MANUAL DO PARTICIPANTE

Laboratório de Inovação - Dataprev

CONTEúDO

ANTES DE COMEçAR

Este documento tem como objetivo apresentar a rede blockchain de **Pessoa Física (b-CPF)** para os novos participantes e as informações contidas aqui podem ser alteradas sem aviso prévio caso entrem em conflito com o estado da rede.

1. SOBRE A REDE

1.1. CONCEITOS

Blockchain

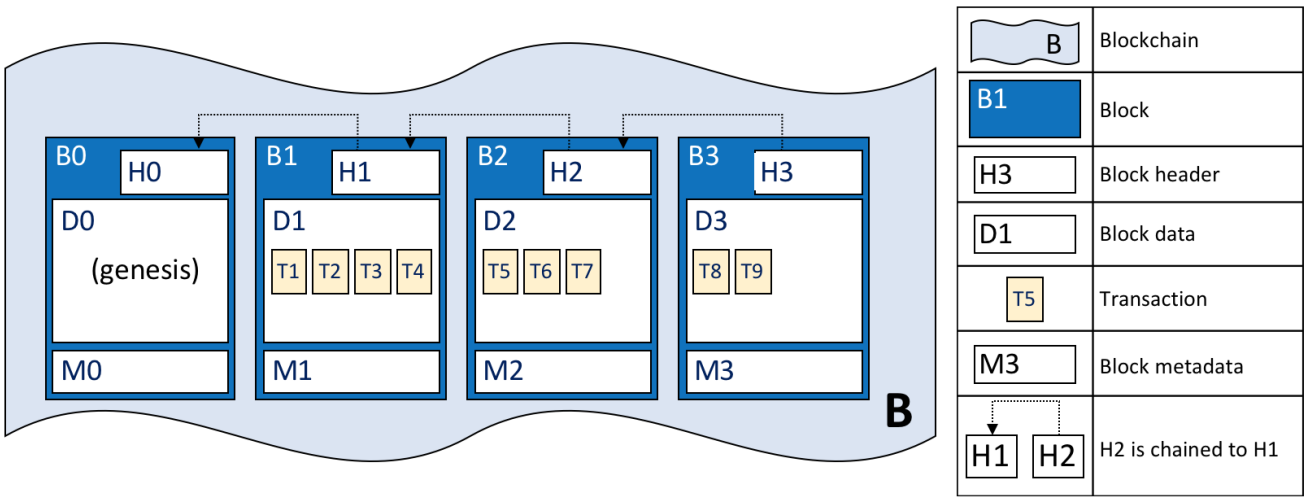
A Blockchain (também conhecida como "o protocolo de confiança") é uma tecnologia de registro distribuído, implementada através de nós de uma rede de computadores, que utiliza a descentralização como medida de confiança.

A partir de um conjunto de nós, a rede blockchain implementa estratégias de compartilhamento de informações e tomada de decisão distribuída, realizando a gestão global dos dados.

Para alcançar esse objetivo, a Blockchain utiliza uma estrutura conhecida como "Livro-caixa" ou "Livro-razão" (ver a seguir) que, analogamente a um livro-caixa contábil, adiciona informações de transações que ocorreram na rede, de modo linear e cronológico.

Protocolos criptográficos garantem que a informação do livro-caixa não pode ser alterada, viabilizando a implementação da não-repudiação.

Livro-Caixa Distribuído - Distributed Ledger



Os Livros-caixa podem ser considerados a fundação da contabilidade, sendo tão antigos quanto o dinheiro e a escrita [1]. Com o advento dos computadores, os livros em papel foram cedendo espaço para registros digitais, e mais recentemente, com o uso de criptografia, tornou-se possível a criação de livros-caixa

distribuídos, ampliando o uso deste conceito em outros campos de aplicação.

Em sua forma mais pura, um livro-caixa distribuído é uma base de dados mantida e atualizada de maneira independente por cada um dos participantes (nós) em uma rede blockchain. Não existe uma figura central, todos os nós possuem uma cópia das transações realizadas, garantindo redundância e integridade na rede.

Nesta arquitetura, toda transação deve ser processada e armazenada por cada um dos participantes, garantindo que apenas as mudanças consentidas por todos tenham validade.

Integridade da Rede

Os participantes de uma rede blockchain tem como atribuição primordial **minerar** os blocos de dados relativos às transações realizadas na rede.

