**CENTRO UNIVERSITÁRIO IESB**

Curso de Pós-Graduação em Tecnologias Disruptivas

Altamiro Dourado Rodrigues

Tarcísio da Cruz Santos

# *Minimum Viable Product* para o Programa Nota Legal DF na *Blockchain Ethereum*

Brasília - DF

Agosto 2019

**Altamiro Dourado Rodrigues**

**Tarcísio da Cruz Santos**

# *Minimum Viable Product* para o Programa Nota Legal DF na *Blockchain Ethereum*

Trabalho de conclusão do curso de Pós Graduação Lato Sensu em Tecnologias Disruptivas

Orientador: MSc. José Deodoro De Oliveira Filho

Brasília - DF

Agosto 2019

## Resumo

O programa de créditos tributários Nota Legal DF, instituído pela Lei nº 4.159, de 13 de junho de 2008, faz a concessão de créditos aos adquirentes de bens e mercadorias e aos tomadores de serviços, chamados de beneficiários, com a finalidade de aumentar a arrecadação tributária do Distrito Federal por meio do incentivo à solicitação de emissão da nota fiscal. Os créditos concedidos podem ser utilizados pelos beneficiários para abatimento do valor dos débitos de IPTU e IPVA. Os créditos também podem ser transferidos entre beneficiários pessoas físicas cadastradas no programa, ou ainda, serem transferidos para a própria conta corrente. O sistema desenvolvido neste MVP busca dar maior credibilidade e transparência aos dados relativos aos créditos, utilizações e sorteios, persistindo os mesmos numa *blockchain* privada (rede permissionada), baseada em *Ethereum* e manipulada por meio de um *Smart Contract* (contrato inteligente).

**Palavras-Chave:** Blockchain. Ethereum. Smart Contract. Nota Legal DF.

**Abstract**

The tax credit program Nota Legal DF, instituted by law No. 4.159, from June 13th 2008, concedes credits to purchasers of goods and services, who are also called beneficiaries, with the purpose of increasing the tax collection in Distrito Federal, as encouraging the emission of invoice. The conceded credit may be used by the beneficiaries in the deduction of debts in IPTU and IPVA. The credits may also be transferred between beneficiaries registered in the program or to the current account. The system developed in this MVP aims to provide a greater credibility and transparency to the data relative to credits, use and draws, in a private blockchain (permissioned network), based on Ethereum and manipulated with a Smart Contract.

**Keywords:** Blockchain. Ethereum. Smart Contract. Nota Legal DF.

## Sumário

## 1 O programa Nota Legal DF

Com o objetivo de aumentar a arrecadação tributária do Distrito Federal, o governo instituiu o programa Nota Legal DF, por meio da Lei 4.159 de 13 de junho de 2008. Os beneficiários adquirentes de bens e mercadorias que comprarem estes produtos nos estabelecimentos credenciados no programa, em regra, farão jus a 7,5% do valor do ICMS (imposto que incide sobre mercadorias e serviços de comunicação) de cada documento fiscal emitido para o respectivo CPF ou CNPJ. Já os beneficiários tomadores de serviços, em regra, farão jus 1,5% do ISS (imposto sobre serviços de qualquer natureza) de cada documento fiscal emitido para o respectivo CPF ou CNPJ.

Os beneficiários poderão utilizar os seus créditos para abater os débitos com IPTU e IPVA. Os que não possuírem débitos poderão transferir seus créditos para outros contribuintes (desde que ambos sejam pessoas físicas) ou indicarem uma conta corrente para receberem os créditos em espécie.

A lei autoriza o Poder Executivo a instituir no âmbito do programa um sistema eletrônico de sorteio, com prêmios em moeda corrente nacional, para os beneficiários pessoa física, cujo CPF conste no documento fiscal. Em regra, para cada documento fiscal emitido, é gerado um número da sorte que habita o beneficiário a participar dos sorteios.

