede, ver Antonopoulos (2014, 2017) ou Narayanan et al. (2016).

[11] Uma explicação mais detalhada/técnica do funcionamento da tecnologia de legitimação de transações das criptomoedas está além do escopo deste artigo. Para uma exposição enxuta, introdutória e bastante didática sobre este assunto, ver Driscoll (2013). Para uma discussão mais completa do ponto de vista da Ciência Econômica, ver Halaburda and Sarvary (2016). Para uma discussão mais completa do ponto de vista computacional, ver Antonopoulos (2014, 2017) e Narayanan et al. (2016).

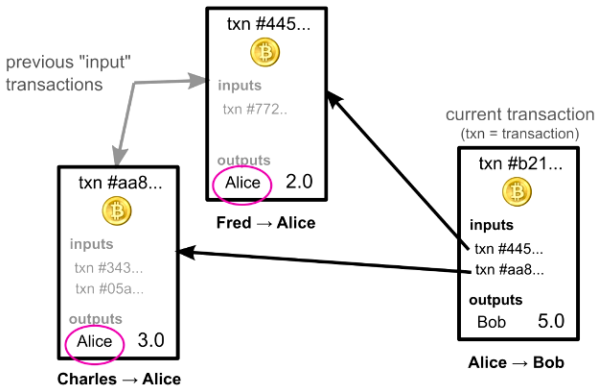


Figura 2: Transações possuem referências a transações anteriores (Driscoll, 2013).

Ao receber a transação informada por `Alice`, a rede de computadores verifica se as transações anteriores por ela referenciadas existem de fato e, adicionalmente, se o saldo obtido por `Alice` nestas transações não foi gasto (referenciado) em outras transações. Caso verificada a existência de saldo suficiente, a transação é aceita pela rede e armazenada por cada um de seus computadores.

Ao armazenar a lista com todas as transações já aceitas como legítimas, a rede de computadores não precisa construir/armazenar o livro-razão com o saldo monetário de cada pessoa a fim de verificar se há saldo disponível para a atual transação. Basta verificar se as unidades de moeda referenciadas como insumos na transação atual existem e não foram gastas até então. De fato, seria necessário conhecer todas as chaves públicas de uma dada pessoa para computar seu saldo monetário: bastando somar os valores das transações nas quais esta pessoa (suas chaves públicas) recebeu moedas e subtrair do resultado os valores das transações nas quais esta mesma pessoa (suas chaves públicas) gastou moedas.

Esta forma de verificação de saldos permite ocultar da rede de computadores o saldo monetário de cada pessoa e, assim, aumentar o grau de anonimato dos usuários. Para isso, o endereço da pessoa na rede da criptomoeda (chave pública) é gerado de forma aleatória, sem relação alguma com sua identidade — embora a chave pública tenha sido ilustrada na figura 2 de maneira simplificada como o primeiro nome do usuário. Adicionalmente, cada pessoa é capaz de gerar várias chaves públicas para armazenar unidades de moeda sem informar a rede de computadores a identidade do proprietário de cada uma das chaves.

Em resumo, é possível participar das transações monetárias com um alto grau de anonimidade, uma vez que a rede de computadores sabe a distribuição de moeda entre as chaves públicas, mas não sabe a distribuição de chaves públicas entre as pessoas[12].

[12]No entanto, o anonimato não é completo na rede Bitcoin. Há formas sofisticadas de se rastrear indivíduos na rede (Antonopoulos, 2014). Tal possibilidade tem motivado contínuo esforço no aprimoramento do protocolo Bitcoin para aumentar seu grau de anonimato. Adicionalmente, novas criptomoedas

1.2 A tecnologia *blockchain*

A assinatura digital da transação provê ao mesmo tempo anonimato e autoria para a mensagem. O anonimato dos usuários também decorre do "armazenamento do livro-razão" por meio do armazenamento da lista completa de transações: sem a totalização do saldo monetário de cada pessoa. A verificação de suficiência de saldo monetário, por sua vez, impede que se gaste o saldo mais de uma vez (*double spending*): ao serem informados de duas transações fazendo referência à uma mesma transação anterior, os computadores da rede (por padrão) aceitam como legítima a primeira transação recebida e descartam a outra como ilegítima.

Em um sistema contábil centralizado, tal verificação de saldo é suficiente para evitar que algum usuário gaste seu saldo mais de uma vez. De forma análoga, se a ordem de recebimento/verificação/aceite das mensagens (transações) fosse a mesma para todos os computadores do sistema descentralizado das criptomoedas, não haveria possibilidade de gasto duplo. Ao receber duas transações fazendo referência a uma mesma transação anterior, ***todos*** os *nós* (computadores) da rede aceitariam a primeira mensagem recebida/verificada e descartariam a segunda.

Lembre-se, no entanto, da característica descentralizada do sistema (cada nó recebe a transação e a repassa para outro nó), a qual faz com que o caminho de cada mensagem até chegar a todos os nós da rede seja diferente[13]. Logo, a ordem de recebimento de cada transação é, em geral, distinta em cada nó. Com isso, em um dado instante do tempo, a *lista ordenada* de transações recebidas por um dado nó é diferente da *lista ordenada* recebida por outros nós. Se utilizado o procedimento de legitimar somente a primeira transação recebida, ocorreria inconsistência entre os "livros-razão" distribuídos na rede. Uma dada transação (e suas consequências contábeis) seria aceita como legítima por uma parte da rede e seria descartada pela outra parte.

Para uniformizar a ordem de *aceite* das transações entre os nós da rede e, assim evitar inconsistências entre os "livros-razão" distribuídos, "o sistema descentralizado '*elege*' um nó de cada vez" para criar um grupo (*bloco*) de transações e comunicá-lo aos demais nós da rede. Após a verificação de que não há transação ilegítima no bloco e de que o autor deste foi de fato eleito, o bloco é aceito pelos demais nós. Assim, haverá concordância entre os nós sobre quais transações devem ser aceitas como legítimas — deve-se aceitar o bloco de transações proposto pelo nó eleito.

A sequência de nós eleitos para construir e propor blocos determina uma sequência (cadeia) de blocos, a *blockchain*, conforme ilustrado na figura 3. A ordenação entre

com grau de anonimato muito maior (como `Zerocash` e `Cryptonote`) foram propostas.

[13]Também importante para tal propriedade, a rede de computadores não é interligada de forma serial. De fato, a rede de computadores (nós) se organiza sem topologia ou estrutura fixa (Antonopoulos, 2014).

os blocos é armazenada por meio do registro em cada bloco (junto com as transações incluídas neste e antes da publicação deste) de uma referência ao bloco anterior.

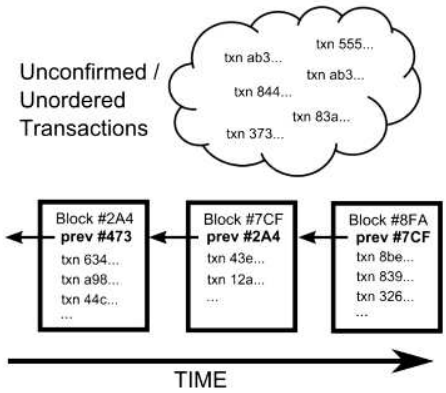


Figura 3: A cadeia de blocos – *blockchain* (Driscoll, 2013).

Na ilustração da figura 3, o último bloco incluído se refere ao bloco anterior registrando o código `#7CF`, denominado a impressão digital (*fingerprint*) do bloco anterior. Analogamente, o código `#2A4` é o *fingerprint* do primeiro bloco da ilustração e o código `#8FA` é o *fingerprint* do terceiro bloco.

Assim como tudo feito pela rede de nós, a referida eleição de nós é executada de maneira descentralizada[14]. Cada nó da rede é capaz de construir seu bloco usando transações que recebeu até então, denominadas *transações não confirmadas* (ver figura 3). Mas o nó será "eleito" para propor seu bloco à rede somente se encontrar uma solução para um problema matemático associado ao bloco construído, denominada *proof of work*. Assim, o primeiro nó a resolver seu problema matemático é reconhecido (descentralizadamente) como o nó eleito para incluir seu bloco na *blockchain*.

1.3 O conceito *Proof-of-Work*

A solução de uniformização da ordem de aceite (ou ainda, uniformização do conjunto de transações aceitas como legítimas) requer que o referido sistema de eleição descentralizada resulte em um único vencedor. Em casos de empate, há mais de um bloco para ser incluído na *blockchain* e, com isso, a inconsistência entre diferentes listas ordenadas de transações se mantém. Como solução, o protocolo das criptomoedas usa como critério de desempate o nó vencedor da eleição seguinte e minimiza a probabilidade de empate[15].

[14]Tal eleição é denominada como mineração (*mining*), pois o nó eleito recebe o direito de emitir (coletar) uma determinada quantidade de (novas) moedas. Nesta nomenclatura, os candidatos na eleição são denominados mineradores (*miners*).

[15]Uma solução trivial para o problema de empates é eleger sempre o mesmo nó. No entanto, isso contraria a característica descentralizada do sistema e, portanto, reduz sua robustez. Ao tornar a rede tão dependente de um só nó, bastaria atacar este nó para atacar toda a rede. De fato, a adoção desta

Após um empate entre nós (blocos) vencedores, cada nó aceita (adiciona ao final de sua cópia da *blockchain*) o primeiro bloco vencedor recebido e descarta os demais. Assim, cada bloco vencedor será aceito por uma parte da rede de nós e, portanto, múltiplas versões da *blockchain* passarão a coexistir na rede — se diferenciando no último bloco. O desempate ocorre em favor do último bloco adicionado na *blockchain* do vencedor da eleição seguinte. A versão armazenada pelo vencedor da próxima eleição é adotada por toda a rede e as demais versões são descartadas[16].

Durante o procedimento de desempate descrito, os blocos vencedores presentes nas versões descartadas da *blockchain* são desfeitos: as transações neles incluídas recebem novamente o *status* de não confirmadas e serão incluídas em blocos futuros (se não está entre — e não há contradição com — as transações presentes na versão atual da *blockchain*). Logo, embora efetivo, o procedimento de desempate aumenta o tempo esperado para confirmação das transações monetárias e, portanto, deve ser evitado.

A fim de reduzir a probabilidade de empate — e, portanto, do procedimento de desempate —, soluções para o problema matemático a ser resolvido pelos nós candidatos, denominadas *proof of work*, são obtidas somente de forma aleatória. Cada um dos nós procura uma solução para o seu problema via tentativa e erro (força bruta) em uma enorme lista de alternativas. Como não é possível *a priori* estabelecer relação alguma entre as eventuais soluções e a lista de alternativas[17], o primeiro nó a encontrar a solução será determinado aleatoriamente.

Quem, por acaso, encontrar uma solução antes dos demais terá obtido uma *proof-of-work* para seu bloco a utilizará para demonstrar aos demais nós da rede descentralizada que o direito de incluir o próximo bloco na *blockchain* foi obtido.

> Qual é a necessidade de requerer dos candidatos a solução para um problema matemático que, na prática, somente pode ser resolvida por tentativa e erro?

Afinal, o procedimento de procura via força bruta consome relevante montante de recursos — principalmente energia elétrica. O ponto central em requerer de cada nó da rede a

solução centralizada é vista como a principal razão pela qual iniciativas de criação de criptomoedas falharam na década de 1990, conforme discutido por Narayanan et al. (2016).

