b-CNPJ

MANUAL DO PARTICIPANTE

DATAPREV

Conteúdo

Antes de começar....3
1. Sobre a Rede....3
1.1. Conceitos....3
1.2. Quem pode participar da Rede?....6
1.3. Quais são os graus de confiança?....6
1.4. Quais dados são gravados na Blockchain?....7
1.5. Como funciona a gestão da Rede?....7
1.6. O Protocolo de Consenso....7
2. Participando da rede....7
3. Segurança da Informação....7
3.1. Gestão de Chaves....7
3.2. Criptografia....8
3.3. Controle de Acesso....8
3.4. Características da Segurança da Rede....8
4. Tecnologia....9
4.1. Ambiente de Referência....9
Glossário....10
Referências....11
Anexo A: Modelo Canônico de Pessoa Jurídica....11

Antes de começar

Este documento tem como objetivo apresentar a rede blockchain de Pessoa Jurídica (b-CNPJ) 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

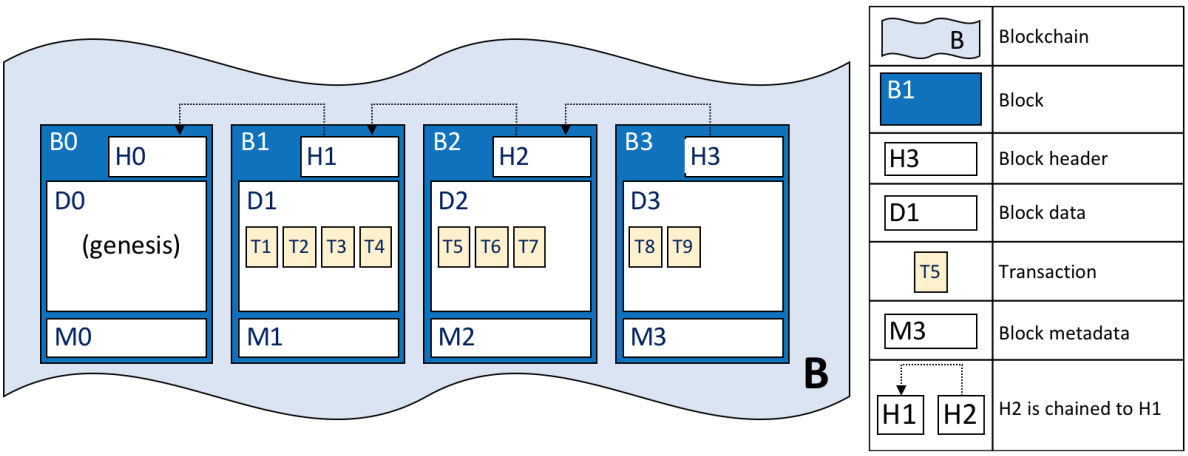
A Blockchain (também conhecida como "o protocolo de confiança") é uma tecnologia de registro distribuído, implementada através de nós de uma rede de computadores, que utiliza a descentralização como medida de confiança.

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 criptomoeda.

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.

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 (SRFB) para receber dados da base CPF ou que estejam amparadas pelo **DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019**.

1.3. Quais são os graus de confiança?

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

- Fundador
  - Receita Federal
- Observador
  - Órgãos participantes consumidoras de informação
- Colaborador
  - Órgãos participantes consumidoras de informação com permissão de escrita na rede blockchain

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 Jurídica serão gravados na blockchain, respeitando o modelo canônico definido pela SRFB. 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 Jurídica é atribuição da SRFB, sendo assim, portanto, mantida sua soberania sobre os dados trafegados na rede blockchain destinados a este fim.

Cabe à SRFB 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 SRFB.

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 têm poder de propor adicionar ou remover novos mineradores se houver o consenso de 50%+1 dos atuais nós mineradores.

