ANÁLISE ECONÔMICA DA CYBERSEGURANÇA APLICADA À BLOCKCHAIN

Cesar Santolim*

Robert SHILLER, Prêmio Nobel de Economia em 2013, em sua recente obra "Narrative Economics: How Stories Go Viral and Drive Major Economic Events"[1], inicia sua abordagem pelo que denomina "Bitcoin Narratives". Para SHILLER, as "narrativas econômicas" consistem em ideias transmitidas mediante histórias "contagiosas" (repetidas "boca-a-boca", individualmente), e os esforços que as pessoas fazem para gerar novas histórias, também contagiosas, ou para tornar as histórias originais ainda mais contagiosas. Estas "histórias contagiosas" têm o potencial de alterar o modo como os agentes econômicos tomam as suas decisões, e as "bitcoin narratives" são um dos exemplos mais evidentes desta situação. Como afirma SHILLER "a narrativa do Bitcoin envolve histórias sobre pessoas jovens e cosmopolitas, contrastando com burocratas sem inspiração; uma história de riqueza, desigualdade, tecnologia da informação avançada e jargão envolvente e misteriosamente impenetrável"[2]. Além disso, o "bitcoin" está associado a uma visão "anarquista", de um "mundo sem autoridades". *Both cryptocurrencies and blockchain ... seem to have great emotional appeal for some*

* Professor da Faculdade de Direito da UFRGS. Mestre e Doutor em Direito (UFRGS). Pós-doutorado em Direito (Universidade de Lisboa). Advogado e Economista.

[1] Princeton: Princeton University Press, 2019.

[2] *Op. cit*, p. 3. No original: "The Bitcoin narrative involves stories about inspired cosmopolitan young people, contrasting with uninspired bureaucrats; a story of riches, inequality, advanced information technology, and involving mysterious impenetrable jargon".

people[3], pois apresenta uma contra narrativa para as mais tradicionais visões do anarquismo, ligadas à violência e ao terrorismo. O "bitcoin" é "contagioso" porque sugere que invenções importantes podem, eventualmente, permitir o desenvolvimento de uma sociedade livre e anárquica.

As primeiras tentativas da criação de um "sistema de pagamento digital", que pudesse funcionar de forma autônoma, e independentemente da existência de intermediários (as *Trusted Third Parties* – "terceiras partes confiáveis", que consagraram a certificação digital, como conhecemos), remontam pelo menos ao eCash proposto por David Chaum, em 1993, que não teve o sucesso esperado, muito provavelmente pelo estágio em que se encontrava o comércio on-line, naquele momento. Com o passar dos anos, contudo, foram retomados os esforços nesse sentido, culminando com o "protocolo de confiança" proposto em 2008 por Satoshi Nakamoto, "um sistema ponto a ponto de dinheiro eletrônico usando uma criptomoeda (moeda digital) chamada Bitcoin".

A sustentação (e aprimoramento) desse sistema exige, como é evidente, a presença de elementos de segurança, sem os quais é disfuncional. "Confiança" somente pode existir em um quadro onde as expectativas das partes intervenientes se amparem em garantias mínimas de respeito às promessas e compromissos assumidos, e essa é uma condição que exige segurança institucional, dada por fatores técnicos e/ou jurídicos.

Dentre diversas soluções tecnológicas que impactam no Direito, a *blockchain* talvez seja aquela que, contemporaneamente, tem merecido um maior destaque. Não apenas porque é base para o funcionamento das moedas virtuais, mas porque, entre outras perspectivas, oferece a possibilidade da superação de diversos problemas decorrentes das relações jurídicas despersonalizadas, reintroduzindo um elemento de confiança antes só

[3] *Op. cit.*, p. 6, em tradução livre: "Tanto as criptomoedas quanto a blockchain ... parecem ter um grande apelo emocional para algumas pessoas."