[16]Obviamente, na ocorrência de um novo empate, o critério de desempate para o novo empate será o vencedor da eleição seguinte a este empate. Veja o capítulo 8 de Antonopoulos (2014) para uma discussão mais detalhada sobre o critério de desempate.

[17]Tal propriedade decorre de o problema matemático ser definido por uma *função hash*, a qual gera para cada ponto x do domínio (conjunto de possíveis blocos de transações) um resultado $f(x)$ no contra-domínio (conjunto de números de tamanho `256 bits = 32 bytes`) sem relação 'aparente' com x. A solução do problema matemático é um ponto x^* do domínio da função *hash* que gera imagem (por meio desta função) abaixo de um determinado valor, $\bar{y}$. Ou seja, x é solução do problema $(f, \bar{y})$ se $f(x) < \bar{y}$. Cada bloco $x = (x_H, x_B)$ é composto pelo corpo do bloco, x_B, onde se localizam as transações, e pelo cabeçalho do bloco, x_H, onde estão os *fingerprints* do bloco atual e do bloco anterior (como na figura 3). Além dos *fingerprints*, o cabeçalho x_H possui um número chamado *nonce*, a ser escolhido durante a procura dos nós pela solução. Mais detalhes podem ser obtidos em Antonopoulos (2014).

procura em uma enorme lista de alternativas (uma tarefa computacionalmente muito custosa[18]) é prover *confiança* às informações registradas na *blockchain* — prover proteção contra fraudes.

Para fraudar as informações registradas na *blockchain*, é necessário propor um novo bloco (o bloco fraudado) à rede nós, mas este bloco somente será aceito se for proposto junto com a respectiva *proof-of-work*. Como toda mudança no bloco (por menor que esta seja) gera um novo problema matemático, cuja solução guarda relação 'aparente' nenhuma com aquela do bloco a ser substituído, a fraude demanda uma nova procura por solução[19].

Observação 1 *Ao elevar o custo computacional da procura pela solução, eleva-se também o custo de fraudar a blockchain.*

Embora necessária para a fraude, a apresentação da *proof-of-work* do bloco fraudado não é suficiente. Enquanto a versão da *blockchain* gerada pela fraude for menor – em número de blocos – do que a versão gerada sem a fraude, os demais nós da rede não aceitarão o bloco fraudado. Se eventualmente a versão do fraudador acumular mais blocos do que a versão não fraudada, toda a rede de nós (por padrão) descartará a *blockchain* legítima em favor da *blockchain* fraudada.

Observação 2 *É necessário e 'suficiente' para uma fraude a apresentação da proof-of-work de cada um dos blocos adicionados a partir do bloco fraudado, em uma velocidade superior àquela do restante da rede na apresentação de soluções dos blocos adicionados na versão não fraudada da blockchain.*

A figura 4 ilustra uma fraude de gasto duplo (*double spending*) bem sucedida, na qual `Alice` foi capaz de acumular blocos em sua versão da *blockchain* mais rapidamente que o restante da rede de nós acumulou em sua versão. `Alice` utilizou as mesmas unidades de moeda em duas transações diferentes: pagou a `Bob` por uma mercadoria na primeira delas e pagou para si as mesmas moedas na segunda.

[18] *Verificar* se uma dada alternativa é solução do problema é uma tarefa computacionalmente trivial. O tempo esperado para *encontrar* uma solução usando um computador típico (pessoal), no entanto, é de vários anos (Driscoll, 2013). Já o tempo esperado para *algum problema ser resolvido* por toda a rede de nós é de (calibrado para) aproximadamente 10 minutos.

[19] De forma mais precisa (menos simplificada), o problema matemático $(f, \bar{y})$ definido na nota de rodapé 17 não se altera com a modificação do bloco. A fraude (modificação do bloco $x = (x_H, x_B)$) é a escolha de um novo x_B modificando alguma transação do bloco x. Como a *proof-of-work* do bloco x (o *nonce* presente em x_H) é válida, tem-se que $f(x) < \bar{y}$. Encontrar o *proof-of-work* do bloco fraudado é encontrar um x^* tal que $f(x^*) < \bar{y}$ e que preserve as transações fraudadas. A única solução conhecida *a priori* é $x^* = x$, mas isso significa desfazer a fraude. É necessário encontrar outro x^*, o qual guarda relação 'aparente' nenhuma com x devido à estrutura *hash* de f.

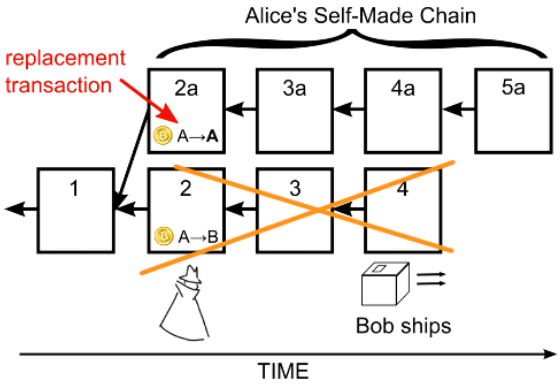


Figura 4: Uma fraude de gasto duplo – *double spending* (Driscoll, 2013).

Após a confirmação de recebimento do pagamento — inclusão na *blockchain* da primeira transação, no bloco `2` —, `Bob` enviou para `Alice` a mercadoria. A fim de ficar com a mercadoria e as moedas pagas a `Bob`, `Alice` emprega seu poder computacional para adicionar um bloco com a segunda transação, bloco `2a`, logo após o bloco `1`. Além de encontrar a *proof-of-work* do bloco `2a` por conta própria, `Alice` precisa encontrar soluções também para os blocos `3a`, `4a` e `5a`, visto que o restante da rede continua trabalhando para adicionar blocos após o bloco `2`. Como o problema matemático do bloco `3a` (por exemplo) possui relação nenhuma com aquele do bloco `3`, `Alice` precisa verificar novamente toda a lista de alternativas a fim de resolver o bloco `3a`.

Assim que `Alice` acumula mais blocos que o restante da rede, todos os nós (por padrão) trocam de versão da *blockchain* para a versão de `Alice`: aceitam os blocos `2a`, `3a`, `4a` e `5a` como legítimos e descartam os blocos `2`, `3` e `4`. Como resultado, as moedas são transferidas para `Alice` e a transação de transferência para `Bob` será considerada ilegítima a partir de então — já que a partir de agora ela referencia moedas já gastas na transferência de `Alice` para `Alice`, registrada no bloco `2a`[20].

Para `Alice` ser bem sucedida em sua fraude, conforme destacado pela observação 2, ela precisa acumular blocos mais rapidamente que o restante da rede e, portanto, necessita possuir um poder computacional suficientemente grande (relativamente aos demais nós em conjunto). Mais concretamente, e para o caso particular da `Bitcoin`, a figura 5 ilustra a probabilidade (eixo vertical) de um fraudador resolver $n \in \{2, 4, 6, 8, 10\}$ blocos mais rapidamente do que o restante da rede, em função da proporção da capacidade computacional da rede em poder do fraudador (eixo horizontal).

[20]Há incerteza sobre o comportamento exato do restante da rede após uma fraude como a ilustrada aqui. Por padrão, cada nó sempre reverte para a versão da *blockchain* como mais blocos. No entanto, a rede provavelmente se recusaria a aceitar a versão fraudada da *blockchain* após detectar ataques como este. Ver seção 5.5 de Narayanan et al. (2016). Para chamar a atenção para esta incerteza, a propriedade de suficiência advogada na observação 2 foi apresentada entre aspas.

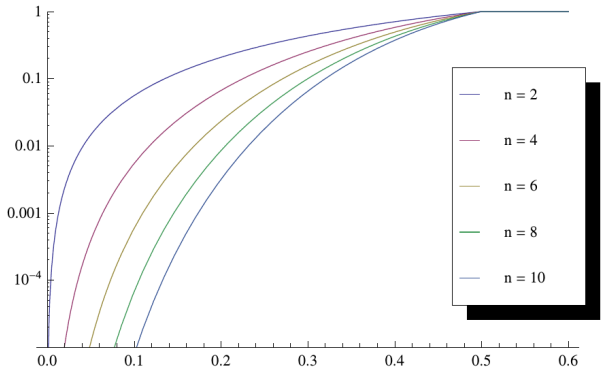


Figura 5: Probabilidade de sucesso em fraudes (Rosenfeld, 2014).

Por exemplo, com cerca de 11% da capacidade computacional da rede, o fraudador resolve $n = 6$ blocos mais rapidamente que o restante da rede com probabilidade aproximada de 0.1%. Para todos os valores de n apresentados na figura, o fraudador consegue acumular blocos mais rapidamente que a rede com probabilidade 1 se adquirir mais do que a metade do poder computacional da rede. Conclui-se disso que, enquanto houver um grande diferencial de poder computacional entre o fraudador e o restante da rede, a possibilidade de fraude é praticamente inexistente.

Em resumo, a combinação do alto custo computacional em encontrar cada *proof-of-work* com um grande diferencial do poder computacional entre o eventual fraudador e o restante da rede assegura a legitimidade das informações registradas na *blockchain*. Somente fraudadores com alto poder computacional e com disposição em incorrer em enorme prejuízo (considere, por exemplo, a despesa com energia elétrica implicada pelo uso dos computadores para fraudar o sistema) podem *teoricamente* fraudar a *blockchain*.

2 Moeda e tecnologias de *record-keeping*

Conforme visto na seção 1, *uma* inovação das criptomoedas foi a viabilização de uma tecnologia contábil (de transações monetárias) confiável sem a necessidade de monitoramento dos responsáveis por seu gerenciamento, uma vez que a tecnologia de legitimação empregada é suficiente para desincentivar fraudes. Para reconhecê-la como *a* inovação monetária fundamental das criptomoedas, é necessário utilizar um conceito de moeda alternativo ao tradicional conceito de moeda. Conforme apresentado em detalhes nas subseções a seguir, a moeda é entendida/interpretada neste conceito alternativo como um substituto para tecnologias de monitoramento – registros (*record-keeping*) – das ações individuais.

2.1 Moeda como substituta para tecnologias de *record-keeping*

Seguindo a abordagem de Desenho de Mecanismos, a moeda é entendida sob o conceito alternativo como parte fundamental de uma instituição criada pela sociedade para resolver o *problema de dupla coincidência de interesses*. No jogo implicado por esta instituição, o uso de um objeto como meio de troca viabiliza a produção e o consumo de bens e serviços em situações sem coincidência dupla de interesses e, com isso, melhora o bem estar dos indivíduos[21,22].

Conforme estabelecido por Kocherlakota (1998a) e discutido de forma mais didática por Kocherlakota (1998b), este conceito alternativo implica na interpretação da

"moeda como um substituto para tecnologias de *record-keeping*"[23].

Mais especificamente, a moeda cumpre o papel social de "registrar" transações ao servir de evidência *confiável* de produção (de bens e serviços) em situações nas quais não há tecnologia de *record-keeping* para cumprir este papel. Esta evidência é então trocada por consumo (de bens e serviços) quando o detentor da moeda encontrar um produtor do bem/serviço no qual ele tem interesse.

