# BNDESToken: Uma Proposta para Rastrear o Caminho de Recursos do BNDES

**Gladstone Moisés Arantes Júnior, José Nogueira D'Almeida Jr., Marcio Teruo Onodera, Suzana Mesquita de Borba Maranhão Moreno, Vanessa da Rocha Santos Almeida**

BNDES – Banco Nacional do Desenvolvimento – Avenida República do Chile, 100 – Rio de Janeiro - RJ - Brasil - 20031-917

{glads, josej, marcio.onodera, suzana, valm}@bndes.gov.br

***Abstract.*** *This paper proposes the creation of a token within a blockchain structure to track the flow of funding disbursements of the Brazilian Development Bank (BNDES). Besides bringing transparency to society regarding disbursements for the supported corporations, the proposal may generate inputs for the creation of new financing products; simplify the operations monitoring, and produce data to subsidize aggregated analysis of the benefits originated by BNDES loans.*

***Resumo.*** *Este artigo descreve uma proposta de criação de token dentro de uma infraestrutura de blockchain para rastrear o caminho dos recursos do BNDES (Banco Nacional de Desenvolvimento Econômico e Social). Além de transparência para a sociedade ao longo do repasse de recursos entre as pessoas jurídicas apoiadas, a proposta pode gerar insumos para criação de novos produtos de financiamento, simplificar o acompanhamento das operações e produzir dados para subsidiar análise agregada dos benefícios originados pelos empréstimos do banco.*

## 1. Introdução

A confiança está em crise em várias partes do mundo [Edelman 2018]. Enquanto a Internet e as redes sociais promovem a divulgação de informações, ampliando o alcance das opiniões pessoais, as instituições e veículos de mídia lidam com o descrédito da população. Em decorrência da desconfiança e das facilidades criadas pela tecnologia da informação, a sociedade demanda um governo mais transparente e ágil.

Governo digital ("e-government") pode ser definido como o uso de tecnologia da informação para prover serviços e engajar cidadãos [CTG 2018]. Várias tecnologias podem ser empregadas em governos digitais, sendo blockchain uma delas. A tecnologia de blockchain é uma nova maneira de viabilizar a realização de transações e armazenar os dados gerados de forma distribuída, sendo uma alternativa aos sistemas centralizados tradicionais, dispensando a necessidade de uma parte intermediária confiável para gerenciar as informações. As informações são armazenadas em uma rede peer-to-peer após o consenso entre os nós. Nestas infraestruturas, não é possível haver alteração em dados previamente armazenados. Quando em redes públicas, como Bitcoin [Nakamoto 2008] e Ethereum [Wood 2014], partes completamente anônimas e que não confiam entre si podem formar uma rede que armazena informações confiáveis [Peck 2017].

Tapscott [Tapscott 2016] afirma que a tecnologia de blockchain pode ser utilizada para melhorar a prestação de serviços ao mesmo tempo que garante integridade e transparência das informações. São exemplos de uso dessa tecnologia em serviços de governos: armazenamento antifraude de registros públicos, como propriedades privadas e antecedentes criminais; identificação digital de pessoa física ou jurídica; e digitalização da moeda nacional.

Este artigo descreve um mecanismo para rastrear o caminho de recursos públicos em projetos de financiamento do BNDES, chamado de BNDESToken. Além disso, o artigo também discute aspectos técnicos da construção desse mecanismo, que está sendo implementado para uso em prova de conceito de alguns financiamentos.

O restante deste documento é dividido da seguinte forma. A Seção 2 descreve a proposta conceitual do token, enquanto a Seção 3 delineia o que já foi implementado e aspectos técnicos relevantes. A Seção 4 detalha trabalhos relacionados e como eles se comparam com a proposta deste artigo. Por fim, a Seção 5 apresenta conclusões e próximos passos.

## 2. Definição da Proposta

O BNDESToken é mecanismo para rastrear a aplicação de recursos públicos em projetos de financiamento do BNDES, fornecendo à sociedade a informação de como esses recursos estão promovendo o desenvolvimento do país.

Cada unidade do BNDESToken equivale a um Real (1:1). A cotação fixa é um modo simples de criar uma marcação na moeda nacional. 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.

