



| TECNOLOGIA • EMERGE UMA NOVA TECNOLOGIA DISRUPTIVA



EMERGE UMA NOVA TECNOLOGIA DISRUPTIVA

| POR EDUARDO HENRIQUE DINIZ

Ao operar como um livro de registros de transações on-line, o *blockchain* tem o potencial de revolucionar não apenas as finanças, mas toda a troca de informações em comunidades de negócios e grupos sociais.

Em outubro de 2008, a crise financeira mundial atingiu seu auge, com diversos governos tidos como liberais e não intervencionistas atuando para salvar as empresas do setor. Foi quando apareceu publicado em um grupo de discussão sobre criptografia o artigo *Bitcoin: a peer-to-peer electronic cash system*, assinado por um obscuro (e até hoje sem identificação confirmada) Satoshi Nakamoto. Esse artigo propunha “uma versão de dinheiro eletrônico que permite pagamentos on-line enviados diretamente de pessoa a pessoa sem passar por uma instituição financeira”. Em sua essência, demonstrava a viabilidade de um sistema de criptografia que garantiria a autenticidade de pagamentos eletrônicos com o uso de uma moeda específica, o *bitcoin*, para quem se dispusesse a participar de um

sistema em rede computacional descentralizada, desenhada especificamente para esse tipo de transação.

Claramente contra o sistema financeiro que estava em convulsão, o artigo propunha um sistema de pagamento baseado em tecnologia de criptografia. Lançada em janeiro de 2009, a nova criptomoeda, *bitcoin*, só foi chamar atenção em abril de 2011, quando a revista *Forbes* publicou uma matéria sobre o tema. Enquanto o interesse pela moeda se acelerava, mais notícias eram produzidas sobre ela, e uma corrida aos *bitcoins* passou a ser percebida.

Depois de atingir um pico de valorização, em junho de 2011, apareceram as primeiras notícias de fraude no mundo *bitcoin*, derrubando seu valor. Essa primeira “crise” do *bitcoin* gerou dois efeitos importantes. O primeiro foi a mobilização da comunidade que apoiava o desenvolvimento

Pelo *blockchain*, a rede inteira mantém o registro atualizado das transações efetivadas em seus domínios, auditável para todos os que dela participam.

da nascente criptomoeda. Nos anos seguintes, a percepção de confiabilidade no sistema de criptografia do *bitcoin* ampliou-se e o *bitcoin* apresentou um ritmo de crescimento e valorização relativamente estável, ganhando milhões de usuários pelo mundo. Depois de 2011, as fraudes registradas concentraram-se no processo de conversão de *bitcoins* em moedas nacionais (dólar, euro, iene, etc.), e não mais no sistema de criptografia.

O segundo efeito foi ainda mais importante. Dentro da própria comunidade de criptografia, várias críticas ao desenho do *bitcoin* já vinham se tornando comuns nas listas de discussão. Ao trabalhar na recuperação do mecanismo que suporta o funcionamento da moeda, as atenções passaram a se voltar mais para esse mecanismo do que para a criptomoeda que havia sido criada. Foi a partir daí que o *blockchain*, o tal mecanismo criptográfico, começou a chamar mais atenção do que o próprio *bitcoin*.

MECANISMO ANTIFRAUDE

Curiosamente, o artigo original de Nakamoto nem mesmo cita a palavra *blockchain*. Ao descrever o funcionamento da ferramenta criptográfica, o artigo menciona a expressão *timestamp* para descrever o elemento central daquela criptomoeda e adota nomenclatura alinhada com os termos já utilizados pela comunidade de criptografia.

Para entender o que isso significa, é preciso uma explicação rápida sobre a elegante solução proposta por Nakamoto para o problema conhecido como *double-spending*, ou seja, a possibilidade de utilizar uma mesma unidade de pagamento em transações diferentes. Uma transação de pagamento é uma informação única e só tem valor se puder garantir que não será utilizada mais de uma vez. É como imaginar que uma nota de R\$ 10 é sempre uma unidade de informação que não pode ser reproduzida. Assim, quando ela passa de quem está pagando para quem está recebendo, o primeiro

reduz o seu estoque de dinheiro enquanto o segundo aumenta o seu na mesma proporção. Caso essa regra seja quebrada, é como se o pagador tivesse o poder de imprimir dinheiro, pois estaria usando a mesma capacidade de pagamento para realizar mais do que uma transação, ou cometendo *double-spending*.