Formalmente, a natureza do argumento apresentado por Kocherlakota (1998a,b) é comparar alocações de equilíbrio em diferentes situações. Compara-se a alocação sob a existência de uma tecnologia perfeita para registro de transações que viabiliza um esquema de crédito (situação `C`) com a alocação sob a inexistência de tecnologia de registros, mas com o uso de moeda para transações (situação `M`). É demonstrado que toda alocação sustentada em equilíbrio na situação `M` pode ser sustentada em equilíbrio na situação `C`. No entanto, nem toda alocação sustentada em equilíbrio com o uso da tecnologia de *record-keeping* (de crédito) pode ser sustentada com o uso de moeda.

A comparação entre alocações é feita em três modelos: no modelo de gerações sobrepostas (Samuelson, 1958), no modelo *Turnpike* (Townsend, 1980) e, por fim, no modelo de *search* (Kiyotaki and Wright, 1991). Nos dois primeiros modelos, a alocação de equilíbrio na situação `M` coincide com a alocação de equilíbrio eficiente da situação `C`. Nestes casos, a moeda é um dispositivo mnemônico perfeito. No terceiro modelo, por sua vez, as

[21] Note, portanto, que o uso da moeda não é imposto pela teoria como em modelos *cash-in-advance* (Lucas Jr, 1982; Lucas Jr and Stokey, 1987). Aqui, o uso da moeda é consequência do interesse social em facilitar trocas.

[22] A subseção 2.2 discute os aspectos fundamentais desta viabilização de produção e consumo, conforme estabelecidos nos modelos monetários de *search* baseados em Kiyotaki and Wright (1989, 1991). Para uma discussão mais geral sobre a atratividade da abordagem de Desenho de Mecanismos para Teoria Monetária, ver Wallace (2010). Sobre Desenho de Mecanismos, uma discussão introdutória é Mookherjee (2008) e uma referência técnica e mais completa e atualizada é Borgers (2015).

[23] Conforme reconhecido por Kocherlakota (1998b), esta interpretação já pode ser encontrada nos trabalhos de Townsend (1987, 1989, 1990) e também em Ostroy (1973), Lucas (1980) e Aiyagari and Wallace (1991).

alocações não coincidem. Em particular, a alocação da situação `M` é Pareto dominada por todas as alocações de equilíbrio da situação `C`. Ou seja, a moeda é um dispositivo mnemônico (severamente) imperfeito.

Nos três casos, a moeda cumpre o papel social de "registrar" transações ao servir de evidência *confiável* de produção no passado. A posse desta evidência é trocada por consumo corrente quando o proprietário da moeda encontrar um produtor do bem no qual ele tem interesse. Já a indisponibilidade desta evidência pune o consumidor ao privá-lo de consumo. Neste sentido, a moeda substitui o histórico de transações dos indivíduos (utilizado no esquema de crédito) como ferramenta para disciplinar recompensas e punições aos consumidores de acordo com seu comportamento quando foram produtores[24].

Kocherlakota (1998a,b) destacam que somente o terceiro modelo (de *search*) captura a ideia de escassez de coincidência de interesses e, com base nesta superioridade de modelagem, o resultado de que a moeda é um dispositivo de memória (severamente) imperfeito é defendido como o mais importante.

2.2 Escassez de coincidência de interesses e a moeda

Uma característica atrativa do modelo monetário de *search* é a modelagem explícita do *problema de dupla coincidência de interesses*. A escassez de coincidência de interesses (e, portanto, dificuldade de trocas) é modelada, por simplicidade, supondo que cada indivíduo na economia encontra um (e somente um) outro indivíduo em cada período e que tais encontros são determinados de maneira involuntária e aleatória. Adicionalmente, o *padrão de interesse de troca* em um dado encontro (pareamento) é determinado pela especialização produtiva e de consumo dos participantes do encontro (denominada *tipo* do participante). Dos três bens de consumo existentes na economia (bem 1, bem 2 e bem 3), indivíduos do tipo $i \in \{1, 2, 3\}$ auferem utilidade somente via consumo do bem i e são capazes de produzir somente o bem $i + 1 \pmod 3$[25]. A tabela 1 apresenta os possíveis padrões de interesse de troca e mostra que não ocorre dupla coincidência de interesses nesta economia.

Indivíduo	tipo 1	tipo 2	tipo 3
tipo 1	–	simples	simples
tipo 2	simples	–	simples
tipo 3	simples	simples	–

Tabela 1: Padrão de interesse de troca.

Um encontro entre um indivíduo do tipo 2 com um indivíduo do tipo 1 é um encontro

[24] A subseção 2.2 a seguir desenvolve, em detalhes e via exemplos, os argumentos deste parágrafo.
[25] Ou seja, tipo 1 produz somente bem 2, tipo 2 produz somente bem 3 e tipo 3 somente bem 1.

com coincidência *simples*[26]: o tipo 1 é capaz de produzir o bem de interesse do tipo 2 (bem 2), mas não possui interesse no bem que o tipo 2 é capaz de produzir (bem 3). Neste caso, o indivíduo do tipo 1 é chamado *produtor* deste encontro e o indivíduo do tipo 2 é denominado *consumidor* deste encontro. Um encontro entre dois indivíduos do tipo 3, por sua vez, é um encontro sem coincidência de interesses: o tipo 3 não é capaz de produzir o bem de interesse do outro indivíduo do tipo 3 (bem 3), uma vez que consegue produzir somente o bem 1.

Tendo em vista a ausência de coincidência dupla de interesses e que a produção de bens gera desutilidade — ao reduzir o consumo de horas de lazer —, os indivíduos não têm incentivo para produzir sem uma *recompensa futura* ao seu esforço de produção. Tal fato evidencia que produção e consumo em situações com coincidência simples de interesse somente podem ocorrer em modelos dinâmicos.

Considere então uma economia com $T = 2$ períodos. Em particular, considere um encontro entre os tipos 1 e 2. Para induzir produção e consumo (troca) neste encontro no primeiro período ($t = 1$), o consumidor (tipo 2) pode prometer ao produtor (tipo 1) que o tipo 3 irá produzir para ele no próximo período ($t = 2$), caso ambos sejam pareados. Em contrapartida ao tipo 3, o tipo 2 se comprometeria a produzir para este em $t = 2$ caso eles sejam pareados neste período. O indivíduo do tipo 2 nesse encontro com o tipo 1 está *tomando crédito* (consumindo hoje em troca do compromisso de produzir no futuro) e o indivíduo do tipo 1 está *ofertando crédito* (produzindo hoje em troca da promessa de consumo futuro).

Caso acredite nesta promessa, o tipo 1 sabe que sua desutilidade ao produzir hoje será recompensada no próximo período com probabilidade 1/3 (a probabilidade de encontrar alguém do tipo 3). Embora arriscada, tal promessa seria suficiente para induzir alguma produção em $t = 1$. De maneira análoga, quando todos os tipos são incentivados por promessas de consumo futuro (via crédito), o tipo 2 produz em $t = 1$ ao encontrar o tipo 3 e o tipo 3 produz $t = 1$ ao encontrar com o tipo 1. Sendo estas trocas voluntárias, ela melhoram o bem estar dos indivíduos envolvidos. A figura 6 ilustra as trocas que seriam viabilizadas em cada período pelo esquema de crédito[27].

[26] Ou seja, um encontro no qual uma pessoa (digamos `Alice`) tem interesse no bem da outra (digamos `Bob`), mas a outra (`Bob`) não tem interesse no bem da uma (`Alice`).

[27] Tecnicamente, a viabilização de produção e consumo via crédito aqui descrita é sustentada em *Equilíbrio de Nash* quando os jogadores acreditam que os demais estão jogando a seguinte estratégia: "produtor em $t = 1$: produzir; produtor em $t = 2$: produzir somente para consumidores que produziram em $t = 1$; consumidor em $t \in \{1, 2\}$: consumir sempre que possível".

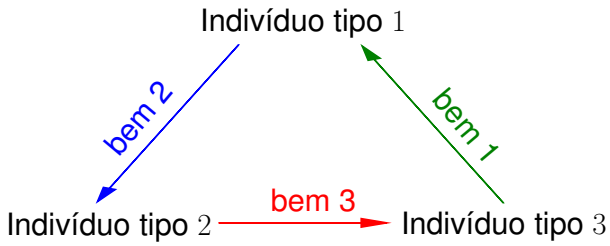


Figura 6: Trocas viabilizadas via promessas de consumo futuro (via crédito).

O ponto crítico aqui é a razoabilidade da crença do tipo 1 na promessa do tipo 2. Ela será defensável se, por exemplo, os indivíduos do tipo 3 são capazes de se comprometer com suas promessas (se possuem *comprometimento*). Ou seja, se eles não são capazes de se negar a cumprir promessas que fizeram no passado, mesmo que *ex post* seja do seu interesse negá-las.

A dificuldade em sustentar trocas com o mecanismo de crédito descrito reside exatamente na incapacidade das pessoas em se comprometer com suas promessas: os indivíduos cumprirão a promessa de produção em $t = 2$ somente se for do seu interesse *ex post* fazê-lo. Logo, pela mesma razão que não há incentivo de produção em economias estáticas (com somente um período), o tipo 3 não possui incentivo *ex post* em produzir na segunda data ($t = 2$): ele não antecipa recompensa futura pelo esforço de produção corrente. Como consequência, a crença do tipo 1 de que o tipo 3 lhe recompensará no futuro não é *defensável*[28]. A crença defensável para o tipo 1 é a de que o tipo 3 não produzirá em $t = 2$, o que o induz a não produzir em $t = 1$.

Como alternativa, os indivíduos poderiam produzir já no momento de sua promessa (em $t = 1$) o produto que prometem entregar em $t = 2$. Ao receber a oportunidade de honrar sua promessa, o tipo 3 (por exemplo) estaria indiferente entre cumpri-la ou não, uma vez que o custo de produção teria sido foi incorrido em períodos anteriores. Neste caso, a crença do tipo 1 (por exemplo) é defensável e, portanto, é possível induzir produção e consumo. O ponto central aqui é que a promessa *de produzir* em $t = 2$ foi trocada pela promessa *de entregar a produção* em $t = 2$, eliminando o incentivo a não prover o consumo em $t = 2$: a antecipação de produção funciona como uma *tecnologia de comprometimento*.

Observe, no entanto, que não ocorre *de fato* uma operação de crédito neste caso. Tanto a desutilidade de produção quanto a utilidade de consumo são auferidas em $t = 1$. Adicionalmente, a mesma alocação emergeria se o tipo 2 entregasse sua produção para o

[28]No sentido de que o equilíbrio de Nash no qual o tipo 1 é incentivado a produzir em $t = 1$ pela promessa produção do tipo 3 em $t = 2$ não é *perfeito em subjogos*. Este resultado persiste mesmo que o número de períodos T seja arbitrariamente alto, mas ainda finito.

tipo 1, em vez de entregar uma promessa de consumo futuro. O tipo 1 levaria a produção do tipo 2 para o (eventual) encontro com o tipo 3 e a trocaria por bem 1. Ou seja, o tipo 1 aceitaria o bem 3 em troca de sua produção, mesmo não auferindo utilidade em consumir bem 3. Ele o faz pois antecipa que o tipo 3 está disposto a ceder bem 1 em troca de bem 3 no futuro. O bem 3, portanto, cumpre o papel de meio de troca. O que ocorre *de fato* é uma intermediação de trocas com o uso de *moeda mercadoria*[29] — o bem 3.

