UTILIZAÇÃO DE BLOCKCHAINS PARA RASTREAMENTO DE RECURSOS PÚBLICOS: O PROJETO "BNDESTOKEN" DO GOVERNO BRASILEIRO

Leonardo Valles Bento[1]

I - INTRODUÇÃO

León (2018, p. 35) afirma, de forma bastante sugestiva, que, provavelmente, é a primeira vez na história que um artigo de apenas oito páginas, escrito por um autor, ou grupo de autores, anônimo(s), que não foi revisado por pares, nem publicado originalmente em nenhuma revista científica, conseguiu, em menos de dez anos, colocar de ponta-cabeça toda a compreensão comum sobre o modo de fazer as coisas.

Em 31 de outubro de 2008, um artigo chamado "*Bitcoin: a peer-to-peer eletronic cash system*" foi publicado por um certo Satoshi Nakamoto em uma lista de e-mails de especialistas em criptografia. O autor misterioso desapareceu em 2010, e sua verdadeira identidade permanece desconhecida.

Contudo, o artigo de Nakamoto não partiu do zero. A infraestrutura conhecida como "registro distribuído" (*distributed ledger*) ou "cadeia de blocos" (*blockchain*) já havia sido desenvolvida desde décadas de pesquisas em criptografia. Até mesmo criar dinheiro digital já havia sido tentado, mas sem muito sucesso. Criar uma moeda virtual possui uma dificuldade que precisa ser superada: evitar o duplo gasto, ou seja, que o mesmo dinheiro seja utilizado múltiplas vezes. Para se evitar a criação de moeda a partir do nada – o que impediria a confiança no sistema monetário – sempre foi necessária uma autoridade central, isto é, uma instituição financeira encarregada de gerenciar os saldos, efetuando créditos e débitos sempre que uma transação é realizada (PINKINGTON, 2016).

No fim do século passado, surgiram os primeiros programas para transferência de arquivos ponto-a-ponto (*peer-to-peer*, ou P2P), uma arquitetura de redes de computadores, na qual não existe diferenciação entre usuário e servidor, mas cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central que conheça o endereço todos os usuários e os coloque em contato. Por não se

[1] Auditor do Ministério da Transparência, Fiscalização e Controladoria-Geral da União do governo brasileiro e professor de Direito Administrativo da Unidade de Ensino Superior Dom Bosco (UNDB). Pesquisador Visitante da Universidade de Valência.

basear em uma arquitetura cliente-servidor, onde apenas o servidor é responsável pela execução de todas as funções da rede, na P2P todos os nós estão interconectados permitindo o acesso a qualquer nó de qualquer nó, sem a necessidade de intermediação de um servidor. Quantos mais *peers* existirem mais estabilidade e mais autonomia ganham, e a rede se torna mais eficiente e rica em recursos, a partir da comunicação direta entre eles. E quantos mais recursos, mais poderosa se torna essa rede.

Todavia, a arquitetura P2P foi criada para compartilhar informação, isto é, um ativo que não está sujeito ao princípio da escassez, que uma pessoa pode compartilhar sem perder a posse dela. Portanto, não existe aqui o problema do duplo gasto acima mencionado. O mérito de Nakamoto, portanto, ao criar o *bitcoin*, foi combinar a arquitetura P2P com a técnica de registro distribuído em cadeia de blocos. Com isso ele resolveu o problema de como intercambiar valor em um sistema descentralizado sem o risco do duplo gasto, prescindindo, assim, de uma autoridade financeira central em que todos confiem (LEÓN, 2018, p. 35).

Apesar de criado para servir como espinha dorsal do bitcoin, logo ficou evidente que sua arquitetura possui um valor em si mesma, de usos potenciais ilimitados, a ponto de estimular especulações sobre se o blockchain representaria um novo paradigma, com efeitos tão disruptivos quanto a própria Internet. Expressões como "blockchain everything" (BOUCHER, 2017), ou mesmo vaticínios sobre uma sociedade sem Estado (ATZORI, 2015) surgiram na literatura.

Sejam ou não procedentes tais especulações, o fato é que administrações públicas ao redor do mundo já investigam e põem em prática esta tecnologia em áreas tão diversas quanto gestão da identidade e de dados pessoais, registros de propriedade, gestão de cadeias de suprimentos, controle de pagamento de subvenções, licitações públicas e até mesmo em processos eleitorais. O objetivo é aprimorar a confiabilidade e a transparência na gestão de informações, bem como aumentar a eficiência dos serviços públicos e dos procedimentos administrativos.

O escopo do presente artigo é relatar sucintamente uma experiência de utilização de blockchains pelo governo do Brasil, por meio de sua principal agência de fomento econômico – o Banco Nacional de Desenvolvimento Econômico e Social (BNDES). Já em fase de prova de conceito, o BNDES pretende utilizar blockchains no monitoramento e divulgação à sociedade dos recursos disponibilizados a empresas no âmbito dos seus programas de financiamento.

Assim, inicialmente, o artigo expõe alguns conceitos essenciais que envolvem a tecnologia blockchain, suas características e vantagens. Em seguida, analisa *en passant* algumas de suas potenciais aplicações no setor público. Em continuação, detalha a experiência do BNEDStoken e de que modo sua utilização pode representar um ganho de eficiência, controle e transparência nas operações do Banco. Por fim, o artigo antecipa alguns desafios e questões ainda a ser enfrentadas na implementação e possíveis replicações dessa experiência.

Este artigo é resultado de um projeto de investigação pós-doutoral realizado junto à Universidade de Valência, com o apoio do governo brasileiro, por meio da política de capacitação de servidores do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

II - O QUE É BLOCKCHAIN?