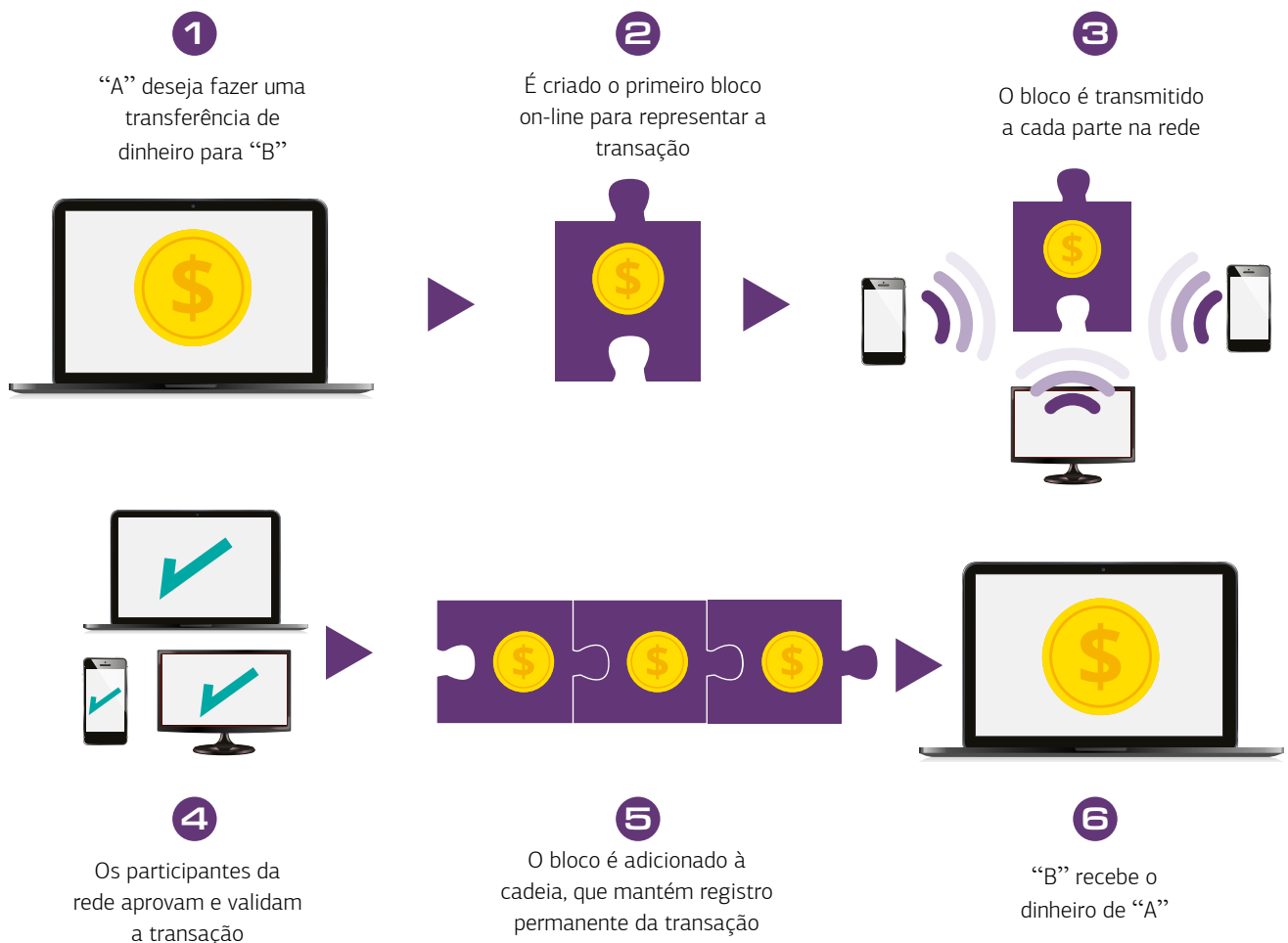
Esse sempre foi o problema fundamental associado à utilização de pagamentos digitais, e é por isso que se confia em uma autoridade central, um banco ou uma empresa que opera os cartões de pagamento, para garantir a veracidade e a unicidade daquela transação entre duas partes. No jargão do sistema financeiro, essa autoridade central garante o *trust* para a realização da transação.

