Pontifícia Universidade Católica
do Rio de Janeiro

Vinicius Portes Giglio

Utilização de Blockchain para monitoramento de pagamentos em programas de Financiamento do Governo:
O Programa Minha Casa Minha Vida como Exemplo

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Orientador: Leonardo Gomes Lima

Rio de Janeiro,

Abril de 2019

Pontifícia Universidade Católica
do Rio de Janeiro

Vinicius Portes Giglio

Utilização de Blockchain para monitoramento de pagamentos em programas de Financiamento do Governo: O Programa Minha Casa Minha Vida como Exemplo

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Prof. Leonardo Gomes Lima
Orientador
Departamento de Administração - PUC-Rio

Prof. Marcelo Cabus Klotzle
Departamento de Administração - PUC-Rio

Prof. Carlos de Lamare Bastian Pinto
Pesquisador Autônomo

Rio de Janeiro,24 Abril de 2019

Vinicius Portes Giglio

Engenheiro de Produção formado pela PUC-Rio (Pontifícia Universidade Católica do Rio de Janeiro), Mestrado em Administração de Empresas com ênfase em Finanças, além de pós-graduação MBA em Management, ambos pela mesma instituição de ensino. Background em Gestão de Projetos, Performance Operacional, Performance Financeira, Empreendedorismo, Mentoria para Start-ups. Possui Competências técnicas em Modelagem Financeira, Análise de Dados Estatísticos, Finanças Corporativas, Valuation, Contabilidade, Econometria, Métodos de Apoio e Decisão, Gestão de Projetos, Estratégia de Negócios, Precificação e Marketing.

Ficha Catalográfica

Giglio, Vinicius Portes

Utilização de Blockchain para monitoramento de pagamentos em programas de financiamento do Governo : o Programa Minha Casa Minha Vida como exemplo / Vinicius Portes Giglio ; orientador: Leonardo Lima. – 2019.

63 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Administração, 2019.

Inclui bibliografia

1. Administração – Teses. 2. Blockchain. 3. Gestão da identidade digital BNDES. 4. BNDESToken. 5. Minha Casa Minha Vida. 6. Governo digital. I. Lima, Leonardo. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Administração. III. Título.

CDD:658

Agradecimentos

Agradecimento a meus pais por todos os ensinamentos ao longo da vida que permitiram ,me desenvolver para me tornar um indivíduo único na sociedade, com senso crítico, opiniões e visões próprias. A minha mãe, que sempre me ensinou a ser uma pessoa humana em um mundo tão “frio” com o ser humano, e que ser o melhor que o ser humano pode ser e é uma mera questão de vontade. A meu pai, que sempre me ensinou que minha liberdade terminava onde a do outro começava e que minha liberdade só era limitada pela minha responsabilidade por meus próprios atos. Antagonismo reflexivo que me fez ser quem sou. Apesar de forma indireta, esses foram os ensinamentos que me passaram, mesmo sem saber, e que carregarei comigo e passarei adiante.

A minha namorada, Nicole Casares, que me viu noites em claro e sua única preocupação era com meu bem-estar, e cuidou de mim do começo ao fim desse processo de escrita. Admirável compaixão e coração que jamais esquecerei.

Agradecimento aos meus companheiros de classe, dos quais tive trocas de oportunidade e pude conhecer outros mercados, visões, opiniões e criar laços com alguns para demais negócios. Em especial a Hugo Carlo e Claudia Bozza, parceiros que levarei para vida.

Agradecimentos aos professores do curso, que tornaram as longas horas do curso mais prazerosas com suas didáticas e conhecimentos excepcionais. Em especial, ao meu Orientador Leonardo Lima, cuja confiança em meu trabalho foi tão grande que me forneceu total autonomia de escolha, modus faciende e permitiu que desenvolvesse algo de interesse de um jeito que acreditei fazer alguma diferença na forma como as transações econômicas ocorrem no Brasil.

Por fim, aos ensinamentos da vida, que não foram poucos, mas que gostaria de resumí-los com uma frase de um grande ídolo: “Toda ação racional é, em primeiro lugar, ação individual. Apenas o indivíduo pensa. Apenas os indivíduos racionalizam. Apenas o indivíduo age.” (Ludwig Von Mises). Que sirva como inspiração para que mais pessoas pensem e ajam por conta própria em pro de um país e mundo melhor.

Resumo

Portes Giglio, Vinicius; Lima, Leonardo Gomes. **Utilização de Blockchain para monitoramento de pagamentos em programas de Financiamento do Governo: O Programa Minha Casa Minha Vida como Exemplo**. Rio de Janeiro, 2019.63p.Trabalho de Conclusão de Curso –Mestrado Profissional em Administração – IAG - Escola de Negócios da PUC-Rio - Departamento de Administração. Pontifícia Universidade Católica do Rio de Janeiro.

Uso da tecnologia Blockchain no setor governamental, permitindo um rastreamento e transparência de suas transações. Inicialmente, realizando um estudo de caso brasileiro do Banco Nacional de Desenvolvimento (BNDES) e,a posteriori, propondo a ampliação para outro programa denominado "Minha Casa Minha Vida". No primeiro caso, apenas pessoas jurídicas estariam cadastradas no modelo, no segundo, seriam necessários nós emissores que fossem pessoas físicas: ou seja, haveria a necessidade da gestão da identidade física digital da população. O estudo proposto prevê a expansão do uso da tecnologia, bem como, o avanço nos benefícios diretos e indiretos ao incluir pessoas físicas no blockchain governamental.

Palavras- chave

Blockchain; Gestão da Identidade Digital; BNDES; BNDESToken; Minha Casa Minha Vida; Governo Digital.

Abstract

Portes Giglio, Vinicius; Lima, Leonardo Gomes (advisor). **Use of Blockchain to monitor payments in Government Financing programs: Minha Casa Minha Vida program as example.** Rio de Janeiro, 2019. 63p. Trabalho de Conclusão de Curso –Mestrado Profissional em Administração – IAG - Escola de Negócios da PUC-Rio - Departamento de Administração. Pontifícia Universidade Católica do Rio de Janeiro.

Use of Blockchain technology in the government sector, allowing tracking and transparency of your transactions. Initially, conducting a Brazilian case study of the National Development Bank (BNDES) and, a posteriori, proposing the extension to another program called "Minha Casa Minha Vida". In the first case, only legal entities would be registered in the model, in the second, we would need issuers that were persons: that is, the need to manage the digital physical identity of the population. The proposed study predicts the expansion of technology use as well as the advancement in direct and indirect benefits by including individuals in the government blockchain.

Keywords

Blockchain; digital physical identity management; BNDES; BNDESToken; My home My Life; Digital Government.

Sumário

1. Introdução 10

2. A Tecnologia Blockchain e SmartContracts 13
2.1. Estrutura da Blockchain 15
2.1.1. Os Blocos 15
2.1.2. Tempo do Bloco 16
2.1.3. Hard Forks 17
2.1.4. Descentralização 17
2.1.5. Tipos de Blockchain 18
2.2. SmartContracts 21
2.2.1. Descrição de SmartContracts 21
2.2.2. Questões de Segurança 22

3. O Modelo de Negócio Minha Casa Minha Vida desenvolvido em Blockchain 23
3.1. Descrição do Programa Minha Casa Minha Vida 23
3.1.1. Quem tem direito 24
3.1.2. Modus Operandi a Ser Analisado 25

4. Aplicação na Gestão Pública com destaque para o caso BNDESToken 26
4.1. Os Casos de Aplicação 26
4.1.1. Votação Eletrônica 26
4.1.2. Gestão de Identidade de Pessoas 27
4.1.3. Controle de Acesso 27
4.1.4. Pagamento de Programas Sociais 27
4.1.5. Controle de Ativos 28
4.2. Caso BNDESToken – Rastreando os recursos do BNDES utilizando Blockchain 29
4.2.1. Contextualização 29
4.2.2. BNDESToken 31

4.2.3. Identificação dos Nós 35
4.2.4. As Transações e Registros 37
4.2.5. Acompanhamento das Operações 38
4.2.6. Transparência 39
4.2.7. Estágio Atual 39
4.3. Outros Casos Correlatos 40

5. Uma Proposta de Modelo do Minha Casa Minha Vida em Blockchain 43
5.1. Modelo operacional da Blockchain 43
5.2. Nós envolvidos e permissionamentos 44
5.2.1. Ministério das Cidades – Nó validador 44
5.2.2. Caixa Econômica Federal – Nó validador 45
5.2.3. Fornecimento de Crédito 45
5.2.4. Retomada do Imóvel 45
5.2.5. Repasse a Construtora 45
5.2.6. Construtora – Nó membro 46
5.2.7. Beneficiários – Nó membro 46
5.3. O Modus Operandi 46
5.3.1. Aprovação de um projeto 47
5.3.2. Fluxo de pagamentos de um beneficiário 49
5.3.3. Cadastro de um beneficiário e Construtora 52
5.4. Vantagens deste Modelo Proposto 53

6. Conclusão 55

7. Referências bibliográficas 59

Lista de figuras

Figura 1 - Processo de Aprovação de um projeto habitacional 47
Figura 2 - Processo de Cadastro de um beneficiário e o modelo de rastreamento de pagamentos 50
Figura 3 - Modelo de Cadastro de um Nó na Blockchain 52

1.Introdução

Em 2008, foi apresentado pela primeira vez, ao grupo “The Cryptography Mailing” um artigo (Nakamoto, 2008), no qual constavam os princípios de funcionamento de uma criptomoeda moeda mundial. Essa moeda digital funcionava em uma rede peer-to-peer, permitindo envio de pagamentos online de forma segura, sem necessidade de intermediários para os participantes da rede. A autoria desse artigo é anônima e está sob o pseudônimo de “Satoshi Nakamoto”.

O software original foi disponibilizado sob licenciamento do MIT e, em 2009, a rede começou a funcionar emitindo seu primeiro bloco. Atualmente, estima-se que existam aproximadamente 18 milhões de bitcoins em circulação.

Suspeitava-se que, em primeiro momento, a criação da rede Bitcoin era de autoria de um grupo de programadores. Entretanto, em versão mais recente,mais precisamente, em maio de 2016, um empresário australiano denominado Craig Wright, se identificou como o mentor e idealizador da criptomoeda. Gavin Andresen, cientista-chefe da Bitcoin Foundation, confirmou em seu blog que está convencido de que Craig e Satoshi são a mesma pessoa. (Techtudo, 2016).

Blockchain é a plataforma tencnológica utilizada por trás da Bitcoin, primeira e mais difundida aplicação da tecnologia Blockchain. Atualmente, existem inúmeras criptomoedas em circulação nomundo, entretanto o Bitcoin é aquele que apresenta o maior marketshare. As aplicações da tecnologiaBlockchain associadas às criptomoedas, fazem parte da primeira geraçãodessa tecnologia e são denominadas Blockchain 1.0.

Após o surgimento das primeiras criptomoedas, vários especialistas começaram a observar propriedades intrínsecas à Blockchain, dentre elas, ressaltam-se a segurança na transação, resiliência, inviolabilidade e imutabilidade. Tais propriedades podem ser aplicadas para solucionar inúmeras questões da sociedade. Sob essa ótica, as plataformas começaram a evoluir, visando permitir a inserção de transações mais complexas através de contratos inteligentes (smart contracts).

Isso culminou no surgimento de uma nova tecnologia denominada Blockchain 2.0.

Essa tecnologia gerou uma grande expectativa e deu um novo rumo à tecnologia Blockchain tanto que, em 2015, a revista Britânica The Economist considerou a tecnologia Blockchian como “The Next Big Thing” (Economist, 2015). E, em 2016, a Gartner posicionou a Blockchain no topo do Gartner Hype Cycle for Emerging Tecnologies (Gartner, 2016), como podemos constatar na imagem abaixo.

Desde então, inúmeros investimentos têm sido realizados na tecnologia Blockchain. Percebemos um crescimento do surgimento de startups com foco nessa tecnologia, bem como o direcionamento de recursos de grandes empresas. Temos como exemplo a IBM, que transferiu o código da sua plataforma de desenvolvimento Blockchain para a Linux Foundation, constituindo, junto com outras iniciativas, a plataforma Hypeledger[1].

“DistributedLedger Technology” (DLT) é o nome genérico da tecnologia, sendo a Blockchain um tipo específico de DLT, entre outros. Muitos especialistas colocam a DLT como o próximo passo da internet, criando a IntenetofValue (internet do valor), que permitiria o dinheiro fluir na rede tão livremente quanto os dados fluem atualmente. Em comparação paralela, essa tecnologia seria capaz de afetar a relação com transações, assim como o GPS afetou o transporte de pessoas, com aplicativos de navegação. (Plansky, et al., 2016).

Com isso exposto, este trabalho tem como objetivo mostrar um modelo de negócios novo, no qual o programa habitacional “Minha Casa Minha Vida”, poderia ser desenvolvido dentro de uma ledger distribuída.

Será apresentado o funcionamento padrão de uma Blockchain, assim como suas funcionalidades, tais como a de Smart Contract, que viabiliza operações complexas com alto grau de segurança e com altíssima velocidade. Veremos, em seguida, as principais aplicações na Gestão Pública, tal como a Gestão de Identidade de Pessoas, principal ganho que será apresentado nessa tese, em relação ao modelo do BNDES Token, que apenas possui pessoas jurídicas como nó.

Demonstraremos como o funcionamento dessa Blockchain funcionaria por meio de um gráfico de uso, além de apresentar iniciativas correlatas ao redor do mundo.

Esse trabalho tem como principal objetivo, demonstrar o ganho da aplicação da Blockchain nesse modelo de negócio de gestão pública em um sistema

[1]https://www.hyperledger.org/about

habitacional.Além disso, objetiva-se ainiciação de uma gestão da identidade Pessoal de cada cidadão do país, permitindo assim, uma maior integração entre sistemas da federação e cruzamento de dados que, não só facilitariam a vida do indivíduo, , como reduziriam os custos de operação do nosso estado.

