BLOCKCHAIN PARA OS NEGÓCIOS

Promessa, Prática e Aplicação da Nova Tecnologia da Internet

WILLIAM MOUGAYAR

PREFÁCIO POR VITALIK BUTERIN

ALTA BOOKS
EDITORA
Rio de Janeiro, 2017

SUMÁRIO

PREFÁCIO

ESTA DÉCADA É UM MOMENTO INTERESSANTE para o desenvolvimento de tecnologias descentralizadas. Embora criptógrafos, matemáticos e programadores tenham trabalhado em protocolos cada vez mais específicos e avançados para conseguir privacidade e autenticidade mais fortes e garantias fora de vários sistemas — de dinheiro eletrônico a votos e transferência de arquivos —, o progresso foi lento por mais de 30 anos. A inovação do blockchain — ou, mais genericamente, a inovação do consenso econômico público de Satoshi Nakamoto, em 2009 — provou ser a peça faltante do quebra-cabeça que, sozinha, permitiu à indústria dar seu próximo e gigantesco passo adiante.

A atmosfera política pareceu se encaixar: a grande crise financeira de 2008 estimulou uma desconfiança crescente na economia, o que incluiu tanto as corporações quanto os governos, que normalmente deveriam regulá-las, e foi o pontapé que levou muitas pessoas a procurarem alternativas. Logo em seguida, as revelações de Edward Snowden, em 2013, que destacou quão ativo o governo era em esferas nas quais os cidadãos acreditavam ter privacidade, foram a cereja do bolo. Apesar de as tecnologias de blockchain não terem sido adotadas de maneira ampla como resultado, o espírito de descentralização que as embasa em grande parte o foi.

Aplicações que vão de celulares da Apple ao WhatsApp começaram a desenvolver criptografias tão fortes que mesmo as empresas que escrevem o software e lidam com os servidores não con-

seguem quebrá-las. Para aqueles que acham que as corporações, e não o governo, são o fantasma, o advento do "consumo compartilhado 1.0" está mostrando sinais de fracasso no cumprimento do que muitos pensaram ser sua promessa. Em vez de simplesmente cortar intermediários arraigados e oligopolistas, gigantes como o Uber estão substituindo os intermediários por eles mesmos, e nem sempre conseguem entregar um resultado melhor.

Blockchains, e todas as tecnologias relacionadas que eu chamo de "crypto 2.0", fornecem uma solução atrativa. Em vez de esperar que as partes com as quais interagimos ajam honrosamente, estamos criando sistemas tecnológicos que inerentemente incluem as propriedades desejadas no sistema, de maneira que elas continuarão funcionando com as garantias que esperamos, mesmo que muitos dos atores envolvidos sejam corruptos.

Todas as transações que ocorrem por meio do "crypto 2.0" vêm com rastros auditáveis de provas criptográficas. As redes descentralizadas peer-to-peer podem ser utilizadas para reduzir a confiança em qualquer servidor individualmente; a chave criptográfica pública poderia criar uma noção de identidades portáteis controladas pelo usuário. Tipos mais avançados de matemática, incluindo assinaturas em anel, criptografias homomórficas e provas de conhecimento-zero, garantem privacidade, permitindo que usuários abram seus dados de modo que algumas propriedades possam ser verificadas, e até mesmo computadas, sem realmente revelar nenhum detalhe privado.

No entanto, o mais surpreendente para os que recém-adotaram essa tecnologia é o quão rápido a adoção institucional se espalhou nos últimos dois anos. De 2011 a 2013, o cenário blockchain — ou, realisticamente, o que era chamado de cenário "Bitcoin" — era, em essência, criptoanarquista, com revolucionários idealistas animados com a ideia de "lutar contra o poder" (ou, mais precisamente, dispersar o poder). Hoje, em 2016, todos os anúncios mais interessantes têm a ver com o anúncio de alguma colaboração com a IBM ou a

Microsoft, uma pesquisa feita pelo Bank of England, ou um consórcio bancário anunciando outra rodada com novos membros.

