PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

OS CONFLITOS ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A TECNOLOGIA *BLOCKCHAIN*

DANIEL RODRIGUES QUEIROZ

GOIÂNIA
2020

DANIEL RODRIGUES QUEIROZ

OS CONFLITOS ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A TECNOLOGIA *BLOCKCHAIN*

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Sibelius Lellis Vieira

Banca examinadora:

Prof. Me. Wilmar Oliveira de Queiroz

Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA

2020

DANIEL RODRIGUES QUEIROZ

OS CONFLITOS ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A TECNOLOGIA *BLOCKCHAIN*

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em _____/_____/_____.

_____

Orientador: Prof. Dr. Sibelius Lellis Vieira

_____

Prof. Me. Wilmar Oliveira de Queiroz

_____

Prof. Me. Gustavo Siqueira Vinhal

_____

Profª. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

GOIÂNIA
2020

AGRADECIMENTOS

Agradeço enormemente aos meus pais por serem o meu porto seguro e apoiarem os meus estudos e os meus objetivos e confiarem no meu potencial. Também agradeço pela orientação e dedicação do Professor Sibelius Lellis Vieira para que este trabalho fosse desenvolvido com êxito, minuciosidade e clareza.

RESUMO

Este trabalho descreve o estudo da Lei Geral de Proteção de Dados Pessoais (LGPD) e sua interação com a tecnologia *blockchain*, baseando-se no regulamento europeu de proteção aos dados, uma vez que este está em vigência e os conflitos com as tecnologias atuais estão definidos. Analisando as questões levantadas na comunidade acadêmica, referentes aos problemas entre o regulamento europeu e a tecnologia *blockchain,* a Lei Geral de Proteção aos Dados foi analisada, para que assim os pontos de conflito fossem identificados, permitindo uma identificação dos problemas mais promissores para serem resolvidos. Desta forma, é possível analisar as possíveis soluções para o direito ao esquecimento, no caso deste trabalho*,* e em particular indicar se são realizáveis e em quais circunstâncias.

Palavras-chave: *blockchain*; *smart contracts*; LGPD; direito ao esquecimento; imutabilidade; conflitos; dados pessoais.

ABSTRACT

This work describes the examination of some aspects of the Lei Geral de Proteção de Dados Pessoais (LGPD) and its interaction with blockchain technology, based on the European data protection regulation, since it is currently running and conflicts with blockchain are defined. Analyzing the issues raised by the scholars, regarding the problems between European regulation and blockchain technology, the LGPD was analyzed, in order to pinpoint the points of conflict, in particular the right to erasure. In this sense, it is possible to indicate the possible solutions to the right to erasure, with some feasible revision in the blockchain technology, and to present the circumstances under which this can be implemented.

Keywords: blockchain; smart contracts; LGPD; erasure; immutability; conflicts; personal data.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

CNPJ	Cadastro Nacional da Pessoa Juridical
GPDR	*General Data Protection Regulation*
GPS	*Global Positioning System*
LGPD	Lei Geral De Proteção de Dados Pessoais
P2P	*Peer to Peer*
PL	Projeto de Lei
UE	União Europeia

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

A geração e captação de dados pessoais cresce continuamente. Em situações nas quais as pessoas estão envolvidas, as organizações coletam seus dados, seja uma compra no cartão de crédito/débito, utilização de aplicativo de transportes, um passeio pela rua, uma simples navegação pela internet, publicações em redes sociais etc. Existem condições para que as empresas produtoras dos modernos aparelhos celulares possam ter acesso às localizações do usuário ainda que o sistema GPS (*Global Positioning System*) esteja desligado. (SANTOS, 2020)

A *General Data Protection Regulation* (GDPR) da União Europeia (UE) tornou-se obrigatória em maio de 2018. Baseia-se na Diretiva de Proteção de Dados de 1995. O objetivo do GDPR é essencialmente duplo. Por um lado, procura facilitar a livre circulação de dados pessoais entre os vários Estados-Membros da EU (SHARMA, 2020). Por outro lado, estabelece um quadro de proteção dos direitos fundamentais, baseado no direito à proteção de dados no Artigo 8 da Carta dos Direitos. (FINCK, 2019)

A Lei Geral de Proteção de Dados Pessoais (LGPD) adotou o modelo do regulamento europeu. A LGPD é mais resumida, mas tem em grande parte, os mesmos fundamentos da GDPR. Conforme Maciel (2019), “A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade”. Isto porque o que se observa é um maior número de situações de vazamento de dados, o que causa preocupação na sociedade de forma geral e pode afetar o valor dos negócios.

Primeiro, o GDPR baseia-se na suposição subjacente de que, em relação a cada ponto de dados pessoais, há pelo menos uma pessoa singular ou coletiva - o controlador de dados - a quem os titulares de dados podem se dirigir para fazer valer seus direitos sob a lei de proteção de dados da UE. (FINCK, 2019).

Para fazer frente ao uso de dados, várias tecnologias têm sido empregadas. Uma das mais promissoras é a que se baseia em um ambiente descentralizado para transações de variados tipos, conhecida como *blockchain*, e que é a base para o protocolo de moedas digitais.

Em essência, um *blockchain* é um banco de dados digital compartilhado e sincronizado, mantido por um algoritmo de consenso e armazenado em vários nós, computadores que armazenam uma versão local do banco de dados. (FINCK, 2019).

As *blockchain*, no entanto, buscam obter descentralização na substituição de um ator unitário por muitos atores diferentes. (FINCK, 2019).

Dada a sua grande diversidade de usos possíveis, os *public blockchain* acabam por trazer grande dificuldade para efetivar medidas de proteção na forma requerida pela lei. Vários são os desafios, tais como o direito ao esquecimento, a responsabilização do controlador dos dados em caso de ilícito, etc. As *blockchain* privadas são mais promissoras, mas não demonstraram na totalidade a condição de resolver os problemas propostos pela legislação.

Neste trabalho, procura-se examinar alguns destes casos e, em particular, apresentar uma discussão em relação ao direito ao esquecimento e a possibilidade de se retirar ou apagar blocos anteriores do *blockchain*, para permitir que as diretrizes da legislação sejam atingidas (REBELO, 2019).

1.2. Objetivo

1.2.1. Objetivo Geral

Este trabalho visa analisar os pontos de conflito e consenso da LGPD com a tecnologia *blockchain*, baseando-se na fundamentação teórica do relacionamento entre esta tecnologia e a GDPR, de forma que se possa definir pontos de mudanças para a obtenção da conformidade entre a tecnologia *blockchain* e a LGPD, em particular em relação ao direito ao esquecimento.

1.2.2. Objetivos específicos

- Identificar os pontos de conflitos entre a LGPD e tecnologia *blockchain*.
- Identificar os pontos de consenso entre a LGPD e tecnologia *blockchain*.
- Definir mudanças na utilização da *blockchain* perante a LGPD.
- Analisar propostas para o direito ao esquecimento e a *blockchain*.