Na “Introdução”, abordamos de forma sucinta a temática do presente trabalho, que, a posteriori, é melhor detalhada. Na seção seguinte, “A Tecnologia Blockchain e SmartContracts”, descrevemos com maior clareza o funcionamento da Tecnologia e seus benefícios de modo geral, visto que esta tecnologia é o cerne para essa tese e será aplicada a um caso prático. No capítulo “O Modelo de Negócio Minha Casa Minha Vida desenvolvido em Blockchain”, utilizamos o caso “BNDESToken” como referência e o ampliamos para inclusão de pessoas físicas no sistema. Não podemos deixar de seguir sem falar das demais formas de “Aplicação na Gestão Pública com destaque para o caso BNDESToken”, afinal, esse foi o pioneiro em nosso País. Por fim, verificamos o programa “Minha Casa Minha Vida” e fazemos “Uma Proposta de Modelo do Minha Casa Minha Vida em Blockchain”, passando por processos que podem ser automatizados, desburocratizando, agilizando e reduzindo custos do programa. Além de fornecer transparência total do fluxo monetário e dos beneficiários do programa. Por fim, na “Conclusão”, demonstramos os benefícios da adoção do programa, além de demonstrar que há ainda dúvidas em relação a regulamentação e adoção do sistema proposto.

2.A Tecnologia Blockchain e SmartContracts

A tecnologia Blockchain pode ser entendida de várias formas. Em linhas gerais, pode-se dizer que se trata de um sistema distribuído de base de dados em log, mantido e gerido de forma compartilhada e descentralizada (através de uma rede peer-to-peer, P2P), na qual todos os participantes são responsáveis por armazenar e manter a base de dados.

De uma forma mais técnica, um blockchain, (Economist, 2015) originalmente blockchain (cadeia de bloco), (Brito, et al., 2013) é um livro razão de registros, chamados blocos, que são ligados usando criptografia. (Economist, 2015). Cada bloco contém um hash criptográfico do bloco anterior, um registro de data e hora e dados de transação (geralmente representados como um hash da raiz da árvore de merkle.

Em outras palavras, Block Chain é uma estrutura de dados, na qual o registro atual, depende de informações do anterior, criando o encadeamento de registros. Um grupo de registros é agrupado em um bloco, e este bloco é criptografado ao bloco anterior. Quando um novo bloco é gerado, este é criptografado no conjunto de blocos criptografados anteriormente, e assim sucessivamente, criando uma Block Chain, cadeia de blocos. Sendo assim, a alteração de um registro, implica na alteração dos registros subsequentes, impossibilitando a alteração de um registro passado, sem que isso seja detectado.

Devido a esse design de blocos, um blockchain é resistente à modificação dos dados. É "um livro aberto e distribuído que pode registrar transações entre duas partes de maneira eficiente e verificável e permanente". (Iansiti, et al., 2017). Para uso como um ledger distribuído, um blockchain é normalmente gerenciado por uma rede ponto a ponto (peer-to-peer),aderindo coletivamente a um protocolo para comunicação entre nós e validando novos blocos. Uma vez registrados, os dados em qualquer um dos blocosmembros,não podem ser alterados retroativamente, sem alteração de todos os blocos subsequentes o que requer consenso da maioria da rede. Embora os registros blockchain não sejam inalteráveis, blockchains podem ser considerados seguros por design e exemplificam um sistema de computação distribuído com alta tolerância a falhas

bizantinas. O consenso descentralizado foi, portanto, reivindicado com uma característica para o funcionamento da blockchain. (Raval, 2016).

Esse Sistema Distribuído de Base de Dados é denominado DistributedLedger Technology (DLT), o novo paradigma de arquitetura de sistemas multipartite, no qual as partes envolvidas em uma transação detém a mesma visão da verdade, asseguradas pelo sistema by design, através de regras de consenso definidas pelo modelo de negócio.

O armazenamento de responsabilidade dos participantes no modelo peer-to-peer, faz com que todos os participantes possuam o registro de todas as transações e, consequentemente, todos podem realizar a auditoria das transações, que são aprovadas por consenso, a depender do modelo escolhido pela blockchain utilizada.

Sendo assim,a tecnologia Blockchain é construída de um DLT que utiliza blockchain, tendo em mente quatro principais características estruturais : segurança das operações, descentralização de armazenamento/ computação, integridade de dados e imutabilidade de transações.

Percebe-se, então, que a blockchain funciona como um “ledgeroffacts” (livro razão dos fatos), no qual os usuários detém uma cópia de todos os registros das transações. Em suma: O “ledger” é um livro de registros digital, em que, uma vez validado o registro pela metodologia da blockchain, este nunca mais poderá ser apagado. O “fact”, por sua vez, pode ser representado por uma transação monetária, por um conteúdo de determinado documento, ou, até mesmo,por um programa de computador, contendo, em algumas plataformas, uma base de dados pequena.

Os peers são os participantes da rede, também chamados de “nós”, que podem ou não ser anônimos, a depender do funcionamento de cada blockchain.

As transações são protegidas por tecnologias criptográficas de assinaturas digitais, inclusive para identificação dos peers emissores e receptores.

Sendo assim, quando um nó deseja adicionar ao ledger um fato novo, é necessário um consenso entre todos ou alguns nós previamente determinados da rede, para decidir se um fato pode ou não ser registrado no ledger. Havendo consenso, o fato será escrito e nunca mais poderá ser apagado.Em tese, um processo levemente semelhante à escritura e registro de um imóvel no Brasil.

Temos, então, por definição:

- Fato: transação, conteúdo digital, programa de computador ou outros permissionamentos e ações.

- Bloco: conjunto de fatos, geralmente com número pré-fixado pela rede.
- Cadeia de blocos (Blockchain): conjunto de blocos encadeados (conectados um a um) seguindo uma lógica matemática, ou seja, dependentes entre si.

  Ledger:Livro razão no qual se encontrarão os registros

A evolução para contratos inteligentes, permitiu um grande progresso nas aplicações de Blockchain. Os referidos contratos são programas de computador replicados e executados por todos os nósda rede ou, por um conjunto predeterminado de nós denominadosvalidadores.Aplicações baseadas em contratos inteligentes são chamadas ”DecentralizedApplications” ou “Dapps”.

2.1.**Estrutura da Blockchain**

Um blockchain é um livro razão digital descentralizado, distribuído e público, que é usado para registrar transações em muitos computadores. De forma que qualquer registro na rede não possa ser alterado retroativamente, sem a alteração de todos os blocos subsequentes, o que requer o consenso de todos os nós membros da rede. (Economist, 2015) (Armstrong, 2016). Isso permite que os participantes verifiquem e auditem transações de forma independente, relativamente barata e em tempo real. (Catalini, et al., 2016). Devido ao consenso e armazenagem nos nós, o banco de dados blockchain é gerenciado de forma autônoma usando uma rede peer-to-peer e um servidor distribuído de timestamping. Eles são autenticados pela colaboração em massa alimentada por interesses coletivos. (Tapscott, et al., 2016) Esse design facilita o fluxo de trabalho robusto, onde a incerteza dos participantes em relação à segurança de dados é marginal. Um blockchain foi descrito como um protocolo de troca de valores. (Bheemaiah, 2015) Umblockchain pode manter os direitos de propriedade porque, quando configurado adequadamente para detalhar o contrato de troca, ele fornece um registro que obriga a oferta e a aceitação.

2.1.1.Os Blocos

Cada bloco contém um lote de transações válidas, que são codificadas em uma árvore Merkle (Economist, 2015). Cada bloco inclui o hash criptográfico do

bloco anterior no blockchain, ligando os dois. Os blocos ligados formam uma cadeia de blocos criptografados entre si (Economist, 2015). Esse processo interativo confirma a integridade do bloco anterior, percorrendo todo o caminho de volta ao bloco da gênese original. (Bhaskar, et al., 2016). Algumas vezes, blocos podem ser produzidos simultaneamente, criando uma bifurcação temporária. Há um histórico seguro baseado em hash: qualquer blockchain tem um algoritmo específico para marcar diferentes versões do histórico, de modo que um com um valor mais alto possa ser selecionado sobre outros. Esses blocos que não foram selecionados para serem incluídos na cadeia,são chamados de blocos órfãos (Bhaskar, et al., 2016). Os pares que suportam o banco de dados têm versões diferentes do histórico de tempos em tempos. O sistema manterá apenas a versão com maior pontuação do banco de dados conhecido. Sempre que um par recebe uma versão com maior pontuação (geralmente a versão antiga com um único novo bloco adicionado), ele amplia ou subscreve seu próprio banco de dados e retransmite a melhoria para seus pares. Não há, entretanto, uma garantia absoluta de que qualquer entrada em particular permanecerá na melhor versão da história para sempre. Para isso, os blockchains são normalmente construídos com a norma de adicionar a pontuação de novos blocos, em blocos antigos, além de receberem incentivos para estender com novos blocos em vez de substituir blocos antigos. Dessa forma, a probabilidade de uma entrada ser substituída é reduzida exponencialmente (Bhaskar, et al., 2016) à medida que mais blocos são construídos sobre ela, eventualmente tornando-se muito baixos. (Economist, 2015) (Antonopoulos, 2014) (Nakamoto, 2008). Por exemplo, o bitcoinutiliza um sistema de prova de trabalho, em que a cadeia com a prova de trabalho mais cumulativa é considerada válida pela rede. Há vários métodos que podem ser usados para demonstrar um nível suficiente de computação. Dentro de uma blockchain, o cálculo é realizado de forma redundante, e não da forma tradicional segregada e paralela.

2.1.2.Tempo do Bloco

O tempo que a Blockchain leva para gerar um bloco extra em sua rede é denominado de tempo de bloqueio.(Ghayas, 2018). Alguns blockchains criam um novo bloco com uma frequência de cinco em cinco segundos. No momento da conclusão do bloco, os dados incluídos se tornam verificáveis. Em cryptocurrency, isso é praticamente quando a transação ocorre, portanto, um tempo de bloqueio

mais curto significa transações mais rápidas. O tempo de bloqueio para Ethereum, utilizada pelo BNDESToken, é definido entre 14 e 15 segundos, enquanto que para bitcoin é de 10 minutos.

2.1.3.Hard Forks

Um Hard Fork é uma mudança de regra. Tal mudança faz com que o software que valida as transações de acordo com as regras antigas, tenham seus blocos inválidos – de acordo com as novas regras. No caso de um Hard Fork, todos os nós destinados a trabalhar de acordo com as novas regras precisam de atualização de software.

Há a possibilidade de falta de consenso, ou seja, um grupo de nós pode optar em continuar a usar o software antigo, enquanto os outros nós usam o novo software, o que pode vir a gerar uma divisão. À exemplo, temos a Ethereum,que se esforçou para se manter únicoaos investidores do The DAO, que haviam sido invadidos, explorando uma vulnerabilidade em seu código. Neste caso, o garfo resultou em uma divisão, criando as atuais correntes Ethereum e Ethereum Classic. Em 2014, a comunidade Nxt foi convidada a considerar um Hard Fork,que teria levado a uma reversão dos registros blockchain para mitigar os efeitos de um roubo de 50 milhões de NXT que ocorreu em uma grande transação dacriptomoeda. A proposta do Hard Fork foi rejeitada e alguns dos fundos foram recuperados após negociações e pagamento de resgate.

Para evitar uma divisão permanente, a maioria dos nós que usam o novo software podem retornar às regras antigas, como foi o caso do bitcoin dividido em 12 de março de 2013. (Lee, 2013)

2.1.4.Descentralização

O armazenamento de dados em rede peer-to-peer, caso do blockchain, elimina inúmeros riscos que acompanham os dados sendo mantidos centralmente. (Economist, 2015). O blockchain descentralizado pode usar passagem de mensagens ad-hoc e rede distribuída.

As blockchainpeer-to-peer, por definição, não possuem pontos centralizados de vulnerabilidade que os hackers de computador podem explorar. Assim sendo, não tem ponto central de falha. Os métodos de segurança Blockchain, incluem o

uso de criptografia de chave pública. (Brito, et al., 2013): Uma chave pública é formada por uma longa seqüência de números aleatórios que servem como um endereço no blockchain. Os tokens da rede são os valores enviados pela rede, sendo que esses são registrados como pertencentes a um endereço. Uma chave privada funciona como uma senha que dá a seu proprietário acesso a seus ativos digitais e os meios para interagir com os vários recursos que blockchains agora suportam. Os dados armazenados no blockchain geralmente são considerados incorruptíveis. (Economist, 2015).

Todos os nós em um sistema descentralizado possuem uma cópia de todoblockchain: ou seja, todos os registros estão copiados em todos os nós. Assim sendo, a qualidade dos dados é mantida e garantida pela replicação de todo o banco de dados massiva (Iansiti, et al., 2017) e na confiança computacional. Nesse modelo, não existe uma cópia "oficial" centralizada e nenhum usuário ostentam grau de confiança a mais do que qualquer outro. (Brito, et al., 2013). As transações são realizadas na rede usando o software. As mensagens são entregues com base no melhor esforço. Os nós carregam o papel de mineração e validam as transações, (Bhaskar, et al., 2016) adicionando-os ao bloco que estão em construção e, posteriormente, transmitem o bloco completo para outros nós. (Antonopoulos, 2014). Blockchains podem usar vários esquemas de marcação de tempo, como prova de trabalho, para serializar alterações. (The Mission to Decentralize the Internet, 2013). Métodos alternativos de consenso incluem comprovação de estaca. (Antonopoulos, 2014) O crescimento de uma blockchain descentralizada é acompanhado pelo risco de centralização, porque os recursos computacionais necessários para processar grandes quantidades de dados se tornam mais caros. (Gervais, et al., 2016).

2.1.5.Tipos de Blockchain

2.1.5.1.Acesso Aberto – Pública

Um blockchain público não tem absolutamente nenhuma restrição de acesso. Qualquer pessoa pode se tornar um nó, ou seja, pode enviar transações e se tornar um validador (qualquer indivíduo, indiscriminadamente, pode participar da execução de um protocolo de consenso). (Catalini, et al., 2016). Geralmente,

essas redes oferecem incentivos econômicos para aqueles que protegem e utilizam algum tipo de algoritmo de Prova de Estaca ou Prova de Trabalho.