## 2 A Blockchain, o Smart Contract e o DApp

Há diversas definições para o que seria uma blockchain. Entre as mais relevantes encontramos a de Daniel Kraus, Thierry Obrist e Olivier Hari:

> Uma blockchain é um livro-razão distribuído que permite o armazenamento e a transmissão de informações pela Internet de maneira transparente e segura, sem a necessidade de contar com uma terceira parte confiável. O banco de dados contém transações que são publicamente auditáveis, validadas, executadas e salvas de maneira cronológica e resistente a violações por uma rede de computadores.(KRAUS *et al.* 2019)

No contexto deste MVP cabe ainda a definição proposta por I. Karamitsos *et al.* (2018) que diz que uma blockchain “é uma cadeia de blocos de informações que registra transações com algumas características”. Estas características são definidas em função da finalidade da aplicação da tecnologia no contexto do problema a ser solucionado.

Acrescente-se ainda a definição adotada por Chuen e Deng (2017, *apud* Levin *et al.* 2016) “blockchain é uma estrutura de banco de dados que apenas pode ser atualizada anexando um novo conjunto (ou bloco) de transações válidas ao log de transações anteriores”.

As redes blockchain podem ser públicas ou privadas. Hileman e Rauchs (2017) entendem que existem três grandes tipos de permissão que podem ser definidos quando está se configurando uma rede blockchain, são elas:

- Read (quem pode acessar o livro-razão (ledger) e ver transações);
- Write (quem pode gerar transações e envia-las à rede) e
- Commit (quem pode atualizar o estado do ledger).

Neste contexto, "pública/privada" refere-se à capacidade de leitura (Read), enquanto "não-permissionada/permissionada refere-se à gravação (Write) e "Commit".

O modelo adotado neste trabalho foi o de rede privada permissionada, onde a autoridade fiscal tem permissão plena de leitura, escrita e commit e os beneficiários autorizados tem permissão de acessar e enviar transações à rede.

As transações enviadas para a rede tanto pela autoridade fiscal quanto pelos beneficiários são processadas por meio de smart contract.

Em linhas gerais, segundo I. Karamitsos *et al.* (2018) um smart contract (contrato inteligente) é um programa de código, escrito em linguagem de alto nível (neste caso Solidity), composto por um conjunto de funções executáveis e variáveis de estado, identificado por um endereço na rede blockchain. Cada transação enviada para a rede possui parâmetros de entrada necessários para a execução de uma função no contrato.

Tendo em mente os conceitos de blockchain e smart contract, podemos chegar à definição de DApp. A DApp nada mais é do que uma aplicação em que utiliza smart contract, fazendo uma interface amigável entre o usuário e o smart contract. O conceito de descentralização parte do princípio de que o código de um smart contract é compilado dentro de uma blockchain que, via de regra, é descentralizada. Uma DApp basicamente é estruturada por uma interface front-end composta por navegador web, HTML, CSS, etc. e uma interface back-end baseada em Web3 e JavaScript.

A interação entre a DApp e a blockchain é feita por meio de requisições, utilizando o protocolo de chamada remota JSON RPC.

## 3 A aplicação da tecnologia *Blockchain Ethereum* no programa Nota Legal DF

A tecnologia blockchain permite a persistência de dados de forma imutável e distribuída, isso proporciona maior segurança para o registro de informações. Outro ponto importante é que a tecnologia blockchain é auditável, ou seja, as transações realizadas na rede são verificáveis por meio de block explorers. Essa transparência traz maior credibilidade sobre as informações armazenadas na rede.

A criptografia empregada na rede assegura a autenticidade das transações e o não-repúdio da autoria.

Os endereços criados na rede são únicos e imutáveis. Associando esta característica às mencionadas anteriormente, conclui-se que é possível desenvolver soluções empregando o conceito de gestão de identidade, vinculando as permissões de transações na rede a grupos de endereços específicos, por meio de contratos inteligentes.

A utilização da tecnologia blockchain no programa Nota Legal DF se mostrou viável ao passo que é possível registrar na rede as transações relativas aos créditos, utilizações e números da sorte para sorteios, vinculados a contas (endereços) únicos para cada beneficiário. A conta criada é única para cada CPF/CNPJ informado no lançamento, garantindo assim que quaisquer créditos lançados para o CPF/CNPJ informado serão atribuídos à sua respectiva conta, independentemente de quantos lançamentos ou quais tipos de documentos fiscais sejam realizados..