1.3. Estrutura do trabalho

Este trabalho apresenta-se dividido em cinco capítulos, sendo o primeiro a introdução, o segundo capítulo composto pela pesquisa bibliográfica, o qual define os fundamentos teóricos do trabalho, a LGPD, a tecnologia *blockchain* e a interação entre LGPD e *blockchain.* No terceiro capítulo encontra-se os materiais e os métodos utilizados para realização da pesquisa. O quarto capítulo descreve um estudo de caso para o qual são feitas alterações em um *blockchain* para prover os requisitos da LGPD. O quinto capítulo apresenta as considerações finais e os possíveis trabalhos futuros.

2. REFERENCIAL TEÓRICO

Neste capítulo são apresentados os conteúdos utilizados para a fundamentação teórica do trabalho, abordando de forma sucinta o tema e seus conceitos, assim como a relação da nova lei brasileira e a tecnologia *blockchain*, visando apresentar as mudanças feitas pela (LGPD) e seu no impacto no uso da tecnologia *blockchain* como elemento de armazenamento de dados pessoais.

2.1 A Lei Geral de Proteção de Dados Pessoais (LGPD)

A sociedade atual vivencia a revolução em decorrência da tecnologia e informação, estando rodeados de aparelhos os quais captam e distribuem os dados concebidos pelas pessoas a todo momento. Devido à grande vazão de dados e informações pessoais dos cidadãos, governos ao redor do mundo decidiram aprovar leis para a proteção das informações dos seus cidadãos. Desde 2018 o Brasil se tornou um dos países a reconhecer a importância da proteção dos dados.

A legislação denominada GDPR é o regulamento de privacidade e proteção aos dados pessoais da União Europeia, na qual a LGPD foi baseada. Elas se diferenciam nas políticas de proteção de dados, transferência internacional de dados fiscalização do cumprimento da lei, a relação entre o controlador e operador entre outros.

2.1.1 Definição e fundamentos

A LGPD, Lei n° 13.709/2018, é a lei brasileira a qual tem o intuito de regular o tratamento dos dados pessoais do cidadão. (BRASIL, 2018)

No Artigo 2° da lei é estabelecido que a disciplina da proteção de dados pessoais tem como fundamentos, o respeito à privacidade, a inviolabilidade da intimidade do cidadão, liberdade de se expressar, comunicar, opinar e se informar, o direto de exercer a liberdade sobre as ações referente aos seus dados, além de dos dignos diretos de livre iniciativa e concorrência, desenvolvimento econômico, tecnológico e a inovação.

2.1.2 Tratamento de dados pessoais

De acordo com Maciel (2019) a lei geral de proteção de dados pessoais define dado pessoal como sendo qualquer “informação relacionada a pessoa natural identificada ou identificável”. Dessa definição pode-se induzir que um dado pessoal comporta um grande número de situações que vão bem além dos nomes, prenomes, endereços e número de cadastro de pessoa física.

O Regulamento 2016/679 da União Europeia (*General Data Protection Regulation* - GDPR), uma das bases para a LGPD, em seu art.4°, n.1, os dados pessoais foram definidos como:

> Dados pessoais: informação relativa a uma pessoa singular identificada ou identificável (<<titular dos dados>>); é considerado identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genético, mental, económica, cultural ou social dessa pessoa singular.

Por outro lado, segundo Maciel (2019) “Há dados que sozinhos não podem identificar uma pessoa, porém quando agregados a outros passam a ter essa capacidade”. Como exemplos, podem ser citados informações empresariais, tais como o Cadastro Nacional de Pessoa Jurídica, o número IP, o número de identificação eletrônica, entre outras. São, portanto, também vistos como dados pessoais, para os propósitos da lei.

Os dados anonimizados são o oposto dos dados pessoais visto que os dados anonimizados seriam aqueles que não tem nome e nem rosto, embora mantenham o conteúdo. O dado anônimo ou anonimizado não é pessoal, pois não permite a identificação do indivíduo a partir deste. Não há uma relação entre este e a pessoa natural. A anonimização implementa uma ocultação de informações de modo que quando forem disponibilizadas para uso, torna-se impossível obter a identificação do perfil que os dados pertenciam antes do processo.

A pseudonimização consiste no tratamento dos dados de forma que qualquer dado perca a possibilidade de associação direta ou indireta a um indivíduo, a não ser pelo o “*uso de informações complementares mantidas de forma separada pelo controlador em ambiente controlado e seguro*” (CUNHA, 2018).

A legislação de proteção de dados pessoais não tem como intuito a burocratização ou proibição do tratamento de dados, mas sim a afirmação de uma base legal constituída pelo Artigo 7° da LGPD. Este explica que os dados podem ser tratados desde que sejam usados pelo consentimento do titular dos dados, cumprindo as obrigações legais ou regulatórias pelo controlador, pela administração pública, utilização por órgãos de pesquisa, proteção da vida ou da incolumidade física do titular ou de terceiros, entre outros.

De acordo com o Artigo 15° da LGPD, o tratamento de dados pessoais pode ser interrompido desde que: o período de tratamento tenha expirado ou o objetivo da utilização dos dados tenha sido alcançado. Além disso o titular dos dados pode exercer seu direito de revogar o seu consentimento (BIONI, 2018). Outro ponto é quando houver algum tipo violação disposta na lei, a autoridade nacional poderá determinar o fim do tratamento destes dados.

2.1.3 Agentes de tratamento

Os agentes de tratamento, de acordo com o Artigo 5° da LGPD são definidos como controladores e operadores, possuindo uma relação hierárquica, sendo o operador um mandatário do controlador o qual audita os procedimentos realizados pelo operador.

O controlador (*controller*), conforme extraído do regulamento europeu, é uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, isoladamente ou conjunto com outras pessoas, determinam os propósitos e meios do tratamento dos dados pessoais. O operador (*processor*), por seu lado, é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

As funções do controlador e do operador podem ser definidas da seguinte forma segundo o artigo 5°, VI e VII da LGPD:

- controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

É o controlador quem determina, portanto, os propósitos que devem ser seguidos pelo operador quando do tratamento dos dados do titular.

