



**INSTITUTO FEDERAL DA BAHIA
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO**

**PROFNIT - PROGRAMA DE PÓS-GRADUAÇÃO EM PROPRIEDADE
INTELECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A INOVAÇÃO**

JOSUÉ COSTA JÚNIOR

**DA CONCEPÇÃO À TRANSFERÊNCIA: DESENVOLVIMENTO DE SOLUÇÃO
BASEADA EM TECNOLOGIA *BLOCKCHAIN* PARA REGISTRO E VALIDAÇÃO DE
ATESTADOS MÉDICOS-ODONTOLÓGICOS**

**SALVADOR – BA
2020**

JOSUÉ COSTA JÚNIOR

**DA CONCEPÇÃO À TRANSFERÊNCIA: DESENVOLVIMENTO DE SOLUÇÃO
BASEADA EM TECNOLOGIA *BLOCKCHAIN* PARA REGISTRO E VALIDAÇÃO DE
ATESTADOS MÉDICOS-ODONTOLÓGICOS**

Projeto de Inovação Tecnológica, apresentado como produto para Defesa de Trabalho de Conclusão de Curso, requisito parcial à obtenção do grau de Mestre em Propriedade Intelectual e Transferência de Tecnologia para a Inovação, pelo Instituto Federal da Bahia.

Orientador: Prof. Dr. Eduardo Oliveira Teles.

**SALVADOR – BA
2020**

Biblioteca Raul V. Seixas – Instituto Federal de Educação, Ciência e Tecnologia da Bahia - IFBA - Salvador/BA.

Responsável pela catalogação na fonte: Samuel dos Santos Araújo - CRB 5/1426.

C837d Costa Júnior, Josué.

Da concepção à transferência: desenvolvimento de solução baseada em tecnologia Blockchain para registro e validação de atestados médicos-odontológicos / Josué Costa Júnior. Salvador, 2020.

173 f. ; 30 cm.

Projeto de inovação tecnológica (Mestrado Profissional em Propriedade Intelectual e Transferência de Tecnologia para a Inovação) – Instituto Federal de Educação, Ciência e Tecnologia da Bahia.

Orientação: Prof. Dr. Eduardo Oliveira Teles.

1. Atestados médicos-odontológicos. 2. Blockchain. 3. Proteção intelectual. 4. Transferência de tecnologia. I. Instituto Federal de Educação, Ciência e Tecnologia da Bahia. II. Título.

CDU 2 ed. 614

**INSTITUTO FEDERAL DA BAHIA
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO**

**PROFNIT - PROGRAMA DE PÓS-GRADUAÇÃO EM PROPRIEDADE
INTELLECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A INOVAÇÃO**

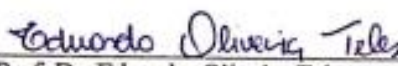
**"DA CONCEPÇÃO À TRANSFERÊNCIA: DESENVOLVIMENTO DE SOLUÇÃO
BASEADA EM TECNOLOGIA BLOCKCHAIN PARA REGISTRO E
VALIDAÇÃO DE ATESTADOS MÉDICOS-ODONTOLÓGICOS"**

JOSUÉ COSTA JUNIOR

Produto(s) Gerado(s): Projeto de Inovação Tecnológica.

Orientador: Prof. Dr. Eduardo Oliveira Teles

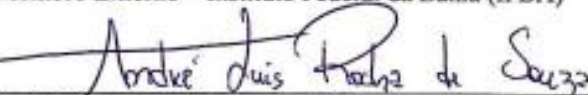
Banca Examinadora:



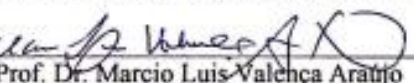
Prof. Dr. Eduardo Oliveira Teles
Orientador – Instituto Federal da Bahia (IFBA)



Prof. Dr. Fábio Marques da Cruz
Membro Externo – Instituto Federal da Bahia (IFBA)



Prof. Dr. André Luis Rocha de Souza
Membro Interno – Instituto Federal da Bahia (IFBA)



Prof. Dr. Marcio Luis Valença Araújo
Membro Interno – Instituto Federal da Bahia (IFBA)

Trabalho de Conclusão de Curso aprovado pela banca examinadora em 19/02/2020

AGRADECIMENTOS

Sou grato a Deus pela vida e pela Sua infinita bondade!