Nakamoto propôs uma solução baseada em um servidor que carimba todos os dados da transação com informações sobre a data e a hora de sua realização (*timestamp*). A cada nova transação, informações das transações anteriores ficam armazenadas, gerando um bloco de transações que leva um novo carimbo, que passa a ser o registro não apenas da última transação, mas inclui também todas as que foram realizadas anteriormente. A cada nova transação, portanto, o sistema vai carimbando a cadeia de blocos, que torna cada transação sempre associada a todas as que a precederam. Essa cadeia de blocos (*blockchain*) cresce e vai documentando todas as transações feitas dentro daquela rede de pagamentos.

Como o sistema funciona em uma rede de computadores, cada nó da rede contém uma cópia fiel dos registros que documentam todas as transações que acontecem na rede. Assim, para ser considerada válida, uma nova transação tem de ser atualizada em todos os nós da rede, e em cada um deles se confere todos os registros passados que estão lá armazenados. Dessa forma, a rede inteira mantém o registro atualizado das transações efetivadas em seus domínios, auditável para todos os que dela participam.

A primeira consequência da desvinculação do *blockchain* do *bitcoin* foi a emergência de novas criptomoedas, com desenhos significativamente diferentes da criptomoeda original. Desde 2012, o número de novos meios de pagamento não para de crescer. A página coinmarketcap.com mantém o registro do valor de mercado de mais de 700 criptomoedas, algumas já almejando rivalizar com o *bitcoin* em um futuro próximo. O movimento internacional de moedas comunitárias, que defende os sistemas de moedas alternativos (ou complementares) como instrumento de intervenção social, também está gradativamente aderindo à arquitetura do *blockchain*. Cada vez mais projetos dessas “moedas sociais” podem ser vistos nas listas publicadas

COMO FUNCIONA O *BLOCKCHAIN*



FONTE: @PDFORREST

pelo grupo Community Currencies in Action (communitycurrenciesinaction.eu) e pelo Research Association on Monetary Innovation and Community and Complementary Currency Systems (ramics.org).

Como não poderia deixar de ser, o *blockchain* também passou a interessar a comunidade financeira internacional, mas por motivos bem diferentes daqueles propostos inicialmente pelos criadores dessa tecnologia. Sem nenhuma intenção de “revolucionar” o sistema do qual fazem parte, as atuais empresas do setor financeiro veem o *blockchain* como uma maneira eficiente de cortar custos e aumentar a segurança em suas operações, automatizando várias camadas de autorização.

DIVERSIDADE DE APLICAÇÕES

Muito além dos sistemas de pagamento, o *blockchain* funciona como um livro de registros (*ledger*, no jargão da comunidade financeira). E o número de atividades comerciais e sociais que dependem de algum tipo de mecanismo centralizado para validação de registros é imensurável. De cartórios a sistemas de registros de transações comerciais, todas essas atividades estão sendo ameaçadas pelo potencial disruptivo do *blockchain*. Já denominado de Blockchain 2.0, essas aplicações fora daquelas de pagamento (identificadas como Blockchain 1.0) tendem a expandir ainda mais a utilização dessa tecnologia.