A mineração é a atividade de validação realizada pelos nós (computadores), onde um desafio matemático é resolvido a fim de comprovar a autenticidade das transações contidas em um novo bloco. A cada novo bloco encadeado a rede impõe maior dificuldade à possibilidade de alterações arbitrárias, mantendo a rede saudável. Em redes blockchain públicas que implementam criptomoedas (ex: BitCoin), o trabalho de mineração pode ser recompensado com frações de cripto-moeda.

Contratos Inteligentes - Smart Contracts

Contratos inteligentes são protocolos eletrônicos, definidos através de linguagem de programação específica, com o objetivo de facilitar qualquer tipo de transação entre duas ou mais partes. Através da aplicação das regras definidas no contrato, garante-se a rastreabilidade, a confiabilidade e a legitimidade das transações e elimina-se a necessidade de envolvimento de terceiros responsáveis pela mediação entre as partes.

Aplicabilidade

Em geral, o uso de blockchain deve se considerado quando a necessidade de negócio tenha as seguintes características [4]:

- Há a necessidade de um banco de dados compartilhado;
- Há diversas partes (organizações) envolvidas na manutenção desta base;
- O processo de decisão destas partes sobre os dados trocados é transparente;
- Há regras uniformes regendo a comunicação entre os participantes da rede;
- Deseja-se manter um histórico de todas as transações que ocorreram na rede e na base de dados;
- Não há uma autoridade central que controla os dados;
- Velocidade na execução de transações não é uma prioridade;

- Volume de transações não é alto (menor do que 10.000 por segundo).

Por fim, historicamente redes blockchain têm sido aplicadas em contextos que podem ser agrupados em três categorias distintas, que são listadas a seguir.

Blockchain C2C (Consumer to Comsumer)

Modelo de comércio entre consumidores, de um para um, e foi o primeiro modelo aplicado ao Blockchain. O caso de uso mais famoso é o Bitcoin, que iniciou o conceito de economias virtuais. É o conceito de redes públicas: participantes anônimos transacionando um ativo relacionado a um valor.

Blockchain B2C (Business to Comsumer)

Modelo transaciona bens de um participante (fonte) para muitos destinatários. Este modelo pode se conectar a aplicações consumidas por usuários ou empresas conectadas ao fornecedor. Neste caso, o blockchain poderá ser parte de uma aplicação mobile, um componente dentro de uma aplicação cliente-servidor ou até registrando transações provenientes de um browser. Graças a capacidade de conectividade que as APIs oferecem, as opções de implementação tecnológica são infinitas.

Blockchain B2B (Business to Business)

Este modelo também é conhecido como permissionado. Numa rede de comércio privada (ou permissionada), os participantes (empresas, sistemas, objetos, áreas, processos ou até pessoas) se conhecem. Este conceito se refere a que o participante é registrado dentro da rede que certifica, identifica, garante a privacidade e a auditabilidade do membro.

A blockchain de Pessoa Física atende apenas ao terceiro cenário, Blockchain B2B.

Benefícios

A IBM cita cinco grandes benefícios alavancados pelo uso do blockchain [3]:

Transparência

Uma vez que o livro de registro de transações é distribuído, sendo ele mantido por todos os nós da rede, há transparência entre os participantes da rede no que se refere às operações realizadas sobre os dados.

Segurança

Numa rede blockchain, diversos mecanismos de segurança zelam pela integridade da mesma. Transações só são adicionadas ao blockchain depois de validadas por determinados nó; quando esta adição ocorre, a transação é encriptada antes de ser armazenada; por fim, o armazenamento dos dados e transações se dá em todos os nós, o que faz com que seja mais difícil que hackers forjem transações ou alterem o passado.

Rastreabilidade

A manutenção de todo o histórico de transações da rede faz com que seja possível mapear o histórico completo de todos os dados trocados.

Eficiência e Velocidade

Processos que envolvem documentos físicos e contratos estipulados em papel são difíceis de validar e suscetíveis a falhas humanas. Se o processo e o contrato forem estipulados digitalmente, de uma maneira que todos os entes envolvidos nele possam validá-lo rapidamente, ganha-se eficiência e velocidade na troca de informações.

Custos Reduzidos

O uso do blockchain elimina intermediários em negociações, pois todos os detalhes que governam a troca de ativos e informações são estipulados na parte lógica da rede: o contrato inteligente. Tendo em vista que este precisa ser instalado por todos os participantes, e que a troca de informações não ocorre caso este não seja igual em todos os pontos da rede, os custos com esta intermediação são reduzidos.