Agradeço a minha esposa pelo amor, apoio, paciência e pela compreensão face à minha ausência em vários momentos nestes últimos dois anos.

À minha mãe e filhos, que acreditaram no meu potencial e torceram por mim.

Ao meu orientador Professor Dr. Eduardo Oliveira Teles, pela parceria, direcionamento, apoio, incentivo, e principalmente por acreditar na proposta deste trabalho.

A todos os professores do PROFNIT IFBA que tive a oportunidade de conhecer, e por toda contribuição dada através da transmissão dos seus conhecimentos.

Aos meus colegas da turma PROFNIT 2018.1, e aos amigos que fiz durante a jornada do curso, especialmente a Samyr Leal Costa Brito por compartilhar as viagens, os desafios, as experiências e as risadas no final.

Aos funcionários do IFBA (Reitoria e campus Salvador), pelo apoio administrativo.

A todos que direta e indiretamente contribuíram para o resultado final deste trabalho, de forma especial à Rafael Elias Bergsten pelo apoio e contribuição técnica.

RESUMO

A crescente dinâmica das transformações sociais e econômicas tem revelado a importância de analisar questões que afetam a sociedade através de estudos cujos resultados sejam traduzidos em novos produtos tecnológicos que resolvam problemas reais no mundo real. Nesse aspecto, a Propriedade Intelectual e a Transferência de Tecnologia são fatores inerentes e essencialmente decisivos, proporcionando um ambiente de estímulo à inovação com garantias de proteção a investimentos. O objetivo desse trabalho é propor um modelo de registro unificado para verificação de autenticidade de atestados médicos-odontológicos com tecnologia blockchain, elencando as possibilidades de proteção intelectual e transferência de tecnologia. Para o alcance desse objetivo, foram necessárias pesquisas de processos que tramitam na esfera jurídica para o entendimento dos impactos socioeconômicos demandados pela falsificação de atestados médicos-odontológicos. Através de estudos prospectivos do Estado da Arte e da Técnica, e a avaliação de variáveis associadas à viabilidade técnica e às possibilidades de Proteção Intelectual e Transferência de Tecnologia, tornou-se possível elaborar e apresentar o modelo proposto envolvendo processos e regras de negócio, e a arquitetura de requisitos para o seu desenvolvimento.

Palavras-Chave: Atestados Médicos-odontológicos. *Blockchain*. Proteção Intelectual. Transferência de Tecnologia.

ABSTRACT

The growing dynamics of social and economic changes have revealed the importance of analyzing issues that affect society through studies whose results are translated into new technological products that solve real problems in the real world. In this respect, Intellectual Property and Technology Transfer are inherent and essentially decisive factors, providing an environment that stimulates innovation with guarantees of investment protection. This work presents a unified registration model for verifying the authenticity of medical-dental certificates with blockchain technology, listing the possibilities of intellectual protection and technology transfer. To achieve this objective, research on processes that are being processed in the legal sphere was necessary to understand the socioeconomic impacts demanded by the falsification of medical certificates. Through prospective studies of the State of the Art and Technology, and the evaluation of variables associated with technical feasibility and the possibilities of Intellectual Protection and Technology Transfer, it became possible to elaborate and present the proposed model involving business processes and rules, and the requirements architecture for its development.

Keywords: Medical-dental Certificates. Blockchain. Intellectual Protection. Technology Transfer.