Adota-se seis premissas que simplificam a adoção da proposta. A primeira é que a emissão do token não representa aumento da base monetária a economia, pois o BNDES deixa de liberar o Real, mas o mantém como lastro. Essa simplificação diminui o risco jurídico/regulatório da solução. A segunda é que o BNDESToken não pode ser repassado indefinidamente. O BNDES emite o token durante a liberação do recurso, o token pode ser transferido algumas vezes na cadeia e depois deve necessariamente ser resgatado perante o Sistema BNDES. Essa premissa visa evitar a criação de um mercado secundário do uso do token, o que poderia introduzir risco regulatório. A terceira é que 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. A quarta premissa é que apenas pessoas jurídicas com e-CNPJ podem receber BNDESToken. Pessoas físicas podem ser contempladas em um momento posterior, a depender de uma análise mais aprofundada. A quinta é que os tokens são fungíveis. Por facilidade de implementação, não existe um identificador único para cada BNDESToken. Se for necessário rastrear algum recurso de forma segregada dos demais, será necessário rever essa última simplificação. A última premissa é que, por simplicidade de implementação, os eventos de transferência não são automaticamente relacionados com marcos do projeto de financiamento.

A figura a seguir ilustra um exemplo de liberação em BNDESToken. O token é representado por uma imagem hexagonal junto com uma pegada digital, expressando a

metáfora de rastreabilidade. No exemplo, o token é criado no momento da liberação para o cliente, transferido para um fornecedor e posteriormente resgatado por Real.

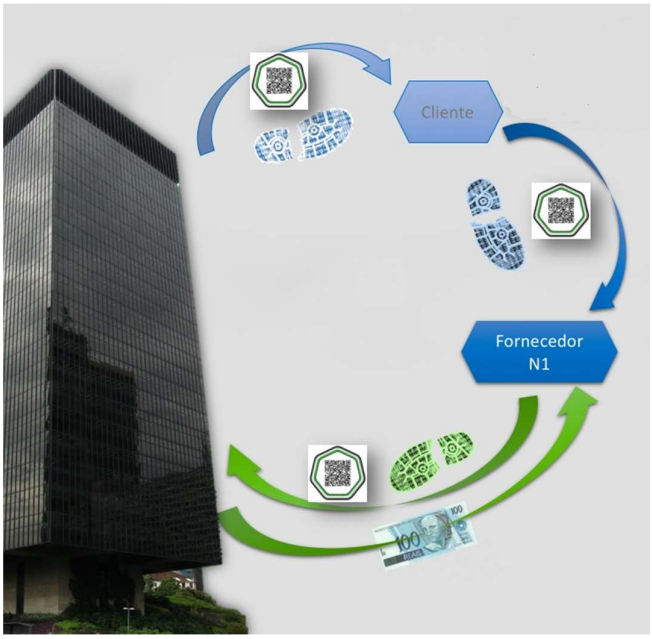


**Figura 1: Representação em alto nível do uso do BNDESToken**

Algumas soluções tecnológicas poderiam ter sido escolhidas para apresentar o caminho dos recursos financiados. Uma primeira solução é criar um sistema com banco de dados tradicional, uma API e uma camada WEB para disponibilizar funcionalidades de criação de contas, transferência de valores e painel de apresentação das informações. A inviolabilidade poderia ser garantida por procedimentos com controles internos e auditorias. A primeira desvantagem dessa solução é que os dados são geridos de forma centralizada. Do ponto de vista de um observador externo, a informação poderia ser manipulada pela instituição responsável com a anuência de auditores. Além disso, as auditorias são realizadas a posteriori enquanto o ideal é uma solução que garanta a inviolabilidade em tempo real. Uma terceira desvantagem é o alto custo e esforço para manter os procedimentos e auditorias citados.

O uso 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.

Uma segunda decisão é o uso de uma rede blockchain permissionada ou pública. A decisão nesse caso foi optar por uma rede pública por três motivos principais. O primeiro motivo é que quanto maior o número de nós que participam da decisão do algoritmo de consenso mais difícil é fraudar os dados. Hoje, existem blockchain públicas com milhares de nós. Para utilizar uma Blockchain permissionada com a mesma capacidade computacional seria necessário construir parcerias com diversas instituições que tivessem o interesse em entrar na rede como um nó, esse esforço inviabilizaria uma

prova de conceito realizada em pouco tempo. Numa rede permissionada com poucos nós, um observador externo poderia entender que existe a possibilidade de acordo entre os nós da rede no momento da execução do algoritmo de consenso. O segundo motivo é a própria transparência, característica, em certa análise, complementar à anterior. As blockchains públicas permitem que o monitoramento dos dados seja realizado sem que seja necessário a utilização de ferramentas fornecidas pelo BNDES. Qualquer um pode conectar seu software de monitoramento na blockchain pública e acompanhar os acontecimentos em tempo real. O terceiro motivo se deve ao fato de o BNDES já estar realizando uma prova de conceito com uma blockchain permissionada como discutido na Seção 4. Dentro da perspectiva de aprendizado organizacional no uso da tecnologia blockchain foi decidido utilizar uma blockchain pública. No entanto, essa decisão pode ser modificada no futuro.