De maneira geral, não só o bem 3 poderia ser usado como moeda, mas todos os bens são candidatos a meio de troca. O bem escolhido para desempenhar a função de moeda mercadoria será aquele com melhor combinação de características úteis para tal: alta durabilidade, alta divisibilidade, baixo custo de estocagem etc. Como para bens de consumo estas características são (praticamente) não configuráveis, o bem utilizado para intermediar trocas será um meio de troca rudimentar.

Moeda, crédito e monitoramento

Com o intuito de apresentar mecanismos mais sofisticados de viabilização de produção em situações sem coincidência dupla de interesses, suponha por simplicidade que não há bem durável na economia para assumir o papel de moeda mercadoria. Adicionalmente, suponha que os indivíduos vivem por $T = \infty$ períodos.

Neste caso, o esquema de trocas baseado em promessas (crédito) é capaz de viabilizar produção em situações com coincidência simples de interesses (Kocherlakota, 1998a). Agora, todos os indivíduos antecipam oportunidades de consumo futuro, em todos os períodos. É possível induzir produção em todos os períodos via promessas *críveis* de consumo futuro: produção e consumo são sustentados utilizando crenças defensáveis[30].

Note, no entanto, que o esquema de promessas demanda uma tecnologia *confiável* para registrar produção passada. Ou seja, faz-se necessária uma tecnologia de monitoramento das ações individuais. É necessário identificar quem de fato recebeu promessa de consumo futuro e ainda não o coletou e identificar quem honrou sua promessa de produção. Sem o registro de propriedade de promessa, todos argumentariam ter produzido no passado (e ainda não ter sido recompensado por isto) a fim de obter consumo presente e, como resultado, ninguém seria acreditado. Sem o registro de falhas no cumprimento de promessa, não seria possível induzir indivíduos sem comprometimento a resgatar suas dívidas via ameaça de punição futura (exclusão do sistema de crédito).

[29]Para mais detalhes sobre moeda mercadoria, ver Kiyotaki and Wright (1989).

[30]Ou seja, existe equilíbrio de Nash perfeito em subjogos no qual há produção e consumo nos encontros com coincidência simples. Mais precisamente, Kocherlakota (1998a) usa o conceito de *Perfect Public Equilibrium* de Abreu et al. (1990).

Havendo uma tecnologia de registros capaz de armazenar todas as informações relevantes das trocas passadas (data da produção, quantidade produzida, tipo de bem produzido, identidade do produtor, identidade do consumidor, históricos de transação do produtor e do consumidor até aquele momento *etc* ...), produção e consumo na economia podem ser sustentados utilizando o esquema de promessas (crédito) descrito.

Embora a tecnologia de registros possibilite o uso do crédito em comunidades relativamente pequenas e pouco sofisticadas, não é possível monitorar perfeitamente todas as atividades de todos os indivíduos em sociedades grandes e sofisticadas. Uma parte das oportunidades de trocas (encontros de coincidência simples) ocorre em situações nas quais não há tecnologia de monitoramento para registrar as informações, ou ainda, em situações nas quais as partes envolvidas não desejam ser monitoradas[31].

Para estudar estas situações, considere o caso em que não há tecnologia de monitoramento *perfeita*. Em particular, a fim de simplificar a exposição, suponha que não há tecnologia alguma de monitoramento. Sob a impossibilidade de evidenciar produção passada via o registro completo do histórico de transações, o consumidor poderia emitir um *certificado* de que recebeu produto de seu parceiro de encontro (o produtor), prometendo produzir no futuro para o portador de tal certificado — emitiriam um *título de dívida*. Por exemplo, no encontro entre os tipos 1 e 2, o produtor (tipo 1) receberia o certificado emitido pelo consumidor (tipo 2) e, ao encontrar com o tipo 3 no futuro, trocaria este certificado por consumo. Em uma data seguinte, ao encontrar com o emissor do certificado (tipo 2), o tipo 3 o trocaria por consumo. Neste mecanismo, o certificado emitido pelo tipo 2 (título de dívida) cumpre o papel de meio de troca: é aceito pelo tipo 1 pela expectativa de que no futuro ele será aceito em troca de bem 3, e não pelo seu valor de resgate (bem 2).

De maneira mais geral, não só os certificados emitidos pelo tipo 2 circulariam na economia desempenhando o papel de meio de troca, mas os certificados emitidos por todos os tipos desempenhariam tal função, conforme ilustrada na figura 7.

A dificuldade com o esquema de certificados descrito reside novamente na incapacidade dos indivíduos em se comprometer com suas promessas, especialmente, em *resgatar* os certificados que emitem. No exemplo da figura 7, o tipo 3 aceita o certificado emitido pelo tipo 2 em troca de produção para o tipo 1 somente se acredita que será capaz de trocá-lo no futuro por consumo, ao encontrar o emissor do certificado. Tal crença, no entanto, não é defensável em termos de perfeição em subjogos *se não houver tecnologia para monitorar as*

[31] O exemplo típico desta situação são atividades ilegais (venda de drogas e armas ilícitas). Mais importante, há transações socialmente desejáveis nas quais pelo menos uma das partes envolvidas deseja manter-se anônima como forma de se proteger de comportamentos oportunistas subsequentes da outra parte. Por exemplo, transações entre desconhecidos na internet. A este respeito, ver Kahn et al. (2005).

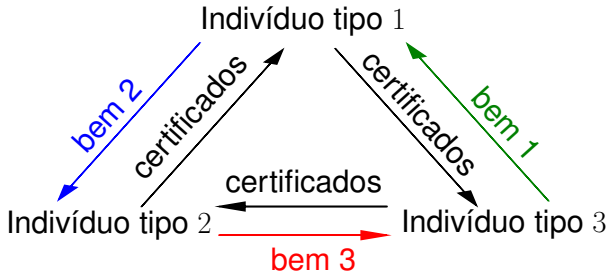


Figura 7: Trocas viabilizadas via certificados (meio de troca).

ações do tipo 2, pois este não teria incentivo *ex post* em resgatar o certificado que emitiu (entregar produção ao tipo 3 em troca do certificado). De fato, resgatar o certificado envolve incorrer em um custo de produção para "comprar" um certificado que pode ser emitido novamente pelo tipo 2 sem custo algum. Ao negar o resgate do certificado, por outro lado, o tipo 2 evita o custo de produção sem consequências futuras: a inexistência de monitoramento permite negar o resgate sem que isso fique registrado e, portanto, chegue ao conhecimento dos futuros parceiros de troca do tipo 2. A combinação de falta de comprometimento com inexistência de tecnologia de monitoramento (*record-keeping*) impossibilita induzir produção e consumo na economia usando o esquema de certificados.

Sob a existência de alguma tecnologia de monitoramento, no entanto, o uso de certificados é capaz de viabilizar produção e consumo. A título de ilustração, considere que é possível monitorar perfeitamente as ações de um subconjunto fixo de indivíduos de cada tipo. Neste caso, a crença do tipo 3 em trocar o certificado por consumo ao encontrar seu emissor é defensável se o emissor fizer parte do grupo de indivíduos monitoráveis: a credibilidade da promessa em resgatar o título se justifica pelo fato de que falhas em cumpri-la são perfeitamente identificadas e registradas e são punidas na história subsequente via exclusão do infrator do setor monitorado[32]. De fato, Cavalcanti and Wallace (1999a,b) demonstram formalmente que este subconjunto de indivíduos monitoráveis — representativo do sistema bancário — é capaz de emitir tais certificados e *crivelmente* prometer resgatá-los no futuro.

Importante destacar que os certificados induzem produção não só quando emitidos e resgatados pelos monitoráveis, mas também quando trocados entre não monitoráveis: ou seja, o certificado cumpre o papel de meio de troca. Na ilustração acima, o certificado emitido por um indivíduo monitorável do tipo 2 é capaz de induzir produção em encontros entre indivíduos dos tipos 1 e 3 sem a necessidade de que estes sejam monitoráveis. Basta o tipo 3 reconhecer que o certificado de produção foi emitido por um indivíduo monitorável para este acreditarna promessa de resgate. Como conclusão, o certificado

[32]Esta ameaça de exclusão é capaz de induzir o resgate de um dado certificado não só pelo respectivo emissor, mas por todos os indivíduos monitoráveis.

(título de dívida) assume o papel de moeda, denominada *inside money* por ser baseada em uma dívida privada[33].

A viabilização de produção e consumo via criação de moeda por indivíduos do setor monitorável (bancário) estudada por Cavalcanti and Wallace (1999a,b) provê uma teoria para moedas privadas baseada em desenho de mecanismos. A aceitação de moeda privada como um *fenômeno de equilíbrio*[34], no entanto, não demanda monitoramento perfeito do comportamento dos bancos (monitoráveis). Basta existir uma tecnologia para registrar publicamente cada resgate de dívida pelo setor bancário (produção de um indivíduo monitorado em troca da dívida/moeda em posse do consumidor). Neste caso, o montante de dívidas (moedas) de cada banco resgatadas pelo sistema bancário seria registrado em um espécie de casa de compensação (*clearing house*). Após o banco j resgatar um montante de dívida/moeda x emitido pelo banco i, o saldo do banco i na casa de compensação é reduzido em x unidades e o saldo do banco j é elevado na mesma quantidade.

Esta tecnologia de monitoramento pode ser suficiente para viabilizar (em equilíbrio) produção e consumo por meio do uso de moedas privadas, conforme demonstrado por Cavalcanti et al. (1999). Sob certas condições, a ameaça de excluir do setor monitorado os bancos que atingem saldo negativo junto a casa de compensação induz a comunicação de resgates de dívidas e, com isso, a emissão disciplinada de moeda privada — como estratégias de proteção contra a "liquidação bancária".

O conceito de moeda fiduciária

O papel da moeda como registro confiável de produção passada é ainda mais evidente sob ausência completa de tecnologia de monitoramento. Emerge neste caso, a *moeda fiduciária*, uma modalidade de moeda mais primitiva que *inside money*, embora conceitualmente mais sofisticada que a moeda mercadoria.

Considere novamente a economia com horizonte infinito ($T = \infty$) e os indivíduos sem comprometimento, mas suponha agora que todos eles são anônimos (não há tecnologia para monitorar/registrar suas ações). Suponha a existência de um objeto durável sem valor intrínseco, no sentido de que seu consumo não gera utilidade para as pessoas e seu emprego em atividades produtivas não aumenta a produção[35]. Por simplicidade, suponha

[33]Para uma apresentação introdutória sobre *inside money* e as demais moedas (denominadas *outside money*), ver Lagos (2010).

[34]Neste tipo de abordagem, as instituições são estudadas como um fenômeno resultante do equilíbrio entre as ações dos indivíduos na sociedade, sem garantia de que este equilíbrio possui boas propriedades de bem estar para a sociedade — como garantido sob a abordagem de desenho de mecanismos.