LISTA DE ABREVIATURAS E SIGLAS

AMES	Associação dos Médicos do Espírito Santos
API	Interface de Programa de Aplicações (do inglês <i>Application Programming Interface</i>)
BPMN	Modelagem de Processos de Negócio e Notação
CAGED	Cadastro Geral de Empregados e Desempregados
CBO	Código Brasileiro de Ocupação
CID	Código de Identificação de Doença
CLI	Interface de Linhas de Comando (do inglês <i>Comand-line Interface</i>)
CFM	Conselho Federal de Medicina
CRM	Conselho Regional de Medicina
DV	Declaração de Veracidade
FEF	Fórum das Entidades e Federações
GRU	Guia de Recolhimento da União
ICT	Instituições Científicas e Tecnológicas
ID	Identidade (do inglês <i>Identity</i>)
IDE	Ambiente de Desenvolvimento Integrado (do inglês <i>Integrated Development Environment</i>)
IFBA	Instituto Federal de Educação, Ciência e Tecnologia da Bahia
INPI	Instituto Nacional de Propriedade Intelectual
IP	Protocolo de <i>Internet</i> (do inglês <i>Internet Protocol</i>)
IoT	Internet das Coisas (do inglês <i>Internet of Things</i>)
LGPD	Lei Geral de Proteção de Dados
LPI	Lei de Propriedade Industrial
NIT	Núcleo de Inovação Tecnológica
RPC	Registro de Programa de Computador
RPI	Revista da Propriedade Industrial
SEI	Instituto de Engenharia de <i>Software</i> (do inglês <i>Software Engineering Institute</i>)
STJ	Superior Tribunal de Justiça
TRT	Tribunal Regional do Trabalho
TRF	Tribunal Regional Federal
TSL	Segurança da Camada de Transporte (do inglês <i>Transport Layer Security</i>)

TT

Transferência de Tecnologia

LISTA DE FIGURAS

Figura 1 - Estrutura do trabalho	25
Figura 2 - Esquema simplificado de uma transação <i>Blockchain</i>	35
Figura 3 - Estrutura de conexão <i>blockchain</i>	48
Figura 4 - Modelo de Arquitetura <i>Blockchain</i> de Execução por Ordem de Validação do <i>Hyperledger Fabric</i>	56
Figura 5 - Caracterização da pesquisa	64
Figura 6 - Delineamento da pesquisa - Fase 1	65
Figura 7 - Delineamento da pesquisa - Fase 2	66
Figura 8 - Delineamento da pesquisa - Fase 3	67
Figura 9 - Delineamento da pesquisa - Fase 4	68
Figura 10 - Percurso metodológico	69
Figura 11 - Passos para a obtenção da primeira visão do modelo	75
Figura 12 - Configuração da equipe especialista	89
Figura 13 - Registro de Programa de Computador (RPC) em 7 passos	99
Figura 14 - Procedimentos para efetuar o peticionamento de Patente (em 8 passos)	101
Figura 15 - Processo de identificação de riscos	108
Figura 16 - Fluxo do processo da operação de usabilidade do Profissional de Saúde	113
Figura 17 - Fluxo do processo da operação de usabilidade da Entidade Utilizadora	114
Figura 18 - Fluxo do processo da operação de usabilidade do Paciente	115
Figura 19 - Modelagem do Processo de Negócio (Requisição para a gravação do atestado)	117
Figura 20 - Modelagem do Processo de Negócio (Requisição para a validação de autenticidade do atestado)	119
Figura 21 - Modelo de arquitetura <i>blockchain</i> para registro de atestados médicos-odontológicos.	122
Figura 22 - Visão da estrutura dos dados nos blocos da <i>blockchain</i> para registro de atestados	124
Figura 23 - Fundamentos da arquitetura do Protótipo	128
Figura 24 - Verificação de atividade da Plataforma	129
Figura 25 - Primeiro acesso: Cadastramento do médico/cirurgião dentista	130
Figura 26 - Identificação do médico/cirurgião-dentista e paciente,	131
Figura 27 - Operação de registro do atestado	132
Figura 28 - Primeiro acesso e cadastramento da Entidade Consumidora	133