A principal vantagem de uma rede blockchain aberta, sem permissão, ou pública, é que a proteção contra os maus atores não é necessária e nenhum controle de acesso é necessário. (Antonopoulos, 2014). Isso significa que os aplicativos podem ser adicionados à rede sem a aprovação ou a confiança de outras pessoas, usando o blockchain como uma camada de transporte. (Antonopoulos, 2014).

O Bitcoin e outras criptomoedas, atualmente protegem seu blockchain exigindo novas entradas para incluir uma prova de trabalho. Para prolongar o blockchain, o bitcoin usa quebra-cabeças Hashcash. Enquanto Hashcash foi projetado em 1997 por Adam Back, a idéia original foi proposta pela primeira vez por Cynthia Dwork e MoniNaor e Eli Ponyatovski em seu artigo de 1992 "Pricing via Processing ou CombattingJunk Mail".

As empresas do setor financeiro não priorizaram os blockchains descentralizados (Buntinx, 2016). Em 2016, o investimento de capital de risco para projetos relacionados à blockchain estavamem declínio nos EUA, mas aumentando na China. (Ovenden, 2016). Bitcoin e muitas outras criptomoedas usam blockchains abertos (públicos). A partir de abril de 2018, o bitcoin tem a maior capitalização de mercado.

2.1.5.2.Acesso Autorizado – Privada

Um blockchain privado é permissionado. (Marvin, 2017). Não é possível ingressar no sistema, a menos que haja convite pelos administradores da rede. O acesso do participante e validador é restrito.

Esse tipo de blockchainé considerado um meio termo para empresas interessadas na tecnologia blockchain em geral, mas que não se sentem confortáveis com o nível de controle oferecido pelas redes públicas. Normalmente, essas empresas buscam incorporar blockchain em seus procedimentos de contabilidade e manutenção de registros, sem sacrificar a autonomia e correr o risco de expor dados sensíveis à Internet pública. É uma forma de criar processos mais eficientes, eficazes e seguros a baixo custo.

Os blockchains permissionados usam uma camada de controle de acesso para determinar quem tem acesso à rede. (Marvin, 2017). Em contraste com as redes públicas de blockchain, os validadores em redes de blockchain privadas,

são controlados pelo proprietário da rede, podendo ser uma entidade jurídica ou, até mesmo, o governo. Eles não dependem de nós anônimos para validar transações, tampoucose beneficiam do efeito de rede. (Prisco, 2016). Os blockchainspermissionadostambém podem ser denominados blockchains 'consorciados' ou 'híbridos'.

O New York Times observou em 2016 e 2017, que muitas corporações estão usando redes blockchain "com blockchains privados, independentes do sistema público". (Popper, 2016) (Popper, 2017).

2.1.5.3.Consortium Blockchain

Um blockchain de consórcio é um blockchainsemi-descentralizado. Ele também é permitido, mas em vez de uma única organização o controlando, existem várias empresas que podem operar um nó em tal rede. Os administradores de uma cadeia de consórcio restringem os direitos de leitura dos usuários como bem entenderem e permitem apenas um conjunto limitado de nós confiáveis para executar um protocolo de consenso.

2.1.5.4.BNDESToken

Atualmente, as redes Blockchain são divididas em dois grandes grupos: (i) as redes públicas ou de acesso aberto (permissionless) e (ii) as redes privadas ou de acesso autorizado (permissioned). A figura a seguir mostra algumas características de tais redes.

As redes públicas, ou não permissionadas,apresentamregras próprias para validação e todos os nós integrantes são validadores, além de poderem iniciar ou receber uma transação. De modo geral, seus validadores são anônimos. O principal exemplo que temos desse tipo de rede é o Bitcoin.

As redes privadas, ou premissionadas, dispõe de regras legais e regulatórias em seu sistema. Apresentam também dois tipos de nós. O primeiro tipo é o nó validador que goza de permissão para validar, iniciar ou receber uma transação. O segundo tipo é o nó membro, que somente inicia e recebe uma transação. Os nós são um grupo pré-selecionado, que podem ou não ser anônimos. Suas principais funções são para meio corporativo e até governamental, utilizando como

identificação do nó, o próprio CPF (Certidão de Pessoa Física) ou CNPJ (Cadastro Nacional de Pessoa Jurídica) para os nós membros.

No estudo de Caso do BNDESToken, perceberemos que eles utilizam o modelo da rede privada, na qual o CNPJ é o identificador do nó, permitindo assim o rastreamento dos pagamentos e liberações de crédito.

O processo de validação ocorre quando um nó da rede, seguindo um conjunto de regras bem definidas, consegue montar um bloco que, nesse exemplo, é um conjunto de transações monetárias utilizando a criptomoeda. Vale lembrar que o nó validador escolhe um número definido de transações não processadas da rede para montar o bloco.

Vários nós estão fazendo a mesma coisa simultaneamente, mas não necessariamente com as mesmas transações, ou seja, o processo de montagem do bloco depende das transações ainda não processadas visíveis ao nó. Há uma competição entre os nós para validar determinadas transações antes dos concorrentes. No Bitcoin, tal processo de validação é denominado mineração, no qual o nó finaliza o processo de montagem do bloco, quando resolve uma expressão matemática computacionalmente custosa.

2.2.**SmartContracts**

2.2.1.Descrição de SmartContracts

Um smartcontract (contrato inteligente) é um protocolo de computador destinado a facilitar, verificar, ou impor digitalmente a negociação ou a execução de um contrato, seguindo as regras pré-programadas de forma eficiente, eficaz e de baixo custo. Contratos inteligentes permitem o desempenho de transações confiáveis, sem o intermédio de terceiros. Essas transações são rastreáveis e irreversíveis, visto que ocorrem em uma Blockchain.

Nos contratos inteligentes, muitas cláusulas contratuais podem ser parcial ou totalmente auto-executáveis, auto-impingidasou ambos. O objetivo dos contratos inteligentes é fornecer segurança superior à lei tradicional dos contratos e reduzir outros custos de transação associados à contratação. Várias criptomoedas implementaram tipos de contratos inteligentes.

Szabo propõe que o contrato inteligente pode ser utilizado por registros de ativos replicados (Szabo, 2014) e a execução do contrato, usando cadeias de hash criptográficas e replicação tolerante a falhas bizantinas. Askemos

implementou essa abordagem em 2002 (Wittenberger, 2002), usando Scheme e,posteriormente, adicionando SQLite (Möbius, 2009) (Watzke, 2010) como linguagem de script de contrato. (Heinker, 2007).

2.2.2.Questões de Segurança

Um contrato inteligente é "um protocolo de transação informatizado que executa os termos de um contrato". (Tapscott, et al., 2016). Um contrato inteligente baseado em blockchain é visível para todos os usuários, nós, do referido blockchain, incluindo todas as suas regras de operação e condicionais. No entanto, isso leva a uma situação em que bugs, incluindo falhas de segurança, são visíveis para todos, mas devido ao consenso da rede, podem não ser rapidamente corrigidos. (Peck, 2016)

Um ataque, difícil de corrigir rapidamente, foi executado com sucesso no DAO, em junho de 2016, drenando US $ 50 milhões em Ether, enquanto os desenvolvedores tentavam chegar a uma solução que obtivesse consenso. (DuPont, 2017). O programa DAO teve um atraso no tempo antes que o hacker pudesse remover os fundos; um Hard Fork do software Ethereum fora realizado para recuperar os fundos do atacante, antes que o tempo limite expirasse.

Questões nos smartcontracts da Ethereum, em particular, incluem ambigüidades e construções fáceis, mas inseguras em sua linguagem contratual Solidity, bugs do compilador, bugs do Ethereum Virtual Machine, ataques à rede blockchain, e à imutabilidade de bugs (Atzei, et al., 2017).

3.O Modelo de Negócio Minha Casa Minha Vida desenvolvido em Blockchain

3.1.**Descrição do Programa Minha Casa Minha Vida**

Devemos começar afirmando que esse Programa está vinculado à Secretaria Nacional de Habitação do Ministério das Cidades, que coordena a autorização dos benefícios, em parceria com a Caixa Econômica Federal, o Banco do Brasil, os governos e as entidades locais.

O Programa “Minha Casa, Minha Vida”, amplamente referenciado como PMCMV, foi lançado em março de 2009, pelo Governo Federal. O PMCMV tem como objetivo o subsídio, a aquisição da casa ou apartamento próprio para famílias com renda até 1,8 mil reais, facilitando as condições de acesso, tais como subsídio de taxas e condições de pagamento específicas, ao imóvel para famílias com renda até de 7 mil. (CEF, 2019) (MdC, 2019). Ressalta-se que a compra da moradia não precisa necessariamente ocorrer em área urbana, podendo ser em área rural também. Sua finalidade, então, é viabilizar o acesso à moradia própria para famílias com renda bruta mensal de até R$ 9.000.

O programa possui cinco modalidades para a Faixa 1 de renda (famílias com renda de até 1,8 mil reais): Empresas, entidades, FGTS, Municípios com até 50 mil habitantes e rural. Cada modalidade visa o atendimento de um público específico. Os recursos do MCMV são do orçamento do Ministério das Cidades repassados para a Caixa Econômica Federal (Portal Brasil, 2019).

No ano de 2017, o programa “Minha Casa, Minha Vida”, no governo de Michel Temer, sofreu algumas mudanças importantes. Inicialmente, o programa teve a adesão da faixa 1,5 entre meio a faixa 1 e 2. O Programa também teve mudanças na renda máxima das faixas 1,5 e 2, aumentando para até R$2.600,00 na Faixa 1,5 e até R$4.000,00 na faixa 2 (PMCMV, 2017).

Vale ressaltar que, desde 2009, foram ofertadas quase 3 milhões de unidades habitacionais. E, em 2016, iniciou-se a fase 3 do Programa, que tem a expectativa de entregar 4,6 milhões de residências até o término da etapa.

Quanto ao prazo de financiamento, o “Minha Casa, Minha Vida”, possibilita financiamentos de até 360 meses, o que equivale a 30 anos, porém há uma faixa

etária limite para a amortização: 80 anos. Sendo assim, em um procedimento individual, a escolha do período máximo para o financiamento, se dá a partir da idade do financiador. Por exemplo, caso a pessoa que proponha o financiamento tenha até 50 anos, ela obtém a capacidade de conseguir um prazo de até 30 anos. Mas caso o comprador tenha 60 anos, as prestações deverão ser feitas em até 20 anos.

3.1.1.Quem tem direito

O Beneficiário é classificado em faixas de acordo com sua renda, conforme classificação abaixo: (PMCMV, 2019).

No Programa “Minha Casa, Minha Vida”, também denominado PMCV, o imóvel financiado pela Caixa Econômica Federal é dado como garantia de pagamento ao financiamento feito própria CAIXA. Isso significa que a família pode utilizar o imóvel durante o tempo em que durar o contrato, mas caso ocorra a inadimplência ou o descumprimento das regras até o fim do contrato desse imóvel, poderá haver a rescisão contratual.

Faixa 1 – Famílias com renda de até R$1.800,00. A Caixa Econômica Federal oferece vantagens para a família. A mesma tem direito até a 90% do valor do imóvel, pagos pelo governo, e, o restante pode ser financiado em até 120 meses, sendo que as parcelas do financiamento jamais deverão ser maiores que 10% da renda mensal familiar.

Faixa 1,5 - Famílias com renda de até R$ 2.600,00. Nessa faixa, é possível a aquisição de um imóvel cujo empreendimento é financiado pela Caixa com taxas de juros de apenas 5% ao ano e até 30 anos para pagar e subsídios de até 47,5 mil reais. Como podemos verificar, há subsídio da taxa quando a comparamos com a taxa SELIC (Bacen, 2019), atualmente em 6,5% ao ano.

FAIXA 2 – Famílias com renda de até R$4.000,00. Nessa faixa, os benefícios do Programa “Minha Casa, Minha Vida” são aplicados de acordo com cada contexto, que possibilitam uma benesse de até R$ 29 mil e os juros equivalentes variam entre 5,5% e 7%.

FAIXA 3: Para famílias com renda bruta de até R$ 9.000,00. Dependendo da renda familiar, a taxa cobrada pode ser de 8,16% às famílias com renda bruta de até R$ 7.000 por mês e de 9,16% às que dispõem de R$ 9.000 mensais. Nessa etapa, não há subsídios para colaborar com a entrada no imóvel. Contudo, as

taxas de juros ao ano têm a vantagem de estarem abaixo do mercado, de modo geral.

Para as famílias que integram as outras Faixas do Programa, com renda bruta mensal de até R$ 9.000, é possível garantir o próprio imóvel contatando a Caixa Econômica Federal, Banco do Brasil ou uma Incorporadora e Construtora parceira do Programa. Nessa situação, os documentos e as opções de imóveis serão analisados, a simulação de financiamento será feita e os requisitos para efetuar a compra serão apresentados no ato.

3.1.2.Modus Operandi a Ser Analisado

Os recursos do PMCMV (programa “Minha Casa, Minha Vida”), são do orçamento do Ministério das Cidades repassados para a Caixa Econômica Federal (CEF), que é o agente operacional do programa.

Para atender à Faixa 1, nas modalidades Empresas e Entidades, a CEF e o Banco do Brasil analisam e aprovam a contratação dos projetos apresentados pelas construtoras, conforme as diretrizes definidas pelo Ministério das Cidades. A liberação dos recursos ocorre a cada medição de obra.

Nas demais faixas de renda e modalidades, os recursos são repassados pelo Ministério das Cidades à CEF diretamente para subsidiar os contratos de financiamento dos interessados na aquisição do imóvel tanto na área urbana como na rural. Espera-se, desse modo, a contrapartida dos municípios de construção da infraestrutura externa, assim como alguns equipamentos públicos como escolas, postos de saúde e creches.

4.Aplicação na Gestão Pública com destaque para o caso BNDESToken

O presente capítulo, tem como propósito demonstrar inúmeros ganhos de aplicação da blockchain para a gestão pública, ressaltando ainda o caso do BNDESToken. O mesmo já se encontra em fase de estruturação, e os elementos operacionais podem ser trazidos para o modelo de negócio que aqui nos propomos a realizar.