Durante séculos, transações econômicas têm sido escrituradas em livros, ou, mais recentemente, em bancos de dados, mantidos por instituições bancárias que gozam da confiança das partes. Da mesma forma, transferências de propriedade de veículos e imóveis, por exemplo, são validadas e registradas por instituições notariais que certificam quem é dono do quê. Graças a esse sistema, é possível checar se as transações são legítimas e que o mesmo dinheiro não será transferido duas vezes, ou que a mesma casa não será vendida por quem não é o dono dela a dois compradores ao mesmo tempo. Assim, por confiarem na instituição intermediária gestora das informações (bancos ou governos), indivíduos que não se conhecem e, portanto, não têm motivos para confiarem uns nos outros, sentem-se seguros para fazer negócios.

O ponto fraco desse sistema é a necessidade do intermediário, que obviamente tem um custo. Tanto bancos quanto instituições notariais cobram taxas associadas a cada transação. Além disso, uma vez que toda informação está sob a custódia desse intermediário, existe sempre o risco de adulteração e fraude na escrituração, ou até mesmo, mais recentemente, de ataques por hackers, desastres, ou qualquer outro evento que pode comprometer a continuidade ou integridade dos registros (BOUCHER, 2017, p. 5).

A forma mais simples de compreender a tecnologia blockchain é defini-la como um sistema de contabilidade descentralizada, ou distribuída. Por meio dele, transações realizadas de uma parte a outra (*peer-to-peer*) são registradas em ordem cronológica, como em livro-diário de contabilidade. No entanto, ao invés de uma autoridade central manter um banco de dados, todos os nós da rede têm uma cópia do histórico de transações e as atualizações são propagadas entre eles em tempo real. Nessas redes, a maioria dos nós deve revisar e validar uma transação antes que ela possa ser registrada e uma vez inserida em um bloco ela se torna imutável. Dessa forma, como o registro é aberto e todos possuem uma cópia e todos podem inspecioná-lo, qualquer tentativa de adulteração geraria uma inconsistência imediatamente perceptível pelos demais participantes, e é isso que torna o sistema confiável (BARRYHILL *et alii*, 2018, 10-11).

III - PRINCIPAIS CARACTERÍSITICAS

Blockchain, portanto, é uma tecnologia para registrar transações e armazenar o histórico dessas transações, que compreende dois elementos: (1) um sistema de contabilidade distribuída, no qual todos os participantes possuem uma cópia dos dados; e (2) as transações validadas são armazenadas em blocos conectados entre si, formando uma sequência, ou cadeia de blocos, daí o nome blockchain.

Uma transação em blockchain é um intercâmbio de valor entre usuários do sistema. Cada nova transação é registrada cronologicamente junto a outras transações formando um bloco, que é conectado ao bloco de transações anterior. Cada bloco contém um conjunto de transações realizadas em período determinado de tempo. A base de dados da cadeia de blocos se constrói a partir da rede de usuários, chamados de nós (CARMONA, 2018, p. 11). Um nó da rede é simplesmente um usuário ou computador

conectado a uma plataforma blockchain que está rodando um software blockchain. Sua função, em linhas gerais, consiste em armazenar uma cópia integral dos registros, receber dados de outros nós, validar as transações e repassá-las, uma vez validadas, aos demais. Convém assinalar que todas essas ações são feitas por algoritmos, e não requerem intervenção manual (BARRYHILL, 2018, p. 11). Transações efetuadas na blockchain não são adicionadas a um bloco automaticamente. Para que os nós possam desempenhar essa função, é necessário que as transações sejam validadas por um consenso entre todos, ou pelo menos a maioria dos nós.

O registro das transações se realiza por meio de criptografia, utilizando um algoritmo de chaves. O sistema de blockchains utiliza uma criptografia de chaves assimétricas, isto é, de duas chaves, uma pública e outra privada, associadas matematicamente, e que todos os usuários (nós) da rede possuem. A chave pública se retransmite e distribui por toda a rede, permitindo a encriptação das transações e a identificação de um usuário frente aos demais, enquanto a chave privada, que é pessoal de cada usuário e conhecida apenas por ele, procede à desencriptação dos dados e proporciona a cada usuário uma assinatura digital para realizar transações. Dessa forma, todos os usuários da rede, utilizando a chave pública, podem obter uma prova matemática de que a transação foi efetivamente realizada por um dado usuário e por ninguém mais, porque mais ninguém possui a sua chave privada (CARMONA, 2018, p. 14).

Depois de validadas, as transações aguardam em uma fila de outras transações pendentes até que um tipo específico de nó, chamado de "minerador", realiza o armazenamento delas em um novo bloco, que será adicionado à cadeia. Um nó minerador é um subgrupo específico de nós, com computadores poderosos, encarregados de publicar as transações em blocos.

Cada novo bloco publicado contém uma marca digital denominada *hash*, que o conecta ao bloco anterior. Assim, os blocos não são independentes uns dos outros, mas estão ligados linear e sequencialmente por meio de uma "impressão digital". Hash é, pois, uma função criptográfica que cria um código único para cada bloco. Se o bloco permanece inalterado, ele irá gerar o mesmo código hash. Porém, se qualquer parte dele, por mínima que seja, for mudada, o código hash se altera de uma forma que não pode ser associada com o código hash original. Este sistema visa garantir que nenhuma informação sobre transações já validadas sejam adulteradas posteriormente à sua publicação em blocos. De fato, devido ao protocolo de consenso necessário para validação pela maioria dos nós, são facilmente perceptíveis quaisquer alterações no código hash, fazendo com que todas as transações associadas sejam rejeitadas. Em virtude desse mecanismo, é possível afirmar que as informações, uma vez armazenadas nos blocos, não podem ser editadas, nem deletadas (KILLMEYER, et. alii., p. 6).