O sistema é segregado em dois grupos, o primeiro é o da autoridade fiscal, que é responsável pela recepção, validação e lançamento dos registros de créditos na blockchain. O segundo é o grupo do beneficiário que passa a ser o proprietário dos créditos a partir do lançamento, sendo responsável pela sua gestão, tendo acesso à blockchain, por meio de uma interface web, para consulta dos lançamentos e também para utilizar os créditos acumulados, definindo o seu destinação.

Sendo a rede blockchain privada, apenas usuários autorizados poderão ter acesso às informações nela contida. Ademais, mesmos os usuários autorizados (no caso os beneficiários) somente terão acesso às informações vinculadas à sua respectiva conta gerada pelo contrato inteligente, garantindo a identidade e privacidade das transações.

# 4 *Minimum Viable Product* (MVP) para o programa Nota Legal DF na *Blockchain Ethereum*

Para demonstrar a viabilidade de utilização da tecnologia blockchain para persistência de dados do programa Nota Legal DF, este projeto apresenta por meio de um MVP (*minimum viable product*) um DApp que simula a geração de uma nota fiscal de mercadorias ou de serviços. A aplicação calcula os valores dos impostos gerados e os respectivos créditos do beneficiário no Programa Nota Legal DF, aplicando-se uma alíquota fictícia (em função da diversidade de alíquotas previstas no Regulamento do ICMS – RICMS-97 e no Regulamento do ISS – RISS-05 não foi possível, no contexto deste MVP, utilizar as alíquotas reais para cada produto ou serviço), registrando estes créditos numa blockchain Ethereum privada por meio de um Smart Contract.

O contrato implementa as regras para criação das contas, atribuição das permissões e as transações possíveis, sendo que os dados somente são persistido na blockchain após execução sem erros da regras contidas no contrato inteligente, evitando assim que informações sejam inseridas “manualmente” na blockchain.

No contexto do programa Nota Legal DF identificamos como partes interessadas (stakeholders), o Governo do Distrito Federal (GDF), a Secretaria de Estado de Fazenda do Distrito Federal (SEFAZ DF), o Tribunal de Contas do Distrito Federal (TCDF) e os beneficiários dos créditos (consumidores de produtos e serviços). A utilização desta tecnologia disruptiva no âmbito do programa traria, entre outros, os seguintes benefícios aos stakeholders:

- **Governo, Secretaria de Fazenda e Tribunal de contas**: o sistema continuaria a auxiliar o Governo a alcançar o objetivo de incrementar a arrecadação de impostos. A Secretaria de Fazenda e o Tribunal de Contas como participantes da rede (tecnicamente a rede seria implantada de forma distribuída nos servidores destes órgãos) teriam acesso pleno à rede, resguardadas as efetivas atribuições legais de cada órgão, sendo que para o SEFAZ DF o benefício mais relevante seria a segurança de ter um banco de dados das transações imutável e

distribuído, já para o TCDF a transparência das informações que estariam registradas na blockchain;

- **Beneficiários**: estes teriam o acesso à rede blockchain como usuários autorizados (sendo este acesso transparente ao usuário), podendo realizar consultas aos seus saldos de créditos e fazer a indicação da utilização num sistema capaz de garantir a autenticidade das transações realizadas, oferecendo maior segurança contra fraudes e um histórico permanente das transações realizadas.

*4.1 Funcionamento da solução*

A solução desenvolvida é composta de 3 (três) camadas:

- **Camada de persistência** – é a blockhain Ethereum propriamente dita. No escopo de MVP optou-se por criar uma rede Ethereum local (não distribuída) para racionalizar recursos financeiros com o provisionamento de servidores distribuídos em cloud.

- **Camada de controle** – é a camada que contém o smart contract. O contrato inteligente é a aplicação responsável pelo processamento das transações enviadas para a rede e contém as regras de negócios para a gravação das informações na blockchain.