4.1.Os Casos de Aplicação

Conforme já mencionado, com os avanços da tecnologia da Blockchain e os smartcontracts, as possibilidades de aplicação da tecnologia cresceram de modo significativo, indo além das criptomoedas – forma pela qual a tecnologia ainda é mais conhecida. Esses avanços permitiram aplicações mais complexas, , tais como controle de imóveis, cadeias de produção e até mesmo gestão de identidade digital de coisas e pessoas.

Essas aplicações, alinhadas com as vantagens da Blockchain, como a maior transparência nas transações (fatos) e seus membros (nós), permitem a redução de fraudes na rede, por exemplo, e o maior compartilhamento de dados, favorecendo o desenvolvimento de inúmeras aplicações, inclusive governamentais.

4.1.1.Votação Eletrônica

Pensando no sistema de votação eletrônica, podemos utilizar a Blockchain como solução. Essa permitiria que o cidadão (nó) ao votar, registrasse seu voto, que seria validado de acordo com normas - biometria, por exemplo - e o voto seria registrado de forma imutável. Além disso, com a norma interna de um registro por nó membro, seria impossível que o indivíduo realizasse dois votos. Logo, teríamos uma confiança maior no modelo, graças à imutabilidade dos registros e pelo fato da auditoria ser realizada de forma mais precisa e eficaz. e eficaz.

4.1.2.Gestão de Identidade de Pessoas

Atualmente, possuímos no Brasil inúmeros registros para um único cidadão, tais como CPF (Certidão de Pessoa Física), Identidade, Número da CNH (Carteira Nacional de Habilitação), além de outros para fins específicos, como militares e previdenciários. A aplicação da Blockchain permitiria a unificação em um único número, além do cruzamento de todos os dados existentes. O cidadão passaria a ter uma Identidade digital, onde tudo seria registrado, desde recebimentos, empréstimos, multas e afins. O cidadão portaria, de forma centralizada e segura, todos os seus dados. E o governo passaria a poder consultar de forma rápida e ágil todos os dados necessários de um determinado cidadão. Agilizando, por exemplo, dados para justiça e declaração de Imposto de Renda - tanto para o cidadão quanto para a receita Federal.

4.1.3.Controle de Acesso

O controle de acesso, ou permissionamento de acesso, pode ser realizado tanto no sentido físico quanto no digital. O histórico de acesso a um determinado documento confidencial, precisaria ser aprovado por nós validadores, sendo assim, teríamos um processo de aprovação do acesso, assim como o registro dos nós que o validaram, como os nós membros que solicitaram o acesso e os que permitiram o acesso.

4.1.4.Pagamento de Programas Sociais

Será utilizado o exemplo do programa Bolsa Família para exemplificar esse item. O Bolsa Família tem como objetivo a distribuição da renda realizando um pagamento por parte do governo a cidadãos que preencham uma determinada lista de requisitos. Com a **Gestão de Identidade de Pessoas** e com o **smartcontracts**, é possível verificar quais cidadãos preenchem esses critérios e, devido à integração e agilidade do sistema, realizar a revisão disso periodicamente de forma automática e com baixíssimo custo. Sendo assim, os beneficiários seriam revistos com uma frequência maior que atualmente, além de não gerar custo para o governo. Temos também o fato de o pagamento ser cadastrado na Blockchain, ou seja, podemos verificar os beneficiários (nós

membros) que receberam tal benefício e em que período receberam. Caso um nó deixe de preencher algum critério, ele automaticamente deixaria de ser beneficiário. Sendo assim, os custos burocráticos para a implementação de Programas sociais como o Bolsa Família, se reduziriam drasticamente, além de reduzir a quase zero o risco de fraude ou desvio de verba pública.

4.1.5.Controle de Ativos

O controle de ativos permite o rastreio e o controle dos ativos, desde a aquisição até o descarte. Esses ativos abrangeriam seu histórico armazenado, permitindo averiguar gastos com manutenção preventiva, assim como, o resultado de sua operação. Podemos citar a gestão de ativos administrativos do governo. A exemplo, gestão de equipamentos do estilo notebook de um estado, que, se controlados via Blockchain, viabilizaria uma compra centralizada com os custos rateados entre as prefeituras, podendo gerar ganhos na negociação devido à escala. Além de compra antecipada em casos de excesso de defeitos ou proximidade de obsolescência.

Estudos de viabilidade desses projetos têm sido amplamente pesquisados ao redor do mundo. A Comissão Européia (CE) está investigando o potencial da Tecnologia, inclusive com aprovação da criação de uma força tarefa dedicada ao estudo do assunto. Além do incentivo, através do Horizon 2020, às startups, juntamente com potenciais investidores, parceiros de negócio, universidade e centros de pesquisa no desenvolvimento de soluções utilizando a tecnologia.

Outro governo interessado é o governo do Reino Unido, que tem tratado o assunto de forma estruturada. No final de 2015, divulgou um relatório denominado “Distributed Ledger Technology: beyond blockchain” (Government Office for Science, 2015). Trata-se de um dos relatórios mais completos realizados por um governo, sobre a tecnologia, suas aplicações, aspectos regulatórios e perspectivas.

Destaca-se também o US Federal Reserve, o banco central dos EUA, que lançou, no início de dezembro de 2016, o relatório sobre a tecnologia denominado “Distributed ledger technology in payments, clearing, and settlement”. Na visão do banco central, as aplicações da tecnologia ainda estão em estágio inicial, ainda terão uma série de desafios a serem superados para o desenvolvimento e adoção de plataformas baseadas em Blockchain em larga escala e de forma cotidiana,

ressaltando-se questões em torno de casos de negócios, barreiras tecnológicas, considerações legais e de gerenciamento de risco.

Dentre outros países e iniciativas, podemos destacar: i) Estônia, com o sistema de e-residency program, com a Identidade Digital e seu plano de saúde com registros médicos rastreáveis; ii) Suíça, com seu sistema de transações imobiliárias; iii) Reino Unido, com seu sistema de distribuição de benefícios, departamento de trabalho e pensões.

A expectativa é alta por parte do mercado, de governos, assim como das comunidades acadêmicas e de desenvolvedores de solução, em relação ao futuro da tecnologia Blockchain. Alguns especialistas chegam a considerá-la o quinto paradigma disruptivo da computação, que poderá trazer uma experiência ubíqua de internet do valor (Swan, 2015).

Durante o Consesus Summit (Coindesk, 2016), foi realizada uma entrevista com 243 especialistas em Blockchain de startups e empresas de grande porte, onde concluiu-se que: i) 86% dos entrevistados acreditam que a tecnologia terá impacto nos serviços financeiros, enquanto 14% acreditam que é muito cedo para concluir algo; ii) 70% acreditam que a tecnologia terá impacto em aplicações de governo e outras áreas não financeiras; iii) 52% acreditam que será necessário ainda de 5 a 10 anos para a uma adoção ampla da tecnologia.

Os bancos centrais têm demonstrado alto interesse e estas instituições provavelmente seguirão avaliando os impactos tecnológicos, regulatórios, oferta de novos serviços, assim como nos modelos de negócios atuais. As principais instituições financeiras estão agora explorando a tecnologia, com destaque para os governos da Ásia, mas no Brasil, o assunto também vem ganhando atenção.

Palestras sobre Blockchain foram apresentadas no Ciab FEBRABAN 2016. No evento, os principais bancos do país, Itaú e Bradesco, anunciaram a associação ao consórcio R3. Os especialistas que se apresentaram no evento foram categóricos ao afirmar que: a Distributed Ledger Technology é uma ruptura tão importante para os serviços financeiros como foi a Internet (Coindesk, 2016).

4.2.**Caso BNDESToken – Rastreando os recursos do BNDES utilizando Blockchain**

4.2.1.Contextualização

A confiança está em crise no mundo inteiro (Edelman, 2018). A internet e as redes sociais deram a possibilidade de propagação de informação, com grau de

alcance superior aos meios de mídia tradicionais e abrangendo um público ainda maior. Em decorrência dessa facilidade e agilidade com a qual a informação é capaz de trafegar na rede, a população começou a demandar uma maior transparência do governo, além de agilidade em suas respostas e resultados.

Uma das soluções mais pesquisadas para suprir tal demanda é o chamado Governo Digital ("e-government") que utiliza de serviços de tecnologia da informação para engajar cidadãos (CTG, 2018). Apesar de inúmeras tecnologias poderem ser utilizadas para suprir essa demanda, a mais pesquisada atualmente é a Blockchain, que tem se mostrado eficaz transmitindo maior transparência e segurança nas transações registradas.

A tecnologia de blockchain é a mais nova maneira de viabilizar transações e armazenar seus dados gerados de forma distribuída, ou seja, onde cada nó possui o registro de todas as transações, sendo uma alternativa aos sistemas centralizados tradicionais. Isso permite que a informação seja imutável, pois mais de um nó deteria a cópia de tudo o que ocorreu, e ao conciliar as contas, teríamos inúmeras "provas reais". Esse modelo também permite dispensar a necessidade de uma parte intermediária confiável para gerenciar as informações, visto que os nós são capazes de gerenciar a rede como um todo. Nesse modelo, as informações são armazenadas em uma rede peer-to-peer, após o consenso, com critérios previamente definidos pela rede blockchain em questão, entre os nós participantes. 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, et al., 2016) afirma que a Blockchain é o caminho para melhorar a prestação de serviços, ao mesmo tempo que garante a integridade e transparência das informações. Os exemplos de uso da tecnologia por parte do governo não se limitam aos supracitados, mas também incluem armazenamento antifraude de registros públicos, como propriedades privadas e antecedentes criminais; identificação digital de pessoa física ou jurídica; e digitalização da moeda nacional.

Veremos a seguir o caso do BNDESToken, mecanismo desenvolvido pelo Banco BNDES, para rastrear os recursos públicos utilizados em projetos de financiamento pelo banco. Abordaremos previamente alguns aspectos técnicos do mecanismo para sua melhor compreensão, para que posteriormente possamos

ver que esse mecanismo pode ser utilizado em modelos similares, como o programa “Minha Casa Minha Vida”.

4.2.2.BNDESToken

O Banco BNDES desenvolveu o BNDESToken, com o intuito de rastrear a aplicação dos recursos públicos em projetos de financiamento do BNDES. Assim, o banco pode fornecer à sociedade informações de como esses recursos estão sendo aplicados e promovendo o desenvolvimento do país.

Um fato importante do BNDESToken é a sua paridade, ou seja, cada unidade do BNDESToken equivale a um Real (1:1). Diferente de criptomoedas de blockchain públicas, cuja cotação é flutuante, a blockchain privada do BNDES apresenta cotação fixa, como um modo simples de criar uma marcação na moeda nacional. Assim sendo, o BNDESToken é distribuído nos financiamentos e, em todo momento, o token é propriedade de quem teria a propriedade do Real referente ao financiamento. Como a blockchain privada do BNDES apresenta como característica o não anonimato, a tecnologia permite verificar quem está em posse do token, obtendo-se, então, 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. Como dito coloquialmente, é a “Tokenização” de um ativo, no caso, do real.

Para que haja a adoção da proposta, é necessário que seis premissas sejam atendidas. A primeira premissa é que a emissão do token não representa aumento da base monetária à economia, afinal, esta é de responsabilidade do Bacen, o BNDES deixa de liberar o Real físico, mas o mantém como lastro. Dessa forma, é possível simplificar e reduzir o risco jurídico e regulatório da operação. A segunda premissa é que o BNDESToken não pode ser repassado indefinidamente. O BNDES somente 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 limitação de transferência, visa evitar a criação de um mercado secundário do uso do token, o que poderia introduzir risco regulatório ou mercado negro. A terceira premissa 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. Ressalta-se que pessoas físicas podem ser contempladas em um momento posterior, com

melhorias de sistema e da tecnologia, como, por exemplo, com a adoção da cidadania digital, previamente mencionada. A quinta premissa é que os tokens são fungíveis. Essa escolha foi feita para facilitar a implementação, não existindo, assim, um identificador único para cada BNDESToken, tornando-os todos iguais. Caso em momento futuro seja necessário rastrear algum recurso de forma segregada ou com mais detalhes que dos demais, será necessário rever essa última simplificação. A sexta e última premissa é que, por simplicidade de implementação, os eventos de transferência não são automaticamente relacionados com marcos do projeto de financiamento.

Dadas as premissas para o funcionamento do sistema, algumas soluções tecnológicas poderiam ter sido escolhidas, para que o rastreamento do caminho dos recursos financiados do banco fosse realizado com eficácia. Uma das possíveis soluções seria criar um sistema com banco de dados nos moldes tradicionais, com uma API e uma camada WEB para disponibilizar as funcionalidades de criação de contas, as de transferência de valores e um painel de apresentação das informações e fluxo do financiamento em questão. Para garantir a inviolabilidade das informações, poderiam ser utilizados mecanismos como os de controles internos e auditorias, tanto próprios quanto de terceiros. Percebemos logo a primeira desvantagem dessa solução: a de que os dados são geridos de forma centralizada. Do ponto de vista de um observador externo, a centralização da informação poderia permitir que essa fosse manipulada pela instituição responsável, tanto de forma consciente como não consciente e com a anuência de auditores. Outro grande porém, é que as auditorias são realizadas à posteriori, enquanto o ideal seria uma solução que garantisse a inviolabilidade em tempo real. Ou seja: os dados poderiam ser violados, e, apenas em gestões futuras, seríamos capazes de identificar o que aconteceu. Já a terceira desvantagem, diz respeito ao alto custo e esforço para manter de forma contínua os procedimentos onerosos de auditorias já mencionados.