O que aconteceu? Em parte, eu concordaria que os criptoanarquistas subestimaram o quão flexíveis, tecnológicas, progressivas, e até mesmo idealistas as grandes corporações e os bancos podem ser. Nós geralmente esquecemos que as corporações são feitas de pessoas, que geralmente têm valores e preocupações parecidas com os de pessoas comuns. Parece que "a máquina da confiança", como o jornal *The Economist* a chama, é puramente uma substituta para as âncoras centralizadas de confiança, tanto nas finanças quanto em quaisquer outros setores, que creem na reputação do mundo real e na fiscalização regulatória, mas a realidade é muito mais complexa. Na verdade, as instituições não confiam completamente umas nas outras, e instituições centralizadas em uma indústria estão tão preocupadas com a centralização em outras indústrias quanto as pessoas comuns. As companhias de energia, que estão envolvidas na produção e venda da eletricidade, estão tão felizes vendendo para um mercado descentralizado quanto para um centralizado, e elas podem até preferir a versão descentralizada se houver um corte menor.

Além disso, muitas empresas já estão descentralizadas (em uma extensão que muitas pessoas de fora dessas indústrias não valorizam), mas de um modo ineficiente — uma maneira que requer que cada companhia mantenha sua própria infraestrutura no que concerne ao gerenciamento de usuários, transações e datas, e no que se refere a realizar conciliações com os sistemas de outras empresas sempre que precisam interagir. A consolidação ao redor de um líder de mercado, na verdade, faria com que essas empresas fossem mais eficientes. Mas nem os competidores deste líder em potencial nem os reguladores da antitruste querem aceitar esse resultado, o que leva a um beco sem saída. Até agora. Com o advento de bases de dados descentralizadas que podem tecnologicamente replicar os ganhos do efeito da rede de conexões de um único monopólio, todos conseguem se unir e se alinhar a seu favor, sem criar esta centralização, com todas as consequências negativas que vêm com ela.

Essa é a história que conduz o interesse de cadeias de consórcios em finanças, aplicações blockchain na indústria da cadeia de suprimentos e sistemas de identidade baseados em blockchain. Eles utilizam bases de dados descentralizadas para replicar os ganhos resultantes do fato de todos estarem em apenas uma plataforma, sem os custos de ter que chegar a um acordo sobre quem controlará a plataforma e então ter que lidar com essa pessoa se ela abusar da posição de monopólio.

Nos primeiros quatro anos após Satoshi lançar o Bitcoin, em janeiro de 2009, houve muita atenção focada na moeda, incluindo seus aspectos de pagamento e seu funcionamento como uma forma alternativa de se estocar valor. Em 2013, a atenção começou a se voltar para aplicações "blockchain 2.0": o uso da mesma tecnologia em que se baseia a segurança e na descentralização do Bitcoin em outras aplicações, indo do domínio do registro de nome, contratos financeiros, financiamento colaborativo e até mesmo a jogos. A visão central por trás da minha própria plataforma, a Ethereum, era a de que uma linguagem de programação Turing completa, embutida no protocolo da camada de base, poderia ser utilizada como a abstração definitiva, permitindo que desenvolvedores criassem aplicações com qualquer tipo de lógica ou propósito de negócios, enquanto teriam os benefícios das propriedades centrais do blockchain. Mais ou menos na mesma época, sistemas tais como os da plataforma de armazenamento descentralizado InterPlanetary File System (IPFS) começaram a surgir, e criptógrafos desenvolveram novas ferramentas poderosas que poderiam ser utilizadas em combinação com a tecnologia blockchain para adicionar privacidade, em particular zk-SNARKs, ou Zero-knowledge Succinct Non-interactive ARgument Knowledge. A combinação da computação blockchain Turing completa, as redes não blockchain descentralizadas que utilizavam tecnologias de criptografia similares e a integração de blockchains com criptografia avançada foram o que escolhi chamar de "crypto 2.0" — um nome que pode ser ambíguo, mas que sinto que captura melhor o espírito do movimento em sua forma mais ampla.

O que é crypto 3.0? Em parte, a continuação de algumas das tendências da crypto 2.0, e especialmente protocolos generalizados que forneçam tanto a abstração computacional quanto a privacidade. Mas tão importante quanto ela é a principal questão tecnológica sobre o blockchain colocada à mesa: a escalabilidade. Atualmente, todos os protocolos blockchain existentes têm a propriedade de que todo computador na rede deve processar toda transação — uma propriedade que fornece altos níveis de tolerância a falhas e segurança, mas a custo de garantir que o poder de processamento da rede seja limitado pelo poder de processamento de um único nó.