A imutabilidade e a descentralização dos dados inseridos na blockchain é que assegura a confiança dos participantes, embora não se conheçam, sem a necessidade de um administrador central. Essa confiança permite, inclusive, uma das mais importantes funcionalidades das blockchains, qual seja, a celebração de contratos inteligentes (*smart contracts*). Algumas plataformas de blockchain permitem a criação de contratos inteligentes, que são pequenos algoritmos que utilizam uma plataforma Blockchain para sua execução. Os contratos inteligentes permitem a criação de fluxos de trabalho auto-executáveis, nos termos do acordo entre as partes, sendo escritos diretamente nas linhas

de código de um software. Os contratos inteligentes são programas de software "se /então" automatizados que se auto-executam quando ocorre um disparo específico, isto é, quando as condições previstas para o seu acionamento se fazem presentes. Eles são executados exatamente como programados, sem qualquer possibilidade de conflito interpretativo, fraude ou interferência de terceiros. Da mesma forma que outras transações blockchain, os contratos inteligentes são registrados e executados de forma distribuída em todos os da rede (BARRYHILL, et. alii. 2018, p. 19).

Atualmente, a plataforma mais desenvolvida para contratos inteligentes é a Ethereum, e foi em razão dessa maturidade que sua plataforma foi escolhida pelo BNDES para hospedar a experiência aqui descrita.

Por fim, importa mencionar que existem dois tipos de redes blockchain: públicas (*permissionless*) e privadas (*permissioned*). Em uma rede pública, como o bitcoin, qualquer usuário pode ter acesso à rede e submeter transações, ao passo que em uma rede privada apenas usuários especificamente autorizados podem participar. Em uma blockchain pública, não há limite de usuários participantes. Assim, qualquer pessoa pode baixar os programas necessários em seu computador e constituir-se em um nó da rede, participando do processo de consenso. As redes públicas baseiam-se na premissa de que quanto maior o número de participantes, maior a quantidade de cópias do histórico das transações distribuídas pelos nós, maior o número de pessoas envolvidas no processo de validação por consenso e, dessa forma, mais difícil é fraudar os registros. Nas redes privadas, ao contrário, os processos de consulta à cadeia de blocos, a validação e o envio de transações estão limitados a usuários considerados confiáveis (MARTINOVIC, 2017, p. 6-7). As redes públicas, naturalmente, correspondem mais ao paradigma implícito na tecnologia blockchain, que consiste precisamente em dispensar a confiança na pessoa do usuário, transferindo-a para a tecnologia de contabilidade distribuída e de imutabilidade da cadeia de blocos.

Na experiência do BNDES, descrita no presente artigo, utiliza-se uma rede blockchain pública. Em primeiro lugar, porque numa rede permissionada com poucos nós, um observador externo poderia entender que existe a possibilidade de conluio entre os nós da rede no momento da execução do algoritmo de consenso, minando assim a confiança no sistema. Assim, uma vez que um dos objetivos de sua utilização é o incremento da transparência das operações do BNDES, as blockchains públicas permitem o monitoramento dos dados sem depender de bases de dados fornecidas pelo próprio banco. Qualquer um pode conectar seu software de monitoramento na blockchain pública e acompanhar o ciclo de financiamento em tempo real (ARANTES JUNIOR et alii., 2018a, p. 3-4).

Portanto, em síntese, pode-se afirmar que as blockchains possuem as seguintes características, segundo Carmona (2018):

1. Descentralização: conforme já mencionado, a contabilidade distribuída que é um dos elementos definidores das blockchains significa que os registros das transações são replicados para todas as partes conectadas, cada uma possuindo uma cópia integral e idêntica do histórico, dispensando assim a como ponto central do sistema. Isso faz com que o sistema seja mais transparente e mais imune a destruição ou adulteração de informações. Uma boa analogia é com o e-mail. Quando um e-mail é enviado, tanto o emissor quanto o receptor guardam uma cópia. Se uma das partes tentar adulterar a

mensagem, isso gerará uma inconsistência com a mensagem que a outra parte possui, tornando a adulteração imediatamente perceptível.

2. Imutabilidade: a reconcialiação dos registros é feita imediata e automaticamente. Todo registro é irreversível, não podendo haver edição depois da transação ser validada e o seu respectivo bloco ser adicionado à cadeia. Isso permite às partes confiar na exatidão e autenticidade das informações registradas quanto ao tempo em que a transação ocorreu e a identidade das partes. Pode-se fazer uma analogia, mas invertida, com as publicações no facebook. Uma mensagem publicada no facebook pode ser editada livremente, alterando-se completamente seu conteúdo, sem perder nenhuma das "curtidas" que recebeu.

3. Transparência e auditabilidade: como todas as transações são registradas de forma irreversível em uma cadeia de blocos, que por sua vez estão gravadas em cada uma das cópias em poder das partes, todos os nós da rede podem verificar o momento em que um determinado ativo foi registrado na cadeia, quem foram seus titulares anteriores e quem é o seu titular atual. O caráter público dos registros e a irrefutabilidade das informações registradas tornam o sistema totalmente transparente quanto às transações, as quais são também completamente rastreáveis.

IV - ALÉM DO BITCOIN: APLICAÇÃO DO BLOCKCHAIN À ADMINISTRAÇÃO PÚBLICA

Apesar de que, até agora, a tecnologia blockchain tenha sido mais aplicada aos serviços financeiros e a criptomoedas como o bitcoin, há consenso na literatura de que ela passou a ter um significado e um valor em si mesma, possuindo inumeráveis aplicações (SAVELYEV, 2016, p. 3). Diversos governos estão formando comunidades dentro e entre setores, e parcerias público-privadas (PPPs) para trabalhar em conjunto na exploração do uso e implicações dos blockchains no setor público. Acredita-se que essa tecnologia pode tornar a gestão da informação e os serviços públicos mais eficientes, confiáveis e transparentes. Centenas de experiências para aplicar blockchain na Administração Pública já estão em andamento, ou sendo testadas, ao redor do mundo, em diversas áreas (BARRYHILL et alii, 2018, p. 22).