existente nas pequenas comunidades, e típicas dos grupos primários (sob a ótica da Sociologia)[4]. "Confiança", sabe-se, está intrinsicamente associada a ideia de "segurança" (em seus aspectos materiais). Situações inseguras despertam desconfiança dos agentes envolvidos, com incremento nos custos de transação[5]. Uma solução tecnológica, como a *blockchain*. que oferece alguma forma de "certificação orgânica" às relações estabelecidas, baseada em um sistema "tecnicamente incorruptível", apresenta-se como alternativa para a reconstrução da confiança, assegurando a legitimidade das transações feitas. Para que isso aconteça, contudo, esse "sistema" deve ser seguro, não permitindo violações não identificáveis, ou de complexa e demorada constatação.

Conforme descrito de forma simplificada, *"fundamentalmente, blockchain é uma combinação de tecnologias já existentes que juntos podem criar redes que protegem a confiança entre pessoas ou partes que de outra forma não têm motivos para confiar umas nas outras. Especificamente, utiliza a tecnologia de contabilidade distribuída (DLT) para armazenar as informações verificadas criptografia entre um grupo de usuários, que é acordado através de um protocolo de rede predefinido, geralmente sem o controle de uma autoridade central. O casamento dessas tecnologias dá às redes blockchain características chave que podem "remover" a necessidade de confiança e, portanto, permitir uma transferência segura de valor e dados diretamente entre as partes"*[6].

---

[4] A noção de "grupos primários" é assente na Sociologia, como se pode observar nas referências feitas por LITWAK e SZLENYI, sendo aqui irrelevante a distinção terminológica a partir de a partir do trabalho de COOLEY (relações "face a face, permanentes, afetivas, não instrumentais e difusas", ou PARSON (relações "particularistas, coletivas, difusas, afetivas e atribuídas).

[5] Conforme Fernando ARAÚJO, "custos de transacção são todos aqueles em que se incorre na troca de utilidades e na afectação comutativa de recursos, quando se busca uma contraparte, se negocia com ela, se preveem e supervisionam as contingências do cumprimento". (*Introdução à Economia,* p. 553).

[6] OECD Blockchain Primer.

Estruturalmente, *"uma blockchain é um livro compartilhado de transações entre partes em uma rede, não controlado por uma única autoridade central. Você pode pensar em um livro como um livro de registro: registra e armazena todas as transações entre usuários em ordem cronológica. Em vez de uma autoridade controlando esse livro (como um banco), uma cópia idêntica do livro é mantida por todos os usuários na rede, chamados nós (nodes)"*[7].

Como se observa, a função preponderante desta tecnologia gira em torno da ideia de segurança, motivo pelo se impõe sejam considerados os elementos de sustentabilidade da sua manutenção, sob esta perspectiva.

No âmbito da Economia, são conhecidos os modelos acerca dos investimentos em segurança, elaborados a partir da noção de custo/benefício, o que significa que todos os agentes econômicos estão propensos a determinado grau de investimento na busca deste recurso ("segurança"), na exata medida do benefício que venham a obter, que estará diretamente relacionado com o ativo que pretendam "proteger" e com o êxito das medidas empregadas.

Esses investimentos em segurança, quando se trate de tecnologia da informação e comunicação (TIC), que se pode designar por "cybersegurança" (*cybersecurity*), obedecem a uma lógica específica, que precisa ser bem compreendida, para um desenho institucional adequado.

SALES, já em 2013[8], alertava para o fato que não havia desenvolvido suficientemente o debate acerca da cybersegurança, e esta situação, em grande medida, permanece a mesma. Como foi então apontado, o tratamento da cybersegurança deve adotar abordagem em torno de sua aproximação com outras áreas críticas em termos de regulação: direito ambiental,

[7] OECD Blockchain Primer.
[8] "The law and policy of cyber-security are undertheorized". *Regulating Cyber-Security*, p. 1507.

legislação antitruste, responsabilidade civil e saúde pública.