Figura 29 - Consulta e utilização do atestado médico.....	134
Figura 30 - Diagrama do Caso de Uso Acesso e Identificação do Médico no <i>Software</i> cliente	137
Figura 31 - Diagrama do Caso de Uso Identificação do Médico na API	139
Figura 32 - Diagrama do Caso de Uso Inclusão do Atestado no <i>Software</i> Cliente	140
Figura 33 - Diagrama do Caso de Uso Inclusão do Atestado:.....	141
Figura 34 - Diagrama do Caso de Uso Identificação da Entidade no <i>Software</i> Cliente.....	142
Figura 35 - Diagrama do Caso de Uso Identificação da Entidade: Operação na API	144
Figura 36 - Diagrama do Caso de Uso Consultar atestado: Operação na API	145
Figura 37 - Diagrama do Caso de Uso Utilizar Atestado – operação na API.....	146
Figura 38 - Etapas envolvendo Autores - NIT/ICT - INPI.....	149
Figura 39 - RPC: Etapas envolvendo Autores - NIT/ICT - INPI	150
Figura 40 - RPC: Etapas envolvendo Empresa - INPI	151
Figura 41 - Etapas da negociação e a transferência da tecnologia	152
Figura 42 - Etapas para a cessão da titularidade dos direitos de proteção	153
Figura 43 - Etapas para o licenciamento de uso e exploração dos direitos	154
Figura 44 - Etapas para o fornecimento de tecnologia por transferência de <i>know-how</i>	155
Figura 45 - Fluxo do processo para averbação do contrato.....	159

LISTA DE QUADROS

Quadro 1 - Obras do tema “ <i>Blockchain</i> ”	32
Quadro 2 - Obras do tema: <i>Blockchain</i> em Sistema Financeiros e Governança Corporativa.	36
Quadro 3 - Obras do Tema: <i>Blockchain</i> e Internet das Coisas (IoT).....	38
Quadro 4 - Obras do Tema: <i>Blockchain</i> e os desafios de aplicação da tecnologia	45
Quadro 5 - Método de consenso: Tolerância Prática a Falhas Bizantinas (PBFT)	50
Quadro 6 - Obras do tema: Arquitetura e segurança na <i>blockchain</i>	52
Quadro 7 - Camadas da arquitetura do <i>Hyperledger</i>	54
Quadro 8 - Obras do Tema: <i>Blockchain</i> e <i>Hyperledger</i>	57
Quadro 9 - Estado da Técnica de soluções similares ou periféricas ao presente estudo	59
Quadro 10 - Resumo comparativo das características gerais das soluções e o modelo proposto nesta pesquisa	61
Quadro 11 - Etapas e atividade metodológicas da Fase 1	70
Quadro 12 - Palavras-chaves e descritores utilizados em estratégias de busca.....	72
Quadro 13 - Descritores e palavras-chaves dos impactos socioeconômicos utilizadas nos motores de busca	73
Quadro 14 - Etapas e atividades metodológicas da segunda fase da pesquisa.....	73
Quadro 15 - Etapas e atividades metodológicas da terceira fase da pesquisa.....	74
Quadro 16 - Etapas e atividades metodológicas da quarta fase da pesquisa.....	78
Quadro 17 - Forma de organização dos estudos para revisão integrativa	83
Quadro 18 - Tecnologias necessárias para a fase do desenvolvimento de um <i>software</i>	85
Quadro 19 - Equipamentos e serviços recomendados à infraestrutura	86
Quadro 20 - Comparativo entre as duas modalidades de servidores.....	87
Quadro 21 - Sistemas e serviços instalados necessários ao funcionamento das máquinas.....	88
Quadro 22 - Demonstrativo de custos com servidor da <i>Amazon</i> ®	91
Quadro 23 - Identificação de riscos atuais do projeto	109
Quadro 24 - Comparativo entre processo atual de emissão de atestados e o modelo proposto	125
Quadro 25 - Elementos da notação gráfica de um Diagrama de Caso de Uso.....	135