1 - Gestão da identidade pessoal e prestação de serviços públicos

Do ponto de vista funcional, a identidade de uma pessoa consiste em uma soma de atributos inerentes ao indivíduo (sexo, altura, idade, data de nascimento, impressões digitais, etc.), atributos acumulados ao longo do tempo (prontuários médicos, preferências de consumo, emprego, renda familiar, etc.) e atributos designados (número do passaporte, de telefone, e-mail, carteira de identidade, etc.) (DÉNIZ, 2018, p. 325). Blockchains podem ser utilizadas para criar uma identidade digital para cidadãos, residentes, empresas, organizações não-governamentais e órgãos públicos. Mudanças de status pessoal podem ser registradas e armazenadas em cadeia de blocos, como nascimentos, casamentos, divórcios e óbitos. Da mesma forma, todos os aspectos da identidade, e as informações a ela relacionadas podem ser gerenciadas por meio dessa tecnologia, por exemplo, recebimento de benefícios sociais, mudanças de residência e de emprego, obtenção de licenças, registros de infrações de trânsito ou criminais, etc.

A Estônia é um país líder na adoção de tecnologias digitais em serviços públicos. Já em 2000, por exemplo, o país declarou o acesso à Internet como um direito humano, um movimento que impulsionou a implantação do acesso à Internet em áreas rurais e impulsionou usos inovadores de tecnologias digitais. Em 2000, Estônia aprovou a Lei de Assinatura Digital, que tornou a assinatura digital equivalente a uma assinatura escrita, e, desde então, todas as autoridades da Estônia são legalmente obrigadas a aceitar documentos assinados digitalmente. Outra parte importante do arcabouço legal é que ele exige a não-duplicação de registros de banco de dados públicos (chamada de escrita única): nenhuma informação é armazenada duas vezes; e qualquer atualização deve ser executada no registro mestre (MARTINOVIC, 2017, p. 9).

Utilizando tecnologia blockchain, o governo da Estônia utiliza duas ferramentas. Uma delas é o *Keyless Signature Infrastructure* (KSI), que gerencia e mantém o blockchain contendo o registro distribuído integrado às principais bases de dados governamentais, incluindo o registro comercial, registro de propriedades, registro de sucessão, arquivos judiciais digitais, entre outros. A outra é o X-Road, uma plataforma de interoperabilidade que integra diferentes interfaces. O X-Road permite transações digitais nas áreas de residência, declaração eletrônica de impostos, validação de cartas de condução e veículos registados, aplicação para benefícios infantis e creches municipais, e intercâmbio de documentos entre agências governamentais.

O governo da Estônia tem se destacado também na utilização de blockchains para prestação de serviços de saúde. O X-Road interliga hospitais, clínicas e outras organizações, implementando um Registro Eletrônico de Saúde unificado que fornece aos médicos informações sobre a saúde dos pacientes, ao mesmo tem em que protege sua privacidade. Um sistema de "receita médica" permite que os médicos prescrevam receitas aos seus pacientes e as disponibilizem imediatamente para as farmácias. Os pacientes podem então coletar seus remédios diretamente da farmácia sem precisar consultar o médico para obter uma cópia impressa da receita médica.

A polícia também tem acesso a este sistema para verificar se um veículo foi relatado como roubado, por exemplo. Consequentemente, os cidadãos da Estónia não precisam portar uma carteira de motorista ou documentos do veículo, porque as autoridades podem verificar essas informações on-line diretamente da fonte (MARTINOVIC, 2017, p. 9).

2 - Benefícios e subvenções

Governos mantêm diversas políticas de auxílio para cidadãos em situações específicas de vulnerabilidade, como doença, invalidez, desemprego ou pobreza. A concessão desses auxílios normalmente envolve um significativo trabalho de verificação das condições de elegibilidade que, em muitos casos, implica consultar diversos outros órgãos ou sistemas, consumindo tempo e recursos humanos e organizacionais. A existência de uma identidade pessoal digital e um histórico atualizado de informações pessoais permitiria realizar esse controle de forma mais rápida, eficaz, talvez até mesmo automatizada (BARRYHILL et. alii, 2018, p. 26).

3 - Registros de propriedade

Registros de propriedade é uma aplicação que naturalmente se apresenta para a utilização de blockchains. Transferências de títulos de propriedade podem ser cronologicamente registradas em cadeia de blocos, utilizando o sistema de contabilidade distribuída, dispensando, assim, em tese, a necessidade de um notário. Como as informações são imutáveis, não há risco de fraude na titularidade do domínio.

O governo sueco está testando um banco de dados blockchain destinado a simplificar transações sobre bens imóveis, permitindo a verificação digital confiável de contratos de compra e venda, hipotecas, entre outras transações. A autoridade de registro sueca de registro de imóveis, disponibilizaria um aplicativo móvel que todas as partes de uma transação imobiliária poderiam usar para trocar informações, assinar digitalmente documentos legalmente vinculantes e executar verificações de títulos de propriedades. Essa arquitetura permite a transferência de títulos de propriedade sem a intermediação de um notário, com uma velocidade e um custo significativamente menor para as partes (CHENG et alii, 2017, p. 4).

4 - Compras governamentais

De um modo geral, a contratação de fornecedores de bens e serviços pela Administração Pública é precedida de um procedimento bastante burocrático para verificar a idoneidade das empresas contratadas. Estas necessitam demonstrar perante a Administração Pública sua capacidade técnica e financeira para executar o contrato, além da regularidade de sua situação jurídica e fiscal. Na maioria dos casos, essa demonstração consiste em apresentar ao órgão público contratante documentos obtidos de outros órgãos administrativos, isto é, as empresas participantes da licitação precisam fornecer a um setor da Administração informações que ela, de algum modo, já possui. No caso da legislação brasileira, por exemplo, é necessário que as empresas demonstrem que estão legalmente constituídas, que estão incluídas no cadastro nacional de pessoas jurídicas, que estão em dia com o pagamento de tributos e de contribuições previdenciárias. Todas estas informações, a exemplo de outras que também se exigem, estão em posse da própria Administração Pública. A tecnologia blockchain abre a perspectiva de um registro único que dispensaria as empresas licitantes de aportar ao processo documentação que já se encontre em poder dos órgãos públicos ou que constem anotados em registros públicos.