[35]Note, portanto, que o uso da moeda não será consequência direta de hipóteses sobre preferências, como em modelos com *moeda na função utilidade* (Sidrauski, 1967), ou sobre tecnologia, como em modelos com *moeda na função de produção* (Sinai and Stokes, 1972; Fischer, 1974). Novamente, o uso da moeda aqui é consequência do interesse social em facilitar trocas.

que este objeto é indivisível e que os indivíduos não são capazes de estocar/armazenar mais de uma unidade deste objeto.

Os indivíduos nesta economia poderiam utilizar este objeto para evidenciar produção no passado. Os objetos seriam distribuídos entre as pessoas, de forma que haveria entre os indivíduos de cada tipo $i \in \{1, 2, 3\}$ pessoas com uma unidade do objeto e pessoas sem o objeto. Isto determinaria um novo padrão de encontros, conforme ilustrado na tabela 2.

Indivíduo		tipo 1		tipo 2		tipo 3	
	Objeto	0	1	0	1	0	1
tipo 1	0	–	–	simples	simples	simples	simples
	1	–	–	simples	simples	simples	simples
tipo 2	0	simples	simples	–	–	simples	simples
	1	simples	simples	–	–	simples	simples
tipo 3	0	simples	simples	simples	simples	–	–
	1	simples	simples	simples	simples	–	–

Tabela 2: Padrão de encontros: interesse de troca.

Os encontros com coincidência simples entre os tipos 1 e 2, por exemplo, agora se diferenciam pela quantidade de objeto em poder dos indivíduos. Há encontros nos quais nenhum indivíduo detém o objeto, $(0, 0)$, e outros nos quais ambos detém o objeto, $(1, 1)$. Há encontros nos quais somente o produtor detém o objeto, $(1, 0)$, e outros nos quais somente o consumidor detém o objeto, $(0, 1)$.

Ainda considerando o encontro entre os tipos 1 e 2, a título de ilustração, o consumidor (tipo 2) *com* o objeto poderia induzir o produtor (tipo 1) *sem* o objeto a produzir bem 2 oferecendo em troca seu objeto. Caso o tipo 1 acredite que no futuro o tipo 3 estará disposto a aceitar o objeto em troca de produção, ele estará disposto a produzir hoje para "comprar" o objeto. De forma similar, o tipo 3 estará disposto a produzir para "comprar" o objeto se acreditar que em datas posteriores o tipo 2 estará disposto a aceitar o objeto em troca de produção. Finalmente, o tipo 2 estará disposto produzir para "comprar" o objeto do tipo 3 se acreditar que, em datas posteriores, o tipo 1 estará disposto a aceitar o objeto em troca de produção. Caso todos acreditem, em todos os períodos, que o objeto será aceito no futuro, ele será aceito no presente. A figura 8 ilustra o fluxo de bens e objeto em cada período neste caso.

A crença do tipo 1 será defensável se a crença (*futura*) do tipo 3 for defensável. A crença (*futura*) do tipo 3 será defensável se a crença (*futura do futuro*) do tipo 2 for defensável. Finalmente, a crença (*futura do futuro*) do tipo 2 é defensável se a crença (*futura do futuro do futuro*) do tipo 1 for defensável. Esta recursividade das crenças é o que suporta a utilização deste objeto sem valor intrínseco como meio de troca.

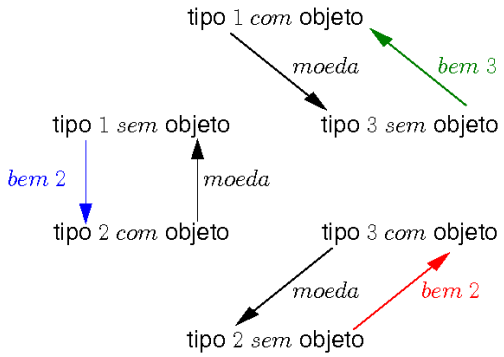


Figura 8: Trocas viabilizadas via moeda fiduciária.

Observação 3 *Se todos acreditam que o objeto será aceito no futuro, então ele será aceito hoje.*

A recursividade sustenta a crença de que "o objeto será aceito *no futuro*" e, portanto, sustenta a sua aceitação hoje. Todos acreditarão no presente que "o objeto será aceito no futuro" quando todos acreditarem que "todos acreditarão, *no futuro*, que o objeto será aceito *no futuro do futuro*". Todos acreditarão no futuro que "o objeto será aceito no futuro do futuro" quando todos acreditarem que "todos acreditarão, *no futuro do futuro*, que o objeto será aceito *no futuro do futuro do futuro*". A cadeia de argumentação para defensabilidade das crenças continua de maneira análoga *ad infinitum*.

O objeto é aceito como meio de troca somente porque as pessoas acreditam que ele será aceito como meio de troca. O objeto é comprado (via produção) porque as pessoas acreditam que ele tem valor, não porque ele tenha valor intrínseco — trata-se de uma *profecia auto-realizável*[36]. Basta que o objeto sirva ao propósito de evidenciar para a sociedade os consumidores que no passado incorreram no custo de produção. Esta evidência é então utilizada para recompensá-los com consumo presente como uma forma de *provisão de incentivos* para produção.

A importância da escassez, da durabilidade e da divisibilidade

Adicionalmente à consistência das crenças, o papel de evidência de produção para induzir produção e consumo nesta economia via moeda fiduciária requer *escassez* e *durabilidade* do objeto utilizado como meio de troca.

Observação 4 *Ao receber o objeto em troca de produção, o indivíduo do tipo* 1 *(por exemplo) precisa acreditar que será capaz de armazenar o objeto até a eventual data em que encontrará um indivíduo do tipo* 3 *sem moeda.*

[36]Interessantemente, esta propriedade já é reconhecida por alguns autores em criptografia. Narayanan et al. (2016), por exemplo, utiliza a expressão "efeito Sininho" (*Tinkerbell effect*) para descrevê-la, uma analogia com o fato de a existência da fada Sininho na clássica história de Peter Pan depender da crença de que ela existe (Narayanan et al., 2016, p.169).

Se o objeto fosse perecível, não seria possível armazená-lo. Se o objeto não fosse escasso (todos possuíssem o objeto), o tipo 1 nunca encontraria alguém do tipo 3 sem moeda[37]. Em ambos os casos, mesmo acreditando que o tipo 3 *sem* o objeto estaria disposto a produzir em troca do objeto no futuro, o tipo 1 não aceitaria "comprar" o objeto hoje.

A escassez do objeto utilizado como meio de troca é especialmente importante na teoria acima. Quando o objeto é abundante, a quantidade de pessoas sem o objeto é pequena em todas as datas. Com isso, a probabilidade de encontrar no futuro alguém sem o meio de troca (e, portanto, disposto a comprá-lo) é baixa. Antecipando a baixa probabilidade de trocar o objeto por consumo no futuro, o tipo 1 atribuirá baixa utilidade (esperada, descontada e indireta) ao objeto. Logo, ele não estará disposto a incorrer na desutilidade em produzir muitas unidades de produto em troca do objeto. Como conclusão, o "preço de compra" do objeto (unidades de produção) será baixo e, portanto, será baixa a capacidade do meio de troca induzir produção e consumo na economia. No limite em que não há escassez (todos possuem o meio de troca), o preço de compra é zero[38].

Observação 5 *Há um canal de relação direta entre a escassez do meio de troca e sua capacidade de induzir produção e consumo em um dado encontro (seu preço de compra).*

Obviamente, no limite em que a escassez é completa (ninguém possui o meio de troca) o preço de compra será alto, mas não haverá produção e consumo no economia. A relação apresentada na observação 5 se refere ao efeito da escassez na *margem intensiva*: quanto maior a escassez de moeda, maior o incentivo em comprá-la. No entanto, há também o efeito de redução na produção via *margem extensiva*: quanto maior a escassez de moeda, menor a quantidade de situações (encontros) nas quais haverá moeda para ser comprada via produção. A quantidade ótima de moeda precisa contrabalancear estes dois efeitos.

Esta discussão sobre escassez reforça o fato de que, sob a ausência completa de monitoramento, os certificados de produção não só são inadequados para intermediar trocas via a promessa de resgate futuro, como também são inadequados para intermediar trocas de maneira fiduciária. A habilidade dos indivíduos em facilmente reproduzir certificados, sem uma tecnologia de monitoramento para disciplinar tal reprodução[39], resulta em

[37]Note que encontrar um indivíduo do tipo 3 *com* moeda é inútil para o tipo 1, pois o tipo 3 não possui interesse em comprar o objeto neste caso. Ele já possui uma unidade, não é capaz de armazenar uma segunda unidade e incorreria no custo de produção para comprar o objeto.

[38]Este argumento pode ser generalizado para o caso com meio de troca divisível e sem limite na quantidade de objetos que cada indivíduo é capaz de estocar. Adicionalmente, o crescimento na quantidade de meio de troca ao longo do tempo é acompanhado de redução no seu valor de compra (*inflação*). Em particular, se tal crescimento futuro for antecipado pelos indivíduos, a redução no valor do meio de troca ocorrerá já no presente.

[39]Como ocorre nos modelos de Cavalcanti and Wallace (1999a,b) e Cavalcanti et al. (1999), nos quais a sociedade utiliza sua capacidade de monitorar os "bancos" para desincentivar emissão descontrolada de moeda.

abundância do meio de troca e consequente deterioração de seu "preço de compra"[40].

Por fim, outro aspecto importante do objeto utilizado como meio de troca é sua divisibilidade. No exemplo simplificado apresentado acima, o objeto possui divisibilidade nenhuma. Com isso, após trocar o objeto por consumo, o indivíduo fica sem o meio de troca. Caso se torne novamente consumidor antes de ser capaz de comprar uma nova unidade de objeto (se tornar produtor para um consumidor com moeda), o indivíduo não será capaz de aproveitar esta oportunidade de consumo por não possuir moeda. Se alternativamente o objeto fosse divisível, seria possível "gastar" somente parte da unidade de objeto e "poupar" a parcela restante para o caso de encontrar novamente um produtor do bem que consome antes de encontrar um consumidor do bem que produz[41].

Assim como acontece com a moeda mercadoria, a escolha sobre qual objeto será utilizado pela sociedade como moeda fiduciária depende em grande parte da combinação de propriedades físicas que cada objeto oferece (por exemplo: escassez, durabilidade e divisibilidade): deseja-se a melhor combinação para servir como evidência de produção. Em ambos os casos, as propriedades do meio de troca não são configuráveis. Elas são escolhidas por meio da escolha do objeto a ser usado como moeda.

3 A relação entre moeda e criptomoeda

O conceito de moeda fiduciária apresentado na seção 2 envolve uma série de elementos que o torna um conceito sofisticado para ser usado como uma primeira ideia do que é moeda. O tradicional conceito de moeda como um objeto que cumpre as funções de unidade de conta, meio de troca e reserva de valor, por outro lado, é uma ideia simples e de fácil justificativa observacional. Muito provavelmente, é este diferencial de sofisticação que justifica introduzir primeiramente o conceito tradicional de moeda[42].

O contato com este conceito simples e introdutório de moeda é de fato bastante útil. Halaburda and Sarvary (2016), por exemplo, admitem que este conceito tem sido incrivelmente útil em permitir aos economistas explicar a razão de alguns objetos serem mais adequados para serem usados como moeda do que outros. Propriedades como escassez,

[40] De maneira análoga, a possibilidade de falsificação do meio de troca reduz sua escassez e, portanto, reduz seu valor real ("preço de compra"). Sobre falsificação de moeda, ver Nosal and Wallace (2007), Cavalcanti and Nosal (2011) e as referências então citadas.