Alguns exemplos permitem visualizar a diversidade de aplicações dessa tecnologia emergente e demonstram como ela pode

se tornar padrão no estabelecimento de troca de informações em comunidades de negócio ou em grupos sociais:

- O Porto de Rotterdam, o maior da Europa, criou um consórcio em parceria com bancos, universidades e outras organizações para rever as aplicações de compartilhamento de informações contratuais ao longo da cadeia logística (porttechnology.org/news/port_of_rotterdam_blockchain_project);
- Empresas da cadeia de comercialização de energia estão estudando como usar o *blockchain* para melhorar os requisitos de comunicação, transparência e divulgação de dados entre os parceiros de negócio do setor (www2.deloitte.com/uk/en/pages/energy-and-resources/articles/blockchain-applications-in-energy-trading.html);
- Cidades holandesas trabalham com a criação de aplicativos desenvolvidos em *blockchain* para gerenciar a cadeia de contratos imobiliários. Além de poder monitorá-los de forma mais eficiente e barata, essa iniciativa permitirá melhor análise de decisões de investimentos futuros na venda, compra e construção de imóveis (thebitcointrend.com/city-of-rotterdam-to-use-a-blockchain-for-lease-agreements);
- O serviço postal dos Estados Unidos tem um grupo de trabalho em *blockchain* desenvolvendo um mecanismo seguro para monitorar suas entregas e criar novas aplicações financeiras, visando comunidades de baixa renda, inclusive com a criação de uma moeda, o *postcoin* (usps.org/document/blockchain-technology-possibilities-us-postal-service);
- O Departamento de Comércio dos Estados Unidos está promovendo discussões sobre como utilizar o *blockchain* para promover o diálogo entre diversos setores da indústria e fortalecer o mercado de comércio on-line (goo.gl/7qfsKu);
- Apostando na possibilidade de o *blockchain* permitir uma relação mais direta entre autores e consumidores na indústria da música, alguns grupos de artistas e advogados de direito autoral preveem maior controle sobre o conteúdo digital sendo baixado, utilizado ou modificado, de forma a garantir o pagamento justo para o uso desse conteúdo, sem a necessidade de uma gravadora ou agência de direitos autorais intermediarem esse controle (goo.gl/p2NYTJ);
- Um grupo de ativistas argentinos está promovendo o uso do *blockchain* para conectar eleitores com seus candidatos, por meio de um mecanismo em que os primeiros possam opinar diretamente em todas as votações legislativas de seus representantes (fastcoexist.com/3062386/democracy-is-getting-a-reboot-on-the-blockchain);

De cartórios a sistemas de registros de transações comerciais, muitas atividades estão sendo ameaçadas pelo potencial disruptivo do *blockchain*.

- Financiados pela União Europeia, um grupo chamado Decentralized Citizens Engagement Technologies (D-CENT) desenvolve projetos com organizações lideradas por cidadãos com o objetivo de criar alternativas de democracia participativa a partir de código aberto, usando *blockchain* como base e atuando em áreas que vão desde a criação de inteligência coletiva ao desenvolvimento de moedas comunitárias (d-centproject.eu).

Estamos no início da era do *blockchain*. A maioria das aplicações descritas aqui está em fase experimental, e não há ainda como saber o que vai se consolidar como solução efetiva. A consultoria em tecnologia Gartner argumenta, por exemplo, que muitos projetos envolvendo *blockchain* não necessitariam dessa tecnologia para produzir valor e é provável que tenham problemas de escalabilidade e flexibilidade.

Entretanto, dado o envolvimento de pessoas e empresas de vários segmentos e o leque de possibilidades, não há como não considerar que essa tecnologia tem elementos para provocar o maior impacto na sociedade e no mundo dos negócios desde o aparecimento da *World Wide Web* no início dos anos 1990. Assim sendo, estamos assistindo à emergência de uma nova tecnologia disruptiva que, como a *web*, transformou o mundo de modo irreversível. ●

PARA SABER MAIS:

- Brett Scott. *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?* UNRISD Working Paper, n. 1, 2016. Disponível em: goo.gl/vm15SK
- MARK WALPORT. *Distributed ledger technology: beyond blockchain*. UK Government Office for Science, 2016.
- Satoshi Nakamoto. *Bitcoin: a peer-to-peer electronic cash system*. 2008. Disponível em: bitcoin.org/bitcoin.pdf

EDUARDO HENRIQUE DINIZ > Professor da FGV EAESP > eduardo.diniz@fgv.br