Quando verificamos a tecnologia blockchain e suas principais características, conforme mencionado em sessões anteriores, constatamos que é um mecanismo para que a sociedade confie na inviolabilidade das informações de forma irrefutável, sem a necessidade de uma relação de confiança com a entidade centralizadora. Essa descentralização não só reduz o custo de transação, como garante maior confiança ao sistema, devido a quase impossível possibilidade de consenso de algo errado. Além disso, permite o monitoramento em tempo real, e não à posteriori como auditorias atualmente fazem, da aplicação dos recursos. Podendo ser implementado por qualquer pessoa interessada,

permite-se o monitoramento das informações na blockchain com seus dados de transação abertos para consulta em tempo real.

Uma segunda decisão seria o uso de uma rede blockchain permissionada ou pública, conforme já descrito e definido anteriormente. A decisão que leva a ação pela blokchain permissionada envolve três motivos essenciais. O primeiro motivo leva em conta a confiança no consenso da rede. Quanto mais nós têm permissão para validar um fato na rede, mais nós participam da decisão do algoritmo, logo, mais difícil é fraudar os dados na blockchain. Nos dias de hoje, poderíamos citar a existência de inúmeras blockchains públicas com milhares de nós. Uma Blockchain permissionada que possuísse a menor capacidade computacional poderia construir parcerias estratégicas com diversas instituições que tivessem o interesse em entrar na rede como um nó. Sendo assim, esse esforço inviabilizaria uma prova de conceito realizada em pouco tempo. Caso a rede permissionada possuísse 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, reduzindo assim a confiabilidade do sistema proposto. O segundo motivo é a própria transparência, característica 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, visto que toda transação é registrada em um book of facts públicos, com os chaveamentos adequados. Sendo assim, qualquer pessoa pode conectar seu software de monitoramento na blockchain pública e acompanhar os acontecimentos em tempo real, ou seja, qualquer pessoa tem a capacidade de ser a própria auditoria do sistema, em tempo hábil e de forma eficaz. O terceiro motivo, se deve ao fato de o BNDES já estar realizando uma prova de conceito com uma blockchain permissionada. 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.

Expostos esses dados, os critérios para a adoção da blockchain envolveram a maturidade da solução e sua capacidade de execução de programas, para expressar as regras do domínio de negócio. A decisão, então foi de utilizar a blockchain da rede Ethereum porque, junto com a Bitcoin, apresenta maior maturidade comparado às demais opções (Bartoletti, et al., 2017). O Ethereum ainda permite a criação de contratos inteligentes (smartcontracts), como visto anteriormente, bastante poderosos (Turing

completo), pois são capazes de garantir que as regras necessárias dos negócios sejam seguidas para serem colocadas no book of facts. Essa capacidade da Ethereum de produzir contratos inteligentes complexos, contrasta com a blockchain do Bitcoin, que apenas suporta scripts relativamente simples. No entanto, outras opções de blockchain podem ser investigadas no futuro, conforme avanço das pesquisas relacionadas ao tema.

A plataforma Ethereum apresenta uma diferença crucial em relação à Bitcoin, nela o conceito de token representa um ativo digital cujo valor pode ou não ter uma correspondência com um ativo real. Sendo assim, a "Tokenização" de ativos reais se torna possível, permitindo uma agilidade em sua troca por meios virtuais, por exemplo. Os tokens são, eles próprios, implementados como contratos inteligentes, que mantém 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 fato da plataforma Ethereum, tendo mais de 500 diferentes tokens criados, que, juntos, gerenciam mais de US$25.000.000.000,00 (Baylina, et al., 2018).

A escolha de uma Blockchain já consolidada traz uma série de vantagens. Em primeiro lugar, podemos citar o fato de os conhecedores da plataforma Ethereum entenderem muito mais facilmente o modus operandi do contrato, uma vez que grande parte dos seus métodos são herdados do token padrão. Em segundo lugar, alguns visualizadores de blockchain como o EtherScan[2] já detém funcionalidades específicas para apresentar informações de contratos ERC-20, ou seja, o usuário já passa a ter uma gama de ferramentas para monitoramento do sistema. Por fim, é possível que programas da plataforma Ethereum, que são capazes de executar métodos de contratos – a exemplo, o MyEther Wallet[3] - podem evoluir 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.

Conclui-se, então, que a parte central da solução consiste em utilizar um contrato ERC-20, padrão da rede Ethereum, para representar o BNDESToken, que possui paridade com o Real Brasileiro (1:1). O contrato contém os saldos

[2]https://etherscan.io/

[3]https://www.myetherwallet.com/

de todas as entidades que possuem BNDESToken e estarão disponíveis, seus métodos de transferência de recursos, emissão e destruição de moeda, além de visualização de saldo para os nós integrantes.

4.2.3.Identificação dos Nós

Deve-se começar esclarecendo que a identificação dos nós que farão parte da rede são os CNPJ para os quais o BNDES fornecerá financiamentos. Porém, seu modelo de identificação pode vir a ser expandido para pessoas físicas e serve como modelo para outros sistemas.

Sendo assim, 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. Assim, podemos garantir que a pessoa jurídica é quem afirma ser. Esse mapeamento, ressalta-se, 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. Garantindo que mudanças nas atividades econômicas das empresas ou até mesmo seu encerramento sejam mapeados e, consequentemente, categorizados como aptos ou não a receber financiamentos de forma adequada.

Idealmente, o governo poderia prestar esse serviço, caso possuísse como programa a cidadania digital, de forma similar ao que é realizado para pessoa física na Estônia, não só pioneira como mais avançada nesse quesito, com o programa de e-residência (e-Estonia, 2018). Se algum serviço oficial do governo registrasse esse mapeamento, tanto de pessoas físicas como de pessoas jurídicas, na blockchain ou provesse um serviço assinado digitalmente com o mapeamento, não haveria uma questão a ser resolvida. Se considerarmos que outras entidades podem precisar do mesmo mapeamento, teríamos redundância de processos, o que poderia ser resolvido com a centralização dessa atividade nas mãos do governo.

Embora essa alternativa ainda não exista, o governo mantém o Instituto Nacional de Tecnologia da Informação[4], que coordena o funcionamento da ICP-Brasil. A ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira[5]- é uma cadeia

[4] http://www.iti.gov.br/

[5]http://www.iti.gov.br/icpbrasil

hierárquica de alta confiança que cuida da emissão de certificados digitais para identificação virtual, tanto para pessoas físicas como para pessoas jurídicas. Um dos tipos de certificado digital é o e-CNPJ, relevante para o cadastro no BNDESToken. 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.

Atualmente, o e-CNPJ é utilizado apenas 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, assumimos como premissa que as pessoas jurídicas que transacionam BNDESToken possuem o e-CNPJ e que este é um dos chaveamentos para controle.

A proposta de mapeamento para identidade consiste em registrar um relacionamento entre o e-CNPJ e um endereço de carteira Ethereum pertencente à pessoa jurídica, ou seja, criando uma relação um-para-um, ou uma chave com a qual podemos identificar tudo relacionado ao e-CNPJ. A pessoa jurídica pode ser qualquer player da operação, desde um cliente do BNDES, um fornecedor do cliente ou, até mesmo, uma entidade de apoio ao financiamento, como é o caso da entidade repassadora para alguns projetos de doação. Cada caso com suas particularidades, por exemplo, se for o cliente, sua liberação de crédito é dividida em subcréditos em função das particularidades do projeto a ser desenvolvido pelo cliente, sendo assim, deverá existir um mapeamento de identidade para cada subcrédito do cliente

Esse mapeamento deve ser mantido de forma descentralizada. A ideia proposta é que o usuário possa assinar com o e-CNPJ um documento que associe explicitamente o seu CNPJ ao endereço da blockchain do BNDES. Este mesmo usuário utiliza o mesmo endereço para enviar o documento assinado para a blockchain. O contrato inteligente que receberá essa informação realizará a validação da assinatura do documento através de um código previamente implementado na própria blockchain. Caso a assinatura seja 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 de então, qualquer caso de uso pode verificar apenas que a associação existe, podendo concentrar seu trabalho nas funcionalidades do seu

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

4.2.4.As Transações e Registros

Após a aprovação e liberação de recursos do BNDEs, novos BNDESToken são emitidos para a conta de um cliente habilitado, conforme discutido anteriormente. Esta transferência aumenta, automaticamente, 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, a depender do tipo de projeto e forma de financiamento solicitado. Cada liberação acontece segundo cronograma acordado com o cliente, que pode, por exemplo, depender de marcos de entregas em um projeto.

O cliente, que agora possui saldo em sua conta, pode registrar ordens de pagamento para fornecedores habilitados no sistema, por exemplo, desde que seu saldo seja suficiente e a operação esteja de acordo com as regras de transferência da blockchain. Em determinados cenários analisados, como pagamento de tributos, o cliente pode precisar resgatar uma parte do valor recebido.

Em algum momento, uma pessoa jurídica “PJ” pode necessitar solicitar a troca de BNDESTokens por Reais. A proposta é que isso ocorra do seguinte modo:

(1) A PJ solicita o resgate de “x” BNDESTokens de um endereço seu, chamado “cnt”;

(2) o contrato inteligente então verifica se as regras de solicitação de resgate foram atendidas – por exemplo, número de transferências do token, prazo para transação e saldo.

(3) uma transferência é disparada no contrato inteligente de “cnt” para um endereço cadastrado previamente para resgate de propriedade do BNDES;

(4) o contrato inteligente destrói a quantidade “x” de tokens solicitadas em resgate 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 – lembrando-se da paridade 1:1;

(6) O BNDES realiza uma transação bancária de “x” Reais para a conta bancária da PJ informada no momento de seu cadastro e publica o comprovante detransferência;

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

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

(9) Um sistema interessado de PJ pode escutar o evento e realizar alguma ação de acordocom seus processos de negócios.

Outras opções podem ser utilizadas, por exemplo, para os passos 6 e 7 acima é enviar ao endereço de PJ um montante equivalente a “x” em moeda digital, no caso Ether, visto que o BNDESToken se baseia na rede Ethereum. 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, assim como todas as criptomoedas. 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.

4.2.5.Acompanhamento das Operações

Assim como na operação padrão do BNDES, após a operação ser contratada, o cliente precisa prestar contas de alocação de recursos realizada. Trata-se do acompanhamento financeiro e físico do projeto financiado com o dinheiro do bando.

Para realizar o acompanhamento financeiro, atualmente o cliente precisa enviar comprovantes bancários com frequência preestabelecida entre ele e o banco ou em determinados marcos ou entregas. Com o BNDESToken, todas as transações passam a ser automaticamente visíveis por todos os players com hora de submissão para a rede e de confirmação da operação, o que minimiza as atividades humanas e, consequentemente, aumenta a confiabilidade das informações.

Para realizar o acompanhamento físico, o cliente precisa enviar documento comprovando a forma como foi realizado cada gasto (por exemplo, uma nota fiscal de um produto adquirido). A proposta prevê o desenvolvimento de uma funcionalidade denominada off-chain, na qual o cliente possa descrever cada um de seus gastos e dar upload em documentos. Vale 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, dessa forma, afeta-se positivamente o fluxo de caixa da companhia, e tem-se todos os benefícios de um fluxo de caixa positivo, não só para a empresa como para a economia.

4.2.6.Transparência

Qualquer stakeholder pode visualizar as informações aderentes ao padrão ERC-20 em um programa navegador da blockchain utilizada. Para o Ethereum, que o BNDES utiliza, existe o previamente mencionado EtherScan. No navegador é possível, por exemplo, verificar o saldo total de BNDESTokens em circulação, quais são os endereços que possuem o token e detalhes das transferências realizadas.

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

4.2.7.Estágio Atual

O BNDES está atualmente trabalhando para conseguir realizar uma prova de conceito conforme descrito em (Rabin, 2018). O projeto foi priorizado para ser realizado após vencer um concurso de inovação interno chamado ideiaLab com mais de trezentos concorrentes. O concurso previu que as propostas vencedoras teriam seis meses para gerar um resultado inicial para o banco, quando então haveria uma reavaliação das prioridades.

O desenvolvimento até o momento contempla uma versão inicial do contrato inteligente do BNDESToken, uma aplicação Web userfriendly e um painel online. O foco principal do início 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, levando em consideração 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.

O módulo de identidade de pessoa jurídica ainda está em debate pela equipe e será 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. 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, linguagem padrão da rede Ethereum, 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.

4.3. **Outros Casos Correlatos**

No Canadá, um órgão de pesquisa e desenvolvimento do governo chamado National Research Council, anunciou um sistema, ainda em fase de protótipo, para publicar como os recursos geridos estão sendo alocados aos projetos (NRC, 2018). O sistema teria como objetivo armazenar 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[6], banco de desenvolvimento Alemão, desenvolveu o TruBudget, um sistema para rastreamento do 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

[6] https://www.kfw.de/

projetos, isto objetivando a minimização do risco de fundos serem utilizados de forma incorreta (KfW, 2017). Por permitir a definição de workflows de forma flexível, esse sistema ainda pode ser utilizado como forma 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 – dado que não há necessidade de remunerar os nós validadores de transações da rede. Além disso, há autonomia para definir quais nós participam da rede e quais podem visualizar as informações armazenadas. Dessa forma, os participantes da rede acordam se o acesso a uma determinada informação na plataforma pode ser dado a outras partes interessadas ou ser aberta ao público tendo em vista que, dependendo do caso, algumas informações podem estar sujeitas a restrições legais. Vale ressaltar que o TruBudget não define um token para pagamento, o que reduz o risco regulatório e o esforço de implantação nos clientes, incluindo impacto em processos de negócios.

O TruBudget está atualmente sendo implantado no BNDES para rastrear as doações de recursos para o Fundo de preservação da 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 nas próximas etapas de teste.

Não são somente bancos e governos que estão utilizando blockchain como solução de rastreio, por exemplo, a Everledger possui um sistema de rastreio da cadeia de suprimentos de diamantes para garantir a procedência do insumo, 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 mais transparentes. Inicialmente utilizado apenas o potencial das criptomoedas para facilitar a remessa de recursos, soluções como o GiveTrack (BitGive, 2018) estão desenvolvendo soluções para doações mais transparentes ao doador, que se interessa em saber se seu recurso chegou de fato ao projeto, se já foi utilizado e como foi utilizado.