- **Camada de aplicação** – trata-se do DApp, interface web permite aos usuários a comunicação com o smart contract e por consequência fazer registros na blockchain.

Em função de não ser possível ter acesso aos conjuntos de dados reais do programa Nota Legal DF, por se tratar de dados sensíveis, para provar a viabilidade da solução foi necessário construir um cenário que simulasse o processamento, por parte da SEFAZ DF, dos documentos fiscais emitidos pelos contribuintes (comerciantes). Os documentos fiscais simulados contêm basicamente o valor total da compra, a denominação do imposto (ICMS ou ISS), o valor total do mesmo e os respectivos números do CPF ou CNPJ do consumidor (beneficiário).

Para ficar mais simples a demonstração do registro das informações na blockchain convencionamos que lançamento dos documentos fiscais que geram os créditos aos beneficiários seria feito por um usuário com perfil denominado “Auditor” – este perfil é uma conta criada previamente na blockchain com credenciais que permitem manipular os dados referentes aos créditos e aos beneficiários.

Convencionamos também que o processamento seria de um documento fiscal de cada vez.

Toda conta criada recebe um endereço exclusivo na blockchain. O smart contract é responsável por identificar qual é o perfil de conta que esta sendo criada ou está acessando a rede.

Assim, temos um sistema com as seguintes funcionalidades básicas:

- **Criar conta de Auditor** – o smart contract cria um endereço na blockchain que recebe os atributos nome, CPF e senha. A autenticação no sistema é realizada pelo usuário com a informação dessas credenciais para permitir o acesso à funcionalidade de lançar créditos.

- **Lançar créditos** – o smart contract recebe o identificador CPF/CNPJ informado no documento fiscal e consulta na blockchain se há um endereço vinculado ao identificador. Se não houver, o smart contract atribui um novo endereço (cria uma conta) e registra o valor do crédito calculado e o respectivo número da sorte. Se uma conta já tiver sido criada para o identificador o contrato inteligente apenas manda adicionar à conta o valor do crédito calculado e o número da sorte correspondente. Esta é a principal funcionalidade da solução, atribuir uma conta única para cada beneficiário e adicionar a esta conta os valores dos créditos a que este tiver direito.

- Consultar créditos – A partir do momento que o smart contract cria uma conta para um beneficiário, este passa a ter acesso à blockchain para realizar a consulta dos seus créditos. Quando o usuário (consumidor) informar o seu identificador (CPF ou CNPJ) o smart contract consulta na blockchain a existência de uma conta para aquele identificar e retorna os dados que estiverem registrados para a mesma. Esta é uma funcionalidade deve ser aprimorada quando da implementação de um sistema para o ambiente de produção, acrescentando-se credenciais para assegurar a autenticação do beneficiário no sistema. Neste escopo de MVP apenas a informação de um identificador que tenha um endereço na blockchain já autentica o usuário beneficiário no sistema.

- Utilizar créditos – Ao consultar os créditos disponíveis o beneficiário poderá utilizá-los, fazendo a indicação da sua destinação. Neste MVP não foram abordados pormenores dos critérios de utilização dos créditos. Esta funcionalidade tem o principal objetivo de subtrair os valores correspondentes aos créditos da conta do beneficiário.

Todas as transações processadas pelo smart contract são registradas de forma permanente e imutável na blockchain, mantendo, assim, um histórico

das contas criadas, dos documentos fiscais geradores dos créditos e dos valores dos créditos movimentados, além dos números da sorte de cada beneficiário (funcionalidade Sorteio não contemplada neste MVP).

### *4.2 Infraestrutura*

A blockchain foi implementada localmente no node00, por meio do Parity Ethereum Client, versão 2.5.1. Este software é o responsável pela mineração dos blocos e pela execução do smart contract. O Parity Ethereum Client faz a comunicação do DApp com a blockchain utilizando o protocolo JSON RPC, por meio da biblioteca Web3. A conexão do node00 com o DApp ocorre na porta 8540.