A crypto 3.0 — pelo menos para mim — consiste de abordagens que vão além dessa limitação, em uma das formas de criar sistemas que ultrapassam a limitação e realmente alcançam a escala necessária para dar apoio à adoção geral (tecnicamente, leitores astutos podem ter ouvido falar em "redes relâmpago", "canais estatais" e "particionamento horizontal").

Então também há a questão da adoção. Além do simples caso do uso da moeda, em 2015, a "crypto 2.0" viu muita gente falando sobre isso, desenvolvedores lançando plataformas de base, mas ainda não havia nenhuma aplicação relevante. Em 2016, estamos vendo tanto startups quanto atores institucionais desenvolverem provas de conceitos. É claro, a grande maioria nunca chegará a lugar algum, e aos poucos irão murchando e morrerão. Isso é inevitável em qualquer campo. No empreendedorismo é fato que 90% de todos os novos negócios fracassam. Mas os 10% que obtêm sucesso provavelmente chegarão ao ponto em que seus produtos alcançarão milhões de pessoas — e é aí que a diversão começa.

Talvez o livro do William te inspire a entender e, talvez, se unir ao aperfeiçoamento do ramo do blockchain.

Vitalik Buterin

Inventor da Ethereum e cientista-chefe,
Fundação Ethereum

2 de abril de 2016

PREFÁCIO DA EDIÇÃO BRASILEIRA

Talvez poucos assuntos tenham movimentado tanto a comunidade financeira como a discussão sobre as possibilidades de revolução do blockchain no mundo.

Durante os últimos anos, protocolos foram criados para diferentes tipos de necessidades, como o SMTP para a troca de emails, o FTP para a troca de arquivos, o HTTP para acesso a conteúdos, entre outros. Faltava resolver os problemas para a troca de valores. O blockchain inicialmente nasce com esta proposta, suportando um dos maiores eventos econômicos da história moderna, o lançamento do Bitcoin — uma moeda virtual, de gestão descentralizada, sem controle de um Banco Central e sem fronteiras geográficas.

Apesar de ser um tema recente, as pesquisas estão avançando em uma grande velocidade. Não apenas o blockchain tem sido foco desses trabalhos, mas também outros modelos de Distributed Ledger Technology (DLTs), tem sido avaliados como solução para diferentes tipos de problemas.

Como exemplo disso, em 2015, foi formado o Consórcio R3 (R3CEV), que hoje possui mais de 70 associados, tais como Barclays, JP Morgan, BBVA, Citi, entre outros, com o objetivo de pesquisar as aplicações práticas de redes descentralizadas no sistema financeiro. Alguns dos principais bancos brasileiros já fazem parte deste grupo.

Apesar de ainda haverem poucos casos práticos de sucesso implementados, não existe dúvida de que a tecnologia é revolucionária, sendo que bilhões de dólares vêm sendo investidos em pesquisas em todo o mundo.

Algumas barreiras precisam ser transpostas, como a capacidade de processamento de grandes volumes de informação, o tempo necessário para que as transações sejam registradas na rede, permissionamento e anonimato, integração de diferentes partes envolvidas em um mesmo novo modelo operacional, entre outros. Mas é questão de tempo. Quem estiver à frente deste movimento certamente terá vantagem em relação aos céticos, antigos defensores das máquinas de escrever.

E, apesar da origem do blockchain ser a de troca financeira, as oportunidades vão muito além. O surgimento dos *smart contracts* abre um novo mundo de possibilidades para o desenvolvimento de aplicações revolucionárias em diferentes mercados. Em lugares onde existe a necessidade de imutabilidade de informações, transparência entre partes, trocas de valores e de ativos entre pessoas e coisas, haverá uma possibilidade de revolução potencializada pelo blockchain.

É um orgulho apoiar a inserção de uma obra tão importante quanto esta no cenário brasileiro. William Mougayar nos ajuda a navegar nos mares das oportunidades, nos convidando a pensar em modelos de negócio que vão além da substituição das tecnologias existentes. Assim como a internet trouxe oportunidades muito além do que o simples ato de trazer folders das empresas para a rede, o blockchain e suas variações têm o potencial de tornar real o que era inimaginável há alguns meses.

Gostaria também de fazer um especial agradecimento ao Edilson Osório, talvez a maior referência sobre o tema no Brasil, que apoiou sempre de maneira tão generosa nossos chamados. O OriginalMy, sua plataforma para registro de propriedade de documentos digitais, prova como problemas tão presentes no nosso dia a dia, podem ser solucionados de forma tão criativa com o uso do blockchain.