Os critérios para a escolha da blockchain foram maturidade da solução e capacidade de execução de programas para expressar as regras do domínio de negócio. A decisão foi utilizar a blockchain da rede Ethereum porque, junto com a Bitcoin, apresenta maior maturidade do que as demais opções [Bartoletti e Pompianu 2017]. O Ethereum ainda permite a criação de contratos inteligentes bastante poderosos (Turing completo), capazes de garantir as regras de negócios necessárias. Essa capacidade de produzir contratos inteligentes complexos contrasta com a blockchain do Bitcoin que suporta scripts relativamente simples. No entanto, outras opções de blockchain podem ser investigadas no futuro.

Na plataforma Ethereum, 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, implementados como contratos inteligentes que mantêm os saldos de cada endereço e podem ser programados de acordo com padrões pré-definidos. A solução proposta utiliza o conhecido padrão ERC-20 como base e o complementa com as regras de negócios necessárias. O ERC-20 é o padrão de facto da plataforma Ethereum, tendo mais 500 diferentes token criados, que, juntos, gerenciam mais de US$25.000.000.000,00 [Baylina e Dafflon 2018].

O uso do padrão traz uma série de vantagens. Em primeiro lugar, conhecedores da plataforma Ethereum entendem muito mais facilmente o contrato, uma vez que grande parte dos seus métodos são herdados do token padrão. Em segundo lugar, alguns visualizadores de blockchain como o EtherScan (https://etherscan.io/) já possuem funcionalidades específicas para apresentar informações de contratos ERC-20. Por fim, é possível que programas da plataforma Ethereum capazes de executar métodos de contratos - como o My Ether Wallet (https://www.myetherwallet.com/) - evoluam para serem capazes de transacionar quaisquer tokens, assim como outros serviços que, com o tempo, possam vir a ser implementados em cima do ERC-20.

A parte central da solução consiste em utilizar um contrato ERC-20 para representar o BNDESToken. O contrato contém os saldos de todas as entidades que possuem BNDESToken e disponibiliza métodos como transferência de recursos, emissão e destruição de moeda além de visualização de saldo.

As subseções a seguir detalham como funciona a identificação de empresas, as transferências dos tokens, o acompanhamento das operações dos clientes e a transparência da solução.

## 2.1. Identificação de Pessoas Jurídicas

Para receber o BNDESToken, as pessoas jurídicas precisam ser previamente identificadas, por isso deve existir um mapeamento da identidade da pessoa jurídica no mundo real com a sua conta do Ethereum, de tal forma que seja uma garantia de que a pessoa jurídica é quem afirma ser. Esse mapeamento deve poder ser lido de forma confiável dentro do contrato inteligente do BNDESToken, ser válido por um período de tempo predeterminado e ser periodicamente revalidado.

Idealmente, o governo poderia prestar esse serviço, de forma similar ao que é realizado para pessoa física na Estônia com o programa de e-residência [e-Estonia 2018]. Se algum serviço oficial do governo registrasse esse mapeamento na blockchain ou provesse um serviço assinado digitalmente com o mapeamento, não haveria uma questão a ser resolvida.

Embora essa alternativa não exista, o governo mantém o Instituto Nacional de Tecnologia da Informação (http://www.iti.gov.br/), que coordena o funcionamento da ICP-Brasil. A Infraestrutura de Chaves Públicas Brasileira (http://www.iti.gov.br/icp-brasil) é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual das pessoas físicas e jurídicas. Um dos tipos de certificado digital é o e-CNPJ. O Certificado Digital e-CNPJ é um documento eletrônico de identidade que garante a autenticidade dos emissores e destinatários de documentos e dados que trafegam na internet, bem como assegura a privacidade e a inviolabilidade destes.

O e-CNPJ é utilizado para enviar ao governo informações trabalhistas, previdenciárias e fiscais. Segundo a Receita Federal [RFB1 2015] [RFB2 2015], desde o início de 2017, o uso de e-CNPJ é obrigatório para todas as pessoas jurídicas, exceto empresas optantes pelo Simples Nacional com até três empregados. Mesmo as pessoas jurídicas que não possuem o certificado podem vir a contratá-lo. Sendo assim, este artigo assume como premissa que as pessoas jurídicas que transacionam BNDESToken possuem o e-CNPJ.