O governo do País Basco vem desenvolvendo uma aplicação de blockchain para registro de empresas, de modo a evitar que elas tenham que comprovar o cumprimento de requisitos legais sucessivas vezes, sempre que desejam participar de uma licitação pública. O governo da Comunidade de Aragão, por sua vez, pôs em marcha um projeto piloto para solicitar aos licitantes que apresentem a identificação eletrônica de sua oferta, por meio de código *hash*. Assim, as propostas ficam registradas e distribuídas em todos os nós da rede, de forma inalterável (TORTOSA, 2018, p. 350-1).

5 - Monitoramento de cadeias de suprimentos

De forma similar ao mecanismo de controle de transferências de títulos de propriedade, o registro de transações em blockchains pode auxiliar no monitoramento de um insumo ou um ativo, desde sua origem, passando por todas as etapas de transporte e manuseio, até a sua compra ou recebimento por um destinatário final. Exemplos potenciais incluem medicamentos, alimentos, donativos, ajuda para o

desenvolvimento, e até recursos naturais como diamantes, permitindo às autoridades e até ao público em geral, conforme o caso, certificarem-se da autenticidade da origem e da efetiva destinação de um determinado bem. A tecnologia blockchain pode prover a infraestrutura para registrar, certificar e rastrear a um baixo custo bens em trânsito. Todos os produtos são identificados exclusivamente por meio de "tokens" e podem ser transferidos via blockchain, com cada transação verificada com registro de data e hora em um processo criptografado, mas transparente. Isso permite o acesso por todas as partes interessadas, sejam fornecedores, transportadores ou compradores. Os termos de cada transação permanecem irrevogáveis e imutáveis, e assim completamente auditáveis a qualquer tempo. Contratos inteligentes também podem ser implantados para executar automaticamente pagamentos e outros procedimentos (BOUCHER, 2017, p. 16).

A iniciativa descrita neste artigo é uma aplicação de blockchains em cadeias de transações, por meio de tokens, conforme se explicará a seguir.

V - A EXPERIÊNCIA DO BNDES

O Banco Nacional de Desenvolvimento Econômico e Social (BNDES), criado em 1952, é a principal agência de fomento econômico do governo brasileiro. Especializou-se na concessão de financiamentos de longo prazo e em investimentos em diversos segmentos da economia brasileira, a fim de estimular a expansão da indústria e da infraestrutura no país. Seus clientes incluem empresas de todos os portes, e até mesmo pessoas físicas. De um modo geral, os financiamentos concedidos pelos BNDES têm por objeto a aquisição de equipamentos, maquinário entre outros insumos de produção, bem como a realização de grandes obras de infraestrutura. O Banco também financia a produção para exportação de equipamentos, maquinários e obras de infraestrutura.

Atualmente, o processo de concessão de financiamento envolve significativo trabalho manual, seguindo trâmites burocráticos tradicionais, em diversas etapas. Inicialmente, o Banco aprova o projeto, ou proposta, de financiamento de um proponente, normalmente uma empresa. Em seguida, um contrato de empréstimo é celebrado, cujas cláusulas definem o cronograma de liberação da quantia a ser emprestada e do respectivo pagamento. Importante ressaltar que o Banco não libera o valor integral do financiamento em uma única parcela, mas o subdivide conforme as etapas previstas na execução do projeto, ficando a etapa seguinte condicionada à comprovação da execução da etapa anterior. O BNDES utiliza um banco comercial para efetuar os repasses do financiamento e a empresa cliente, por sua vez, utiliza os recursos para contratar fornecedores, tantos quantos necessários, para a consecução do projeto, utilizando também os serviços de um banco comercial. Em seguida, o cliente apresenta ao BNDES documentos que comprovam os gastos realizados, normalmente recibos ou notas fiscais que atestam que o cliente de fato contratou fornecedores, a identidade dos fornecedores, quais produtos ou serviços foram adquiridos e por que valor. O objetivo desse processo é assegurar que os recursos emprestados foram realmente utilizados de acordo com as especificações do projeto e do contrato. O Banco então aprova essa prestação de contas e a divulga à sociedade por meio de portais de transparência, para que toda a sociedade possa ver como o dinheiro foi usado (ARANTES JUNIOR, 2018b, p. 1182).

Arantes Junior et. al.(2018b, p. 1182) destacam alguns problemas nessa sistemática. O primeiro é que as informações do processo de financiamento encontram-se fragmentadas entre o Banco de Desenvolvimento, o cliente e os fornecedores contratados por este. Assim, o monitoramento da aplicação correta dos recursos emprestados envolve um trabalho de conciliação documental que, como se disse acima, é realizado manualmente, com elevados custos de auditoria. Além disso, em relação à transparência, a sociedade só possui acesso às informações após a análise e aprovação da prestação de contas, e sempre tendo o Banco como intermediário da divulgação. Uma maior integração de informações e um processo automatizado de conciliação de dados melhoraria a eficiência do processo, reduzindo o custo do controle, e permitiria à sociedade acessar informações sem intermediação, o que representaria um incremento na transparência pública.

Outro inconveniente é que, embora o Banco não disponibilize a quantia total do financiamento de uma única vez, mas em parcelas, conforme de mencionou acima, estas parcelas representam ainda assim grandes quantias de dinheiro, que seus clientes levam algum tempo para gastar. Isso é de algum modo inevitável, pois uma subdivisão maior das liberações acarretaria um aumento significativo da burocracia. Enquanto, os clientes não gastam o dinheiro eles devem investi-lo, normalmente em algum fundo de renda fixa. Se o valor da taxa de juros desse investimento for maior do que o valor da taxa de juros do empréstimo cobrada pelo Banco, os clientes têm incentivos para adiar o cronograma do projeto, a fim de lucrar com a diferença. O ideal, portanto, é que a disponibilização de dinheiro ao cliente se dê o mais próximo possível da data de pagamento de seus fornecedores.