O órgão de distribuição de alimentos da ONU, WFP (World Food Programme) está utilizando uma solução baseada em tokens que podem ser trocados por alimentos, em regiões de ajuda humanitária como campos de refugiados da Síria (WFP, 2018). O projeto, chamado BuildingBlocks, que também contém uma solução de identificação pessoal por análise biométrica, tem por

objetivo ser um meio mais eficiente e barato para distribuição da ajuda, almejando inclusive integração com informação proveniente de órgãos de educação e saúde.

5.Uma Proposta de Modelo do Minha Casa Minha Vida em Blockchain

Tem-se como objetivo o desenvolvimento de um Blockchain para rastreamento do fluxo financeiro do programa “Minha Casa Minha Vida”, para isso precisamos definir as premissas para o funcionamento, assim como as funções que cada nó possuirá na rede.

5.1.**Modelo operacional da Blockchain**

Precisa-se ressaltar as seguintes premissas como sendo as premissas essenciais para o funcionamento adequado e desenvolvimento do Blockchain.

Blockchain privada, também conhecida como permissionada, que será usada para o sistema em questão. Para isso, deverá ser desenvolvida para esse propósito e com integração a outros sistemas do governo já existentes, tanto para coleta de insumos para seu funcionamento como para fornecimento de insumos para outros órgãos públicos.

A gestão da identidade jurídica digital será verificada. Como no caso do BNDESToken, pode-se utilizar o e-CNPJ como identificador para cadastro de Pessoas Jurídicas em Blockchain, no entanto, propõe-se, aqui, uma ampliação do caso. Fazer com que toda empresa já nasça com um CNPJ na Blockchain do governo, permitindo, assim, o rastreamento de todas as suas transações. É nesse cenário que estará sendo trabalhado o caso.

A gestão de identidade física digital, tem por premissa a criação de uma identidade para pessoas físicas em Blockchain, permitindo o rastreamento de seus recebimentos (como salários, dividendos, proventos, etc) assim como seus pagamentos. Essa base do governo seria capaz de rastrear todo fluxo financeiro do cidadão em questão. Hoje, entretanto, não há uma centralização das informações do cidadão brasileiro, apenas o cruzamento de dados, lembrando que

um cidadão possui Identidade Civil[7], Certidão de Pessoa Física[8], Carteira Nacional de Habilitação[9], Certificado de Reservista, Título de Eleitor[10], dentre outros. A unificação destes certificados evitaria uma falsidade ideológica que, tendo em vista a quantidade de documentos e, consequentemente, burocracias, que se comunicam, devem ser mais comuns do que imaginamos.

O Token da Blockchain "Minha Casa Minha Vida" utilizaria o mesmo modelo do BNDESToken, onde a Blockchain possuiria um token com paridade com o real. O token circularia livremente pelos nós, conforme suas transações. O token seria criado para pagamento e destruído para cada resgate na Blockchain, não alterando a quantidade de Reais em circulação.

5.2.**Nós envolvidos e permissionamentos**

Precisamos definir e entender quais são os principais agentes do Programa "Minha Casa Minha Vida" e como esses se comportam, assim como a relação que existe entre eles. Sendo assim, passaremos *en passant*[11] na atuação de cada um dos membros para decidir e definir se esses serão nós validadores ou nós membros, bem como quais os tipos de transações que podem vir a ser realizados por cada um dos membros.

5.2.1.Ministério das Cidades – Nó validador

O Ministério das Cidades tem como principal função o repasse de verba para a Caixa Econômica Federal. Claramente esse repasse não se dá de forma arbitrária, sendo assim, um conjunto de critérios pré-estabelecidos devem ser preenchidos para que o repasse seja feito. Por causa disso, o Ministério das Casas se torna um nó validador, pois ele possuirá um smartcontract (contrato inteligente)

[7]http://www.detran.rj.gov.br/_documento.asp?cod=1438

[8]http://receita.economia.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf

[9]http://www.detran.rj.gov.br/_documento.asp?cod=1407

[10]https://www.tre-rj.jus.br/

[11] Locução adverbial: De passagem; de maneira rápida; rapidamente: o juiz escreveu, *en passant*, a sentença e se retirou do tribunal.

que avaliará todos os casos de solicitação de repasse e os fará de acordo com sua norma interna.

5.2.2.Caixa Econômica Federal – Nó validador

A Caixa Econômica Federal apresenta várias frentes que podem ser solucionadas com smartcontracts (contratos inteligentes) distintos. Vamos analisar cada um deles.

5.2.3.Fornecimento de Crédito

Como há critérios de elegibilidade para o programa “Minha Casa Minha Vida”, esses critérios podem ser automatizados via um smartcontract, no qual, junto com a gestão de identidade física digital, a CEF seria capaz de averiguar se o beneficiário teria ou não direito ao programa. Além disso, seria capaz de analisar de forma precisa sua saúde financeira, o que melhoraria o índice de inadimplência da CEF.

5.2.4.Retomada do Imóvel

Como dito anteriormente, caso o beneficiário não cumpra determinadas regras, esse perderá o direito a sua habitação. Sendo assim, um smartcontract (contrato inteligente) seria capaz de analisar a saúde financeira do beneficiário (graças a gestão da identidade física digital) além dos critérios como pagamento e sinalizar tal situação em tempo real e hábil. Caso esses critérios não estejam sendo atendidos de forma adequada, o contrato inteligente iniciará o processo de retomada da habitação do beneficiário.

5.2.5.Repasse a Construtora

A construtora, por sua vez, possui projetos que podem ser elegíveis ao programa social em questão. Assim sendo, critérios de avaliação do projeto podem ser automatizados pela CEF por um smartcontract. Após a elegibilidade do projeto ser aprovada no programa, é possível acompanhar o fluxo de

pagamentos realizados para garantir que o projeto continue com seu objetivo, sem comprometer os critérios previamente definidos, visto que a Blockchain seria aberta e os fluxos estariam visíveis a todos os nós membros.

5.2.6.Construtora – Nó membro

A construtora, por sua vez, apenas recebe e realiza pagamentos. Seja aos seus fornecedores como recebimento de seus clientes, que, por sua vez, são elegíveis ao “Minha casa minha vida”. Isso também permitiria um mapeamento do mercado de interesse da construtora de forma mais ágil e simples, visto que os cidadãos já estariam classificados e a informação de elegibilidade estaria disponível. Além disso, a visibilidade dos dados, como a saúde financeira do beneficiário, seria essencial para que a análise de crédito dos beneficiários seja capaz de reduzir a inadimplência e aumentar a efetividade do programa. Permitindo assim, a construtora mitigar o risco de inadimplência e, consequentemente, não comprometer o projeto, ou até mesmo alavancar e correr o risco de inadimplência.

5.2.7.Beneficiários – Nó membro

Após avaliação da CEF e por passar pelos critérios para se tornar beneficiário do programa ”Minha Casa Minha Vida”, o beneficiário se torna um nó membro, visto que as únicas ações que conseguiria tomar na rede são de solicitação de crédito a CEF e de pagamento das mensalidades a CEF. Obviamente que este ainda estaria sujeito à revisão dos critérios periodicamente, visto que, por estar em blockchain, esta revisão poderia ser realizada com frequência muito superior a atual utilizada.

5.3.**O Modus Operandi**

Vamos considerar os seguintes diagramas de processos desenvolvidos pelo escritor, utilizando a ferramenta Bizagi BPMN Modeler, para demonstrar o funcionamento e interação entre os nós membros da Blockchain do Programa Habitacional analisado. Serão apresentados dois diagramas de processos. O primeiro visa demonstrar o processo de aceitação ou negação de um projeto de uma Construtora submetido para análise do programa Habitacional. O segundo,

visa demonstrar os ganhos da automatização do processo utilizando a blockchain, tanto em eficiência, como no desenvolvimento de um blockchain capaz de rastrear o fluxo de pagamentos de um cidadão, que serve como uma parte de um projeto de gestão da cidadania digital.

5.3.1.Aprovação de um projeto

Inicialmente, analisaremos o caso de aprovação de um projeto por parte da construtora à Caixa Econômica Federal e sujeito à aprovação e liberação de verba do Ministério das Cidades.

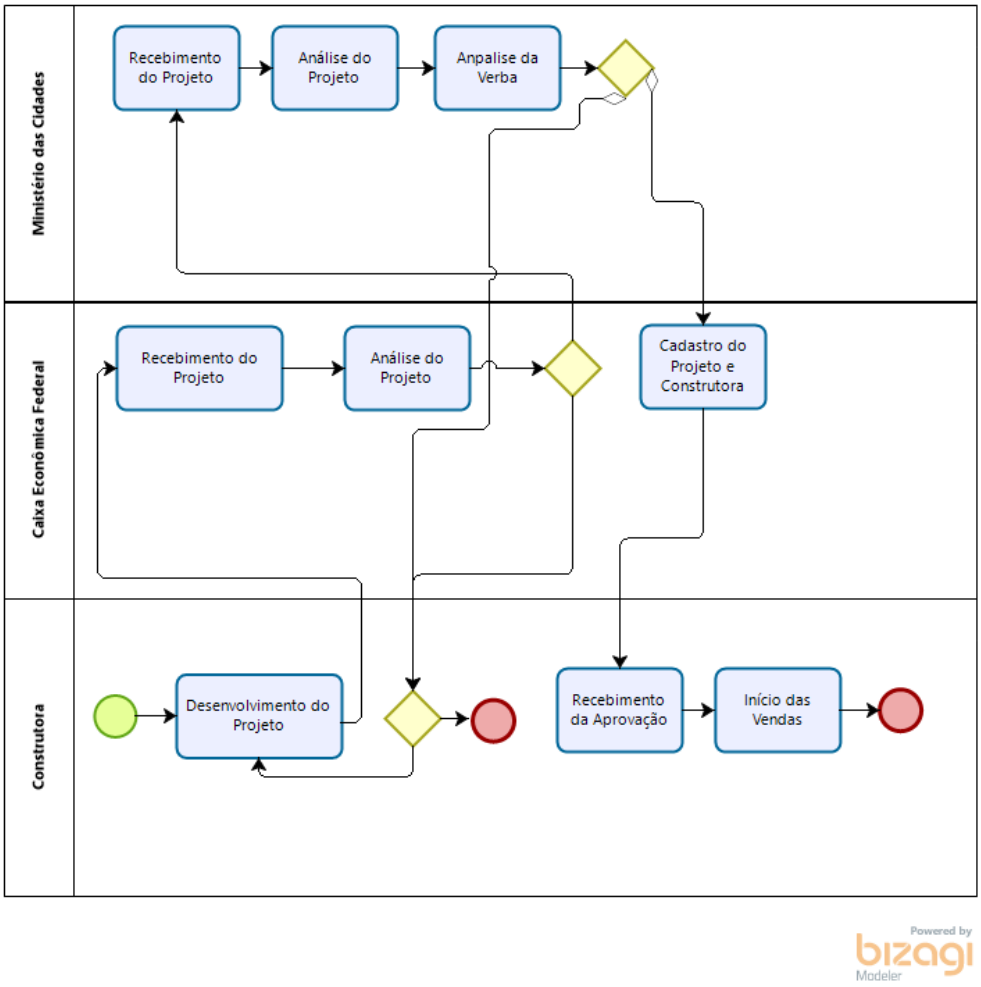

Figura 1 - Processo de Aprovação de um projeto habitacional

01. **Desenvolvimento do Projeto.** Construtora desenvolve um projeto de acordo com os critérios para aprovação da Caixa Econômica Federal.

02. **Recebimento do Projeto.** Caixa Econômica Federal recebe o projeto da Construtora para análise.
03. **Análise do Projeto.** O projeto será analisado de acordo com os critérios do programa habitacional
    03.01. Nesse caso, um SmartContract[12] seria utilizado para analisar o projeto de acordo com critérios pré-estabelecidos. Processo, atualmente, manual que pode ser automatizado gerando agilidade, o que traria benefícios para a Construtora, e redução de custos para a Caixa Econômica Federal.
    03.02. **Se negado**, envia-se à construtora para revisão. Que pode optar em **Desenvolver o Projeto** novamente ou em encerrar esse processo.
    03.03. **Se aprovado**, envia-se para o Ministério das Cidades
04. **Recebimento do Projeto.** Ministério das Cidades recebe projeto.
05. **Análise do Projeto.** Ministério das Cidades analisa o projeto de acordo com seus critérios.
06. **Análise da Verba.** Ministério das Cidades analisa a disponibilidade de verba para o programa habitacional, bem como a quantia solicitada pela Construtora.
    06.01. SmartContract[13]analisa o projeto de acordo com os critérios pré-estabelecidos, tanto critérios de aprovação como os critérios de verba.

[12] Para a análise em SmartContract dos Critérios de aprovação por parte da Caixa Econômica Federal, é necessário que haja uma interface onde a construtora possuirá um formulário eletrônico para preenchimento e submissão a CEF, ou até mesmo um template desenvolvido pelo banco para que a análise seja feita de forma automatiza. Essa agilidade gera uma confiança maior à Construtora que se beneficiará diretamente, assim como a CEF que poderá desprender recursos para outras atividades, gerando economia nesse processo assim como uma realocação de recursos para outros processos morosos que ainda não possam vir a ser automatizados como esse.

[13] A análise de verba por parte do Ministério das Cidades inclui algumas interfaces, tais como: i) acesso ao orçamento previsto para o programa habitacional; ii) acesso ao fluxo de caixa de desembolso da verba já comprometida bem como a previsão de desembolso do projeto em questão; iii) Critérios para seleção e priorização dos projetos submetidos pela CEF para o programa em questão. Essas interfaces aumentam a transparência do Governo em relação ao projeto, bem como uma segurança de

06.02. **Se aprovado**, tanto nos quesitos do projeto habitacional como nos de verba, envia-se alvará para que a Caixa Econômica Federal dê continuidade ao processo.

06.03. **Se negado**, Construtora e Caixa Econômica Federal receberão a informação. Ficando a cargo da empresa decidir se deseja voltar a etapa de Desenvolvimento do Projeto ou encerrar o Processo.