Aos leitores, se acomodem em um lugar calmo e confortável... e se entreguem às possibilidades que estão à nossa frente. Boa leitura!

Marcelo Bradaschia

CoFundador da FintechLab

Novembro 2016

INTRODUÇÃO

SE O BLOCKCHAIN ainda não te chocou, garanto que o fará em breve.

Eu não vejo nada parecido desde o início da internet em termos de capturar a imaginação das pessoas, inicialmente um número pequeno, e então se espalhar rapidamente.

Bem-vindo ao novo mundo de blockchain e blockchains.

Em sua essência, o blockchain é uma tecnologia que grava transações permanentemente de uma maneira que não podem ser apagadas depois, somente podem ser atualizadas sequencialmente, mantendo um rastro de histórico sem fim. Essa descrição aparentemente simples de seu funcionamento tem implicações gigantescas. Está fazendo com que repensemos as maneiras antigas de criar transações, armazenar dados e mover ativos, e é apenas o começo.

O blockchain não pode ser descrito apenas como uma revolução. É um fenômeno em curso, avançando lentamente como um tsunami, gradualmente envolvendo tudo em seu caminho pela força de sua progressão. Basicamente, é a segunda sobreposição significativa à internet, assim como a web foi a primeira camada nos anos 1990. Esta nova camada se relaciona muito com confiança, então poderíamos chamá-la de *camada de confiança*.

Blockchains são enormes catalisadores para mudança que atingem governança, modos de vida, modelos corporativos tradicio-

nais, sociedade e instituições globais. A infiltração do blockchain encontrará resistência, pois é uma mudança extrema.

Ele desafia velhas ideias que estão em nossa mente há décadas, se não há séculos. Os blockchains desafiarão a governança e as maneiras centralizadas e controladas de realizar transações. Por exemplo: por que pagar por uma garantia para liberar um seguro se o blockchain pode verificar isso de uma maneira irrefutável?

Blockchains liberam a confiança, que está nas mãos de instituições centrais (tais como bancos, legisladores, financiadores, governos, grandes corporações), e permitem que ela se esvaia desses velhos pontos de controle. Por exemplo: e se a validação da contraparte pudesse ser feita no blockchain, em vez de por uma câmara de liquidação?

Uma analogia seria quando, no século XVI, associações medievais ajudaram a manter o monopólio de alguns trabalhadores sobre forasteiros ao controlar a impressão do conhecimento que explicaria como copiar o trabalho deles. Eles conseguiram esse tipo de censura ao conspirarem com a Igreja Católica e com governos da maioria dos países da Europa, que regulavam e controlavam a impressão com o requerimento de licenças. Esse tipo de controle centralizado e monopólio não durou muito, e logo o conhecimento estava livre após uma explosão na impressão. A impressão do conhecimento como uma atividade ilegal seria impensável nos dias de hoje. Poderíamos pensar nos tradicionais detentores da confiança como as associações medievais de hoje, e poderíamos questionar o porquê de eles continuarem a manter a confiança se a tecnologia (os blockchains) consegue cumprir essa função tão bem ou melhor do que eles.

Os blockchains colocam as funções de segurança em liberdade, assim como instituições medievais foram forçadas a ceder o controle da impressão.

É ilusório ver o blockchain primariamente como um registro distribuído, porque isso representa apenas uma de suas muitas

dimensões. É como descrever a internet como apenas uma rede, ou apenas uma plataforma de publicações. Essas são condições ou propriedades necessárias, mas não suficientes; os blockchains também são maiores do que a soma de suas partes.

Os proponentes do blockchain acreditam que a confiança deveria ser livre, e não estar nas mãos de forças centrais que a taxam, ou a controlam de uma maneira ou de outra (como taxas, direitos de acesso ou permissões). Eles acreditam que a confiança pode e deve ser parte de relações *peer-to-peer*, facilitadas por uma tecnologia que pode reforçá-la. A confiança pode ser codificada e computada para ser verdadeira ou falsa na certeza matemática, que é reforçada por uma criptografia poderosa para cimentá-la. Em essência, a confiança é substituída por provas criptográficas e mantida por uma rede de computadores confiáveis (nós honestos) que garantem sua segurança, conforme contrastado com entidades únicas que criam uma burocracia cara ou desnecessária sobre ela.