A proposta de mapeamento para identidade deste artigo consiste em registrar um relacionamento entre o e-CNPJ e um endereço de carteira Ethereum pertencente à pessoa jurídica. A pessoa jurídica pode ser o cliente do BNDES ou um fornecedor do cliente (ou, em alguns casos, uma entidade de apoio ao financiamento, como é o caso da entidade repassadora para alguns projetos de doação). Se for o cliente, sua liberação de crédito é dividida em subcréditos em função das particularidades do projeto a ser desenvolvido pelo cliente. Deverá existir um mapeamento de identidade para cada subcrédito do cliente.

O mapeamento deve ser mantido de forma descentralizada. A ideia é que o usuário assine com o e-CNPJ um documento que associe explicitamente o CNPJ ao endereço da blockchain. Este mesmo usuário utiliza o mesmo endereço para enviar o documento assinado para a blockchain. O contrato inteligente que recebe essa informação realiza a validação da assinatura do documento através de um código implementado na própria blockchain. Se a assinatura for validada, como o próprio contrato tem certeza de que o dono do endereço foi quem executou a transação, fica explícito e garantido que a associação é válida.

A partir daí, qualquer caso de uso pode verificar apenas que a associação existe, podendo concentrar seu trabalho nas funcionalidades do seu próprio negócio. O caso de

uso de identificação da proposta deste artigo pode realizar as verificações necessárias ao cadastro do BNDES (por exemplo, impedimentos legais de uma empresa, certidões etc) antes de habilitar a pessoa jurídica a transacionar BNDESToken.

O mapeamento deve ser público. Com as informações abertas, observadores externos podem auditar e encontrar possíveis problemas na base de dados.

### 2.2. Transferências

Novos BNDESToken são emitidos quando ocorre uma liberação de recursos do BNDES para uma conta de um cliente habilitada, conforme discutido na subseção anterior. Esta transferência aumenta o saldo do cliente e o saldo total de tokens emitidos. Em geral, uma operação de financiamento pode ser realizada em uma ou mais liberações. Cada liberação acontece segundo cronograma acordado com o cliente, que pode, por exemplo, depender de marcos de entregas em um projeto.

O cliente pode registrar ordens de pagamento para fornecedores habilitados desde que possua saldo suficiente e a operação esteja de acordo com as regras de transferência. Em alguns cenários analisados, como pagamento de tributos, o cliente pode precisar resgatar uma parte do valor recebido.

Em algum momento, uma pessoa jurídica "pj" solicita a troca de BNDESTokens por Reais. A proposta é que isso ocorra do seguinte modo:

(1) a pessoa jurídica "*pj*" solicita o resgate de "*x*" BNDESTokens de um endereço seu, chamado "*cnt*";

(2) o contrato inteligente verifica se as regras de solicitação de resgate foram atendidas – por exemplo, o token já passou pelo número mínimo de pessoas jurídicas necessários e a solicitação está dentro do prazo;

(3) uma transferência é disparada no contrato inteligente de "*cnt*" para um endereço conhecido de resgate de propriedade do BNDES;

(4) o contrato inteligente destrói uma quantidade "*x*" de tokens e dispara um evento de solicitação de resgate;

(5) um sistema do BNDES recebe o evento de solicitação de resgate, verifica regras de negócios para garantir a validade e segurança da transação e, se necessário, realiza as realocações financeiras necessárias para viabilizar a transferência de "*x*" Reais - considerando a cotação de 1 Real - 1 BNDESToken já mencionada;

(6) O BNDES realiza uma transação bancária de "*x*" Reais para a conta bancária da pessoa jurídica "*pj*" informada no momento de seu cadastro e publica o comprovante de transferência;

(7) O BNDES registra que a transação bancária foi realizada e o contrato inteligente registra a realização da transferência bancária juntamente com algum dado de comprovação (por exemplo, o hash do documento de comprovação publicado no passo anterior);

(8) O sistema dispara um evento para indicar que realizou o resgate solicitado;

(9) Um sistema interessado de "*pj*" pode escutar o evento e realizar alguma ação de acordo com seus processos de negócios.