Assim como a proteção do meio ambiente, a tutela da cybersegurança é primariamente preocupada com externalidades negativas:

> *Just as firms tend to underinvest in pollution controls because some costs of their emissions are borne by those who are downwind, they also tend to underinvest in cyber-defenses because some costs of intrusions are externalized onto others…*
> *…*
> *Because firms do not bear the full costs of their vulnerabilities, they have weaker incentives to secure their systems.*[9]

Cybersegurança igualmente possui semelhança com questões relacionadas ao direito da concorrência, pois, como esta área se dedica a combater práticas anticompetitivas, há ceticismo quando às possibilidades de medidas cooperativas entre os agentes econômicos envolvidos:

> *Antitrust law seeks to prevent anticompetitive behavior, and it traditionally has been skeptical of coordination among competitors. Some interfirm cooperation could improve cyber-security – sharing information about vulnerabilities and threats, for example, or developing industry-wide security standards. Yet firms are reluctant to do so because they fear antitrust liability.*[10]

Raciocínio semelhante se aplica às proximidades com a responsabilidade civil: o direito que versa sobre a responsabilidade por fato/defeito do produto vale-se a possibilidade da determinação de indenizações monetárias como incentivo para que

---

[9] *Op. cit.*, p. 1508, em tradução livre: Assim como as empresas tendem a subinvestir nos controles de poluição, porque alguns custos de suas emissões são suportados por aqueles que sofrem seus efeitos, eles também tendem a desvalorizar as defesas cibernéticas porque alguns custos de intrusões são externalizados em outros ... Como as empresas não arcam com os custos totais de suas vulnerabilidades, elas têm incentivos mais fracos para proteger seus sistemas.

[10] *Op. cit.*, p. 1508, em tradução livre: A lei antitruste busca prevenir o comportamento anticoncorrencial e tradicionalmente é cética quanto à coordenação entre concorrentes. Algumas cooperações entre empresas poderiam melhorar a segurança cibernética - compartilhando informações sobre vulnerabilidades e ameaças, por exemplo, ou desenvolvendo padrões de segurança para toda a indústria. No entanto, as empresas relutam em fazê-lo porque temem a responsabilidade antitruste.

as empresas adotem precauções razoáveis quando colocam seus produtos no mercado, mas este incentivo é baixo, no caso da cybersegurança:

> *Companies face little risk of liability to those who are harmed by attacks on their systems or products, and they therefore have weaker incentives to identify and patch vulnerabilities.*[11]

Por fim, há elementos a considerar na semelhança com a saúde pública, pois um objetivo fundamental nesta área, sob o ponto de vista do Direito, é a prevenção, o que também é válido para a cybersegurança:

> *A key goal of public health law is prevention-keeping those who have contracted a disease from spreading it to the healthy, a form of negative externality. Public health law uses vaccinations to promote immunity, biosurveillance to detect outbreaks, and quarantines to contain infectious diseases. Cyber-security has similar goals-ensuring that critical systems are immune to malware, quickly detecting outbreaks of malicious code, and preventing contaminated computers from infecting clean systems-and could use similar tools.*[12]

O propósito deste estudo é destacar a importância de refletir sobre o caráter destes investimentos em segurança e sua compatibilidade com o modelo proposto para a *blockchain*, no sentido de indicar a presença de algumas dificuldades estruturais que devem ser resolvidas.

Como assinalado por KOBAYASHI[13], o "modelo padrão" utilizado pela teoria econômica observa a presença de

---

[11] *Op. cit.*, p. 1508, em tradução livre: As empresas enfrentam pouco risco de responsabilidade para aqueles que são prejudicados por ataques a seus sistemas ou produtos e, portanto, têm incentivos mais fracos para identificar e corrigir vulnerabilidades.