Encontra-se em fase de teste e implementação o projeto BNDESToken, que pretende substituir essa sistemática tradicional pela tecnóloga blockchain, a fim de rastrear a aplicação de recursos públicos em projetos de financiamento, fornecendo à sociedade informações sobre como esses recursos estão sendo utilizados, incrementando assim a transparência pública e o controle social. O Banco irá utilizar uma rede blockchain pública (*permissionless*) hospedada na rede Ethereum, que permite a criação de contratos inteligentes. O projeto prevê que os financiamentos concedidos pelo Banco sejam feitos por meio da plataforma Ethereum, utilizando uma moeda virtual – o *token.* O conceito de token representa um ativo digital cujo valor pode ou não ter uma correspondência com um ativo real. Os tokens são eles próprios contratos inteligentes que gerenciam os saldos de cada usuário e podem ser programados de acordo com padrões pré-definidos. No projeto cada token equivale a 1 real brasileiro. Ou seja, em vez do Banco realizar liberações em dinheiro aos seus clientes, ele liberará uma representação deste, na forma de uma moeda virtual. Os clientes também irão contratar seus fornecedores pagando-os em tokens, que ao final serão resgatados por esses fornecedores junto ao Banco. De acordo com Arantes Junior et al. (2018a, p. 2):

> O BNDESToken é distribuído nos financiamentos e, em todo momento, o token é propriedade de quem teria a propriedade do Real. Ao adotar uma tecnologia que permite verificar quem está em posse do token, obtém-se um mecanismo para rastrear os recursos em tempo real. Na prática, portanto, o BNDESToken é apenas uma representação digital do Real, análogo a um título de crédito para futuro recebimento do recurso.

Convém ressaltar, no entanto, que não se trata de uma criptomoeda. Em primeiro lugar porque a emissão do token terá sempre o Real como lastro, de modo que sua

emissão não representa aumento da massa monetária. Em segundo lugar, o BNDESToken não pode ser repassado indefinidamente. O BNDES emite o token no momento da liberação do recurso, e ele pode ser transferido algumas vezes na cadeia de fornecedores, mas depois deve necessariamente ser resgatado perante o Sistema BNDES. Essa premissa visa evitar que o token se converta em um ativo financeiro negociável em um mercado paralelo. Por fim, o total de BNDESToken de uma conta não se modifica ao longo do tempo. Ou seja, não há correção de inflação no saldo de tokens de uma conta, nem há opções de investimento para que rendam mais tokens. Todas essas precauções visam minimizar os riscos jurídicos/regulatórios inerentes ao mercado de criptodivisas (ARANTES JUNIOR, 2018b, p. 1183).

Inicialmente, tanto clientes quanto fornecedores desse cliente precisam se registrar no sistema, de modo a receberem uma identidade digital. Isso permite correlacionar a identidade real da empresa (cliente ou fornecedora) com a sua conta no Ethereum, de forma a assegurar que a empresa é quem afirma ser. Não existe no Brasil um sistema de identidade digital semelhante ao e-residency da Estônia. No entanto, desde 2001 existe a Infra-Estrutura de Chaves Públicas Brasileira, gerenciado por uma autoridade certificadora raiz, que emite um certificado digital para identificação virtual das pessoas jurídicas, uma espécie de documento eletrônico de identidade que garante a autenticidade dos emissores e destinatários de documentos e dados que trafegam na Internet, bem como a privacidade e a inviolabilidade destes dados. Empresas usam essa identidade digital para enviar ao governo informações trabalhistas, previdenciárias e fiscais. Segundo o modelo proposto pelo BNDES, as empresas clientes e fornecedoras poderão utilizar essa identidade digital para registrar um endereço de carteira Ethereum, habilitando-se a realizar transações com tokens (ARANTES JUNIOR, 2018b, p. 1184).

Concluído esse registro, o cliente está habilitado a receber os desembolsos do Banco e outras empresas fornecedoras estão aptas a serem contratadas pelo cliente. O Banco então solicita ao sistema a realização de um desembolso ao cliente. O sistema verifica a validade da operação, isto é, se ela está autorizada por um contrato, bem como a identidade do recebedor, e transfere a esse uma quantidade determinada de tokens, como representação do dinheiro. Um “evento de desembolso” do financiamento fica então registrado na blockchain.

O cliente, em seguida, solicita ao sistema a efetuação de pagamentos aos seus fornecedores. O sistema checa a validade dos pagamentos da mesma forma e transfere a quantia solicitada em tokens, operação que também é registrada na blockchain como “evento de pagamento”. No passo seguinte, os fornecedores contratados solicitam ao sistema a conversão dos tokens em dinheiro. O sistema confere a validade da operação e a identidade dos fornecedores e, caso validado, efetua um “evento de resgate”, registrado na blockchain. Uma vez realizado o resgate em moeda nacional, um código de contrato inteligente destrói a quantidade correspondente de tokens. Sempre que um evento de resgate é registrado, um código de contrato inteligente publica a informação que pode ser consultada por toda a sociedade (ARANTES JUNIOR, 2018b, p. 1184).

Uma deficiência da proposta é que, por facilidade de implementação, não existe um identificador único para cada BNDESToken. Assim, não é possível rastrear um subgrupo de recursos de forma segregada dos demais. Trata-se, no entanto, de uma característica que não é conceitual do sistema, de modo que pode ser revista no futuro (ARANTES JUNIO, 2018a, p. 2).

O BNDES está trabalhando para conseguir realizar uma prova de conceito da proposta descrita acima. Até o momento, o projeto contempla funcionalidades de transferência do token, acompanhamento do cliente e um painel online. O módulo de identidade de pessoa jurídica ainda está sendo debatido pela equipe técnica. Blockchain tem se mostrado uma tecnologia muito promissora para o BNDES, no sentido de monitorar a movimentação dos recursos após o desembolso.