1.2. QUEM PODE PARTICIPAR DA REDE?

Entidades que possuam convênio vigente com a Secretaria Especial da Receita Federal do Brasil (RFB) para receber dados da base CPF ou que estejam amparadas pelo Decreto 8789/2016.

1.3. QUAIS SãO OS GRAUS DE CONFIANçA?

Os participantes da rede estão organizados nos seguintes graus de confiança:

Fundador

Receita Federal

Colaborador

Entidades com permissão de escrita na rede blockchain

Observador

Consumidores, parceiros e demais participantes da rede b-CPF

Estes graus indicam as permissões que uma determinada entidade tem em relação ao cadastro de Pessoa Física e são geridos pela Receita Federal.

1.4. QUAIS DADOS SãO GRAVADOS NA BLOCKCHAIN?

Apenas os dados relativos à entidade Pessoa Física serão gravados na blockchain, respeitando o modelo canônico definido pela RFB. O modelo canônico está disponível para consulta no anexo deste documento.

1.5. COMO FUNCIONA A GESTãO DA REDE?

A gestão dos dados de Pessoa Física é atribuição da RFB, sendo assim, portanto, mantida sua soberania sobre os dados trafegados na rede blockchain destinados a este fim.

Cabe à RFB definir quais participantes têm autoridade para incluir atualizações de Pessoa Física na blockchain, prerrogativa da qual poderá compartilhar apenas quando desejar ou quando outro participante possuir prerrogativa sobre a gestão de dados complementares ao modelo canônico.

Toda e qualquer atualização submetida por um participante da Rede será automaticamente bloqueada, sendo sua liberação de inteira responsabilidade da RFB.

1.6. O PROTOCOLO DE CONSENSO

Para alcançar o consenso na rede blockchain b-CPF utilizamos o algoritmo PoA - *Proof of Authority*. Nesse algoritmo, há um rodízio entre os nós mineradores para definir qual deles terá maior prioridade de mineração. A menos que o nó prioritário esteja offline ou com alta latência, o nó é assinado por ele e enviado à rede, que o aceita prontamente e o inclui na cadeia de blocos (*chain*). Não havendo disponibilidade do nó eleito, um novo nó recebe maior prioridade e assume a responsabilidade da mineração.

Nesse protocolo, os nós mineradores tem poder de propor adicionar ou remover novos minereadores se houver o consenso de 50%+1 dos atuais nós mineradores.

2. PARTICIPANDO DA REDE

Conforme modelo de negócio, é responsabilidade da RFB, fundadora da rede privada "b-CPF", prover os acordos de cooperação necessários com os demais órgãos interessados em participar da rede. Além da adesão consentida à rede por sua fundadora, o órgão interessado deverá adotar uma das modalidades de participação conforme previsto no modelo de negócio.

3. SEGURANçA DA INFORMAçãO

3.1. GESTãO DE CHAVES

A gestão das chaves privadas baseia-se na modalidade de utilização da rede adotada pelo órgão participante. As modalidades que lhe confere autonomia na gestão da infraestrutura também lhes atribui a responsabilidade de garantir a segurança da chave. Ao ser contratada para prover a infraestrutura necessária à adesão a uma rede, a Dataprev garante a segurança da chave privada através de suas tecnologias e serviços conforme descritos no modelo de negócio.

3.2. CRIPTOGRAFIA

A rede blockchain utiliza recursos de criptografia para garantir a integridade e a comunicação segura dos dados entre seus participantes, evitando que operações de atualização sejam realizadas sem o devido reconhecimento de seu emissor ou o acesso indevido aos dados.

3.3. CONTROLE DE ACESSO

A adesão à rede é realizada através da autorização de participação por parte do fundador da rede e da contratação do serviço junto à Dataprev conforme modalidades previstas no modelo de negócio. Apenas órgãos autorizados serão capazes de aderir à rede, pois receberão as informações necessárias (identificação da rede, identificador dos demais participantes e arquivo de gênesis). Ademais, após instanciação do nó participante, o fundador da rede registrará um contrato inteligente descrevendo as capacidades de acesso do participante.