2. Participando da rede

Conforme modelo de negócio, é responsabilidade da SRFB, fundadora da rede privada "b-CNPJ", 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 backend 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-CNPJ 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

HARDWARE

Para a realização das atividades de instalação recomenda-se a utilização de máquina virtual ou física com a seguinte configuração de hardware:

- Servidor A: Nó Ethereum (chain/ledger)
  - 8 GB de RAM
  - 500 GB de Disco Rígido
  - Processador Dual Core ou Superior
- Servidor B: Banco de dados (Postgres)
  - 8 GB de RAM
  - 750 GB de Disco Rígido
  - Processador Dual Core ou Superior
- Servidor C: Aplicação b-CNPJ (Node.JS)
  - 8 GB de RAM
  - 50 GB de Disco Rígido
  - Processador Dual Core ou Superior

SOFTWARE

É necessária a utilização de sistema operacional Linux, com as atualizações de segurança em dia e configurados para acessar a internet caso necessário.

Sistema Operacional

Software	Versão
Ubuntu Server	18.04.2 LTS
Debian Stable	10 (Buster)
Red Hat Enterprise Linux	7.4 ou Superior
CentOS	7
Oracle Linux	7.4 ou Superior

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 Jurídica

O modelo canônico no b-CNPJ está dividido em tabelas conforme demonstrado abaixo

DADOS DA EMPRESA			
CNPJ	14	N	NÚMERO DE INSCRIÇÃO NO CNPJ
NOME EMPRESARIAL	150	A	RAZÃO SOCIAL OU NOME EMPRESARIAL DA EMPRESA
NATUREZA JURÍDICA	4	N	CÓDIGO DA NATUREZA JURIDICA*
QUALIFICAÇÃO DO RESPONSÁVEL	2	N	CÓDIGO DA QUALIFICAÇÃO DO RESPONSÁVEL*
PORTE DA EMPRESA	2	A	CÓDIGO DO PORTE DA EMPRESA* 00 - NAO INFORMADO; 01 - MICRO EMPRESA; 03 - EMPRESA DE PEQUENO PORTE; 05 - DEMAIS
CAPITAL SOCIAL DA EMPRESA	14	N	VALOR DO CAPITAL SOCIAL DA EMPRESA (FORMATO IIIIIIIIIIIIDD - 12 INTEIROS E 2 DECIMAIS)

* A DESCRIÇÃO É ENVIADA NAS TABELAS DE DOMÍNIO

DADOS DO ESTABELECIMENTO			
CNPJ	14	N	NÚMERO DE INSCRIÇÃO NO CNPJ
MATRIZ/FILIAL	1	N	IDENTIFICA SE O ESTABELECIMENTO É MATRIZ OU A FILIAL: 1 – MATRIZ; 2 – FILIAL
NOME FANTASIA	55	A	NOME FANTASIA DO ESTABELECIMENTO
SITUAÇÃO CADASTRAL	2	N	CÓDIGO DA SITUAÇÃO CADASTRAL DO ESTABELECIMENTO* 01 – NULA; 02 – ATIVA; 03 – SUSPENSA; 04 – INAPTA; 08 – BAIXADA
MOTIVO DA SITUAÇÃO CADASTRAL	2	N	CÓDIGO DO MOVITO DA SITUAÇÃO CADASTRAL DO ESTABELECIMENTO *
DATA SITUACAO CADASTRAL	8	N	DATA DO ÚLTIMO EVENTO DE ALTERAÇÃO DA SITUACAO CADASTRAL (FORMATO AAAAMMDD)
SITUAÇÃO ESPECIAL	25	A	DESCRIÇÃO DA SITUAÇÃO ESPECIAL
DATA DA SITUACAO ESPECIAL	8	N	DATA DA SITUAÇÃO ESPECIAL (FORMATO AAAAMMDD)
DATA DE CADASTRO	8	N	DATA DE CADASTRO DO ESTABELECIMENTO (FORMATO AAAAMMDD)
CNAE FISCAL	7	N	CÓDIGO DA ATIVIDADE ECONÔMICA PRINCIPAL DO ESTABELECIMENTO*