O código do smart contract foi escrito em Solidity – linguagem de alto nível orientada a objetos para a implementação de contratos inteligentes - e deve ser compilado a partir da versão 0.5.0 da linguagem.

Para que o smart contract possa ser executado em uma rede Ethereum é necessário que o mesmo seja compilado, que seja gerado um código binário e que seja feito o *deploy* deste código na blockchain. Para executar estas tarefas foi utilizado o framework Truffle.

A camada de aplicação ou interface gráfica de usuário (GUI) foi desenvolvida a partir do framework progressivo Vue.js. A partir da integração desta interface com o blockchain é que chegamos ao conceito de DApp.

## 5 Discussão

O estudo de viabilidade de uma solução para persistência de dados presente neste trabalho pôde demonstrar que alguns aspectos relacionados ao armazenamento de dados podem ser aprimorados com a utilização da tecnologia disruptiva blockchain.

O uso desta tecnologia para persistir dados, em uma rede privada e distribuída, de forma imutável e manter o histórico permanente das transações realizadas vem com um propósito muito simples de aprimorar a segurança das informações armazenadas, sem deixar de lado a transparência dos registros, que podem ser facilmente auditáveis pelas autoridades responsáveis pela rede.

Com este propósito em mente, este trabalho apresenta num escopo de *minimum viable product* (MVP) uma solução moderna, conceitualmente no modelo de DApp, que permite fazer a persistência de dados no âmbito do programa Nota Legal DF. Dados estes referentes aos créditos obtidos pelos beneficiários do programa, bem como o registro das transações de utilização dos mesmos e outros dados pertinentes exigidos por lei.

A solução contempla principalmente o aspecto da segurança da informação armazenada e a individualidade das contas recebedoras dos créditos, garantindo que a informação do identificador (CPF/CNPJ) na emissão do documento fiscal no estabelecimento comercial quando lançada no sistema do programa Nota Legal DF, enviará o crédito para a conta (endereço na blockchain) vinculado ao respectivo identificador.

O uso de smart contract permitiu a criação desta solução, sendo ele o responsável pela execução das transações de acordo com as funções escritas no seu código e o registro das informações na blockchain.

Outro fator importante é a disponibilidade da aplicação. O fato de o código compilado do smart contract rodar diretamente na blockchain e que a proposta é de que esta esteja numa rede distribuída nos servidores dos órgãos participantes significaria dizer que dificilmente a aplicação ficaria indisponível.

Acrescente-se que, obviamente, por se tratar de um MVP nem todas as funcionalidades estão contempladas no projeto, mas que o as possibilidades de melhoramento da solução são viáveis.

Considerando ainda que em função de se tratar de informações fiscais, que são de grande relevância do ponto de vista econômico e que há a obrigação de se

manter o sigilo das informações fiscais por parte da Secretaria de Estado de Fazenda do Distrito Federal, não foi possível ter acesso às regras de negócio específicas, sendo implementadas no projeto apenas regras básicas, obtidas apenas por meio da experiência dos autores e da literatura consultada.

## 6 Conclusão

Este trabalho apresentou sob a forma de um *minimum viable product* (MVP), uma solução para persistência de dados do programa Nota Legal DF, empregando a tecnologia disruptiva blockchain.

A aplicação desenvolvida neste trabalho foi implementada em uma rede privada baseada na blockchain Ethereum. Os recursos disponibilizados pela tecnologia permitiram a criação de uma solução que adota o moderno conceito de DApp – aplicação que faz uma interface amigável entre o usuário e o smart contract (contrato inteligente) que roda de forma descentralizada na blockchain.

O desafio do estudo para desenvolvimento desta solução era chegar a um produto viável que pudesse aprimorar a segurança das informações registradas, bem como ampliar a transparência em relação às transações realizadas quantos aos créditos do programa Nota Legal DF. O alcance deste desafio ficou demonstrado na solução por meio da simulação de um sistema emissor de documento fiscal numa interface web. Os dados lançados neste sistema são as entradas para as transações que processadas por um smart contract e o resultado do processamento de cada transação é gravado de forma sequencial numa estrutura de dados em forma de blocos, denominada blockchain.