Outra opção avaliada para os passos 6 e 7 acima é enviar ao endereço de "*pj*" um montante equivalente a "x" em moeda digital, no caso Ether. A vantagem dessa opção é que toda a transação financeira seria realizada na própria blockchain, sem envolver o sistema bancário. No entanto, essa opção não foi adotada, pelo menos num primeiro momento, por três motivos. O primeiro é o alto risco cambial associado a variação do valor do Ether em relação a moedas fiduciárias. O segundo são os custos associados ao uso de uma corretora para trocar a moeda digital por moeda fiduciária, caso o solicitante de resgate queira utilizar moeda fiduciária. Por fim, essa opção introduz riscos regulatórios e maior mudança cultural de quem solicita o resgate.

### 2.3. Impactos no acompanhamento das operações

Depois que a operação é contratada, o cliente precisa prestar contas de alocação de recursos realizada. Trata-se do acompanhamento financeiro e físico.

Para realizar o acompanhamento financeiro, atualmente o cliente precisa enviar comprovantes bancários periodicamente ou depois de alguns marcos. Com o BNDESToken, todas as transações passam a ser automaticamente visíveis com hora de submissão para a rede e de confirmação da operação, minimizando atividades humanas e aumentando a confiabilidade das informações.

Para realizar o acompanhamento físico, o cliente precisa enviar documento comprovando como foi realizado cada gasto (por exemplo, nota fiscal de um produto adquirido). A proposta prevê o desenvolvimento de uma funcionalidade off-chain na qual o cliente possa descrever cada gasto e dar upload em documentos. Interessante observar que essa mudança incentiva que a comprovação seja realizada no momento da transferência do recurso para o fornecedor, e não a posteriori como é normalmente realizada atualmente.

### 2.4. Transparência

Qualquer observador externo pode visualizar as informações aderentes ao padrão ERC-20 em um programa navegador da blockchain utilizada. Para o Ethereum existe o previamente mencionado EtherScan. O navegador apresenta, por exemplo, o saldo total de BNDESTokens, quais endereços possuem o token e detalhes das transferências realizadas.

Para visualizar as informações específicas do domínio do BNDESToken, um observador pode desenvolver sua própria aplicação que lê os dados da blockchain, se registrar para receber eventos emitidos pelo contrato inteligente e acessar dados de serviços públicos que julgue confiáveis.

A proposta deste artigo prevê o desenvolvimento de um painel responsivo online, com o objetivo de facilitar o acompanhamento das transações, já que tal acompanhamento não depende de uma ferramenta construída pelo BNDES. Nessa aplicação, os dados da blockchain podem ser relacionados com dados off-chain para facilitar a interpretação do usuário. Por exemplo, o painel pode apresentar o nome de pessoas jurídicas ao invés do endereço do Ethereum e demonstrar as informações em gráficos de forma granular ou agregada. Além de apresentar detalhes para rastreamento das transferências, a proposta prevê que o painel tenha links adicionais para o EtherScan, para prestação de contas do cliente, para dados coletados de serviços online - como porte e localização das pessoas

jurídicas - e para dados gerenciados pelo BNDES como detalhamento dos projetos de financiamento.

## 3. Estado Atual de Implementação

O BNDES está trabalhando para conseguir realizar uma prova de conceito da proposta descrita na Seção 2 conforme descrito em [Rabin 2018]. O projeto foi priorizado para ser realizado após vencer um concurso de inovação interno com mais de trezentos concorrentes. O concurso, chamado ideiaLab, previu que as propostas vencedoras teriam seis meses para gerar um resultado inicial para o banco, quando então haveria uma reavaliação das prioridades. No momento atual, o BNDESToken possui pouco mais de três meses de projeto e uma equipe de cinco pessoas.

O desenvolvimento até o momento contempla uma versão inicial do contrato inteligente do BNDESToken, uma aplicação Web para facilitar a interação dos usuários e um painel online. O foco inicial do desenvolvimento foram as funcionalidades de transferência do token, acompanhamento do cliente e painel online. O desenvolvimento atual pressupõe a existência de clientes e fornecedores, sendo que o token sempre é desembolsado pelo BNDES para um cliente, que o repassa para um ou mais fornecedores. Estes fornecedores não podem repassar novamente o token, precisando solicitar o resgate ao BNDES, implementando, dessa forma, a segunda premissa descrita na Seção 2.

O módulo de identidade de pessoa jurídica ainda está sendo debatido pela equipe e será provavelmente implementado como um contrato inteligente independente para criar uma solução genérica a ser reutilizada por outras aplicações no futuro. O projeto tem como objetivo deixar esse legado para o país e está buscando parcerias, inclusive com o próprio ITI, para trabalhar nesse sentido. No momento atual, o próprio contrato inteligente do BNDESToken contém um mapeamento para pessoa jurídica de forma a viabilizar o uso das outras funcionalidades da aplicação.