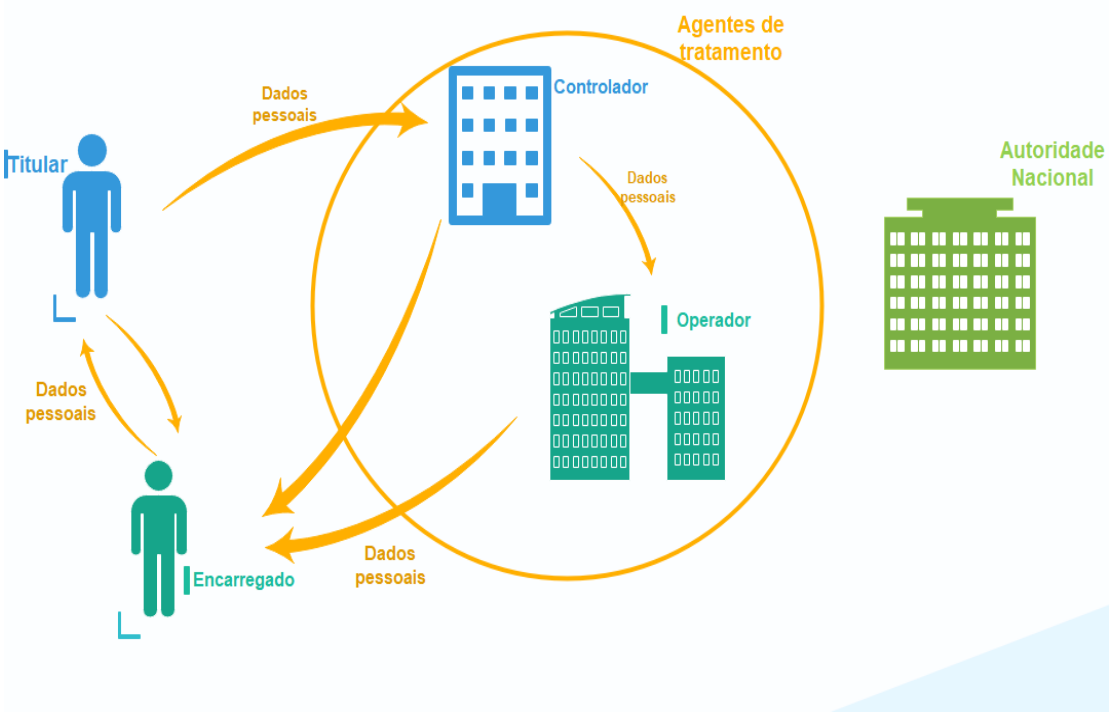
Algumas atribuições que os operadores devem ter perante a LGPD são as de realizar as alterações dos dados conforme as normativas fornecidas pelo controlador, não tendo ingerência sobre a inteligência destas alterações, ou melhor, devem seguir o observado pelo controlador. Devem também manter o registro das ações de processamento ou histórico dos tratamentos realizados e eventualmente, cumprir obrigações acessórias.

Para realizar o tratamento de dados um responsável por esse processo deve ser indicado pelo controlador e operador conforme definido no Artigo 5°, VIII. Este é o encarregado, ou *Data Protection Officer*, que é a pessoa natural ou jurídica indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL, 2018).

Os encarregados têm como atribuições aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e adotar providência, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Na Figura 1 é ilustrado a esquematização da interação dos dados do titular com os agentes de tratamento, sendo que os dados do titular são enviados para o controlador que então repassa para o operador. Ainda, os dados são compartilhados com o encarregado para que o mesmo possa ter plena comunicação para com o titular a respeito. O encarregado cumpre obrigações e como tal não pode ser punido por tal atribuição. Neste sentido, para que não haja problemas de relacionamento entre estes agentes, é interessante que seja um componente terceirizado, a parte do controlador.

Figura 1 – Esquema de interação das partes



Fonte: Elaborado pelo autor

Esse canal de comunicação estabelecido entre os envolvidos no tratamento de dados é de vital importância porque define e centraliza na pessoa do encarregado as informações das providências tomadas ou que devam ser tomadas, ou seja, é ele quem deve ser procurado para todos os esclarecimentos e requerimentos que dizem respeito ao tratamento de dados. Daí a importância da documentação e registro de todos os atos (SANTOS, 2020).

2.1.4 O titular dos dados

O titular dos dados é qualquer pessoa natural, não podendo, portanto, ser pessoa jurídica, conforme a dicção do artigo 17 da LGPD, o qual assegura a titularidade de seus dados pessoais a estes. Em conjunto com o que preconiza o artigo 18, que estabelece o direito do titular dos dados, forma-se o subsistema do titular na LGPD. Pode o titular requisitar ao controlador informações a respeito de seus dados, tais como por exemplo, a confirmação da existência de tratamento, acesso aos dados, correção dos dados, eliminação dos dados pessoais, além de informações de com quais entidades públicas e privadas os dados foram compartilhados.

Os direitos do titular são exercidos em relação ao controlador, que é obrigado a atender às solicitações do titular, podendo tais solicitações implicar em situações em que o operador esteja envolvido, pois este é quem realiza o processamento dos dados a critério do controlador. Portanto, embora o operador não tenha que responder diretamente ao titular dos direitos, é natural seu envolvimento no processo.

2.1.5 Direito ao esquecimento

Um dos mais notáveis pontos da LGPD é o direito do titular dos dados ao esquecimento, ou seja, ao titular dos dados é assegurado de que os seus dados serão devidamente apagados ou desativados quando não mais forem ser utilizados ou quando o próprio se sentir na necessidade de solicitar sua exclusão. Conforme descrito por Cunha (2018) a remoção de dados pessoais sempre foi considerada um empecilho para que fosse solicitada, o que fazia com que a maioria das pessoas declinasse deste direito. As novas legislações sobre dados pessoais procuram resgatar este direito fundamental.

Não apenas o titular poderá solicitar o esquecimento dos dados como é determinado no Artigo 15° da Lei, mas também a autoridade nacional, conforme observado na legislação. Também interessa à sociedade brasileira como um todo o respeito aos dados pessoais. Logo, mesmo havendo consentimento individual, poderá a Autoridade Nacional impedir o tratamento dos dados, se entender que trata de um direito transindividual.

Existem exceções as quais são especificadas no Artigo 16 da Lei, que permitem a retenção dos dados, que podem ser vistas como uma mudança de base legal.

Os Artigos 16 e 17 definem o termo esquecimento, que tem um significado dúbio quando colocada desta forma. Pode-se supor que o entendimento da palavra deve vir do bom senso da terminologia utilizada. Quando se pensa em esquecimento de dados, logo se vem em mente a exclusão dos dados, ainda que se possa pensar na destruição do *hardware* no qual os dados estão guardados. Esta ambiguidade é um problema tanto na LGPD quanto da GDPR como explica Rebelo (2019). Além deste âmbito, também caberá perguntar o que efetivamente constitui a noção de “esquecimento”. Será que representa o total desaparecimento dos dados do mundo

real e/ou virtual, ou basta que haja técnicas de proteção que tornem os mesmos criptografados de forma irreversível?

2.2 A tecnologia *Blockchain*

Em essência, um *blockchain* é um banco de dados digital compartilhado e sincronizado, mantido por um algoritmo de consenso e armazenado em vários nós (computadores que armazenam uma versão local do banco de dados). As *blockchains* são projetadas para obter resiliência por meio da replicação, o que significa que muitas vezes há muitas partes envolvidas na manutenção desses bancos de dados.

Cada nó armazena uma cópia integral do banco de dados e pode atualizar o banco de dados independentemente. Nesses sistemas, os dados são coletados, armazenados e processados de maneira descentralizada. Além disso, *blockchains* são *ledgers*, ou seja, um conjunto de transações ordenadas de acordo com alguma regra, seja temporal ou por classe, aos quais os dados podem ser adicionados, mas removidos apenas em circunstâncias extraordinárias (FINCK, 2019).