[41] Esta estratégia de seguro pode ser implementada mesmo no modelo simplificado acima, caso permitido o uso de loterias sobre "pagamentos monetários": o consumidor gastaria sua unidade de objeto com probabilidade $\lambda \in [0, 1]$, mas receberia o produto com certeza. Por este motivo, a utilização de loterias em modelos com meio de troca indivisível pode ser vista como uma aproximação do caso com moeda divisível.

[42] Como analogia, ao apresentar o conceito de raiz quadrada de um número real pela primeira vez, afirma-se não existir (estar bem definido) o número $\sqrt{-1}$. Posteriormente, esta imprecisão é qualificada ao introduzir o conceito de número imaginário $i = \sqrt{-1}$ e, portanto, de números complexos.

divisibilidade, durabilidade e uniformidade são alguns dos atributos já identificados via este conceito introdutório como importantes para um dado objeto performar bem as três funções de moeda[43].

É motivação e ponto de partida deste artigo, no entanto, que este conceito é limitado e precisa ser qualificado antes de se analisar temas mais sofisticados como o das criptomoedas[44]. Como limitação fundamental, a definição tradicional de moeda é mais uma *descrição* das funções que esta desempenha do que um *explicação* do que é moeda (Kocherlakota, 1998b). Em certa medida, esta definição é circular — ela diz que moeda é algo que está sendo usado como moeda — e dependente do contexto em análise — já que nenhum objeto cumpre as três funções de moeda em todos os contextos (Halaburda and Sarvary, 2016). Para analisar o tema criptomoedas, especificamente, o uso deste conceito de moeda induz a análise a concluir prematuramente que elas não são moedas e, com isso, não permite reconhecer sua inovação monetária fundamental.

As subseções 3.1 e 3.2 ilustram a relevância dos conceitos de moeda *inside* e moeda fiduciária, apresentados na seção 2.2, para reconhecer com a devida atenção a importância da tecnologia de legitimação sem monitoramento desenvolvida e utilizada pelas criptomoedas (a *blockchain technology*).

3.1 Limitação do conceito tradicional: uma breve ilustração

O tradicional conceito de moeda é definido pelas seguintes três funções, conforme apresentado por Mankiw (2011), uma referência bastante adotada no ensino de macroeconomia em nível de graduação:

> Como uma *reserva de valor*, a moeda representa um meio de transferir o poder de compra do presente para o futuro (...) Como uma *unidade de conta*, a moeda estabelece os termos pelos quais os preços são determinados e as dívidas registradas (...) Como um *meio de troca*, a moeda é aquilo que utilizamos para adquirir bens e serviços (Mankiw, 2011, p. 64).

Os trabalhos que utilizam este conceito para estudar criptomoedas se limitam a estudar o comportamento da sequência de preços reais (em unidades de bens) e alguns outros aspectos da criptomoeda para avaliar se esta cumpre as três funções básicas de moeda. Lo and Wang (2014), dentre outros, citam a alta volatilidade do câmbio entre bitcoins e dólares (ilustrada na Figura 9) como uma dificuldade para a utilização da Bitcoin como meio de troca. Sob tal volatilidade, os comerciantes sabem pouco sobre a quantidade

[43]Retomando a analogia com o conceito de raiz quadrada, uma grande quantidade de questões matemáticas podem ser analisadas sem o uso do (ainda mais sofisticado) conceito de número imaginário.

[44]De forma análoga, a qualificação de $\sqrt{-1}$ foi importante para o *Teorema de Green*, bastante utilizado no contexto de eletromagnetismo (Nahin, 2010).

de bens que conseguirão comprar com a criptomoeda recebida e, portanto, muitos se recusam a acetá-la[45].

Figura 9: Evolução do preço de compra da Bitcoin.

Yermack (2015), por sua vez, cita elevado o tempo necessário para as transações serem confirmadas no sistema Bitcoin[46] e a dificuldade em adquirir bitcoins como elementos importantes para o baixo uso da bitcoin como meio de troca.

Embora Lo and Wang (2014) destaque que quase metade do estoque de bitcoins não são gastos nos três meses seguintes ao recebimento, Lo and Wang (2014), Yermack (2015) e Ali et al. (2014) defendem que a Bitcoin tem dificuldades em cumprir o papel de reserva de valor. Lo and Wang (2014) e Ali et al. (2014) ponderam que a Bitcoin é suscetível a especulações e é sujeita a bolhas pelo fato de o seu valor depender apenas de uma profecia autorrealizável[47]. Além disso, usuários pouco ambientados com o meio digital podem ter dificuldades em proteger suas bitcoins de roubos digitais (Yermack, 2015).

Finalmente, a função de unidade de conta é relegada a segundo plano. Mesmo os comerciantes que aceitam pagamentos em bitcoins, preferem exibir seus preços em outras moedas (Lo and Wang, 2014). Caso exibissem seus preços em bitcoins, precisariam recalcular o preço muitas vezes por dia e as várias casas decimais poderiam confundir os consumidores (Yermack, 2015).

[45]Segundo Yermack (2015), a volatilidade da bitcoin em 2013 foi de 142%, contra uma volatilidade de 22% do ouro no mesmo período. Este inconveniente motivou o surgimento de oferta de seguro contra variações cambiais entre bitcoin e dólar, no qual algumas casas de câmbio trocam imediatamente bitcoin por dólares.

[46]Lembrando que cada bloco de transações demora em média 10 minutos para ser incluído na *blockchain*, conforme visto na nota de rodapé 18.

[47]Segundo os autores, isso decorre do fato de que, diferentemente das moedas mercadoria e das moedas fiduciárias emitidas por governos soberanos, o valor de mercado da Bitcoin depende apenas da expectativa que os usuários têm sobre a aceitação futura da criptomoeda a um valor mais alto. Como não é possível saber de antemão qual a expectativa dos agentes em relação à criptomoeda, seu valor é bastante incerto. Não se configurando, portanto, em um bom instrumento de transferência de riqueza para o futuro.

Considerando, em particular, o material bibliográfico sobre criptomoedas produzido pelo meio acadêmico em Economia no Brasil, nota-se grande predominância de monografias de conclusão de curso em Ciências Econômicas[48]. Embora fundamentados em diferentes abordagens (quase todas keynesiana, marxista ou austríaca), estes estudos concluem que as criptomoedas não são moedas se baseando no baixo desempenho das três funções de moeda discutido acima.

Um artigo acadêmico, van der Laan (2014), e uma economista consultada em um artigo de jornal, Ferreira (2017), destacam a importância/necessidade de haver um Estado dando suporte legal para a moeda, o qual é inexistente para as criptomoedas. Uma exceção aos trabalhos citados anteriormente é o livro de Ulrich (2017). Utilizando a abordagem da escola austríaca para analisar a Bitcoin, o autor a qualifica como moeda por esta satisfazer o *Teorema da Regressão* de Mises, conforme desenvolvimentos posteriores feitos por Hayek.

Por fim, o trabalho de Barossi Filho and Sztajn (2015) merece especial atenção. Embora também concluindo que as criptomoedas (precisamente, a Bitcoin) não se configuram como moedas[49], os autores apresentam aspectos econômicos, jurídicos e históricos sobre moedas bastante consistentes com o material teórico apresentado na seção 2 deste artigo.

Combinando conhecimentos econômicos e jurídicos, os autores destacam que a moeda virtual não é ilegal, constituindo-se em expressão da autonomia do setor privado. Destacam que moeda foi aceita pelos indivíduos por muito tempo sem a necessidade de curso forçado e tratam da evolução da moeda considerando-a uma solução para a escassez de coincidência de interesses. Enfatizam a participação do setor bancário na criação e gerenciamento da moeda, assim como a importância da criação dos bancos centrais como forma de fiscalizar/monitorar a atuação dos bancos no sistema monetário. Ainda mais próximo da discussão da seção 2, citam a necessidade de supervisionar a atuação da autoridade monetária a fim de disciplinar a emissão monetária oportunamente cobiçada pelos governantes para aquecer a economia.

Os autores esclarecem que o curso forçado da moeda não só é desnecessário para a caracterização de moeda como também é consistente com inovações privadas para meios de troca: "a criação de moeda, monopólio do Estado, autoridade monetária, só incide sobre a de curso forçado, que não pode ser recusada, mas não elimina o exercício da autonomia privada na criação de instrumentos que perfaçam a função de bem intermediário de troca" (Barossi Filho and Sztajn, 2015, p.1682).

[48] Como exemplos, ver Barros (2017), Costa (2014), de Senne Garcia (2014), Martins (2016), Ribeiro (2017), Scarinci (2015) e Silva (2016). Há também material bibliográfico produzido em outras áreas, em particular, nas áreas de Direito e de Sistemas de Informação.

[49] "Bitcoin não é moeda, mas meio de troca, cuja função primordial é evitar custos" (Barossi Filho and Sztajn, 2015, p.1689).

Como conclusão, o conceito de moeda apresentado na seção 2 e sua relação com criptomoedas são pouco disseminados no meio acadêmico brasileiro de Economia e nas discussões de políticas públicas[50].

3.2 A inovação monetária das criptomoedas

A despeito do histórico de comportamento dos preços das criptomoedas até aqui (e em contraste com a maior parte da literatura em Economia produzida no Brasil), as criptomoedas podem ser vistas como moedas. Nenhuma discussão sobre a taxa de troca entre bens/serviços e moeda foi necessária na seção 2 para a apresentação detalhada do conceito alternativo de moeda.

O que se discutiu na seção 2, essencialmente, foi o uso da moeda como evidência *confiável* de produção passada a fim de justificar consumo corrente e, com isso, facilitar trocas. A análise do protocolo (desenho) das criptomoedas, discutido na seção 1, mostra que ele foi cuidadosamente elaborado para garantir confiabilidade no sistema de registro de transferências de propriedade das unidades de moeda. Teoricamente, uma vez adquirida a confiança dos indivíduos na legitimidade do sistema de registros, restaria a coordenação de crenças em sua aceitação futura[51] para as criptomoedas serem adotadas mais amplamente como meio de troca.

A discussão sobre moeda como um instrumento para viabilizar trocas em situações sem dupla coincidência de interesses deixa evidente a inutilidade de meios de troca – de moeda – em economias com capacidade de manter um registro completo das ações de todos os indivíduos (com tecnologia perfeita de monitoramento – *record-keeping*). Neste caso, um esquema de crédito (promessas) é capaz de induzir produção e consumo de forma tão bem sucedida que a utilização ou não de um meio de troca é irrelevante para o bem estar dos indivíduos.

A necessidade de monitoramento das ações individuais para induzir trocas por meio do sistema de crédito decorre da incapacidade dos indivíduos em se comprometer a cumprir suas promessas (indivíduos não possuem comprometimento – *commitment*). A tecnologia de *record-keeping* é utilizada para identificar, registrar e divulgar publicamente eventuais falhas de cumprimento de promessas. A sociedade então utiliza o histórico de descumprimento de promessas do indivíduo para puni-lo via a exclusão do esquema de crédito e, portanto, das trocas por ele viabilizadas. Ao antecipar esta punição, os indivíduos são induzidos a cumprir suas promessas.