Importante ressaltar que a proposta descrita é replicável para ser utilizada por outros órgãos de governo ou outras entidades que desejem rastrear os recursos desembolsados e analisar como foram utilizados. O Brasil é um país que descentraliza recursos por meio de numerosos instrumentos, tanto para entidades privadas, quanto para as unidades federativas. Assim a tecnologia blockchain tem potencial para se tornar o mecanismo padrão de acompanhamento da aplicação de recursos públicos descentralizados.

Segundo Arantes Junior at. al. (2018, p. 3):

> A adoção da tecnologia blockchain permite que a sociedade confie na inviolabilidade das informações de forma irrefutável, sem a necessidade de uma relação de confiança com a entidade centralizadora. Também permite que o monitoramento em tempo real da aplicação dos recursos seja implementado por qualquer pessoa interessada, bastando, para isso, monitorar as informações na blockchain.

Contudo, apesar de promissora, persistem ainda muitos desafios, inclusive regulatórios. Não está claro, por exemplo, quando começam a contar os juros do empréstimo. Que tipo de ativo financeiro é o BNDESToken em caso de uma disputa jurídica? Considerando que a blockchain é pública, como tratar o sigilo empresarial e bancário, entre outros dados pessoais? Como funciona o recolhimento de tributos quando uma transação é paga com BNDESTokens, e não com a moeda oficial? Essas são algumas das questões que ainda precisam ser debatidas, conforme reconhecem seus próprios formuladores (ARANTES JUNIOR, 2018a, p. 11).

VI - DESAFIOS PARA O FUTURO

Apesar dos benefícios e das abundantes aplicações das tecnologias blockchain no setor público, a literatura também apresenta diversos desafios que precisam ser enfrentados. Nesse sentido, estes desafios podem ser classificados, de modo geral, em três aspectos: (1) tecnológicos; (2) organizacionais; e (3) ambientais (BATUBARA et. alii, 2018).

Os desafios tecnológicos são de longe os problemas mais destacados que podem constituir obstáculos à aplicação dos blockchains. Esses problemas estão relacionados com a escalabilidade, capacidade computacional e de armazenamento de dados, uma vez que à medida que a rede acumula mais e mais partes que transacionam, e à medida que se acumula o histórico de transações, torna-se cada vez mais difícil que cada nó da rede possa suportar uma cópia integral do registro distribuído.

Outro problema frequentemente apontado é o da interoperabilidade. Ølnes, Ubacht e Janssen (2017, p. 360). observam que não existe "o" blockchain, mas blockchains, no sentido de que há várias soluções e desenhos possíveis, com diferentes propriedades, cada qual com suas vantagens e desvantagens. As principais variáveis são blockchains públicas e privadas, permissionadas ou não permissionadas, mas pode haver outras escolhas. Tais variáveis devem ser cuidadosamente discutidas para sua aplicação ao governo eletrônico, de acordo com as necessidades do setor que pretenda empregar essa tecnologia. Os autores advertem para o fato de que muitas experiências e soluções podem estar sendo guiadas pela tecnologia, ao invés de orientar-se pelos problemas sociais que requerem a atenção dos governos. Noutras palavras, ao invés da tecnologia desenvolver-se em resposta às necessidades e aos valores do setor público, é o setor público que se adapta à tecnologia, como uma panaceia (ØLNES et. alii, 2017, p. 362). A implementação da tecnologia blockchain não pode seguir uma lógica linear e determinista, requerendo, ao contrário, uma abordagem pragmática, de tentativa-erro, a fim de compreender melhor sua aplicabilidade e limitações.

Essa estratégia, porém, tende a uma fragmentação no uso dos blockchain por diversas organizações públicas, com cada experiência resultando em diferentes sistemas. Essa fragmentação, embora natural no processo de compreensão e amadurecimento da tecnologia, é prejudicial para interoperabilidade, resultando em ineficiência e duplicação desnecessária de trabalho. Assim, convém que, no longo prazo, as experiências de uso de blockchain se orientem para o desenvolvimento de uma plataforma geral padronizada que comporte suas múltiplas aplicações.

Tais desafios, apontados pela literatura, relacionam-se com o estágio ainda imaturo da tecnologia e o limitado conhecimento de que ainda se dispõe sobre o seu potencial.

Embora menos frequentes, há autores que salientam que o uso da tecnologia blockchain na Administração Pública demanda novos modelos de governança, para melhor aproveitar os seus benefícios. Destaca-se, especialmente, a necessidade de integração, cooperação e compartilhamento de informações entre múltiplos setores da Administração, que, normalmente, possuem cada qual seus próprios sistemas e bases de dados (BATUBARA et. alii, 2018, p. 7).

Por fim, do ponto de vista ambiental, a necessidade de um suporte regulatório é o fator mais destacado pelos especialistas para o sucesso do blockchain na Administração Pública. Um marco legal que proporcione segurança jurídica e esclareça os direitos e responsabilidades dos participantes é tido como essencial. Outro fator relevante é o da inclusão digital. A utilização das blockchain no setor público não irá produzir os resultados esperados de maior transparência e eficiência nos serviços públicos se parte significativa da população não tem acesso à Internet (BATUBARA et. alii, 2018, p. 7).

VII - CONCLUSÕES

O desenvolvimento do mecanismo que gera a tecnologia blockchain, ou tecnologia de registro distribuído, deve acelerar a expansão da digitalização das

transações econômicas, fenômeno conhecido como Internet do Valor, conforme vai adquirindo maturidade (SEMPERE, 2018, p. 79).

O presente artigo teve como objetivo apresentar em breves linhas a experiência piloto do governo brasileiro, implementada pelo BNDES. Inicialmente, foram apresentadas as características mais importantes e os conceitos envolvendo a tecnologia blockchain, assim como algumas de suas aplicações possíveis e em fase de concepção, ou de teste na Administração Pública. Ao final, buscou-se demonstrar como essa tecnologia pode contribuir para aperfeiçoar a sistemática de monitoramento pelo Banco dos recursos desembolsados em seus programas de financiamento, no sentido de um maior controle e transparência.