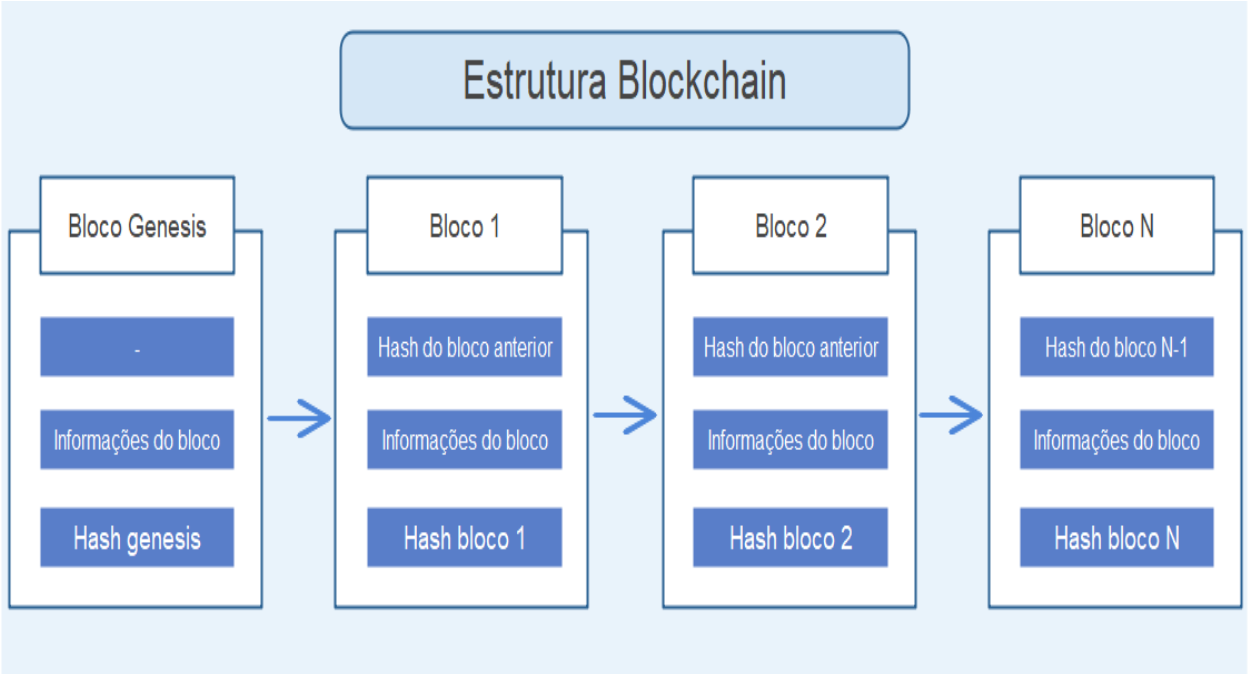
Um modelo centralizado assume controle central por uma autoridade, enquanto um modelo descentralizado não assume controle. Há também o elemento de (des) centralização arquitetônica, em que uma solução clássica, como um banco, possui um ponto de conexão que unifica todos os nós do sistema, tornando-o centralizado. O *blockchain*, por outro lado, utiliza uma rede *peer-to-peer* (P2P) sem ponto central de falha, que conecta todos os nós de maneira semelhante à Web, tornando-o descentralizado da arquitetura (RAMSAY, 2018).

2.2.1 Estrutura do blockchain

A estrutura de dados da *blockchain* não é completamente diferente de um catálogo de cartões de biblioteca físico, em que cada cartão tem uma referência a um livro que está sendo armazenado em algum lugar da biblioteca. Em vez dos cartões seguirem uma ordem cronológica, eles consultariam o cartão anterior, criando uma cadeia de cartões. Essa ideia descreve uma imagem mais precisa da estrutura de dados de *blockchain*. A Figura 2 ilustra um encadeamento de blocos que é composto por blocos contendo: um cabeçalho de bloco, uma referência ao cabeçalho de bloco anterior, e dados de transação contidos em uma estrutura

semelhante a uma árvore de decisão, desde que pode criar ramificações. Esses componentes formam um bloco, um conjunto de blocos, compõem o *blockchain* (RAMSAY, 2018).

Figura 2 – Estrutura *blockchain*



Fonte: Elaborado pelo autor

2.2.2 Criptografia de dados

Um *hash* criptográfico é uma função matemática que alimenta um valor de entrada, o qual é transformado em um valor de saída de comprimento fixo. Para entender as funções de *hash*, é imperativo observar que a mesma entrada sempre produz a mesma saída (o que significa que elas são determinísticas). Além disso, não é possível deduzir a entrada de uma função de *hash* através de seu resultado de saida (FINCK, 2019).

A *blockchain* também utiliza um modelo criptográfico matemático chamado criptografia assimétrica, também conhecida como criptografia de chave pública, que possibilita a leitura de dados criptografados usando uma chave, ao contrário dos quebra-cabeças de *hash* que só podem ser resolvidos pelo poder computacional. A criptografia assimétrica envolve o uso de dois conjuntos de chaves, uma para criptografar os dados, ou seja, transformá-los em algo ilegível e outra chave usada para descriptografar os dados, transformando-os em algo legível, ao contrário da

criptografia simétrica, que usa uma chave para criptografar e descriptografar.(RAMSAY, 2018).

2.2.3 Armazenamento offchain

Dependendo do caso de uso específico da *blockchain*, pode não ser necessário armazenar todos os dados transacionais na própria *blockchain*. Em vez disso, esses dados poderiam ser armazenados em outro banco de dados fora da cadeia e apenas vinculados ao livro distribuído por meio de um *hash*, um processo que teria várias vantagens do ponto de vista da proteção de dados (FINCK, 2019).

2.2.4 Blockchain privado

Existem três categorias de aplicações do *blockchain*: público, consórcio e privado.

As permissões de gravação privadas são mantidas centralizadas em uma única organização ou parte dela. As permissões de leitura podem ser públicas ou restritas a um conjunto de participantes conhecidos. Em suma, existem realmente duas categorias, pública e privada. O consórcio é um derivado do *blockchain* privado com vários membros/participantes identificados e com permissão (BAMBARA; ALLEN, 2018).

Um *blockchain* público é composto por uma quantidade N nós, onde é permitido o ingresso de qualquer usuário, além de permitir realizar operações e participar de processos de consenso. Assim, o *blockchain* público é completamente descentralizado o que faz necessário os nós estarem sempre sincronizados, e a cadeia de blocos de *blockchains* públicos são em sua maioria muito grandes, o que implica em uma grande quantidade de tempo e esforço para realizar as operações.

Diferente dos públicos, os *blockchains* privados necessitam de permissão para que usuários e nós possam ingressar em sua rede. (DHULAVVAGOL; BHAJANTRI; TOTAD,2020). Comparado ao *blockchain* público, o *blockchain* privado é muito mais rápido, seguro, eficiente, e neste caso, todas as permissões são realizadas de forma centralizada.

Recentemente, o conceito de *blockchains* privados se tornou popular dentro de discussões sobre esta tecnologia, principalmente entre instituições financeiras. Ao invés de ser uma rede totalmente descentralizada aberta ao público com partes

anônimas, é possível criar um sistema onde cada parte é identificada e recebe permissões para alterar ou ler o *blockchain*. Essas cadeias de bloqueio privado também estão lidando com o problema de desempenho porque o consenso é realizado em menos nós. Na verdade, é provável que haja muitas redes *blockchain* com cada rede servindo a um conjunto diferente de objetivos e aplicativos de negócios distintos (BAMBARA; ALLEN, 2018).