[12] *Op. cit.*, p. 1508, em tradução livre: "Um objetivo-chave da legislação sobre saúde pública é a prevenção, impedindo que aqueles que contraíram uma doença a disseminem para os demais, uma forma de externalidade negativa. A legislação sobre saúde pública utiliza vacinas para promover a imunidade, o biomonitoramento para detectar surtos e quarentenas para conter doenças infecciosas. A segurança cibernética tem objetivos semelhantes - garantir que sistemas críticos sejam imunes a malwares, detectar rapidamente surtos de códigos mal-intencionados e impedir que computadores contaminados infectem sistemas limpos - e pode usar ferramentas semelhantes."

[13] KOBAYASHI, Bruce H. *Private versus Social Incentives in Cybersecurity: Law and Economics.*

incentivos privados e de incentivos sociais (ou "públicos"), para gastos com segurança.

Despesas privadas em segurança são adequadas na medida que geram benefícios privados (cadeados e cofres que protegem os ativos de A não geram benefícios diretos para B). Mesmo neste caso, existem "efeitos de disseminação", positivos (*general deterrence*, quando ocorre diminuição dos benefícios brutos/gerais para os ladrões, diminuindo o benefício dos roubos) e negativos (*diversion*, quando ladrões migram para onde não há proteção). Ademais, despesas privadas em segurança podem ser socialmente excessivas, pois o principal objetivo "da sociedade" é reduzir o volume total de recursos gastos para impedir as violações de segurança ("transferências ilícitas de recursos"), ao passo que o objetivo das vítimas é minimizar as suas "perdas" de ativos e as suas "despesas" para impedir as violações e o objetivo dos "criminosos" é maximizar a quantidade de ativos obtidos, a um mínimo de "despesas" com as violações. Como resultado dessa diferença de "objetivos" entre "vítimas" e "criminosos", se produz uma "corrida armamentista", que é socialmente ineficiente (um "desalinhamento" entre o interesse da "sociedade" e o interesse dos "privados"), pois ocorre um aumento generalizado dos gastos (com segurança e com as tentativas de quebra de segurança), o que é socialmente indesejado.

Já a "segurança pública" (que é fornecida indistintamente a toda a sociedade, também referida nos modelos como "segurança nacional", quando especialmente relacionada à proteção dos Estados, uns em relação aos outros) é considerada, na doutrina econômica, como exemplo de *bem público*, exatamente por ser "um caso extremo de externalidade positiva"[14]. Não é possível submeter um "bem público" às soluções de mercado, pois não há sinalização por preços, e não há incentivo adequado para a produção privada destes bens.

Os "bens públicos" possuem a característica do consumo

[14] ARAÚJO, Fernando. *Introdução à Economia*, p. 579.

"não exclusivo" e "não exaustivo"[15], pois os custos de exclusão de beneficiários não pagantes que consomem o recurso são altos o suficiente para impedir que qualquer empresa voltada para o lucro privado se disponha a fornecê-lo (consumo não exclusivo) e o consumo do bem por um agente não exclui a possibilidade do seu aproveitamento por outro (não há como determinar o quanto está sendo "apropriado" por cada agente econômico, gerando a "indivisibilidade" do recurso – consumo não exaustivo, ou "não-rival").

Considerando que as despesas em cybersegurança consistem essencialmente na obtenção de informação sobre a natureza e frequência dos ataques passados, ataques pendentes, vulnerabilidades e defesas em potencial, essa informação tem natureza de um bem público. Diversamente do que ocorre na produção de incentivos para a segurança convencional, onde há presença de caráter privado, até um certo nível – mesmo havendo áreas típicas de bem público, como a segurança "pública" e "defesa nacional" – (a) a produção dessa informação está submetida à troca entre incentivos sociais para o uso livre da informação e o incentivo para restringir esse uso (para estimular a criação da informação) e (b) essa informação não pode ser um bem coletivo livremente disponível para todos, uma vez produzida (se for, não pode haver uso não-exclusivo, estimulando aquilo que se denomina "efeito carona", ou "free riding"[16]).