Nesse sentido, blockchain tem se mostrado uma tecnologia muito promissora para o BNDES a fim de avaliar como os recursos de fomento econômico são movimentados na economia após o seu desembolso, servindo de insumo para pesquisas futuras acerca da efetividade das políticas de desenvolvimento, bem como de mecanismo de accountability contra desvios e desperdício de recursos.

Embora tenha um escopo bastante específico, o de rastrear desembolso dos financiamentos, o projeto poderá servir de ponto de partida para a expansão do blockchains para outras aplicações, tais como identidade digital e transferência de ativos, os quais, futuramente, podem convergir para uma mesma plataforma. Além disso, conforme se disse acima, trata-se de um sistema que pode ser replicado para outros instrumentos de transferência financeira. Convênios, contratos de repasse, termos de parcerias e outros acordos que são celebrados entre a Administração Pública e organizações privadas, ou entre unidades da federação também podem, no futuro, evitar o envio imediato de dinheiro, valendo-se de tokens, até o momento do seu resgate, reduzindo assim o risco de desvio e os custos do controle.

Naturalmente, o aprofundamento no entendimento da tecnologia durante o desenvolvimento da prova de conceito é que irá determinar de forma mais concreta tanto as suas potencialidades, quanto os seus limites, isto é, a que novos produtos essa tecnologia pode dar origem e que problemas e dificuldades devem ser superados.

VIII - REFERÊNCIAS

ARANTES JÚNIOR, G. M.; D'ALMEIDA JUNIOR, J. N.; ONODERA, M. T.; MORENO, S. M. de B. M.; ALMEIDA, V. da R. S (2018a). **BNDESToken**: uma proposta para rastrear o caminho de recursos do BNDES. XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Sociedade Brasileira de Computação (SBC), Laboratório de Redes de Computadores (LARC) Disponível em: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/05-181662.pdf. Acesso em: 2 de outubro de 2018.

ARANTES JÚNIOR, G. M.; D'ALMEIDA JUNIOR, J. N.; ONODERA, M. T.; MORENO, S. M. de B. M.; ALMEIDA, V. da R. S (2018b). **Improving the Process of Lending, Monitoring and Evaluating through Blockchain Technologies**: an Application of Blockchain in the Brazilian Development Bank (BNDES). Conference

on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing. DOI 10.1109/Cybermatics_2018.2018.00211
Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics. p. 1181-1188.

ATZORI, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Disponível em: https://ssrn.com/abstract=270971. Acesso em: 15 de setembro de 2018.

BARRYHILL, J.; BOURGERY, T.; HANSON, A. (2018). **Blockchains unchained**: blockchain technology and its use in the public sector. OECD Working Papers on Public Governance, nº 28, OECD Publishing, Paris. Disponível em: http://dx.doi.org/10.1787/3c32c429-en. Acesso em: 15 de setembro de 2018.

BATUBARA, F.; UBACHT, J.; JANSSEN, M. (2018). **Challenges of blockchain technology adoption for e-government**: a systematic literature review. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. Disponível em: https://dl.acm.org/citation.cfm?id=3209317. Acesso em: 21 de setembro de 2018.

BOUCHER, P. (2017). **How blockchain technology could change our lives**. European Parliament. European Parliamentary Research Service. Scientific Foresight Unit. Disponível em: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf. Acesso em: 15 de setembro de 2018.

CARMONA, A. M. M (2018). **Implicaciones jurídicas del uso de blockchains en la Administración Pública**. 103f. Dissertação (Mestrado em Direito) - Facultad de Derecho, Universidad de Murcia.

CHENG, S.; DAUB, M. DOMEYER, A., LUNDQVIST, M. (2017). **Using blockchain to improve data management in the public sector**. Disponível em: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector. Acesso em: 15 de setembro de 2018

DÉNIZ, R. L. (2018). Hacia una identidade digital basada en blockchain dentro de la Administración Pública. In: MOYA, R. V. **Blockchains: aspectos tecnológicos, empresariales y legales**. Thomson Reuters. p. 321-338.

KILLMEYER, J.; WHITE, M.; CHEW, B. (2017). **Will blockchain transform the public sector?** Deloitte University Press. Disponível em: https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf. Acesso em: 16 de setembro 2018.

LEÓN, P. J. P. (2018). Blockchain, un nuevo padrón tecnológico. In: MOYA, R. V. **Blockchains: aspectos tecnológicos, empresariales y legales**. Thomson Reuters. p. 35-77.

MARTINOVIC, I. (2017) **Blockchains for governmental services**: design principles, applications, and case studies. Centre for Technology and Global Affairs, Department of Politics and International Relations, University of Oxford. Disponível em: https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickelloslu ganovic.pdf. Acesso em: 15 de setembro de2018.

ØLNES, S.; UBACHT, J.; JANSSEN, M. (2017). Blockchain in government: benefits and implications of distributed ledger technology for information sharing. **Government Information Quarterly,** 34, p. 355–364.

PILKINGTON, M. (2016). **Blockchain technology**: principles and applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar. Disponível em: SSRN: https://ssrn.com/abstract=2662660. Acesso em: 22 de outubro de 2018.

SAVELYEV, A. (2016). **Contract law 2.0**: «smart» contracts as the beginning of the end of classic contract law. National Research University (Moscow), Hicher School of Economics. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241. Acesso em: 15 de setembro de2018.

SEMPERE, M. del C. P. (2018). Internet del valor. In: MOYA, R. V. **Blockchains: aspectos tecnológicos, empresariales y legales**. Thomson Reuters. p. 79-119.

TORTOSA, F. G. (2018). Una tecnología para facilitar los processos de participación, cooperación y transparencia en el sector público. In: MOYA, R. V. **Blockchains: aspectos tecnológicos, empresariales y legales**. Thomson Reuters. p. 339- 359.