[50] Como evidência adicional, uma pesquisa via internet em 02/04/2018 pelo termo 'Bitcoin' nas principais revistas acadêmicas brasileiras em Economia resultou em somente uma referência: Viana (2014), uma breve nota de Sociologia e Política sobre as direções futuras da Economia, sem detalhamento aprofundado sobre criptomoedas.

[51] No sentido da recursividade de crenças discutida na seção 2 e de acordo com a observação 3.

A inexistência de uma tecnologia perfeita de *record-keeping*, em ambientes nos quais os indivíduos não possuem *commitment*, gera atratividade para o uso de meios de troca com forma de induzir produção e consumo na economia. O meio de troca substitui a tecnologia de *record-keeping* (ou ainda, o crédito) no papel social de facilitar trocas.

1. Se a imperfeição da tecnologia de monitoramento for parcial[52], a utilização de certificados de produção como meio de troca (*inside money*) é capaz de superar/amenizar o problema de dupla coincidência de interesses, conforme estabelecido por Cavalcanti et al. (1999) e Cavalcanti and Wallace (1999a,b). Neste caso, emerge um sistema monetário controlado descentralizadamente pelos indivíduos monitoráveis (bancos e Banco Central) e regulado centralizadamente pela sociedade via monitoramento e punição de eventuais comportamentos oportunistas.

2. Se a imperfeição da tecnologia de monitoramento for completa, no sentido de que é impossível monitorar ações individuais, o uso de um objeto sem valor intrínseco (moeda fiduciária) como evidência de produção de bens/serviços é útil para viabilizar trocas, conforme estabelecido por Kiyotaki and Wright (1989, 1991) e Kocherlakota (1998a,b). Caso os indivíduos coordenem suas crenças na aceitação futura deste objeto como meio de troca, este objeto circulará na economia induzindo produção e consumo (ver figura 8). A performance deste objeto na função de moeda (indução de trocas) dependerá de quão boas são suas propriedades de, por exemplo, escassez, durabilidade e divisibilidade. Assim, o sistema monetário que emerge com o uso de moeda fiduciária é controlado e regulado em grande parte de forma exógena pela evolução das propriedades dos objetos sendo utilizados como moeda.

Nos sistemas de trocas observados ao longo da história da humanidade, alguma tecnologia de monitoramento é empregada juntamente com o uso de meios de troca — há coexistência entre diversos tipos de meio de troca. Moeda *inside* (por exemplo, depósitos à vista) e moeda fiduciária coexistem: algumas trocas são intermediadas pela primeira, enquanto outras trocas são facilitadas pela segunda.

Essa coexistência de meios de troca, no entanto, não é estática: a imperfeição dos meios de troca no desempenho da função de moeda motiva contínuo esforço no aprimoramento dos sistemas monetários. O depósito à vista, por exemplo, que no passado era utilizado via a emissão de cheques ao portador, hoje é utilizável via o uso de cartões de débito. O conceito de moeda fiduciária, por sua vez, antes embutido em objetos encontrados na natureza com oferta fixa, hoje se faz presente no papel-moeda sem lastro: objetos

[52]No sentido de que é possível monitorar perfeitamente somente um subconjunto de indivíduos da sociedade, como em Cavalcanti and Wallace (1999a,b), ou de que é possível registrar publicamente resgates de dívidas (moedas) privadas, como em Cavalcanti et al. (1999).

reproduzíveis (embora dificilmente falsificáveis) cuja emissão é controlada pela sociedade e delegada ao Estado.

A viabilização do uso de cartões de débito como meio de troca, em particular, é um dos resultados da grande evolução dos sistemas contábeis utilizados por indivíduos monitoráveis (bancos). O que no passado era registrado em livros-razão em papel, hoje é registrado em livros-razão eletrônicos/virtuais. Essa evolução dos sistemas de registro melhorou o desempenho da moeda *inside* como meio de troca, mas não modificou sua essência: ela continua baseada na capacidade da sociedade em monitorar os indivíduos responsáveis pelo seu gerenciamento (o sistema bancário).

A inovação conceitual do protocolo das criptomoedas é utilizar a tecnologia contábil eletrônica já utilizada pelo sistema bancário sem a necessidade de monitoramento pela sociedade dos responsáveis pelo seu gerenciamento. Quem controla e regula o sistema monetário baseado em criptomoeda é a tecnologia de legitimação na qual estas se baseiam.

Proposição 1 *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.*

Em sistemas de registros monitorados centralizadamente — como aquele utilizado pelo sistema bancário —, a confiabilidade nos registros de transferência de propriedade da moeda (evidência de produção passada) decorre da capacidade da sociedade em monitorar a entidade encarregada de manter e gerenciar o livro-razão (*ledger*) da moeda[53].

No protocolo das criptomoedas, por outro lado, a confiabilidade decorre da dificuldade tecnológica (computacional) em se fraudar a *blockchain*, a qual é imposta pela exigência de apresentação da *proof-of-work* de cada bloco de transações a ser adicionado na cadeia de blocos. Neste caso, a proteção contra fraudes não demanda monitoramento dos fraudadores a fim de identificá-los e puni-los no futuro: é o custo incorrido no ato da fraude que desincentiva comportamentos oportunistas[54]. O desenho do protocolo (especialmente, a *blockchain*) funciona como uma *tecnologia de comprometimento* em gerenciar de forma adequada o sistema monetário. Ao aderirem ao protocolo da criptomoeda, os gerenciadores bloqueiam *ex ante* seu incentivo *ex post* em fraudar o sistema monetário — de forma

[53] Considere, por exemplo, o enorme e sofisticado esforço que os Bancos Centrais fazem para monitorar as atividades dos bancos, a fim de impedir comportamentos oportunistas baseados na posição privilegiada que estes ocupam no sistema monetário.

[54] Assim, não há necessidade de centralização da manutenção e gerenciamento do *ledger* da criptomoeda e, portanto, pode-se usufruir os benefícios que a descentralização do sistema proporciona: robustez, anonimidade, eficiência *etc.* Ver Antonopoulos (2014).

semelhante à maneira com que a antecipação de produção (uso de moeda mercadoria) resolve o problema de comprometimento quando há bens duráveis.

Ao não demandar monitoramento, as criptomoedas se diferenciam da moeda *inside* e do papel moeda sem lastro e se assemelham aos objetos sem valor intrínseco utilizados como moeda fiduciária ao longo da história[55]. A confiabilidade de seus registros não demanda monitoramento de ações individuais, ela decorre do próprio desenho da moeda. Por outro lado, na medida em que possuem configuração de propriedades bastante flexível, as criptomoedas se diferenciam da moeda fiduciária e se assemelham às moedas baseadas em monitoramento (*inside money* e papel moeda sem lastro).

As propriedades (escassez, durabilidade e divisibilidade) do objeto candidato a moeda fiduciária não são configuráveis, elas são dadas para a sociedade. A margem de configuração do meio de troca se limita a escolha de qual objeto será usado como moeda. A configuração da moeda *inside* e do papel moeda sem lastro, por sua vez, é bastante flexível, bastando especificar (anotar) no meio de troca a propriedade desejada. Analogamente as moedas baseadas em monitoramento, a característica eletrônica das criptomoedas provê enorme flexibilidade de formatação: é possível configurar o protocolo (desenho) da criptomoeda para otimizar propriedades importantes para o desempenho da função de intermediação de trocas.

Em consonância com as observações de Garratt and Wallace (2018), não se trata de uma moeda *inside* (pois a criptomoeda não é um certificado de dívida privada que circula como meio de troca), mas sim de uma moeda *outside*. Também não se trata de uma moeda soberana (de curso forçado garantido pelo Estado), mas sim de uma moeda privada.

A criptomoeda é uma moeda privada *outside* e fiduciária.

Em resumo, a criptomoeda pode ser vista como uma combinação de boas propriedades das moedas baseadas em monitoramento (*inside* e papel sem lastro) com boas propriedades da moeda puramente fiduciária. Ela possui a flexibilidade de configuração das moedas baseadas em monitoramento e a dispensabilidade de monitoramento de gerenciadores das moedas fiduciárias baseadas em objetos encontrados em oferta e formatos fixos na natureza.

[55] A título de ilustração, Halaburda and Sarvary (2016) relatam o uso de *conchas marinhas* (carapaças de moluscos) para intermediação de trocas na África e de *dentes de baleia* em Fiji.

4 Considerações Finais

Observação central deste artigo, a grande inovação monetária das criptomoedas foi **viabilizar** a geração de evidência *confiável* e *flexível* de produção de bens/serviços *sem* o uso de *monitoramento* de ações dos responsáveis por sua emissão e gerenciamento. Não há neste artigo, no entanto, uma discussão sobre a **atratividade** do uso de monitoramento para tal geração de evidência para além daquela decorrente da flexibilidade de configuração de propriedades do meio de troca que o monitoramento possibilita.

O emprego de monitoramento ainda pode ser útil como forma de delegar parte do gerenciamento da criptomoeda — por exemplo, a política monetária. A regra de política monetária das criptomoedas é definida no protocolo da moeda, não havendo margem para discricionariedade em sua emissão e gerenciamento. Se a política monetária ótima precisa reagir às condições da economia, esta inflexibilidade é não atrativa[56].

No caso particular da Bitcoin, o protocolo prevê uma taxa de crescimento na quantidade de moeda decrescente no tempo que implicará em uma quantidade máxima de moeda emitida. A partir da *Teoria Quantitativa da Moeda*, isso implicará uma deflação de preços se a velocidade da moeda não acompanhar a taxa de crescimento da economia. Embora a *Regra de Friedman* prescreva a otimalidade de políticas desta natureza, a atratividade de deflações não é consenso entre os economistas. Um forte argumento contrário é a observação de que a sociedade, ao longo de sua história, escolheu inflação baixa e positiva, embora deflação fosse uma opção disponível.

Por outro lado, a definição de uma regra clara e não manipulável reduz a incerteza na economia e protege a política monetária de comportamentos oportunistas. Menor incerteza aumenta a previsibilidade, facilitando o planejamento dos agentes econômicos. Maior proteção impede que subgrupos de indivíduos manipulem a política monetária em benefício próprio e em prejuízo da sociedade — como frequentemente políticos pressionam o Banco Central em favor de políticas mais expansionistas. A definição da regra de política monetária no desenho da moeda pode ser vista como o limite máximo de *Independência do Banco Central*, no sentido de que suas decisões não podem ser afetadas por pressão política, já que elas seriam pré-estabelecidas na criação da moeda. Ou seja, pode ser vista como uma tecnologia de comprometimento contra o incentivo *ex post* em ceder à pressão dos políticos.

Embora sem resolução clara, a discussão de atratividade entre regras e discricionariedade tem motivado propostas de delegação de política monetária de criptomoedas ao Banco Central por meio da criação de *criptomoedas soberanas*[57]. Diversos formatos tem

[56] Esta discussão de atratividade entre regras e discricionariedade é um assunto clássico da Teoria Econômica. Ver Kydland and Prescott (1977).

[57] Ver, por exemplo Bech and Garratt (2017), Kumhof and Noone (2018) e as referências então citadas.

sido considerados, mas o que se propõe essencialmente é aproveitar a inovação tecnológica das criptomoedas sem renunciar ao controle da política monetária.