---

[15] FRANCO, A.L.S., *apud* ARAÚJO, Fernando. *Op. cit.*, p. 580: "1. a não-susceptibilidade de exclusão, querendo isso dizer-se q1ue ninguém consegue ser *eficientemente* afastado da fruição directa e integral do bem – caso em que, podendo haver meios para prevenir o acesso indiscriminado, eles são mais caros que os ganhos que adviriam da discriminação no uso e consumo –; 2. A não-rivalidade ou não-exclusividade do uso, que significa que o acesso de cada um ao bem não interfere relevantemente no acesso e uso por parte de qualquer outro – podendo haver uma ligeira diminuição na utilidade do bem advinda do simultâneo do bem, mas não tão forte que determine qualquer reacção de elasticidade na procura do bem, assim concluindo que os "consumos adicionais" se fazem "a custo zero" –.

[16] ARAÚJO, Fernando. *Introdução à Economia*, p. 585: "O problema essencial que determina a falha de produção dos bens públicos é o já referido *efeito de boleia*, o facto de as características do bem público tornarem racional, para cada um, esperar

Examinando-se o caso da blockchain ("livro-razão" global / protocolo de confiança), e suas principais aplicações (as criptomoedas e os *smart contracts*, que são pedaços de código de propósito específico, que executam um conjunto complexo de instruções da blockchain, fornecendo um meio para a atribuição de direitos de utilização para outra parte[17]), evidencia-se o paradoxo existente entre a forma esperada de seu funcionamento e a natureza dos incentivos para investir em segurança .

Mais recentemente, pesquisadores da Carnegie Mellon University (David A. Tepper School of Business)[18] sugeriram um modelo acerca da escalabilidade do "bitcoin", concluindo pela sua insustentabilidade, nas suas atuais características:

> *Bitcoin falls dramatically short of the scale provided by banks for payments. Its ledger grows by the addition of blocks of ~ 2000 transaction every 10 minutes. Intuitively, one would expect that increasing the block capacity would solve this scaling problem. However, we show that increasing the block capacity would be futile. We analyze strategic interactions of miners, who are heterogeneous in their power over block addition, and users, who are heterogeneous in the value of their transactions, using a game-theoretic model. We show that a capacity increase can facilitate large miners to tacitly collude artificially reversing back the capacity via strategically adding partially*

pela respectiva produção pelos demais, para depois retirar benefícios da sua existência sem ter que suportar os custos correspondentes".

[17] Conforme lembram MARSH e DEWEY, **in** *The loan market, blockchain, and smart contracts*: "The term "smart contracts" can be misleading especially for lawyers who have a definite idea of what must be shown for there to be a binding legal agreement between parties. At a minimum, a contract requires there to be an offer by one party, an acceptance by another party, and some form of consideration to exist. When the term is used by software engineers, it means computer code that is self-executing (the type of code will depend on the protocol on which the code is implemented)". Em tradução livre: "O termo "contratos inteligentes" pode ser enganoso, especialmente para advogados com uma ideia definida do que deve ser considerado para que exista um vínculo de natureza jurídica entre as partes. No mínimo, um contrato exige que haja uma oferta por uma parte, uma aceitação por outra parte e alguma forma de *consideration* (isso no sistema do Common Law, n.a.) para existir. Quando o termo é usado pelo software engenheiros, significa código de computador que é auto-executável (o tipo de código dependerá o protocolo no qual o código é implementado).

[18] MALIK, ASERI, SINGH e SRINIVASAN, *Why Bitcoin Will Fail to Scale?*

filled blocks in order to extract economic rents. This strategic partial filling crowds out low value payments. Collusion is sustained if the smallest colluding miner has a share of block addition power above a lower bound. We provide empirical evidence of such strategic partial filling of blocks by large miners of Bitcoin.