2.3 Tecnologia Ethereum

O *Ethereum* foi criado para servir como uma plataforma para a construção baseada no *blockchain* ou em aplicações descentralizadas. Desenvolvida pela fundação *Ethereum*, uma organização sem fins lucrativos da Suíça, que possui contribuições de todo o mundo (BAMBARA; ALLEN, 2018)

O *Ethereum* é bem aplicado para aplicações que precisam ser construídas rapidamente e que interagiam com eficiência e segurança em um ecossistema *blockchain*. O *Ethereum* é projetado para atua como uma infraestrutura programável, ou seja, é uma plataforma de desenvolvimento mais adaptável e flexível. Permite a construção inteligente de contratos e aplicações com suas próprias regras arbitrárias de propriedade, formatos de transação e logica de transição de estado (BAMBARA; ALLEN, 2018).

2.3.1 Contas Ethereum

No *Ethereum*, o estado atual é composto de objetos comumente chamados de contas. *Ethereum* pode ser visto como uma máquina de estado baseada em transações, começando com a estado gênese e transações de execução incremental que transformam o estado em um estado final. O estado final é o que é considerado a “versão” canônica no mundo do *Ethereum*. O estado inclui qualquer coisa que atualmente possa ser representada por um computador, como saldos de contas, reputações, acordos de confiança e dados que representam informações no mundo físico. Transações, portanto, representam uma transição válida entre dois estados (BAMBARA; ALLEN, 2018). Cada conta no *Ethereum* tem um Endereço (ou identidade) de 20 bytes e o objeto é composto por quatro atributos ou campos, que são:

• *Nonce:* Contador que é usado para garantir que cada transação possa ser processada uma vez e apenas uma vez.

• Saldo de éter: O valor atual da conta.

• Código do contrato: Um contêiner opcional para lógica.

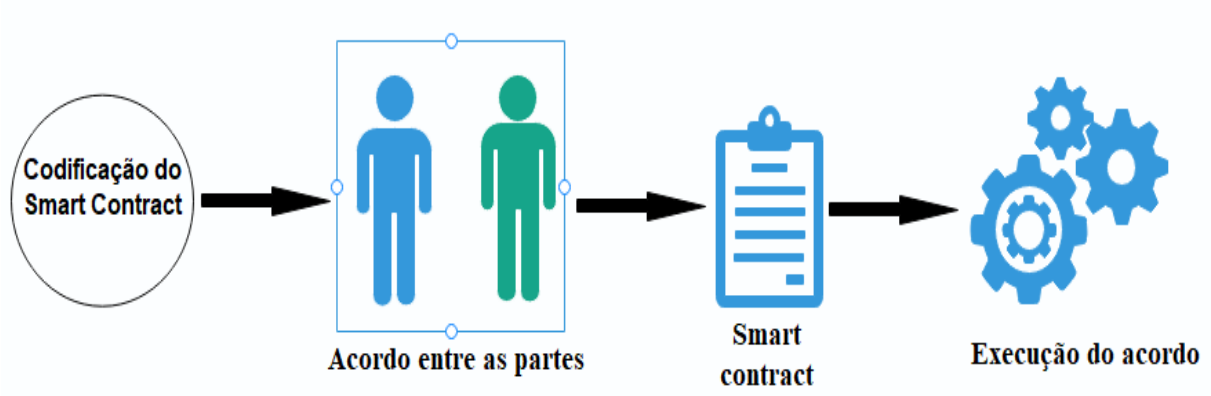
• Armazenamento: Vazio por padrão.

2.3.2 Smart Contracts

O blockchain pode executar os contratos inteligentes ou *smart contracts*. Estes são programas que são replicados juntamente com as transações do *blockchain* e os nós que executam os *smart contracts* ao receber as transações, dessa forma permitindo um consenso distribuído a respeito da execução de um acordo codificado no *blockchain.*

Utilizando-se da ideia de condições previamente programadas, a interface com o usuário é uma das razões principais para a evolução do *blockchain.* Um contrato regido por leis na realidade é nada mais que uma promessa entre as partes signatárias que acordaram em tornar legal, e o *smart contract* detém a mesma essência, exceto por ser completamente determinístico. Contratos inteligentes em um *blockchain* podem permitir a eliminação do banco, do advogado e do tribunal apenas escrevendo um programa que define quanto dinheiro deve ser transferido em resposta a certas condições (SCHWERIN, 2018). A Figura 3 ilustra o funcionamento de um acordo com *smart contracts,* onde o contrato é codificado e atribuído as partes negociantes para que então possa ser executado.

Figura 3 – Funcionamento de um acordo com *smart contracts*



Fonte: Elaborado pelo autor

2.3.3 Algoritmo Pruning

Um algoritmo de “poda” ou no inglês *pruning* é utilizado para excluir localmente o maior número de informação que puder, sem corromper o programa. Este algoritmo é implantado e executado em cada nó da rede. Para o desenvolvimento do algoritmo de *pruning* é necessário fazer o levantamento e análise das informações dos usuários que não são importantes para o *blockchain*, assim definindo quais informações podem ser removidas com segurança sem prejudicar a integridade do *blockchain*.

2.4 A interação entre a LGPD e o blockchain

A LGPD, teve sua base formada através da GDPR. Esta que em certos pontos diverge com a tecnologia *blockchain*, como explica Finck (2019), A compatibilidade entre a tecnologia *blockchain* e o GDPR só pode ser determinada caso a caso, levando em consideração os respectivos fatores técnicos e contextuais (como a estrutura de governança). Sua relação geral é apresentada adiante para chamar a atenção à interação de elementos específicos da tecnologia e da estrutura legal.

Ao discutir as disposições centrais do GDPR e ter conhecimento sobre como o *blockchain* funciona, é possivel perceber e traçar linhas entre o *blockchain* e o GDPR. Os princípios, direitos e obrigações centrais se aplicam à *blockchain* e, portanto, é importante identificar os principais atores e componentes da *blockchain* para poder avaliar a responsabilidade e os direitos, conforme previsto pelo GDPR. (RAMSAY, 2018).

2.4.1 Conflitos entre LGPD e blockchain

Um dos maiores conflitos ligados na relação *blockchain* e a LGPD é o direito ao esquecimento, ou seja, a capacidade de apagar os dados e registros pessoais. Por outro lado, a tecnologia *blockchain* impede o exercício desse direito do titular dos dados, pois de acordo com Rebelo (2019) em princípio todos os dados lançados no *blockchain* seriam tendencialmente indestrutíveis, imutáveis e impassíveis de modificações, o que claramente representa um problema na visão da GDPR.

Um outro ponto de conflito é a centralização da informação, que segundo a LGPD deve-se encontrar nas mãos dos agentes de tratamento e do encarregado dos dados. Isso diverge de uma propriedade da *blockchain* como é explicado nas diretrizes da GDPR por Ramsay (2018): o *blockchain* desafia a suposição de que a responsabilidade centralizada sempre é imposta, pois o núcleo da tecnologia *blockchain* é eliminar os serviços de intermediários.