As consequências de uma eventual criptomoeda soberana são incertas, no entanto. Alguns autores[58] advogam que a migração dos indivíduos da moeda *inside* oferecida pelos bancos (depósito à vista) para a eventual criptomoeda do Banco Central tornaria o sistema bancário mais estável. A competição com o meio de troca eletrônico do Banco Central dificultaria a captação de recursos via depósito à vista pelo sistema bancário, o que aumentaria a maturidade dos recursos captados. Ao aproximar a maturidade das captações (passivos) com aquela dos empréstimos (ativos), os bancos reduziriam seu papel de *transformação de maturidade* (via *reserva fracionária*) e, portanto, sua exposição à *corridas bancárias*[59].

Stevens (2017), no entanto, alerta para o risco de desorganização da economia ao privar o sistema bancário de sua principal fonte de financiamento para empréstimos. Destaca que, ao canalizar parte da poupança da economia para fora do sistema bancário, a criação de uma moeda eletrônica limitaria a capacidade dos bancos em ofertar crédito para importantes projetos de investimento.

A breve discussão sobre a delegação (ou não) da política monetária das criptomoedas aqui destacada não exaure as questões relacionadas a atratividade do emprego de monitoramento para a delegação de partes do gerenciamento das criptomoedas. Ela, no entanto, ilustra a riqueza de perguntas econômicas provocadas pelo fenômeno de surgimento de criptomoedas[60] e, em particular, pelo reconhecimento de sua inovação fundamental: viabilizar a geração de evidência *confiável* e *flexível* de produção de bens/serviços *sem* o uso de *monitoramento* de ações dos responsáveis por sua emissão e gerenciamento.

[58] Ver Ketterer and Andrade (2016), Stevens (2017) e Holden and Malani (2018).

[59] Uma exposição introdutória sobre a relação entre corridas bancárias e transformação de maturidade é Diamond (2007). Diamond and Dybvig (1983) é a referência clássica. Para resultados recentes sobre instabilidade bancária, ver Bertolai et al. (2014, 2018), Bertolai and Melo (2017) e as referências então citadas.

[60] Como evidência adicional para a riqueza de perguntas econômicas, ver Abadi and Brunnermeier (2018) e as referências então citadas.

Bibliografia

J. Abadi and M. Brunnermeier. Blockchain economics. Technical report, mimeo Princeton University, 2018.

D. Abreu, D. Pearce, and E. Stacchetti. Toward a theory of discounted repeated games with imperfect monitoring. *Econometrica: Journal of the Econometric Society*, pages 1041–1063, 1990.

S. R. Aiyagari and N. Wallace. Existence of steady states with positive consumption in the kiyotaki-wright model. *The Review of Economic Studies*, 58(5):901–916, 1991.

R. Ali, J. Barrdear, R. Clews, and J. Southgate. The economics of digital currencies. *Bank of England Quarterly Bulletin*, 2014.

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

A. M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. "O'Reilly Media, Inc.", 2017.

M. Barossi Filho and R. Sztajn. Natureza jurídica da moeda e desafios da moeda virtual. *Revista Jurídica Luso-Brasileira*, pages 1669–1690, 2015.

D. M. Barros. Moeda e criptomoeda: uma análise do bitcoin sobre a perspectiva pós-keynesiana. 2017.

M. L. Bech and R. Garratt. Central bank cryptocurrencies. *BIS Quarterly Review*, 2017.

J. D. Bertolai and M. Melo. Fragilidade bancária com (e sem) serviço sequencial. *Revista Brasileira de Economia*, 71(3):261–299, 2017.

J. D. Bertolai, R. d. O. Cavalcanti, and P. K. Monteiro. Run theorems for low returns and large banks. *Economic Theory*, 57(2):223–252, 2014.

J. D. Bertolai, R. d. O. Cavalcanti, and P. K. Monteiro. Bank runs with many small banks and mutual guarantees at the terminal stage. *Economic Theory*, forthcoming, 2018.

T. Borgers. *An introduction to the theory of mechanism design*. Oxford University Press, USA, 2015.

R. G. Brown. A simple explanation of how money moves around the banking system. *Thoughts on the future of finance.*, 2013. URL https://gendal.me/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-bar

R. Cavalcanti and E. Nosal. Counterfeiting as private money in mechanism design. *Journal of Money, Credit and Banking*, 43(s2):625–636, 2011.

R. d. O. Cavalcanti and N. Wallace. Inside and outside money as alternative media of exchange. *Journal of Money, Credit and Banking*, pages 443–457, 1999a.

R. d. O. Cavalcanti and N. Wallace. A model of private bank-note issue. *Review of Economic Dynamics*, 2(1):104–136, 1999b.

R. d. O. Cavalcanti, A. Erosa, and T. Temzelides. Private money and reserve management in a random-matching model. *Journal of Political Economy*, 107(5):929–945, 1999.

E. T. d. Costa. Bitcoin: análise da moeda virtual descentralizada e suas implicações. 2014.

R. de Senne Garcia. Moedas virtuais são moedas? um estudo de caso para o bitcoin e o litecoin. *Monografia - UNICAMP*, 2014.

D. W. Diamond. Banks and liquidity creation: a simple exposition of the Diamond-Dybvig model. *Economic Quarterly*, 93(2):189–201, 2007.

D. W. Diamond and P. H. Dybvig. Bank runs, deposit insurance, and liquidity. *Journal of Political Economy*, 91(3):401–419, 1983.

S. Driscoll. How bitcoin works under the hood. *Imponderable Things. Blogger.*, 2013. URL http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html.

P. Ferreira. Além do cara ou coroa: bitcoin ultrapassa fronteiras e ganha mais usuários. *Agência Brasil*, Maio 2017. URL http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/alem-do-cara-ou-coroa-bitcoin

S. Fischer. Money and the production function. *Economic Inquiry*, 12(4):517–533, 1974.

R. Garratt and N. Wallace. Bitcoin 1, bitcoin 2, ...: An experiment in privately issued outside monies. *Economic Inquiry*, 2018.

H. Halaburda and M. Sarvary. *Beyond Bitcoin: The Economics of Digital Currencies*. Palgrave Macmillan US, 2016. ISBN 9781137506429.

R. Holden and A. Malani. Why the irs fears bitcoin. *The New York Times*, 2018.

C. M. Kahn, J. McAndrews, and W. Roberds. Money is privacy. *International Economic Review*, 46(2):377–399, 2005.

J. A. Ketterer and G. Andrade. Digital central bank money and the unbundling of the banking function. Technical report, Inter-American Development Bank, 2016.

N. Kiyotaki and R. Wright. On money as a medium of exchange. *Journal of political Economy*, 97(4):927–954, 1989.

N. Kiyotaki and R. Wright. A contribution to the pure theory of money. *Journal of economic Theory*, 53(2):215–235, 1991.

N. R. Kocherlakota. Money is memory. *journal of economic theory*, 81(2):232–251, 1998a.

N. R. Kocherlakota. The technological role of fiat money. *Federal Reserve Bank of Minneapolis. Quarterly Review-Federal Reserve Bank of Minneapolis*, 22(3):2, 1998b.

M. Kumhof and C. Noone. Central bank digital currencies-design principles and balance sheet implications. *Staff Working Paper*, 2018.

F. E. Kydland and E. C. Prescott. Rules rather than discretion: The inconsistency of optimal plans. *Journal of political economy*, 85(3):473–491, 1977.

R. Lagos. Inside and outside money. In *Monetary Economics*, pages 132–136. Springer, 2010.

S. Lo and J. C. Wang. Bitcoin as money? *Current Policy Perspectives - Federal Reserve Bank of Boston*, 2014.

R. E. Lucas. Equilibrium in a pure currency economy. *Economic inquiry*, 18(2):203–220, 1980.

R. E. Lucas Jr. Interest rates and currency prices in a two-country world. *Journal of Monetary Economics*, 10(3):335–359, 1982.

R. E. Lucas Jr and N. L. Stokey. Money and interest in a cash-in-advance economy. *Econometrica: Journal of the Econometric Society*, pages 491–513, 1987.

N. G. Mankiw. *Macroeconomia*. LTC, 7ª edition, 2011.

M. M. Martins. Entendendo moedas virtuais à luz das teorias monetárias: o caso do bitcoin. *Monografia - Universidade de Brasília*, 2016.

D. Mookherjee. The 2007 nobel memorial prize in mechanism design theory. *The Scandinavian Journal of Economics*, 110(2):237–260, 2008.

P. Nahin. *An Imaginary Tale: The Story of* $\sqrt{-1}$. Princeton Science Library. Princeton University Press, 2010. ISBN 9781400833894.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

E. Nosal and N. Wallace. A model of (the threat of) counterfeiting. *Journal of Monetary Economics*, 54(4):994–1001, 2007.

J. M. Ostroy. The informational efficiency of monetary exchange. *The American Economic Review*, 63(4):597–610, 1973.

L. d. O. Ribeiro. Estudo do bitcoin enquanto moeda e investimento. *Monografia - FURG*, 2017.

M. Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

P. A. Samuelson. An exact consumption-loan model of interest with or without the social contrivance of money. *Journal of political economy*, 66(6):467–482, 1958.

F. D. Scarinci. A factibilidade do bitcoin enquanto moeda um estudo acerca das criptomoedas. *Monografia - UFRGS*, 2015.

M. Sidrauski. Rational choice and patterns of growth in a monetary economy. *The American Economic Review*, pages 534–544, 1967.

R. M. P. Silva. A evolução da moeda e a bitcoin: um estudo da validade da bitcoin como moeda. *Revista da Graduação - PUC/RS*, 9(2), 2016.

A. Sinai and H. H. Stokes. Real money balances: An omitted variable from the production function? *The Review of Economics and Statistics*, pages 290–296, 1972.

A. Stevens. Digital currencies : Threats and opportunities for monetary policy. *Economic Review - National Bank of Belgium*, (i):79–92, June 2017.

R. M. Townsend. Models of money with spatially separated agents. *Models of monetary economies*, pages 265–303, 1980.

R. M. Townsend. Economic organization with limited communication. *The American Economic Review*, pages 954–971, 1987.

R. M. Townsend. Currency and credit in a private information economy. *Journal of Political Economy*, 97(6):1323–1344, 1989.

R. M. Townsend. *Financial structure and economic organization: Key elements and patterns in theory and history*. Blackwell, 1990.

F. Ulrich. *Bitcoin: a moeda na era digital*. LVM Editora, 2017.

C. van der Laan. É crível uma economia monetária baseada em bitcoins? limites à disseminação de moedas virtuais privadas. *Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado (Texto para Discussão nº 163)*, 2014.

D. Viana. Novos dinheiros para novas economias. *Página 22*, 0(89):35, 2014. URL `http://bibliotecadigital.fgv.br/ojs/index.php/pagina22/article/view/38918`.

N. Wallace. The mechanism-design approach to monetary theory. In *Handbook of Monetary Economics*, volume 3, pages 3–23. Elsevier, 2010.

D. Yermack. Is bitcoin a real currency? an economic appraisal. In D. L. K. Chuen, editor, *Handbook of digital currency*, pages 31–43. Elsevier, 2015.