Se os blockchains são uma nova maneira de implementar transações confiáveis sem intermediários da confiança, logo teremos menos intermediários. Legisladores que regulam instituições "confiáveis", como bancos, enfrentarão um dilema. Como regular algo que está evaporando? Eles precisarão atualizar seus velhos regulamentos.

A confiança controlada por intermediários desenvolveu alguns atritos, mas, agora, o blockchain pode livrá-la deles. Então, quando a confiança for "livre" (mesmo que ainda precise ser conquistada), o que acontecerá? Naturalmente, a confiança seguirá o caminho de menor resistência e gradualmente se tornará descentralizada nos limites da rede.

Os blockchains também possibilitam que ativos e valores sejam trocados, fornecendo um caminho novo e mais rápido para valores em movimento de quaisquer tipos, sem que haja intermediários desnecessários.

Como uma infraestrutura de suporte, os blockchains são metaforicamente computadores incessantes. Uma vez lançados, eles nunca param de funcionar, devido à quantidade imensa de resiliência que oferecem. Não há um ponto único de fracasso. Ao contrário dos sistemas bancários e dos serviços baseados em nuvem, que caem, os blockchains genuínos continuam computando.

A internet substituiu alguns intermediários. Agora, o blockchain substituirá outros. Mas também criará alguns novos. Com a web foi a mesma coisa. Intermediários atuais deverão entender como seus papéis serão afetados, enquanto outros estão tentando achar seu lugar na corrida para "descentralizar tudo".

O mundo está preocupado em dissecar, analisar e prognosticar o futuro do blockchain; tecnologistas, empreendedores e empresas estão se perguntando se ele deve ser considerado um veneno ou um antídoto.

Hoje, dizemos que o blockchain faz isto ou aquilo, mas, amanhã, ele será bastante invisível; falaremos mais sobre o que ele possibilita. Assim como a internet ou a web, e assim como as bases de dados, o blockchain traz com ele uma nova linguagem.

A partir de meados dos anos 1950, conforme a TI evoluiu, nos acostumamos com uma nova linguagem: mainframes, bancos de dados, redes, servidores, softwares, sistemas operacionais e linguagens de programação. Desde o início dos anos 1990, a internet inaugurou um outro léxico: browsing, website, Java, blogging, TCP/IP, SMTP, HTTP, URLs e HTML. Hoje, o blockchain traz com ele ainda mais repertório: algoritmo consensual, contratos inteligentes, registros distribuídos, oráculos, carteiras digitais e blocos de transação.

Bloco a bloco, acumularemos nossa própria cadeia de conhecimento e aprenderemos e entenderemos o blockchain, o que muda com ele e as implicações de tais mudanças.

Hoje, pesquisamos tudo no Google, principalmente informações ou produtos.

Amanhã, faremos o equivalente à pesquisa no Google para verificar registros, identidades, autenticidade, direitos, trabalhos feitos, títulos, contratos e outros processos valiosos relacionados a ativos. Haverá certificados digitais de propriedade para tudo. Assim como não podemos mais duplicar dinheiro digital (graças à invenção de Satoshi Nakamoto), não poderemos fazer cópias ou forjar certificados oficiais uma vez que estejam documentados em um blockchain. Esta é a peça que faltava na revolução da informação.

Eu ainda me lembro de toda a animação por sermos capazes de acompanhar pela web uma encomenda enviada quando essa capacidade foi introduzida pela primeira vez pelo FedEx, em 1994. Hoje, sempre contamos com esse tipo de serviço, mas ele foi um divisor de águas que demonstrou o que poderíamos fazer no início da web. A mensagem por trás dele era a de que um serviço antes privado poderia se tornar abertamente acessível a todos os que tinham acesso à internet. Uma gama de serviços veio em seguida: bancos online, pagamento de impostos, compra de produtos, estoques comerciais, pagamento de compras e muitos outros. Assim como acessamos serviços que pesquisam bancos de dados públicos, procuraremos por uma nova classe de serviços que utilizarão o blockchain para confirmar a veracidade da informação. O acesso a ela não será suficiente. Também vamos querer acesso confiável, e perguntaremos se houve alguma modificação em certos registros, esperando a mais completa transparência daqueles que os detêm. O blockchain promete servir e expor a transparência em sua forma mais bruta.

O velho ditado: "Está em um banco de dados?" será substituído por "Está no blockchain?".

O blockchain é mais complicado do que a web? Definitivamente.

Permita-me levá-lo nesta jornada para decifrá-lo.