07. **Cadastro da Construtora e do Projeto.** Caixa Econômica Federal realizará o cadastro da Construtora e do Projeto em blockchain por onde será rastreado o fluxo financeiro desse projeto, bem como seus beneficiários.
08. **Recebimento da Aprovação.** Construtora é informada e começa a dar início ao projeto.
09. **Início das Vedas.** Construtora dará início às vendas, o que encerra esse processo e inicia o processo de Vendas que veremos a seguir.

5.3.2.Fluxo de pagamentos de um beneficiário

O próximo processo seria o de cadastro de um beneficiário, rastreamento do fluxo de pagamento das prestações e de repasse à construtora. Utilizou-se o Bizagi BPMN Modeler para o diagrama de processos.

imparcialidade na análise dos projetos, bem como a clareza das regras expostas abertamente ao público.

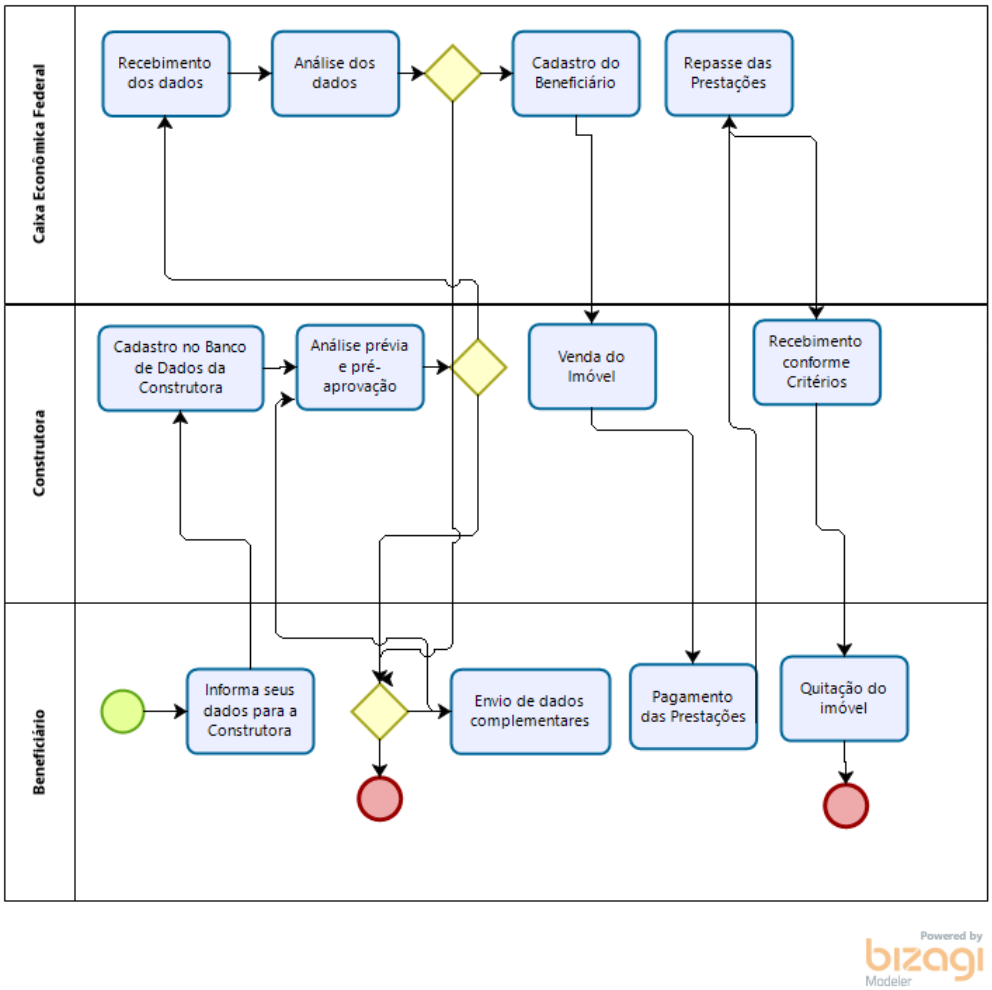

Figura 2 - Processo de Cadastro de um beneficiário e o modelo de rastreamento de pagamentos

01. **Informa seus dados para a Construtora.** O cliente que deseja adquirir um imóvel de um projeto aprovado pela Caixa Econômica Federal deverá informar sua intenção de compra para a Construtora, junto com os dados referentes ao cadastro no programa.
02. **Cadastro no Banco de Dados da Construtora.** A construtora realiza um cadastro em seu Banco de Dados, assim como a verificação da veracidade[14] dos documentos apresentados.

[14] Ressalta-se que, em casos de maior maturidade da Gestão da Identidade Digital, a construtora não necessitaria cadastrar as informações, estas poderiam ser consultadas diretamente em banco de dados do governo. Assim como a aprovação por parte do programa que selecionou. Essa grande integração permitiria, inclusive, que o beneficiário

03. **Análise prévia e pré-aprovação.** Após o cadastro em seu banco de dados, a Construtora verificará os critérios necessários para que o beneficiário esteja apto à compra.
    03.01. Nesse caso, um SmartContract seria utilizado para analisar os dados de acordo com critérios pré-estabelecidos.
    03.02. **Se negado**, envia-se um aviso ao beneficiário para que este opte em enviar uma documentação complementar ou encerrar o processo.
    03.03. **Se aprovado**, envia-se os dados do beneficiário para a Caixa Econômica Federal.
04. **Recebimento dos dados.** Caixa Econômica Federal recebe os dados enviados pela construtora.
05. **Análise de dados.** CEF realiza análise dos documentos enviados.

    Os itens 3, 4 e 5 podem ser unificados em um smartcontract com aprovadores. No caso, a construtora e a CEF são nós validadores que enviam as informações para a próxima etapa. Já a análise seria feita de forma automática pelo sistema. O que permitiria, inclusive, que a construtora soubesse se o beneficiário será aprovado ou não, antes de enviar para a CEF, realizando consultas prévias com precisão total.

    05.01. **Se negado**, envia-se um aviso ao beneficiário para que este opte em enviar uma documentação complementar ou encerrar o processo.
    05.02. **Se aprovado,** segue para o processo de cadastramento do beneficiário e aprovação da venda ao beneficiário, que iniciará os pagamentos.

    Nesse momento, os Tokens da blockchain referentes ao imóvel são criados. A construtora recebe os Tokens que serão contabilizados como um “Contas a Receber” bloqueado pela CEF e regras do programa habitacional. Ao mesmo tempo, cria-se um empréstimo ou “Contas a Pagar” para o beneficiário, sujeito as regras do programa e ao modelo de financiamento escolhido. Conforme realizado o pagamento, o saldo de Tokens do beneficiário é reduzido e transferido a

soubesse se está apto ou não de forma automática, o que economizaria tempo e esforço de todos os elos caso não estivesse.

CEF, que serve como intermediária. Quando a construtora atinge os critérios, o valor referente ao pagamento é liberado no “Contas a Receber” da Construtora, que possuía a possibilidade de resgatar esse dinheiro, ou seja, transformar o Token em Reais, respeitando a paridade, e destruição dos Tokens. Esse processo se seguirá até a quitação total do imóvel.

5.3.3.Cadastro de um beneficiário e Construtora

Como dito anteriormente, a grande vantagem da blockchain para programas do governo é a rastreabilidade e a transparência gerada, o que aumenta a confiabilidade e imparcialidade do sistema.

Sendo assim, os beneficiários seriam cadastrados e o banco de dados seria de consulta pública. O mesmo sistema para cadastro dos beneficiários serve para o cadastro de todo e qualquer nó, inclusive as construtoras. Sendo assim, o código aqui apresentado pode ser usado para cadastro de todos que fazem parte do processo. Propomos a utilização do Cadastro de Pessoa Física (CPF) como código de identificação para pessoas físicas e o Cadastro Nacional de Pessoa Jurídica (CNPJ) para as pessoas jurídicas.

O código pode ser adaptado para contemplar mais informações, a depender da necessidade de cada programa. O modelo a seguir foi desenvolvido pelo escritor.

```
functioncreate(bytes4 flags, bytes contents) externalreturns (bytes20 Id) {
// Gera uma identidade única para o cadastro de ID. Pode ser utilizado o CPF para pessoas físicas e o CNPJ para pessoas jurídicas.
Id = bytes20(keccak256(msg.sender, block.blockhash(block.number - 1)));
// Certifica-se de que o ID não foi utilizado previamente, inclusive no mesmo bloco no qual será inserido.
while (Info[Id].blockNumber != 0) {
Id = bytes20(keccak256(Id));
}
// Armazena as Informações (Info) em um estado.
      Info[Id] = Info({
flags: flags,
revisionCount: 1,
blockNumber: uint32(block.number),
owner: (flags & ANONYMOUS != 0) ? 0 :msg.sender,
});
// Armazena as informações em um log do bloco atual.
Store(Id, 0, contents);
}
```

Figura 3 - Modelo de Cadastro de um Nó na Blockchain

Essa é apenas uma das partes do código, as demais partes, como as de aprovação de projeto e fluxo de recebimento dos Tokens, dependem de cada um dos casos e das regras vigentes. Sendo assim, os nós responsáveis pelas regras teriam a necessidade de reescrever e adaptar os códigos conforme as novas regras surjam.

Esse cadastro dos beneficiários é um passo importante para a gestão da identidade digital dos cidadãos do país. É de suma importância que, ao se criar uma blockchain do Sistema Financeiro Nacional, os cidadãos estejam cadastrados, para que possam ser auditados a qualquer momento, e, de forma automatizada. Esse projeto proposto serve então como um MVP (Minimum Viable Product – produto com mínima viabilidade) para que, aos poucos, se expanda para todos os cidadãos.

Podemos fazer um paralelo desse MVP com a biometria nas eleições [15]do Rio de janeiro em 2018, na qual o DETRAN-Rio forneceu para o governo seu banco de dados de cadastro dos cidadãos, para que esse usasse como teste regional para depois expandir a nível nacional.

5.4. **Vantagens deste Modelo Proposto**

Pode-se perceber inúmeras vantagens no sistema, dentre eles, podemos citar que a transparência total dos critérios permitiria que todos tivessem a visão de quais são os reais beneficiários do programa e o porquê deles receberem tal benefício. Além disso, como os critérios de repasse e de reclassificação dos beneficiários se encontrariam em smartcontracts, não só a revisão seria feita de forma rápida e ágil, como também, seria possível reduzir custos burocráticos dos órgãos que analisam tal documentação.

O rastreamento do fluxo do dinheiro do programa seria transparente a todos da sociedade. Isso permitiria calcular o retorno real do programa para a nação. Seja por quantidade de pessoas atingidas, como de formas mais qualitativas, como o valor investido versus o impacto social ou inclusão que ocorreu no período. Isso também permitiria verificar quais projetos foram mais eficientes e o porquê, o que levaria a uma busca pela eficiência do Programa como um todo.

[15]https://g1.globo.com/rj/rio-de-janeiro/eleicoes/2018/noticia/2018/10/07/biometria-de-surpresa-e-urnas-quebradas-formam-filas-em-secoes-no-rj.ghtml

Devido ao rastreamento do fluxo de dinheiro, também seria possível rastrear exatamente o imposto e as taxas a serem recolhidas em cada uma das etapas, sabendo-se, assim, o que de fato foi pago pelo imóvel e o quanto foi pago por burocracia.

A retomada do imóvel e tentativa de vendê-lo novamente, se tornaria mais ágil, o que reduziria um altíssimo custo atrelado ao default do beneficiário, tempo de re-aquisição do imóvel até o tempo de venda desse novamente.

Análises regionais impactadas, por faixa de renda, por tipo de imóvel, por situação atual versus situação da região pós projeto, dentre outras análises seriam possíveis de forma mais rápida e clara.

6.Conclusão

A Blockchain tem se mostrado uma tecnologia muito promissora, principalmente para a área governamental. No caso do Brasil, o BNDES apresenta essa tecnologia para averiguação dos movimentos na economia após o desembolso do recurso. Tendo sido pioneira, inclusive por causa de seu porte, tem servido de insumo para pesquisas acerca da efetividade da blockchain nessa aplicação e na contribuição para o desenvolvimento do país. Ressalta-se que a proposta descrita 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, e até mesmo para aqueles que desejam dar passos a mais.

Com os atuais investimentos e o aprofundamento na tecnologia, diversas vantagens adicionais podem ser citadas, 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. Esse último foi o foco de interesse do presente trabalho. Pode-se concluir que com o crescimento da adoção da tecnologia, o compartilhamento de dados tenderá a aumentar massivamente.

A introdução do BNDESToken, é uma possível mudança no modelo de negócio, com impacto na forma com a qual 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. A nova tecnologia, permitiu o adiamento do repasse de Reais até o resgate do BNDESToken, aprimorando o fluxo de caixa do banco, o que permitiria, inclusive, desenvolver mais projetos.

Porém, como percebemos, o projeto do BNDES explora apenas pessoas jurídicas, o que, no caso do programa “Minha Casa Minha Vida”, não ocorreria. Seria necessário a inclusão de pessoas físicas, o que torna o projeto um MVP para a gestão da identidade física digital, e que é fator crucial para agilizar o processo de implementação a nível nacional.

As vantagens da adoção da gestão de identidade física digital são inúmeras, como as já citadas: não sonegação de impostos, rastreamento de todas as

transações econômicas de um país, maior transparência, além do tratamento individualizado do cidadão devido a sua solvência financeira.

Existem vários passos futuros para o projeto. Um primeiro ponto é explorar em mais detalhes a solução de identificação de pessoas físicas, pois inúmeras possibilidades estão presentes. É necessário também pensar em como aumentar a flexibilidade da solução, de forma a melhorar a governança e responsabilização dos funcionários das pessoas jurídicas, assim como a governança nos nós validadores para que não ocorram erros humanos.

Um outro ponto, é como tornar a experiência do usuário mais simples, visto que os conceitos e ferramentas de blockchain ainda não estão em estágio de massificação 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. Dito isto, a sociedade, em geral, não apresenta o amadurecimento teórico dos conceitos para entender por que o uso da tecnologia aumenta a confiabilidade das informações apresentadas.