>>>

3.4. CARACTERíSTICAS DA SEGURANçA DA REDE

As seguintes características são encontradas na rede b-CPF:

- A solução mantém em máquinas diferentes a etapa de mineração e o back-end da solução;
- A solução deixa o assinador de transações numa máquina separada e com acesso restrito;
- A Chave Pública de um nó não precisa ser exposta fora da rece b-CPF pois sua permissão se baseia no código *hash* da chave;
- A API implementada no nó tem acesso autenticado;
- A sistemática de permissões por perfis na blockchain é implementada via Smart Contract, que soluciona através de API específica para esse tipo de solução;
- A solução para definição do smart contract válido é implementada com protocolo https.

4. TECNOLOGIA

4.1. AMBIENTE DE REFERêNCIA

O ambiente de referência tem como base a seguinte configuração:

CPU

Processador Quad Core

Disco Rígido

Mínimo de 1 TB

Memória RAM

16 GB

Temos as seguintes estimativas de capacidade processamento para um nó na rede blockchain de Pessoa Física, considerando um modelo canonico com **24 campos / atributos**:

- 1 bloco a cada **15 segundos**
- **5760 blocos** gerados por dia
- **3000 transações** por bloco
- Aproximadamente **17 milhões de transações por dia**

Atualmente, temos a previsão de recebimento dos seguintes volumes de dados:

- Aproximadamente **60000 atualizações / inserções** na base de dados de Pessoa Física por dia
- Considerando o pior caso, com **24 atributos** sendo atualizados, temos um total de **aproximadamente 1 milhão e 400 mil transações por dia**, divididas em cerca de **500 blocos**.

Em relação ao armazenamento, temos as seguintes estimativas:

- O tamanho de um bloco pode variar entre **0.1 MB** e **1.3 MB**
- Espera-se que **53 GB** de dados sejam gerados mensalmente

GLOSSáRIO

Backend

Sistema responsável pelas regras de negócio, webservices e APIs de uma aplicação.

Contrato Inteligente

Código que contém a lógica que governará as transações e trocas de informação realizadas na rede blockchain.

Geth

Implementação, em linguagem Go, do protocolo Ethereum.

HSM

Hardware Security Module. Dispositivo físico que armazena chaves privadas com total segurança.

JSON

Formato de troca de dados.

Node

Interpretador de código Javascript.

NPM

Node Package Manager. Faz a gestão dos pacotes do Node.js, um interpretador de código Javascript.

REST

Representational State Transfer. Estilo de arquitetura baseado em HTTP que define operações de escrita e leitura para persistência de dados.

RPC

Remote Procedure Call, ou chamada remota de procedimento. É uma tecnologia de comunicação que permite que um processo localizado em um nó chame um procedimento que se encontra em outra máquina, suportando assim a comunicação entre sistemas remotos e distribuídos.

SGBD

Sistema de gerenciamento de banco de dados.

Solidity

Linguagem de programação criada especialmente para o desenvolvimento de contratos inteligentes Ethereum.

web3

API Javascript do Ethereum. Ela implementa o protocolo JSON RPC.

REFERêNCIAS

[coindesk] - What is a Distributed Ledger? https://www.coindesk.com/information/what-is-a-distributed-ledger/

[ethereum] - Site Oficial da Plataforma Ethereum https://www.ethereum.org/

[hyperledger] - Benefícios do Uso de Blockchain - IBM https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[medium] - Quando usar a tecnologia Blockchain https://medium.com/swlh/hyperledger-chapter-3-when-to-use-the-blockchain-technology-a5c414221bdf

ANEXO A: MODELO CANôNICO DE PESSOA FíSICA

Fazem parte do escopo da blockchain de Pessoa Física os seguintes atributos do modelo canônico:

Atributo	Formato	Tamanho	Descrição
cpf	Numérico	11	Número de inscrição no Cadastro de Pessoas Físicas.
nome	Alfa	60	Nome da Pessoa Física.
nomeSocial	Alfa	100	Nome Social da Pessoa Física
situacaoCadastral	Numérico	1	Indicativo da Situação Cadastral do CPF: 0 = Regular; 1 = Cancelada por Encerramento de Espólio; 2 = Suspensa; 3 = Titular Falecido; 4 = Pendente de Regularização; 5 = Cancelada por Multiplicidade; 8 = Nula; 9 = Cancelada de Ofício;
residenteExterior	Numérico	1	Indicativo de residente no exterior. 1 = Residente exterior e 2 = Residente no Brasil.
codigoPaisExterior	Numérico	4	Alguns registros apesar do Indicativo de Residente no Exterior igual a 1, apresentarão este valor como 0000(Brasil), uma vez que é informado o endereço de um representante no Brasil.
nomePaisExterior	Alfa	60	Idem informação anterior, o nome do país nos casos de informar o endereço de um representante no Brasil, virá em branco.
nomeMae	Alfa	60	Nome da Mãe da Pessoa Física: Ø Pode haver registro com o Nome da Mãe em Branco; Ø Pode haver registro com a constante “MAE DESCONHECIDA”.
dataNascimento	Numérico	8	Data de Nascimento da Pessoa Física.
sexo	Numérico	1	Indicativo de Sexo da Pessoa Física 1 = Masculino; 2 = Feminino; 9 = Sem informação.
naturezaOcupação	Numérico	3	Se o contribuinte não entrega DIRPF esta informação virá 000
ocupacaoPrincipal	Numérico	3	Se o contribuinte não entrega DIRPF esta informação virá 000
exercicioOcupacao	Numérico	4	Se o contribuinte não entrega DIRPF esta informação virá 0000

Atributo	Formato	Tamanho	Descrição
tipoLogradouro	Alfa	20	É o nome do tipo do logradouro do domicílio do CPF consultado.
logradouro	Alfa	60	O logradouro do domicílio do CPF consultado.
numeroLogradouro	Alfa	6	O número no logradouro do domicílio do CPF consultado.
complemento	Alfa	50	O complemento do logradouro do domicílio do CPF consultado.
bairro	Alfa	50	O bairro do domicílio do CPF consultado.
codigoMunicipio	Numérico	4	O código do município do estabelecimento consultado.
nomeMunicipio	Alfa	50	O nome do município do domicílio do CPF consultado, conforme tabela TOM Municípios.
UF	Alfa	2	A sigla da Unidade da Federação (Estado) do domicílio do CPF consultado.
cep	Numérico	8	O CEP do domicílio do CPF consultado.
DDI	Alfa	4	Será informado valores de 0000 a 9999. Caracteres restantes à direita virão com espaços
DDD	Alfa	2	Será informado valores de 11 a 99.
telefone	Alfa	12	Número do Telefone. "Será informado valores de 1 a 99999999999. Caracteres restantes à direita virão com espaços."
codigoUnidadeAdminstrativa	Numérico	7	Código da unidade administrativa que atende ao CPF. Será informado valores de 0110100 a 1010100
nomeUnidadeAdminstrativa	Alfa	50	Nome da unidade adminstrativa que atende ao CPF
anoObito	Numérico	4	Ano do óbito no formato AAAA.
estrangeiro	Numérico	1	Indicativo de pessoa estrangeira, sendo 0 para não estrangeiro e 1 para estrangeiro
codigoPaisNacionalidade	Numérico	4	País de nacionalidade. Serão informados valores de 0000 à 9999.
nomePaisNacionalidade	Alfa	60	Nome do país de nacionalidade. Quando o Código Pais de Nacionalidade for diferente de 0000, será informado o nome do país, senão espaços. Caracteres restantes à direita virão com espaços.

Atributo	Formato	Tamanho	Descrição
codigoMunicipioNaturalidade	Numérico	4	O código do município de naturalidade no CPF, conforme tabela TOM – Tabela de Órgãos e Municípios da RFB. Pode haver registros sem esta informação.
nomeMunicipioNaturalidade	Alfa	50	O nome do município de naturalidade no CPF, conforme tabela TOM – Tabela de Órgãos e Municípios da RFB. Pode haver registros sem esta informação.
ufMunicipioNaturalidade	Alfa	2	A sigla da Unidade da Federação (Estado/DF) do município de naturalidade. Quando o Código do Município de Naturalidade for diferente de 0000, será informado a UF, senão espaços
dataInscricao	Numérico	8	Data de inscrição no CPF. Formato "AAAAMMDD". Pode haver registro com data de inscrição zerada, indicando nesse caso a operação ter sido realizada antes de 10/nov/1990.
dataAtualizacao	Numérico	8	Data de inscrição do CPF ou da última operação de atualização. Formato "AAAAMMDD" Poderá ser igual à data de inscrição se não houve nenhuma operação de alteração. Pode haver registro com essa data zerada, indicando nesse caso a operação ter sido realizada antes de 10/nov/1990."