LISTA DE TABELAS

Tabela 1 - Resumo comparativo entre <i>Ethereum</i> , <i>Hyperledger</i> e R3 Corda	31
Tabela 2 - Custos com equipe de projeto no período de um ano	90
Tabela 3 - Custos com recursos de processamento/hora de servidor.....	92
Tabela 4 - Primeira projeção de custos de viabilidade técnica	94
Tabela 5 - Segunda projeção de custos de viabilidade técnica	94
Tabela 6 - Terceira projeção de custos de viabilidade técnica	95
Tabela 7 - Quarta projeção de custos de viabilidade técnica	96
Tabela 8 - Totalização dos custos estimados em todas as projeções.....	96

SUMÁRIO

1 INTRODUÇÃO	16
1.1 Contextualização da Situação-Problema	18
1.2 Justificativa.....	21
1.3. Objetivo Geral	24
1.4 Objetivos Específicos	24
1.5 Estrutura do trabalho	25
2 ESTADO DA ARTE	27
2.1 <i>Blockchain</i> – Funcionamento, Evolução e Aplicações	27
2.2 Tendências de aplicações da <i>blockchain</i>	34
2.3 Desafios da aplicação da tecnologia <i>blockchain</i>	38
2.4 Aspectos para elaboração de arquitetura com base em <i>blockchain</i>	46
2.5 <i>Blockchain Hyperledger</i>	53
2.6 Modelo de Arquitetura <i>Blockchain</i> de Execução por Ordem de Validação do <i>Hyperledger Fabric</i>	56
3 ESTADO DA TÉCNICA	59
4. PROJETO DE INOVAÇÃO TECNOLÓGICA	63
4.1 Métodos	63
4.1.1 Caracterização da Pesquisa	63
4.1.2 Etapas e Procedimentos da Pesquisa	68
4.2 Estudos de viabilidade da inovação.....	84
4.2.1 Viabilidade técnica.....	84
4.2.2 Análise das variáveis econômico-financeiras associadas à viabilidade técnica	89
4.2.3 Aspectos associados à viabilidade de Proteção Intelectual e Transferência de Tecnologia (TT)	97
4.4 Riscos	107
5. RESULTADOS	111
5.1 Modelagem dos fluxos de processos de negócio do modelo proposto.....	111
5.2 Modelo de arquitetura <i>blockchain</i> , para o registro de atestados médicos-odontológicos	120
5.3 Modelo de arquitetura para o protótipo	126
5.3.1 Regras de negócio e requisitos funcionais	127

5.3.2 Modelo de arquitetura de requisitos por casos de uso	134
5.4 Possibilidades de proteção e Transferência de Tecnologia (TT)	147
5.4.1 Proteção por patente de invenção implementada por Programa de Computador	148
5.4.2 Processo para proteção por Registro de Programa de Computador (RPC)	149
5.4.3 Processo para Transferência da Tecnologia	151
5.5 Processo proposto para a averbação do contrato de transferência de tecnologia	156
6 CONCLUSÕES	160
REFERÊNCIAS	163

1 INTRODUÇÃO

Conceber soluções inovadoras está intrinsecamente ligado ao ato de identificar oportunidades de inovação e criar soluções que tragam alto valor para usuários-consumidores de uma sociedade.

Para a efetividade deste ato inovativo, etapas que garantam a propriedade intelectual devem ser planejadas desde a concepção das invenções até o registro da proteção das criações intelectuais, de modo a garantir os direitos de seus autores e incentivá-los a manter ativo o seu processo criativo.

Entretanto, é importante ressaltar que a propriedade intelectual não se resume à concessão de pedidos de proteção por patentes e registros, mas amplia-se à transferência da tecnologia, etapa que garante que a invenção, uma vez protegida, chegue ao mercado produtivo e se transforme em inovação efetiva.

A Transferência de Tecnologia é o meio pelo qual conhecimentos, habilidades e procedimentos que possuam caráter de aplicabilidade e resolução de problemas da produção, são transferidos de uma organização à outra (BARTON, 2007; LUZ, 2012).