Tabela 1 – Conflitos entre LGPD e o *blockchain*

Blockchain	**LGPD**	**Conflitos**
Descentralizada	Impõe Centralização da informação	A LGPD almeja a centralização dos dados enquanto o *blockchain* possui uma estrutura descentralizada
Os dados armazenados no *blockchain* não podem ser editados ou apagados	Impõe que os dados devem ficar armazenados apenas durante ao período de tratamento, podendo ser excluídos ou editados a vontade do titular.	Enquanto a LGPD garante a capacidade de esquecimento para os dados do titular o *blockchain* não pode editar ou remover informações.

Fonte – Elaborado pelo autor

Em outras palavras, aqueles que geralmente são controladores de acordo com o Artigo 4° no GDPR. Na Tabela 1 é possível identificar os conflitos de forma sumarizada nas situações abordadas.

2.4.2 Tecnologia blockchain como meio para atingir os objetivos da LGPD

Se em alguns pontos a tecnologia *blockchain* pode divergir da LGPD, em outros esta tecnologia pode auxiliá-la, como foi descrito por Finck (2019). Um relatório recente do Parlamento Europeu destacou que a tecnologia *blockchain* pode fornecer soluções para as disposições de proteção de dados por *design* na implementação do GDPR com base em seus princípios comuns de garantir dados seguros e autogovernados.

3 MATERIAIS E MÉTODOS

O objetivo deste capítulo é apresentar os materiais de estudo e os métodos utilizados no desenvolvimento do trabalho, assim como as etapas seguidas para a estruturação e embasamento teórico, para que permita um melhor entendimento sobre a LGPD e a tecnologia *blockchain*.

3.1 Materiais

Foram utilizados dispositivos legais para este trabalho no âmbito legislativo, tais como a LGPD e a GDPR, bem como referências atuais sobre o tema. Por se tratar de um estudo exploratório e de caráter descritivo, os estudos foram centrados nas possibilidades mais promissoras desenvolvidas em protótipos atuais.

3.2 Métodos

3.2.1 Pesquisa bibliográfica

A primeira etapa consistiu em buscar e analisar trabalhos que abordam as áreas da lei geral de proteção aos dados, do regulamento europeu e da tecnologia *blockchain*. Para facilitar este entendimento a busca foi expandida para trabalhos referentes a LGPD em como ela se assemelha com a GDPR. O material bibliográfico que contempla o trabalho relaciona os principais conceitos do assunto com abordagens teóricas e analíticas.

3.2.2 Pesquisa descritiva

Nesta etapa da pesquisa foram identificados e analisados trabalhos no âmbito do regulamento europeu sobre a GDPR e em na forma como ela interage com a tecnologia *blockchain*. Ainda nesta etapa procurou-se identificar as possíveis diferenças entre a lei geral de proteção aos dados brasileira para entender quais critérios se diferenciavam da GDPR. Além disso foi analisado as tecnologias *blockchain*, disponíveis para escolha da mais adequada para a análise, no caso, a ethereum, para que assim fosse possível discernir os conflitos com a GDPR.

4 RESULTADOS

Neste capítulo é apresentado o estudo de caso no cenário sobre imutabilidade do *blockchain*, para o qual o processo de modificação do *blockchain* e a solução encontrada para o problema são caracterizadas.

Estudo de Caso:

Supõe-se a existência da empresa Z que atua no ramo de aluguéis, utilizando o *Ethereum blockchain* e *smart contracts* para armazenar as informações e acordar os termos com seus clientes, e que tem como objetivo se adequar à nova lei geral de proteção aos dados, analisando-se os seguintes aspectos:

- Por quanto tempo as informações são retidas no *blockchain?*
- As informações retidas dos clientes no *blockchain*, podem ser apagadas?
- As informações após serem apagadas podem ser recuperadas?

A partir das questões levantadas é necessário validar os pontos que estão de acordo ou que conflitam com a LGPD, a fim de manter as operações e processos desta empresa em acordo com a lei. O mercado de empresas como a empresa Z partiu de desenvolvimentos de negócios de venda e revenda até chegar em plataformas mais flexíveis, tais como as de aluguel de curto prazo. A empresa Z permite que pessoas físicas possam negociar objetos em quaisquer lugares do planeta, tais como quartos, bicicletas, roupas de inverno, entre outras. São situações em que pessoas entram em contato para disponibilizar ou buscar produtos e/ou serviços de curto prazo, a princípio não utilizado, e sem burocracia.

Para estes negócios, um contrato de transação eletrônica tem que ser rápido, flexível, e de preferência, não requerer um ambiente centralizado para mediar os interesses das partes. Normalmente, as plataformas existentes não têm estas funcionalidades, pois são centralizadas e armazenam uma série de informações sobre os itens e os clientes, ou as transações. Pagamento seguro e válido. Como observado, essas plataformas utilizam um terceiro de confiança, que opera a plataforma, e que acabam apresentando uma série de desvantagens, tais como a diversidade de plataformas, taxas, rastreamento das transações, com a

possibilidade de um ponto de falha único, segurança, vazamento de informações, regulações de governos locais, quando se trata de operações internacionais.

A empresa Z, na forma que opera, não enfrenta este problema, mas possui outros aspectos críticos. Um deles é o custo de armazenamento de transações no *blockchain*. A possibilidade de permitir ao cliente escolher os dados que serão usados nas transações, bem como o esquecimento também pode melhorar os aspectos das transações, tanto no que diz respeito aos aspectos de segurança, legais e de custos.

Em um primeiro momento necessita-se destacar que além da LGPD, as medidas legais envolvendo outros aspectos deste tipo de avença devem ser consideradas pela empresa, fazendo com que além de estar de acordo com a nova lei a empresa necessita também atender a estas legislações vigentes, de forma que as mesmas não impeçam o devido funcionamento do *blockchain* e da LGPD ou que estes não conflitem com as mesmas. Por exemplo, questões que demandam prova de contrato e pagamento devem ser mantidas por um determinado tempo para averiguação processual, se for o caso, como prova da avença.

Neste estudo de caso é abordada a situação para a qual não é permitida a retenção de informações pessoais referentes aos clientes no *blockchain* da empresa além do período necessário entre ambas as partes. A empresa opera por meio de *smart contracts* e suas informações são armazenadas diretamente no *ethereum blockchain*. Normalmente a utilização do *blockchain* conflita diretamente com a lei do esquecimento da LGPD, impossibilitando que informações sejam apagadas independente do tempo que estão sendo retidas.

Este estudo de caso pode ser avaliado da seguinte forma: A empresa Z de forma alguma pode manter os registros das informações após determinado período. Caso a retenção dessas informações seja ultrapassada, esta empresa estará violando a LGPD como informa o "*Art.16°[...] os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades [...]"*.