We show that a protocol design intervention can breach the lower bound and eliminate collusion. However, this also makes the system less secure. On the one hand, collusion crowds out low-value payments; on the other hand, if collusion is suppressed, security threatens high-value payments. Thus, its untenable to include range of payments with vastly different outside options, willingness to bear security risk and delay onto a single chain. Thus, we show economic limits to the scalability of Bitcoin. Under these economic limits, collusive rent extraction acts an effective mechanism to invest in platform security and build responsiveness to demand shocks. These traits are otherwise hard to attain in dis-intermediated setting owing to the high cost of consensus.[19]

[19] Em tradução livre: "O Bitcoin fica dramaticamente aquém da escala fornecida pelos bancos para pagamentos. Seu livro-razão (contábil) cresce pela adição de blocos da transação de aproximadamente 2000 transações a cada 10 minutos. Intuitivamente, seria de esperar que o aumento da capacidade do bloco resolvesse esse problema de dimensionamento. No entanto, mostramos que aumentar a capacidade do bloco seria inútil. Analisamos interações estratégicas de mineradores, que são heterogêneos em seu poder sobre a adição de blocos, e usuários, que são heterogêneos no valor de suas transações, usando um modelo de teoria dos jogos. Mostramos que uma capacidade aumentada pode facilitar que grandes mineradores consigam conspirar tacitamente, invertendo artificialmente a capacidade, adicionando estrategicamente blocos parcialmente cheios, a fim de extrair rendas econômicas. Esse preenchimento parcial estratégico aglomera pagamentos de baixo valor. A colusão é mantida se o menor minerador em conluio tiver uma parcela do poder de adição de bloco acima de um limite inferior. Fornecemos evidências empíricas desse preenchimento parcial estratégico de blocos por grandes mineradores de Bitcoin. Mostramos que uma intervenção de projeto de protocolo pode violar o limite inferior e eliminar conluio. No entanto, isso também torna o sistema menos seguro. Por um lado, o conluio aglomera pagamentos de baixo valor; por outro lado, se o conluio for suprimido, a segurança ameaça pagamentos de alto valor. Portanto, é insustentável incluir uma gama de pagamentos com opções externas muito diferentes, disposição para suportar riscos de segurança e atrasar uma única cadeia. Assim, mostramos limites econômicos à escalabilidade do Bitcoin. Sob esses limites econômicos, a extração coletiva de renda atua como um mecanismo eficaz para investir em segurança da plataforma e criar capacidade de resposta a choques de demanda. De outra forma, essas características são difíceis de obter

O problema também não escapou a MARSH e DEWEY, no mesmo trabalho já citado:

> *Distributed ledger technology can be implemented with or without access controls, depending on whether an open, public network is used, or a restricted, permissioned network is chosen. The decentralized digital currency, Bitcoin, is likely the most well-known example of an open, public network where anyone can query the ledger and broadcast transactions without any authorization (assuming, of course, the individual has the proper computer equipment and software). In a public blockchain, ledgers are replicated across many computers referred to as "nodes", which are connected to a common network over the internet. Those operating the nodes are referred to as "miners". In contrast, a closed, permissioned network is restricted to certain individuals who have been given permission and the necessary credentials to access the ledger by a trusted third party.*
>
> *It is not surprising that the financial services industry is currently favoring the implementation of permissioned networks. Because of anti-money laundering ("AML"), know-your-customer ("KYC"), and privacy considerations (discussed more fully below), public networks are not really feasible in financial services at this time. A Bitcoin miner that is anonymous on a public network should be subject to the requirements of the Bank Secrecy Act and a financial institution's own KYC program as if it were to be involved in a similar function in the financial services industry for a bank Thus, it is understandable that given current frameworks, a bank's systems cannot be integrated with public networks, but as technology develops this, too, could change.*[20]

em ambientes desintermediados, devido ao alto custo do consenso.