Este processo ocorre quando uma empresa necessita de uma nova tecnologia e não optou ou não dispôs de recursos próprios para desenvolvê-la, adquirindo de terceiros o conhecimento e a tecnologia que já proporciona oportunidades pelos resultados apresentados, ou quando a tecnologia ainda é incipiente ou não existe necessidade de melhorias adjacentes (PINTO, 2016; VIDAL-QUADRAS TRIAS DE BES, 2015).

A Transferência de Tecnologia pode ser realizada de maneiras diversas a depender das demandas e dos objetivos a serem alcançados e dos negócios jurídicos celebrados como: um desenvolvimento industrial ou a necessidade de um conhecimento de terceiro para realizar determinado projeto (BARTON, 2007; LUZ, 2012; PINTO, 2016).

A efetivação das aquisições e transferências de tecnologias só ocorrerá mediante a celebração de um Contrato de Transferência de Tecnologia. Este instrumento apoia o processo de inovação, amparado pela Lei de Inovação (Lei nº 10.973/2004).

De acordo o Instituto Nacional de Propriedade Industrial - INPI (2019), os contratos de transferência de tecnologia, se dividem em: Licença de direitos (exploração de patentes ou uso de marcas) que permitem a exploração de marcas registradas ou patentes concedidas ou com pedidos depositados no INPI, e a aquisição de conhecimentos tecnológicos (fornecimento de tecnologia e prestação de serviços de assistência técnica e científica) e de franquias.

De acordo Prado (1997), as cláusulas dos contratos de transferência de tecnologia estão previstas em três classes:

- Centrais (aquelas que tratam do objeto do contrato, a definição da tecnologia, as garantias, as melhorias, o território para a exploração, as regras de sublicenciamento, os serviços de assistência técnica e os aspectos de exploração mínima);
- Complementares (as que tratam dos aspectos de exclusividade, as regras de confidencialidade e da licença mais favorecida);
- Usuais (cláusulas próprias dos contratos internacionais como, dificuldades, força maior, termo inicial, duração, renovação, arbitragem, foro e lei aplicável).

Do mesmo modo, é desejável em contratos de transferência de tecnologia, que se atente também para situações e cláusulas que devem ser evitadas nesses instrumentos quando estas ferirem: a livre concorrência e, a liberdade de iniciativa (ASSAFIM, 2013; BARBOSA, s/d).

Para que os termos que tratam dos direitos de propriedade industrial, acordados em suas cláusulas, provoquem efeitos e para que ocorram os devidos trâmites de transferência de tecnologia, os contratos devem ser registrados ou averbados junto ao INPI, em conformidade Art. 126 da Lei nº 5.648, de 11 de dezembro de 1970 (SILVA; BOVÉRIO, 2018).

Outra relevante menção no processo de transferência de tecnologia é o papel dos Núcleos de Inovação Tecnológica (NIT) que, de acordo Costa (2013), são setores de inovação que promovem e auxiliam a utilização do conhecimento e de novas tecnologias produzidas nas universidades e institutos de pesquisa brasileiros.

Os NITs passaram a existir a partir da publicação da Lei nº 10.973/2004 (Lei de Inovação), regulamentados pelo Decreto nº 5.563/2005, com a missão de gerir a política de inovação das ICT - Instituições Científicas e Tecnológicas (BRASIL, 2005, Art.17).

Os NITs atuam nas ICT como agentes que viabilizam a transferência de tecnologia desenvolvida, interna ou externamente, para o setor produtivo promovendo a inovação e a integração com a comunidade (BRASIL, 2005; LOTUFO; TOLEDO; SANTOS, 2009; SILVA *et al.*, 2015).