Para que a Secretaria de Estado de Fazenda do Distrito Federal adote a tecnologia blockchain para a persistência dos dados do programa ainda serão necessários alguns estudos sobre os processos de migração de tecnologia, custos envolvidos e legislação vigente.

Os resultados alcançados com este trabalho demonstraram a viabilidade do produto proposto e a sua adequação à realidade no âmbito do programa Nota Legal DF.

**Referências**

CHUEN, David LEE Kuo; DENG, Robert H. (org.) **Handbook of Blockchain, Digital Finance, and Inclusion: Cryptocurrency, FinTech, InsurTech, Regulation, ChinaTech, Mobile Security, and Distributed Ledger**. [*S.l.*]: Academic Press, 2017.

KRAUS, Daniel; OBRIST, Thierry; HARI, Olivier. **Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law**. [*S.l.*]: Edward Elgar Publishing, 2019.

KARAMITSOS, I., PAPADAKI, M. e AL BARGHUTHI, N.B. (2018) **Design of the Blockchain Smart Contract: A Use Case for Real Estate**. Journal of In-formation Security, 9, 177-190.

HILEMAN, Garrick e RAUCHS, Michel. **2017 Global Blockchain Benchmarking Study** (22 de setembro de 2017)

BRASÍLIA. **Lei nº 4.159, de 13 de junho de 2008**. Dispõe sobre a criação do programa de concessão de créditos para adquirentes de mercadorias ou bens e tomadores de serviços, nos termos que especifica. Brasília: Câmara Lesgislativa do Distrito Federal, [2008]. Disponível em: http://www.fazenda.df.gov.br//aplicacoes/legislacao/legislacao/TelaSaidaDocumento.cfm?txtNumero=4159&txtAno=2008&txtTipo=5&txtParte=COMPILADO. Acesso em 5 ago. 2019.

BRASÍLIA. **Decreto nº 18.955, de 22 de dezembro de 1997. (Regulamento do ICMS – RICMS/97)**. Regulamenta o Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte

Interestadual e Intermunicipal e de Comunicação - ICMS. Brasília: Palácio do Buriti, [1997]. Disponível em: http://www.fazenda.df.gov.br/aplicacoes/legislacao/legislacao/TelaSaidaDocumento.cfm?txtNumero=18955&txtAno=1997&txtTipo=6&txtParte=. Acesso em 5 ago. 2019.

BRASÍLIA. **Decreto nº 25.508, de 19 de janeiro de 2005**. Regulamenta o Imposto Sobre Serviços de Qualquer Natureza - ISS. Brasília: Palácio do Buriti, [2005]. Disponível em: http://www.fazenda.df.gov.br/aplicacoes/legislacao/legislacao/TelaSaidaDocumento.cfm?txtNumero=25508&txtAno=2005&txtTipo=6&txtParte=A)%20TEXTO%20ORIGINAL. Acesso em: 05 ago. 2019.

**Guia de normalização de trabalhos acadêmicos da Faculdade de Biblioteconomia e Comunicação da UFRGS**. Porto Alegre: Universidade Federal do Rio Grande do Sul. Biblioteca da Faculdade de Biblioteconomia e Comunicação. – 2019. Disponível em: http://www.ufrgs.br/bibfbc/a_biblioteca/documentos/guia-normalizacao. Acesso em 5 ago. 2019.

Parity. **Parity Ethereum Client**.Disponível em: https://www.parity.io/ethereum/**.** Acesso em 5 de ago. 2019.

Solidity. **Solidity**.Disponível em: https://solidity-portuguese.readthedocs.io/pt/latest/. Acesso em 5 ago. 2019.

Truffle. **Truffle**. Disponível em: https://www.trufflesuite.com/docs/truffle/overview. Acesso em 5 ago. 2019.

Vue. **Vue.js**. Disponível em https://br.vuejs.org/v2/guide/. Acesso em 5 ago. 2019.

## Anexo A – Código fonte arquivo Obito.sol

## Anexo B – Código fonte arquivo node_routes.js

## Anexo C – Código fonte arquivo contract.js