TIPO DE LOGRADOURO	20	A	DESCRIÇÃO DO TIPO DE LOGRADOURO DO ENDEREÇO DO ESTABELECIMENTO
LOGRADOURO	60	A	LOGRADOURO DO ENDEREÇO DO ESTABELECIMENTO
NUMERO	6	A	NÚMERO DO ENDEREÇO DO ESTABELECIMENTO
COMPLEMENTO	156	A	COMPLEMENTO DO ENDEREÇO DO ESTABELECIMENTO
BAIRRO	50	A	BAIRRO DO ENDEREÇO DO ESTABELECIMENTO
UF	2	A	SIGLA DA UNIDADE DA FEDERAÇÃO DO ENDEREÇO DO ESTABELECIMENTO (EX – EXTERIOR)
CEP	8	A	CEP DO ENDEREÇO DO ESTABELECIMENTO
CÓDIGO DO MUNICIPIO	4	N	CÓDIGO DO MUNICÍPIO DO ESTABELECIMENTO (A DESCRIÇÃO É ENVIADA NAS TABELAS DE DOMÍNIO)
CIDADE NO EXTERIOR	55	A	NOME DA CIDADE NO EXTERIOR
PAÍS	3	A	CÓDIGO DO PAÍS DO ESTABELECIMENTO
DDD-1	4	A	DDD DO TELEFONE 1 DO ESTABELECIMENTO
TELEFONE-1	8	A	NÚMERO DO TELEFONE 1 DO ESTABELECIMENTO
DDD-2	4	A	DDD DO TELEFONE 1 DO ESTABELECIMENTO
TELEFONE-2	8	A	NÚMERO DO TELEFONE 2 DO ESTABELECIMENTO
EMAIL	115	A	CORREIO ELETRÔNICO DO ESTABELECIMENTO

* A DESCRIÇÃO É ENVIADA NAS TABELAS DE DOMÍNIO

CNAE SECUNDÁRIA			
CNAE SECUNDÁRIA	693	N	CÓDIGOS DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS DO ESTABELECIMENTO*

* A DESCRIÇÃO É ENVIADA NAS TABELAS DE DOMÍNIO

DADOS DOS SOCIOS			
CNPJ	14	N	NÚMERO DE INSCRIÇÃO NO CNPJ
IDENTIFICADOR DE SOCIO	1	N	IDENTIFICA O TIPO DE SÓCIO: "1 – PESSOA JURÍDICA 2 – PESSOA FISICA 3 – ESTRANGEIRO"
CNPJ/CPF DO SÓCIO	14	N	CPF OU CNPJ DO SOCIO, NO CASO DE SÓCIO ESTRANGEIRO É PREENCHIDO COM 'NOVES' O ALINHAMENTO PARA CPF É FORMATADO COM ZEROS À ESQUERDA.
QUALIFICACAO DO SOCIO	2	N	CÓDIGO DA QUALIFICAÇÃO DO SÓCIO
ENTRADA NA SOCIEDADE	8	N	DATA DA ENTRADA NA SOCIEDADE
PAÍS	3	A	CODIGO PAIS DO SOCIO ESTRANGEIRO
NOME DO PAÍS		A	
SOCIO ESTRANGEIRO	150	A	NOME DO SÓCIO ESTRANGEIRO
CPF DO REPRESENTANTE LEGAL	11	N	NUMERO DO CPF DO REPRESENTANTE LEGAL
QUALIFICACAO REPRESENTANTE LEGAL	2	N	CÓDIGO DA QUALIFICAÇÃO DO REPRESENTANTE LEGAL

SIMPLES/MEI

OPÇAO PELO SIMPLES / MEI	2	A	Período de opção pelo Simples Nacional (SN) Período de Enquadramento no MEI (ME)
DATA DA OPÇAO	8		Data início do período AAAAMMDD
DATA DA EXCLUSÃO	8		Data fim do período AAAAMMDD, caso seja um período aberto será informado 00000000