Um ponto crucial, é que, atualmente, todos os dados gravados na blockchain, são públicos. Contudo, é possível que o sigilo empresarial (como datas, preços e quantidade de insumos adquiridos, por exemplo) torne necessário fornecer graus de privacidade a algumas informações. Embora a transparência total gere benefícios para o todo, entende-se que essa transparência não será feita de um dia para o outro, e que um processo de amadurecimento da população precisa ser feito para que isso ocorra.

Outro ponto, é reavaliar se Ethereum é realmente a plataforma de blockchain mais adequada para a solução, apesar de ser a que mais possui recursos atualmente para suportar o presente trabalho, o crescimento e dinamismo do mercado de blockchain faz com que seja necessário um acompanhamento mais próximo do que temos de mais inovador. Além disso, nada impede que seja feito o seu próprio sistema para garantir uma estabilidade maior, caso se julgue necessário.

O autor vislumbra também a construção de novos casos de uso em torno de Blockchain governamentais. Tais como: cobrança automática de tributos, simplificação do sistema tributário, transferência de ativos associados a nota fiscal eletrônica, gestão orçamentária, impostos de renda de pessoa física e jurídica.

No caso da blockchain para o programa social “Minha Casa Minha Vida”, estendem-se o uso para a pessoa física, diferenciando-se do caso do BNDESToken, cujo foco era o cadastro de pessoas jurídicas em seu sistema.

Dessa forma, há a ratificação da necessidade de implementação da gestão da identidade física digital do cidadão.

Há inúmeras vantagens em relação à essa identidade, conforme já previamente mencionado, e a mesma deveria ser tratada como prioridade total por parte do governo para sua implementação. Além disso, a gestão da identidade física digital do cidadão é uma das premissas para que o modelo proposto possa funcionar de forma adequada.

O sistema proposto traria ganho em eficiência operacional, reduzindo custos burocráticos, além da redução de fraudes no sistema. Outro ponto positivo, seria a capacidade comparativa de eficiência dos projetos, para que sejam tiradas lições aprendidas e, nos próximos projetos, tenha-se resultados ainda melhores, aumentando a relação benefício/custo em relação ao imposto pago pelo cidadão brasileiro.

Além de todas as vantagens supracitadas, encontramos na Blockchain a capacidade de integrar e oferecer soluções viáveis para inúmeros avanços tecnológicos, tais como IoT - Internet of Things (internet das coisas), Inteligência Artificial (IA), RPA – Robotics Process Automation (automação de processo robóticos), ML – Machine Learning (Aprendizado de máquinas). A medida que os protocolos se tornam mais avançados e os pontos da rede se tornam mais dispersos. A segurança é e continuará sendo uma grande preocupação e uma grande aliada no processo de adoção da tecnologia. Portanto, a tecnologia blockchain torna-se chave para as implementações bem-sucedidas desses protocolos, e a padronização se torna um balizador essencial. Hoje, ainda não há uma padronização oficial, porém, a International Organization for Standardization, está em vias de criar uma norma de padronização, a ISO/TC 307, que estabelece padrões para terminologia e conceitos relacionados às tecnologias blockchain e ledger distribuído. (“ISO/TC 307: Blockchain and Distributed Ledger Technologies,” International Organization for Standardization).[16]

Ressalta-se uma série de questões emblemáticas que ainda se apresentam em torno da tecnologia, como, por exemplo: o que exatamente essa mudança tecnológica pode implicar contratualmente? Visto que o Brasil é um dos países que mais desenvolve leis secundárias. Além do fato que gera o registro, a partir de que data (fato) deve-se contar para quesitos como pagamentos, juros e afins? Leva-se a crer que mais categorias do que simplesmente o receptor e o emissor

[16]https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0.

são necessários para que haja total controle das transações do país. Existiria algum impacto regulatório na Blockchain? Esses e outros questionamentos estão aquém dos esclarecimentos do autor, uma vez que há uma quantidade considerável de variáveis exógenas a seu controle. Apenas deve-se torcer para que os representantes eleitos nos órgãos com competência para julgar cada um desses casos, o faça de forma imparcial e visando o bem-estar da população, e não, apenas como uma mera regulação burocrática e onerosa ao cidadão.

7.Referências bibliográficas

Antonopoulos, Andreas M. 2014.*Mastering Bitcoin. Unlocking Digital Cryptocurrencies.* Sebastopol, CA : O'Reilly Media, 2014. ISBN 978-1449374037.

Armstrong, Stephen. 2016. Move over Bitcoin, the blockchain is only just getting started. [Online] 8 de 2016. https://www.wired.co.uk/article/unlock-the-blockchain.

Atzei, Nicola, Bartoletti, Massimo e Cimoli, Tizian. 2017. A survey of attacks on Ethereum smart contracts. [Online] 2017.

Bacen, Banco Central do Brasil. 2019. Taxas de juros básicas – Histórico. [Online] 01 de 2019. https://www.bcb.gov.br/controleinflacao/historicotaxasjuros.

Bartoletti, M. e Pompianu, L. 2017.*An empirical analysis of smart contracts: platforms,.* s.l. : Financial Cryptography and Data Security, Springer, 2017.

Baylina, J. e Dafflon, J. 2018.ERC-777. [Online] Ethereum Community Conference, 2018. https://www.youtube.com/watch?v=qcqhryzGTy0.

Bhaskar, Nirupama Devi e Chuen, David Lee Kuo. 2016.*Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* 2016. pp. 47-51. ISBN 978-0-12-802117-0.

Bheemaiah, Kariappa. 2015. Block Chain 2.0: The Renaissance of Money. *Wired.* 2015.

BitGive. 2018. GiveTrack: Donation Tracking. [Online] 2018. https://www.bitgivefoundation.org/givetrack-static/.

Brito, Jerry e Castillo, Andrea. 2013. Bitcoin: A Primer for Policymakers. [Online] 09 de 2013. https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

Buntinx, J.P. 2016.*The Road To Bitcoin Adoption Passes Through Many Stages.* s.l. : News BTC., 2016.

Catalini, Christian e Gans, Joshua S. 2016. Some Simple Economics of the Blockchain. *SSRN Electronic Journal. .* 11 de 2016.

Catalini, Christian e Tucker, Catherine E. 2016.*Seeding the S-Curve? The Role of Early Adopters in Diffusion.* SSRN Electronic Journal : s.n., 2016.

CEF, Caixa Econômica Federal. 2019. Minha Casa Minha Vida - Habitação Popular | Caixa. [Online] 01 de 2019.

http://www.caixa.gov.br/voce/habitacao/minha-casa-minha-vida/Paginas/default.aspx.

Coindesk. 2016. Coindesk. [Online] 2016. http://www.coindesk.com/events/consensus-2016/.

—. 2016. Coindesk. *Coindesk.* [Online] 2016. http://www.coindesk.com/research/state-of-Blockchain-q3-2016.

CTG, Center for Technology in Government. 2018. A working definition of egovernment. [Online] University at Albany, 2018. https://www.ctg.albany.edu/publications/reports/future_of_egov?chapter=2.

DuPont, Quinn. 2017. Experiments in Algorithmic Governance: A history and ethnography of "The DAO", a failed Decentralized Autonomous Organization. [Online] 2017.

Economist. 2015. The great chain of being sure about things. [Online] 31 de 10 de 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

Economist, The. 2015. Blockchain, The Next Big Thing. [Online] 05 de 2015. http://www.economist.com/news/special-report/21650295-or-it-next-big-thing.

Edelman, R. 2018.*Edelman.* [Online] 2018. https://www.edelman.com/trustbarometer.

e-Estonia. 2018. e-Identity. [Online] 2018. https://e-estonia.com/solutions/e-identity/e-residency/.

Everledger. 2018. Diamond Time-Lapse Protocol. [Online] 2018. https://www.everledger.io/.

Gartner. 2016. Hype Cycle for Emerging Tecnologies. *Gartner.* [Online] 2016. 3-trends-appear-in--the-gartner-hype-cycle-for-emerging-technologies-2016.

Gervais, Arthur, et al. 2016. Is Bitcoin a Decentralized currency? [Online] InfoQ & IEEE computer society, 10 de 10 de 2016.

Ghayas, Muhammad. 2018. What does "Block Time" mean in cryptocurrency? *Quora.* [Online] 21 de 01 de 2018.

Government Office for Science, United Kingdom. 2015. [Online] 2015. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Heinker, RA Markus. 2007. Beweiswürdigung elektronischer Dokumente im Zivilprozess unter vergleichender Betrachtung von qualifizierten elektronischen Signaturen nach dem Signaturgesetz und dem Askemos-Verfahren. [Online] 2007.

Iansiti, Marco e Lakhani, Karim R. 2017. The Truth About Blockchain. [Online] Harvard Business Review. Harvard University, 01 de 2017. https://hbr.org/2017/01/the-truth-about-blockchain.

KfW. 2017. Blockchain boosts effectiveness of development cooperation. [Online] 2017. https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Press-Releases/Pressemitteilungen-Details_426112.html.

Lee, Timothy. 2013. Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%. [Online] 12x de 03 de 2013.

Mari, A. 2018. Brazilian and German development banks agree blockchain partnership. [Online] 2018. http://www.zdnet.com/article/brazilian-and-german-development-banksagree-blockchain-partnership/.

Marvin, Bob. 2017. Blockchain: The Invisible Technology That's Changing the World. [Online] 2017.

MdC, Ministério das Cidades. 2019. Ministério das Cidades. *www.cidades.gov.br.* [Online] 2019. http://www.cidades.gov.br/index.php/habitacao/programa-minha-casa-minha-vida-pmcmv/67-snh-secretaria-nacional/programas-e-acoes/1298-legislacao-geral-pmcmv%7CPrograma.

Metamask. 2018. Metamask - Bring Ethereum to your browser. [Online] 2018. https://metamask.io/.

Möbius, Martin. 2009. Erstellung eines Archivierungskonzepts für die Speicherung rückverfolgbarer Datenbestände im Askemos-System. [Online] 2009.

MultiChain. 2018. MultiChain – Open Platform for Building Blockchains. [Online] 2018. https://www.multichain.com/.

Nakamoto, Satoshi. 2008. Bitcoin.org. [Online] 2008. e-mail: satoshin@gmx.com. www.bitcoin.org/bitcoin.pdf.

NRC, National Research Council of Canada. 2018. Blockchain Publishing Prototype. [Online] 2018. https://nrc-cnrc.explorecatena.com/en/.

Ovenden, James. 2016. Blockchain Top Trends In 2017. [Online] The Innovation Enterprise, 04 de 12 de 2016.

Peck, M. E. 2017. Do You need a Blockchain. *IEEE Spectrum .* [Online] 2019 de 2017. https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain.

—. 2016. Ethereum's $150-Million Blockchain-Powered Fund Opens Just as Researchers Call For a Halt. [Online] IEEE Spectrum. Institute of Electrical and Electronics Engineers, 28 de 05 de 2016.

Plansky, John, O'Donnell, Tim e Richards, Kimberly. 2016. A Strategist's Guide to Blockchain. *Price Whaterhouse Cooper.* 82, 2016.

PMCMV, Programa Minha Casa Minha Vida. 2019. Minha Casa Minha Vida - Habitação Urbana. [Online] 2019. http://www.caixa.gov.br/voce/habitacao/minha-casa-minha-vida/urbana/Paginas/default.aspx.

—. 2017. Reformas no programa - Minha Casa Minha Vida Caixa. [Online] 15 de 03 de 2017. http://programaminhacasaminhavida.net/reformas-programa-minha-casa-minha-vida-caixa/.

Popper, Nathaniel. 2017. Business Giants to Announce Creation of a Computing System Based on Ethereum. [Online] 27 de 02 de 2017.

—. 2016. Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's. [Online] 27 de 03 de 2016.

Portal Brasil. 2019.«Entenda como funciona o Minha Casa Minha Vida». [Online] 2019. http://www.brasil.gov.br/infraestrutura/2014/04/entenda-como-funciona-o-minha-casa-minha-vida.

Prisco, Giulio. 2016. Sandia National Laboratories Joins the War on Bitcoin Anonymity. [Online] Bitcoin Magazine, 25 de 08 de 2016.

Rabin, C. G. 2018. BNDES Criará Token no Blockchain da Ethereum. [Online] 2018. https://portaldobitcoin.com/bndes-criara-token-no-blockchain-da-ethereum/.

Raval, Siraj. 2016.*What Is a Decentralized Application?* 2016. p. Capítulo 1.

RFB1 , Receita Federal do Brasil. 2015. Informações sobre a Obrigatoriedade de Utilização de Certificado Digital. [Online] 2015. http://idg.receita.fazenda.gov.br/orientacao/tributaria/senhas-eprocuracoes/.

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

Swan, Melanie. 2015.*Blockchain: Blueprint for a New Economy.* s.l. : O'Reilly, 2015.

Szabo, Nick. 2014. Secure Property Titles with Owner Authority. [Online] 15 de 01 de 2014.

Tapscott, D. e Tapscott, A. 2016.*Blockchain Revolution: How the Technology.* 2016.

Tapscott, Don e Tapscott, Alex. 2016. Here's Why Blockchains Will Change the World. *Forbes.* 2016.

Techtudo. 2016. Identidade Satoshi Nakamato. [Online] 2016. http://www.techtudo.com.br/noticias/noticia/2016/05/quem-e-satoshi-nakamoto-identidade-do-Portanto.

The Mission to Decentralize the Internet. **Kopfstein, Janus. 2013.** New York : The New Yorker, 2013.

Watzke, Tom-Steve. 2010. Entwicklung einer Datenbankschnittstelle als Grundlage für Shop-Systeme unter dem Betriebssystem Askemos. [Online] 2010.

WFP, World Food Programme. 2018. Building Blocks. [Online] 2018. http://innovation.wfp.org/project/building-blocks.

Wittenberger, Jörg F. . 2002. Askemos a distributed settlement. [Online] 2002.

Wood, G. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum.* [Online] 2014. https://ethereum.github.io/yellowpaper/paper.pdf, Março..