O contrato inteligente do token é escrito em Solidity e está implantado na rede Rinkeby, uma das redes de teste do Ethereum. Para assinar as transações, o usuário precisa utilizar uma extensão do navegador, como o Metamask [Metamask 2018], cuja implementação ainda suporta apenas alguns navegadores. A aplicação utiliza linguagem JavaScript, sendo Angular e Typescript na camada de apresentação e NodeJS no servidor. O banco de dados MongoDB é utilizado para armazenar as informações que não vão para a blockchain. As integrações das aplicações desenvolvidas com os sistemas internos do banco não foram implementadas.

### 3.1. Armazenamento de dados

As estruturas de dados relevantes do contrato inteligente do BNDESToken são ilustradas na Tabela 1. Como mencionado na Seção 2, o BNDESToken segue o padrão ERC-20 e, portanto, mantém o saldo de cada endereço que se cadastra para utilizar o token (ver linha 1 da Tabela 1). Além disso, o contrato também contém qual o CNPJ de cada endereço Ethereum e, caso seja um cliente, a informação de qual a identificação do subcrédito do projeto de financiamento que está associado (ver linhas 2-6 da Tabela 1).

Tabela 1: Estruturas de dados mais relevantes do contrato inteligente do BNDESToken.

```
1. mapping (address => uint256) public balanceOf;
2. struct PJInfo {
```

```
3.      uint cnpj;
4.      uint idSubcredito;
5. }
6. mapping (address => PJInfo) public pjsInfo;
```

A aplicação WEB atualmente armazena no MongoDB informações cadastrais associadas a cada CNPJ – como email, telefone, localização, razão social, CNAE e dados bancários. Algumas dessas informações deixarão de ser armazenadas localmente quando forem desenvolvidas integrações para buscar dados associados a um CNPJ.

Para cada ordem de pagamento registrada, as seguintes informações são armazenadas em banco de dados: dados de identificação de origem e destino, descrição e documentos de suporte ao acompanhamento, o hash da transação gerada e data e hora que a transação foi solicitada pelo cliente. Estes dados são utilizados para compor a funcionalidade de acompanhamento de operações descrito na Subseção 2.3 e o painel online.

Para cada resgate, as seguintes informações são armazenadas em banco de dados: dados de identificação do fornecedor solicitante, dados bancários do fornecedor no momento da solicitação de resgate, a informação se o resgate está liquidado ou não, o hash da operação de solicitação da liquidação e da operação de liquidação propriamente dita e data e hora que a transação foi solicitada pelo fornecedor. Estes dados são utilizados para compor a funcionalidade de liquidação do resgate descrita no passo 7 da Subseção 2.2 e o painel online.

## 4. Trabalhos Relacionados

Um órgão de pesquisa e desenvolvimento do governo canadense, chamado National Research Council, anunciou recentemente um sistema, ainda em protótipo, para publicar como os recursos geridos estão sendo alocados aos projetos [NRC 2018]. O sistema armazena informações de projetos na blockchain pública do Ethereum. Apenas o desembolso inicial é tratado. Não há rastreio do que aconteceu com os recursos após a primeira movimentação da forma proposta por este trabalho.

O KfW (https://www.kfw.de/), banco de desenvolvimento Alemão, desenvolveu um sistema chamado TruBudget para rastrear o caminho dos recursos por meio do registro de cada passo dos fluxos de trabalho e aprovação, realizados por diferentes instituições parceiras que trabalham conjuntamente no financiamento e na implementação de projetos, minimizando o risco de fundos serem utilizados de forma incorreta (KfW 2017). Por permitir a definição de workflows de forma flexível, o sistema pode ser utilizado como instrumento de monitoramento e registro em diferentes cenários de uso de um projeto ou processo.

O TruBudget foi desenvolvido utilizando MultiChain [MultiChain 2018]. Por ser uma blockchain permissionada, as transações são realizadas sem a cobrança de taxa de encargo – uma vez que não é necessário remunerar os validadores das transações da rede. Além disso, é possível ter autonomia para definir quais nós participam da rede e quem visualiza as informações armazenadas. Dessa forma, os participantes da rede podem acordar se o acesso à informação na plataforma pode ser dado a outras partes interessadas ou ser aberta ao público tendo em vista que, dependendo do caso de uso, algumas informações podem estar sujeitas a restrições legais. Importante destacar que o TruBudget não define um token para pagamento, o que implica em menor risco regulatório e menor

esforço de implantação nos clientes, incluindo impacto em processos de negócios. Por outro lado, a utilização do token proposto por este artigo torna a solução mais segura visto que a transferência de recursos é inseparável do registro de cada passo do workflow do caminho do recurso.