A utilização de um *blockchain* "comum" não mais poderia ser aplicado a esse cenário uma vez que ele é imutável, ou seja, as informações jamais poderiam ser apagadas, independentemente do período necessário para sua manutenção do

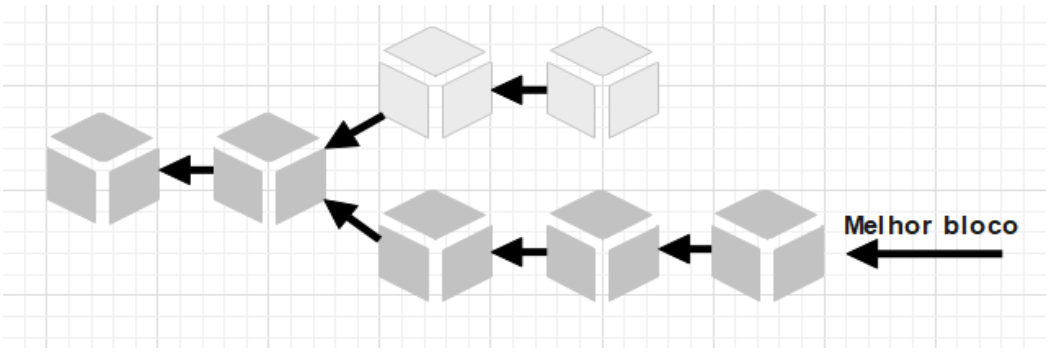
ponto de vista legal. Para que a empresa continue a utilizar essa estrutura, a capacidade de remover informações deve ser possibilitada, e neste sentido o *blockchain* deve-se tornar alterável e assim possibilitar a remoção das informações após o término do período necessário.

Um *blockchain* mutável é possível utilizando como base no *ethereum blockchain*, juntamente com um algoritmo de poda, assim possibilitando a exclusão de transações e mantendo a funcionalidade. Como conceitos base do *blockchain* devem ser alterados alguns requisitos, que devem ser atendidos da seguinte forma: o *blockchain* deve ser resistente à violações, as informações precisam ser distribuídas a todos os nós da rede de modo que novos nós possam ser integrados a rede posteriormente e por fim as transações (bloco) podem ser excluídas após um período determinado.

A empresa Z utilizaria *smart contracts* nos quais é acordado os termos do serviço prestado pela empresa e pelo valor pago pelo cliente, e um dos itens no contrato é a quantidade de tempo em que as informações tais como, nome, endereço, data e horário de uso e o quarto utilizado pelo cliente serão mantidas no *blockchain*, e após esse tempo especificado os dados contidos no bloco onde foram armazenados serão apagados juntamente ao bloco.

O smart contracts possui acesso apenas ao estado, ou seja, mesmo que blocos antigos sejam excluídos, sua funcionalidade não é prejudicada. Diversas soluções para o sucessor de um bloco podem ser encontradas, uma delas sendo a criação de duas ou mais ramificações no *blockchain* (como mostrado na Figura 4). Com isso uma ramificação de blocos pode ser substituída por outra ramificação maior.

Figura 4 – Exemplo de *blockchain* com ramificações



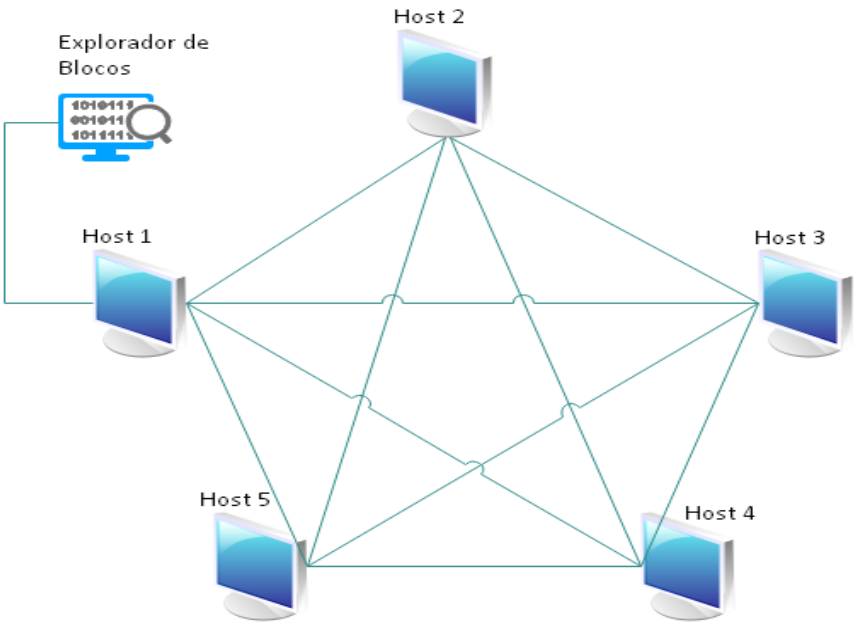
Fonte: Adaptado de Farshid, Reitz, Roßbach (2019)

Pode-se fazer o armazenamento de uma lista contendo os blocos opcionais. Entretanto, assume-se que nenhum novo nó pode ser adicionado e um histórico de transação é desnecessário. Levando em conta essas restrições um recurso pode ser implementado, com a capacidade de excluir blocos após um certo período, de forma que atenda o princípio do esquecimento.

Os bancos de dados armazenam partes de cada bloco como os dados do cliente, dados de transação e dados do recibo e estado, cada um sendo armazenado separadamente. Como cada nova transação aumenta o tamanho do *blockchain* a poda de estado, que é um recurso já implementado é utilizada permitindo maior escalabilidade. A poda de estado não tem a capacidade de excluir os dados de recibo e de transação automaticamente, sendo para isso necessária uma função de apoio que deve ser adicionada e que irá excluir os demais dados armazenados sobre um bloco dos bancos de dados.

Para que o processo citado possa ter efeito em uma rede distribuída, cada elemento participante desta rede deve executar o *software* modificado. Além disso um explorador de bloco deve ser utilizado em conjunto para que possa ser feito o monitoramento da exclusão da informação por completo. A Figura 5 ilustra esta interação em rede.

Figura 5 – Topologia com explorador de blocos



Fonte: Adaptadp de Farshid, Reitz, Roßbach (2019)

Uma interface de usuário pode ser utilizada em cada elemento permitindo uma interação mais direta com o *blockchain* através de um elemento, enquanto o explorador de blocos mostra em tempo real o desaparecimento das transações após o tempo definido.

Com essas modificações no *blockchain* da empresa pode-se entender que o problema com a lei do direito ao esquecimento pode ser contornado, permitindo a empresa continuar utilizando a tecnologia.

É necessário, entretanto, responder a alguns questionamentos típicos de um cenário de negócios que são discutidos a seguir.

Um questionamento é garantir que o *blockchain* é seguro, mesmo não tendo um histórico completo que pode ser verificado porque cada mudança de estado pode ser verificada, ou validada após a mudança, ou seja, os interessados devem utilizar o explorador de blocos para identificar as alterações em tempo real, pelo menos por um tempo compatível com o armazenamento garantido. Após este período, a verificação não pode ser feita, pois as transações mais antigas podem ser excluídas.

Outra questão que diz respeito às alterações é saber se algum participante pode fazer um *backup* dos blocos, de forma que sua exclusão não é completa. Este requisito não faz parte do *blockchain*, na medida que como em qualquer sistema *blockchain*, os blocos são distribuídos e sempre é possível que alguém que faça parte do sistema faça um *backup*. O que é ou pode ser excluído são os blocos da cadeia, ou seja, um ou outro bloco da cadeia padrão de blocos. Obviamente, nem todos os blocos devem ser excluídos e os que forem, por questões individuais, podem ser mantidas por algum participante, de forma privada.

