

## Isac Costa: Criptoativos e direito de propriedade

*\*o texto é baseado em palestra conduzida em 21.jun.2022 por mim, em painel com o doutor Eduardo Salomão Neto e a doutora Juliana Sato, da 110ª Reunião de Debates do IBR (Instituto Brasileiro de Empresas), presidido pelo professor Paulo Fernando Campos Salles de oportunidade de ter participado deste debate tão qualificado.*



Isac Costa  
professor e advogado

### Estado, mercado e direito de propriedade

Estado e mercado não são adversários na economia, pois o Direito dá forma ao mercado, como diz NATALINO IRTI, e o contrato é a "veste jurídica de uma operação econômica", como ensina ENZO ROPPO. A segurança jurídica é necessária para estabilizar as expectativas dos agentes econômicos e o direito de propriedade é elemento essencial do sistema capitalista.

A concreção da propriedade depende de tecnologias de escrituração, isto é, do devido mapeamento entre *sujeitos de direito e objetos de direito*. Ainda, precisamos registrar a dinâmica dos fatos jurídicos, das transações que resultam do exercício da atividade econômica.

Tradicionalmente, recorremos a entes centralizados estatais ou privados para assegurar o sigilo, a integridade e a autenticidade dos dados relativos a direitos de propriedade.

O desenvolvimento de algoritmos criptográficos fortaleceu os sistemas mantidos por esses entes centrais. *A criptografia é um conjunto de métodos matemáticos para viabilizar a comunicação na presença de um adversário*: não queremos que o teor da mensagem seja conhecido (confidencialidade), que esta seja adulterada (integridade), nem que um terceiro se faça passar por uma das partes (autenticidade). Por isso, a criptografia é importante para sistemas que gerenciam a propriedade de bens.

Tomamos como naturais todos os registros de pessoas, imóveis, notas e títulos, juntamente com os prestadores de serviços de escrituração, custódia, depositária central, centrais registradoras e infraestruturas de mercado financeiro. Achamos natural que o Banco Central *seja central*.



## Descentralização e interoperabilidade

Com a criação do *bitcoin*, surgiu uma arquitetura de sistemas fundada no armazenamento compartilhado de dados e no processamento de transações em rede, com a colaboração de seus participantes.

Como alternativa a sistemas centralizados relativamente isolados, nos sistemas *descentralizados* o registro completo das informações é compartilhado e alterado em sincronia por todos os participantes à medida que as transações ocorrem. Segundo um metronomo digital, todos mantêm uma cópia idêntica de um "livro razão" ao longo do tempo — os algoritmos criptográficos eliminam incentivos para que as cópias sejam adulteradas.

O contraste entre sistemas centralizados e descentralizados é semelhante ao dilema entre *firma* (hierarquia) e *mercado*, identificado por RONALD COASE, ao investigar quando um agente econômico decide internalizar uma atividade e quando opta por realizá-la mediante um contrato em mercado.

As *firmas* de COASE são como os sistemas centralizados, que mantêm internamente os dados necessários para o seu funcionamento. Quando novos dados são necessários, podem buscá-los externamente (em uma chamada pontual de programa, como no caso do *open banking*) ou, então, negociar o compartilhamento antecipado e sincronizado dos dados, a fim de tornar a comunicação mais eficiente.

A decisão entre internalizar ou não decorre da avaliação dos custos de transação. Por exemplo, o custo (político, econômico e social) de um sistema de pagamentos global impede a unificação dos sistemas de pagamentos dos Estados, levando a um mercado de câmbio com burocracias, taxas e ineficiências, dificultando o fluxo internacional de capitais.

O problema das transferências internacionais de recursos foi justamente um dos motivos determinantes da criação do *bitcoin* — seria possível ter uma moeda comum global para transações eletrônicas, independente de uma empresa ou de um Estado? Extrapolando esse raciocínio, por que não temos hoje um "cartório" global? Por que é difícil inventariar os bens de uma empresa quando estão geograficamente dispersos? Por que é difícil garantir operações com bens situações no estrangeiro? Por que uma oferta pública de ações é circunscrita a um único país? Por que precisamos de mecanismos como *depository receipts* para negociar ações de uma companhia em múltiplos países?

## Blockchain e o futuro do direito de propriedade

A arquitetura *blockchain*, que dá suporte ao funcionamento do *bitcoin*, pode ajudar a resolver esses problemas. Essa tecnologia foi expandida para outras aplicações com o surgimento da rede Ethereum em 2015.

Podemos afirmar que o *bitcoin* está para uma calculadora (capaz de fazer as quatro operações aritméticas) como o Ethereum está para um *smartphone* (com um sistema operacional que nos permite programar aplicativos diversos, inclusive uma calculadora, mas não só).

De modo simplificado, a representação de valor em uma rede *blockchain* é um título digital (*token*), sendo possível escrever programas para automatizar transações com esses *tokens*.



Imagine um contrato de distribuição de livros, envolvendo uma editora, distribuidoras, livrarias e autores. Com uma solução *blockchain*, todo o fluxo de vendas, pagamentos e conciliações pode ser realizado dentro de uma “carteira digital” com os valores denominados em uma (cripto)moeda específica. Quando um consumidor paga por um livro, o valor é automaticamente repartido entre todos os envolvidos, conforme regras previamente estabelecidas.

*\*Na segunda parte do texto, que será publicada nesta terça-feira (28/6), veremos como os tokens se tornaram verdadeiros ativos, a partir da automatização de transações por meio de smart contracts, gerando um mercado especulativo que chamou a atenção dos reguladores e, de certa forma, ofusca alguns benefícios mais permanentes da tecnologia blockchain.*

Continua [parte 2](#).