[20] Em tradução livre: "A tecnologia de "livro-razão distribuído" pode ser implementada com ou sem controles de acesso, dependendo do uso de uma rede pública aberta ou de uma rede com permissão restrita. A moeda digital descentralizada, Bitcoin, é provavelmente o exemplo mais conhecido de uma rede pública aberta, onde qualquer pessoa pode consultar o "livro-razão" e transmitir transações sem qualquer autorização (supondo, é claro, o indivíduo tenha o equipamento de computador adequado e *software*). Em uma blockchain pública, os livros contábeis são replicados em muitos computadores referenciados como "nós", que são conectados a uma rede comum pela Internet. Aqueles que operam os nós são chamados de "mineradores". Por outro lado, uma rede fechada e com permissão é restrita a certas pessoas que receberam permissão

Assim, as soluções possíveis para esse problema envolvem intervenções regulatórias, com a fixação de padrões mínimos de segurança (com o natural risco de erros no padrão) e a designação de responsabilidades pelo gerenciamento (ou controle) do sistema da Blockchain, o que colide frontalmente com a visão predominante sobre sua funcionalidade, na atualidade.

Apesar da existência de uma "narrativa" romântica sobre o funcionamento "anárquico" (isto é, sem regulação) da blockchain, WEINSTEIN e PARKER[21] observam que

> *While it is often said that cryptocurrencies and blockchain technology are unregulated, nothing could be further from the truth. Numerous federal and state agencies in the United States, as well as agencies in other countries, regulate applications for this technology in some fashion. But the disparate approaches taken by different countries, or even by different agencies within the U.S., have led to confusion on the part of blockchain companies about the jurisdictions and regulatory regimes to which their products and services will be subject.*[22]

---

e as credenciais necessárias para acessar o "livro-razão" por terceiros confiáveis. Não é surpreendente que o setor de serviços financeiros esteja atualmente favorecendo a implementação de redes autorizadas. Devido a considerações de combate à lavagem de dinheiro ("AML"), conhecimento do cliente ("KYC") e privacidade (discutidas mais detalhadamente abaixo), as redes públicas não são realmente viáveis em serviços financeiros no momento. Um minerador de Bitcoin anônimo em uma rede pública deve estar sujeito aos requisitos da Lei de Sigilo Bancário e ao programa KYC de uma instituição financeira, como se estivesse envolvido em uma função semelhante no setor de serviços financeiros para um banco Assim, é compreensível que, dadas as estruturas atuais, os sistemas de um banco não possam ser integrados às redes públicas, mas à medida que a tecnologia se desenvolve, isso também pode mudar."

[21] *Promoting innovation through education.* Tradução livre: "Embora seja comum dizer que as criptomoedas e a tecnologia blockchain não são regulamentadas, nada poderia estar mais longe da verdade. Inúmeras agências federais e estaduais nos Estados Unidos, bem como agências em outros países, regulam os aplicativos para essa tecnologia de alguma maneira. Mas as abordagens díspares adotadas por diferentes países, ou mesmo por diferentes agências nos EUA, levaram a confusão por parte das empresas da blockchain sobre as jurisdições e regimes regulatórios aos quais seus produtos e serviços estarão sujeitos."

[22] Em tradução livre: "Embora seja comum dizer que as criptomoedas e a tecnologia blockchain não são regulamentadas, nada poderia estar mais longe da verdade. Várias agências federais e estaduais nos Estados Unidos, bem como agências em outros países, regulam os aplicativos para essa tecnologia de alguma maneira. Mas as

A *blockchain* somente funciona com fundamento na confiança (é um "ato de fé"), e baseado no pressuposto de que todos os agentes (privados) garantem-se reciprocamente, mas, como já foi dito, em se tratando de cybersegurança, a produção de incentivos privados não é eficiente. A questão, então, passa a ser, fora de um gerenciamento central, como gerar incentivos públicos (ou "sociais") na atividade. A concepção do "protocolo da confiança" é de que ele se sustenta na própria rede, mas, em se tratando de um "bem público", a conclusão invencível é de que não há sustentabilidade econômica ao sistema, dessa forma.

O tema está diretamente relacionado com a governança da Internet (a expressão *"Internet Governance"* é utilizada para designar os processos e mecanismos que permitem o funcionamento da rede): como a Internet é uma rede de comunicação e troca de dados que foi desenhada para funcionar sem um "centro" de controle, seu gerenciamento é complexo e compartilhado por várias entidades. Nenhuma pessoa, companhia, organização ou governo, individualmente, faz funcionar a Internet.