Na questão do tempo de armazenamento dos blocos, se for necessário armazenar, dados por um intervalo de tempo maior, deve-se considerar que os dados não são armazenados nas transações, pois os dados nas transações não ficam disponíveis para os *smart contracts* e as transações permanecem por apenas alguns dias. O que se infere é que as informações não devem ser armazenadas nas transações e sim no estado do *smart contract.*

Por fim, uma vez que o histórico vai sendo apagado, o primeiro bloco, comumente denominado bloco gênese, pode ou vai deixar de existir, e não poderá ser utilizado como ponto inicial de sincronização, como é o caso padrão no sistema *blockchain*. Portanto, se houver a entrada de um novo bloco na cadeia, a confiança deve ser estabelecida em relação aos blocos de forma diferente, solicitando que os nós um bloco no meio da cadeia para verificar se os mesmos reconhecem esse bloco. Este caso é tratado no segundo ponto a seguir.

A abordagem apresentada resolve o problema da imutabilidade, porem traz consigo limitações, pois em um primeiro momento pode-se afirmar que esta proposta é impossível de ser aplicada em um ambiente que não seja restritamente controlado, pois a abordagem não tem controle das possíveis ações que possam ser realizadas pelos participantes, uma vez que não se pode controlar o que os mesmos fazem.

Um outro ponto é encontrado na inclusão de novos nós, conforme observado anteriormente, desde que o bloco gênese não pode ser usado como a origem da sincronização, um bloco recente é designado como o bloco de origem da sincronização, mas não antes de ser verificada a confiança nesse bloco por parte de todos os outros nós, o que implica em complexidade e tempo para realizar essa sincronização.

O último problema encontrado é visto no cenário quando um nó é desabilitado por um certo período de tempo, ele então perderá a sincronia com a rede, visto que os blocos entre o último registrado por este nó e o bloco mais recente já possam ter sido removidos, e com isso será necessário refazer todo o processo de configuração mais uma vez para este nó.

5 CONCLUSÃO

A Lei Geral de Proteção aos Dados foi criada com o intuito de adequar o Brasil as novas estruturas de proteção de dados pessoais, um fenômeno mundial, tanto a qual foi baseada no regulamento geral de proteção de dados desenvolvido na União Europeia. Com a chegada da LGPD grandes mudanças no cenário tecnológico no Brasil começaram a ocorrer afetando diretamente empresas e tecnologias utilizadas. Uma das tecnologias impactadas pela LGPD foi o *blockchain* o qual tem como pressupostos que conflitam diretamente com as propostas da lei.

A proposta deste trabalho foi o estudo sobre a LGPD e o impacto causado na tecnologia *blockchain*, de forma a qual foi possível construir um estudo de caso levando em conta os conflitos entre a lei e a tecnologia, levando em conta um dos aspectos importantes do blockchain, a imutabilidade, e sua incompatibilidade com o LGPD, o direito ao esquecimento. Este estudo possibilitou a identificação de uma aplicação de transação imobiliária que pode ter a adequação de um *blockchain* privado para com a LGPD, avaliando também as limitações que poderiam surgir através dessa relação.

Esta análise tem o intuito de contribuir futuramente para o estudo e desenvolvimento de novos métodos a respeito deste tema. Atualmente o conteúdo a respeito é escasso e de difícil compreensão desde que a LGPD ainda não está em vigor.

5.1 Contribuições

O trabalho desenvolvido apresentou as seguintes contribuições:

- Através deste trabalho novos caminhos para a evolução da tecnologia *blockchain* podem ser traçados para a conformidade com a LGPD.
- Pode ser utilizado como base para desenvolver *blockchains* editáveis e expandir o conhecimento nesta área.
- Utilidade para empresas privadas a qual necessitam de ideias a respeito da adequação com a LGPD de suas *blockchains* privadas.

5.2 Limitações

Durante a pesquisa do material e estudo do problema as maiores limitações foram:

- Materiais como artigos, livros, estudos e documentos referentes a LGPD foram difíceis de serem encontrados.
- Matérias de pesquisa a respeito dos conflitos entre o *blockchain* e a LGPD são quase inexistentes, o que aumenta a dificuldade em encontrar soluções adequadas.

5.3 Trabalhos futuros

Ao concluir este trabalho e apresentar as contribuições e as limitações que o cercaram ainda é possível apontar os seguintes trabalhos futuros.

- Desenvolvimento de uma nova tecnologia não determinística baseada no *blockchain* na qual mantem a integridade, anonimato, segurança porem permite a edição de informações e não apenas a exclusão de blocos.
- Análise da LGPD na visão da tecnologia, de forma a permitir exceções na lei para tecnologias as quais não correspondem inteiramente a suas diretrizes.

6 REFERENCIAS BIBLIOGRAFICAS

BAMBARA, Joseph J.; ALLEN, Paul R. **Blockchain**: A Practical Guide to Developing Business, Law, and Technology Solution. Estados Unidos da América: McGraw-Hill Education, 2018. 302 p. *E-book*.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: **Lei Geral de Proteção de Dados Pessoais (LGPD**). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 maio 2020.

CUNHA, Mauro. **Comentários à Lei de Proteção de Dados Pessoais**: Para Boas Práticas e Reflexões Pragmáticas. 1. ed. Brásilia: S.n, 2018. cap. 2, p. 24-32. ISBN 9781790479740. *E-book*.

DHULAVVAGOL, Praveen M; BHAJANTRI, Vijayakumar H; TOTAD, S G. Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. **International Conference on Computational Intelligence and Data Science (ICCIDS 2019)**, Elsevier B.V, p. 2056-2515, 2020.

FARSHID, Simon; REITZ, Andreas; ROßBACH, Peter. Design of a forgetting blockchain: A possible way to accomplish GDPR compatibility. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 2019, 61., 2019, Hawaii. **Proceedings of the 52nd Hawaii International Conference on System Sciences.** S.I: Hawaii International Conference On System Sciences, 2019. p. 7087-7095.

FINCK, MICHÈLE. **Blockchain and the General Data Protection Regulation**: Brussels: European Union, 2019.

CUNHA, Mauro. **Comentários à Lei de Proteção de Dados Pessoais**: Para Boas Práticas e Reflexões Pragmáticas. 1. ed. Brásilia: S.n, 2018. cap. 2, p. 24-32. ISBN 9781790479740. *E-book*.

MACIEL, Rafael Fernandes. **MANUAL PRÁTICO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (Lei nº 13.709/18).**: atualizado com a medida provisória nº 869/18. Goiânia: RM Digital Education, 2019.

RAMSAY, Sebastian. **The General Data Protection Regulation vs. The Blockchain**: a legal study on the compatibility between blockchain technology and the gdpr. Stockholm: Stockholm University, 2018.

REBELO, Maria Paulo. **OS DESAFIOS DO RGPD PERANTE AS NOVAS TECNOLOGIAS BLOCKCHAIN,** Revista de Bioética y Derecho, Universitat de Barcelona, 2019.

SANTOS, Regiane Martins dos. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: S.i, 2020

SCHWERIN, Simon. Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. **The JBBA**, [*S. l.*], v. 1, p. 1-75, 19 abr. 2018.

SHARMA, Sanjay. **Data Privacy and GDPR Handbook**. Hoboken: John Wiley & Sons, 2020.