O TruBudget está atualmente sendo implantado no BNDES para rastrear as doações de recursos para o Fundo Amazônia cuja procedência de recurso é majoritariamente da Noruega e Alemanha, por meio do KfW [Mari 2018]. O BNDES planeja executar provas de conceitos com beneficiários do Fundo Amazônia ainda esse semestre.

Além de bancos e governos, é possível encontrar soluções de rastreio de informações utilizando blockchain em outros domínios. Por exemplo, a Everledger possui um sistema de rastreio da cadeia de suprimentos de diamantes para garantir a procedência, minimizando falsificações e maximizando a utilização de um processo de extração adequado [Everledger 2018]. Entidades de recolhimento de recursos para caridade também estão utilizando blockchain para habilitar doação "ultra-transparente". Tendo inicialmente utilizado apenas o potencial das criptomoedas para facilitar a remessa de recursos, soluções como o GiveTrack [BitGive 2018] estão sendo desenvolvidas para dar mais transparência ao doador, que se interessa em saber se seu recurso chegou ao projeto, se já foi utilizado e como foi utilizado. Por fim, o órgão de distribuição de alimentos da ONU, WFP (World Food Programme) está utilizando uma solução para distribuição de tokens que podem ser trocados por alimentos em regiões de ajuda humanitária como campos de refugiados da Síria [WFP 2018]. O objetivo do projeto, chamado Building Blocks, que também contém uma solução de identificação pessoal por análise biométrica, é ter um meio mais eficiente e barato para distribuição da ajuda almejando inclusive integração com informação proveniente de órgãos de educação e saúde.

## 5. Conclusões e Próximos Passos

Blockchain tem se mostrado uma tecnologia muito promissora para o BNDES apresentar como esses recursos são movimentados na economia após o desembolso, servindo de insumo para pesquisas acerca da efetividade na contribuição para o desenvolvimento do país. Importante ressaltar que a proposta descrita neste artigo é generalizável para ser utilizada por outros bancos de desenvolvimento, órgãos de governo ou outras entidades que desejem rastrear os recursos desembolsados e analisar como foram utilizados.

O aprofundamento no entendimento da tecnologia durante o desenvolvimento da prova de conceito tem também despertado os autores do artigo para vantagens adicionais – como a simplificação do processo de acompanhamento para o cliente, a possível criação de novos produtos financeiros e a possibilidade de medir os reais efeitos das políticas de desenvolvimento. Os autores ainda entendem que, com a adoção crescente da tecnologia blockchain, o mundo terá cada vez mais compartilhamento de código, diminuindo os custos de transações de troca de valor.

Uma questão relevante originada com a mudança do modelo negócio pela introdução do BNDESToken é o possível impacto na forma como a relação de crédito é estabelecida. Atualmente o repasse de recursos do contrato em moeda fiduciária corrente se inicia no momento da liberação de crédito para o cliente. Com o uso da nova tecnologia, o momento da transferência de Reais é postergado até o resgate do BNDESToken.

Uma série de questões se apresentam, como, por exemplo: o que exatamente essa mudança pode implicar contratualmente? Quando começa a contar os juros do empréstimo? Como o BNDES pode investir os Reais que ainda não saíram do caixa? Existe algum impacto regulatório? Que tipo de instrumento financeiro é o BNDESToken em caso de uma disputa jurídica? Como tratar o sigilo empresarial e ou bancário quando as operações envolvem empresas? Como funciona o recolhimento de tributos quando uma transação é paga com BNDESTokens, e não com Reais? Quais procedimentos e verificações são necessários para habilitar um fornecedor? Essas são questões cruciais que os autores entendem que precisam ser debatidas.

Existem vários passos futuros para o projeto. Um primeiro ponto é explorar em mais detalhes a solução de identificação de pessoas jurídicas. Na proposta atual, aqueles funcionários que possuem acesso ao certificado digital possuem o poder total sobre os BNDESTokens. É necessário refletir como aumentar a flexibilidade da solução de forma a melhorar a governança e responsabilização dos funcionários das pessoas jurídicas.