Uma vez que a "governança" da Internet é feita mediante várias entidades, conforme áreas específicas, e resulta da adesão voluntária destas redes autônomas e de seus usuários, a sustentabilidade da *blockchain* fica na dependência de algum arranjo institucional que crie os incentivos adequados para investimentos em sua segurança.

Já existem substanciais esforços nesse sentido, como foi exemplificado ao longo deste trabalho, mas ainda há um bom percurso a percorrer para que se possa falar e viabilidade da blockchain como um sistema eficiente de registro de transações online.

---

abordagens díspares adotadas por diferentes países, ou mesmo por diferentes agências nos EUA, levaram à confusão das empresas de blockchain sobre as jurisdições e os regimes regulatórios aos quais seus produtos e serviços estarão sujeitos."

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Fernando. *Introdução à Economia, 3ª ed.* Coimbra: Almedina, 2012.

EICHENSEHR, Kristen E. *Public-Private Cybersecurity.* Texas Law Review, vol 467. Austin: University of Texas School of Law, 2017.

GLOBAL LEGAL INSIGHTS. *Blockchain & Cryptocurrency Regulation 2019*. London: Global Legal Group, 2019.

KELLY, Brian B. *Investing in a Centralized Cybersecurity Infrastructure: Why Hacktivism Can and Should Influence Cybersecurity Reform*. Boston University Law Review, vol 92. Boston: Boston University Press, 2012.

KOBAYASHI, Bruce H. *Private versus Social Incentives in Cybersecurity: Law and Economics,* **in** "The law and economics of Cybersecurity", edited by Mark F. GRADY e Francesco PARISI. New York: Cambridge University Press, 2006.

KOSSEF, Jeff. *Defining Cybersecurity Law.* Iowa Law Review, vol. 103, issue 3 (2018). Iowa City: University of Iowa Press, 2018.

MALIK, Nikhil; ASERI, Manmohan; SINGH, Param Vir; SRINIVASAN, Kannan. *Why Bitcoin Will Fail to Scale?* (January 26, 2019). Disponível em SSRN: https://ssrn.com/abstract=3323529 ou http://dx.doi.org/10.2139/ssrn.3323529

MARSH, Bridget; DEWEY, Josias. Dewey. The loan market, blockchain, and smart contracts: The potential for transformative change, **in** IOSCO (International Organization of Securities Comission). *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading*

Platforms. CR 02/2019, in www.iosco.org, acessado em 11/01/2020.

LITWAK, Eugene; SZLENYI, Ivan. *Primary Group Structures and Their Functions: Kin, Neighbors, and Friends.* American Sociological Review, Vol. 34, nº 4 (Aug. 1969), pp. 465-481, published by American Sociological Association, **in** www.jstor.org/stable/2091957, acessado em 09/01/2020.

OECD Blockchain Primer, **in** www.oecd.org/finance, acessado em 09/01/2020.

SALES, Nathan Alexander.

Regulating Cyber-Security. Northwestern University Law Review, vol. 107, nº 4. Chicago: Northwestern University Pritzker School of Law, 2013.

Privatizing Cyber-Security. UCLA Law Review, vol. 620. Los Angeles: UCLA School of Law, 2018.

SHILLER, Robert. *Narrative Economics: How Stories Go Viral and Drive Major Economic Events.* Princeton: Princeton University Press, 2019.

WEINSTEIN, Jason; COHN, Alan Cohn; PARKER, Chelsea. *Promoting innovation through education: The blockchain industry, law enforcement and regulators work towards a common goal* **in** *IOSCO (International Organization of Securities Comission). Issues, Risks and Regula-tory Considerations Relating to Crypto-Asset Trading Platforms. CR 02/2019, in www.iosco.org, acessado em 11/01/2020.*