Um segundo ponto é como tornar a experiência do usuário mais simples. Os conceitos e ferramentas de uso não estão massificados na sociedade. No caso estudado, por exemplo, os usuários que enviam transações para a rede Ethereum precisam instalar o Metamask e ter Ether para pagar a taxa de encargo da blockchain. E a sociedade em geral precisa ter mais amadurecimento nos conceitos para entender por que o uso da tecnologia aumenta a confiabilidade das informações apresentadas.

Um terceiro ponto é que atualmente todos os dados gravados na blockchain são públicos, mas é possível que o sigilo empresarial (como datas, preços e quantidade de insumos adquiridos, por exemplo) torne necessário dar privacidade a algumas informações. Esse requisito não foi considerado na proposta até o momento.

Outro ponto é reavaliar se Ethereum é realmente a plataforma de blockchain mais adequada para a solução. É necessário acompanhar o dinâmico desenvolvimento e amadurecimento do mercado de blockchain considerando os requisitos da solução, especialmente privacidade dos dados.

Os autores vislumbram também a construção de novos casos de uso em torno do BNDESToken. Por exemplo, cobrança automática de tributos, transferência de token associada a nota fiscal eletrônica e controle da região geográfica em que o BNDESToken pode ser utilizado impedindo, por exemplo, que seja utilizado fora de uma cidade ou que seja enviado para fora do Brasil.

Por fim, deve-se evoluir o desenvolvimento da prova de conceito e fazer teste em cenários reais para ter uma visão dos principais problemas a serem resolvidos e qual a prioridade de cada um deles.

## Referências

Bartoletti, M., Pompianu, L. (2017) “An empirical analysis of smart contracts: platforms, applications, and design patterns”, Financial Cryptography and Data Security, Springer.

Baylina, J., Dafflon, J. (2018) “ERC-777”, Ethereum Community Conference, France, https://www.youtube.com/watch?v=qcqhryzGTy0, Março.

BitGive (2018) “GiveTrack: Donation Tracking”, https://www.bitgivefoundation.org/givetrack-static/, Março.

Center for Technology in Government CTG (2018) “A working definition of e-government”, University at Albany https://www.ctg.albany.edu/publications/reports/future_of_egov?chapter=2, Março.

Edelman, R. (2018) “2018 Edelman Trust Barometer”. https://www.edelman.com/trust-barometer, Março.

e-Estonia. “e-identity” https://e-estonia.com/solutions/e-identity/e-residency/

Everledger (2018) “Diamond Time-Lapse Protocol”, https://www.everledger.io/, Março.

KfW (2017) “Blockchain boosts effectiveness of development cooperation”, https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Press-Releases/Pressemitteilungen-Details_426112.html, Março.

Mari, A. (2018) “Brazilian and German development banks agree blockchain partnership”, http://www.zdnet.com/article/brazilian-and-german-development-banks-agree-blockchain-partnership/, Março.

Metamask (2018) “Metamask - Bring Ethereum to your browser”, https://metamask.io/, Março.

MultiChain (2018) “MultiChain – Open Platform for Building Blockchains”, https://www.multichain.com/, Março.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, Março.

National Research Council of Canada NRC (2018). “Blockchain Publishing Prototype”, https://nrc-cnrc.explorecatena.com/en/, Março.

Peck, M. E. (2017) “Do You Need a Blockchain?”, https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain, IEEE Spectrum, Março.

Rabin, C. G. (2018) “BNDES Criará Token no Blockchain da Ethereum”, https://portaldobitcoin.com/bndes-criara-token-no-blockchain-da-ethereum/, Março.

Receita Federal do Brasil RFB1 (2015) “Informações sobre a Obrigatoriedade de Utilização de Certificado Digital”, http://idg.receita.fazenda.gov.br/orientacao/tributaria/senhas-e-procuracoes/senhas/certificados-digitais/informacoes-sobre-a-obrigatoriedade-de-utilizacao-de-certificado-digital-com-atualizacoes-da-in-rfb-no-1-036-2010, Março.

Receita Federal do Brasil RFB2 (2015) “Resolução nº 125”, http://www8.receita.fazenda.gov.br/simplesnacional/noticias/NoticiaCompleta.aspx?id=8bb40fb6-5eff-418d-b38b-987f8b90e762, Março.

Tapscott, D. and Tapscott, A. (2016) “Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World”.

World Food Programme WFP (2018) “Building Blocks”, http://innovation.wfp.org/project/building-blocks, Março.

Wood, G. (2014) “Ethereum: A secure decentralised generalised transaction ledger”, https://ethereum.github.io/yellowpaper/paper.pdf, Março.