A partir do Novo Marco da Inovação (Lei 13.243/2016), os NITs assumem um perfil mais diligente, de caráter proativo e mais integrado com o mercado e a sociedade. Segundo essa Lei, em seu Artigo 16, Parágrafo 1º, dos incisos VII ao X, estão dentre as competências dos NITs:

- VII - desenvolver estudos de prospecção tecnológica e de inteligência competitiva no campo da propriedade intelectual, de forma a orientar as ações de inovação da ICT;
- VIII - desenvolver estudos e estratégias para a transferência de inovação gerada pela ICT;
- IX - promover e acompanhar o relacionamento da ICT com empresas, em especial para as atividades previstas nos arts. 6º a 9º;
- X - negociar e gerir os acordos de transferência de tecnologia oriunda da ICT (BRASIL, 2016. Art.16. Parágrafo 1º, Incisos VII a X).

Tais competências reforçam a atuação de um NIT como um canal de integração entre as constantes demandas apresentadas pelas empresas conectando os detentores do conhecimento das ICTs e promovendo a transferência de tecnologia. As vantagens visam o desenvolvimento socioeconômico de uma determinada classe ou região através das políticas ligadas à inovação (BAGNATO; ORTEGA; MARCOLAN, 2014).

Assim como a relevante criação dos NITs, novas leis Governamentais (a exemplo das Leis 13.787/2018 e 13.874/2019), criaram incentivos para iniciativas de pesquisas, desenvolvimento e transferência de novas tecnologias que possam suprir lacunas existentes nos mais diversos setores da esfera pública e privada, criando outros mecanismos para inovação tecnológica.

A partir desses incentivos, e do aprofundamento de suas pesquisas, esse trabalho constatou a lacuna que expõe a situação-problema deste estudo.

1.1 Contextualização da Situação-Problema

Documentos falsificados são inevitavelmente utilizados em múltiplas e variadas ocasiões envolvendo desde pequenos procedimentos, como a simples compra de uma passagem aérea, até procedimentos mais complexos que vão desde operações comerciais ou financeiras até provas falsas em processos judiciais ou administrativos.

Tal prática é facilitada pelo fácil acesso a modernos equipamentos que envolvem tecnologia de ponta e a sofisticados *softwares* de *design* gráfico que podem gerar perfeitas réplicas de documentos físicos. Além disso, documentos ofertados em formato eletrônico aumentam ainda mais a margem dos meios facilitadores, estimulando significativamente a prática da falsificação por meios digitais.

A partir da Lei 11.419/2006, iniciou-se a difusão dos “processos eletrônicos” nos tribunais brasileiros com toda a utilização de documentação incorporada em formato eletrônico, facilitando a informatização do processo judicial, porém tornando-se também um fator estimulador para a ocorrência de falsificações de documentos por meios digitais

(PARODI, 2018).

Esta Lei instituiu o processo “eletrônico” ou “digital” no Brasil tratando da validade legal dos documentos produzidos eletronicamente e das eventuais arguições de falsidade, assim como a definição de responsabilidade pela guarda dos documentos digitalizados.

De acordo Parodi (2018), há duas tipologias em se tratando de documentos digitais. Uma refere-se a documentos que foram gerados a partir de computadores ou outros dispositivos sem nunca terem sido impressos. Outra se refere a um documento convertido de um formato físico, através de meios de digitalização como escaneamento ou foto digital.

Em qualquer uma das tipologias haverá a possibilidade de falsificação, uma vez que digitalizados o conteúdo desses documentos poderá ser alterado em sua totalidade, ou em uma parte dele ou, ainda, ter seu conteúdo “criado” sem nenhum precedente por meios digitais (PARODI, 2018).

Os artigos 297 e 298 do Código Penal Brasileiro (Decreto-Lei Nº. 2.848, de 7 de dezembro de 1940), preveem como ato ilícito falsificar ou alterar documento verdadeiro seja público ou particular, seja de forma completa ou uma parte dele, resultando em multa e pena de reclusão de um a cinco anos.

Ainda dentro do Código Penal, há previsão de punição para o caso da utilização do documento falso, conforme versa o artigo 304 do mesmo Decreto, que dispõe sobre o uso destes documentos falsificados ou alterados se tratando de prática ilícita também passível de detenção.

Uma pesquisa realizada por Braga, Ertler e Pereira (2018), através de uma análise jurisprudencial na área de consulta de julgados de 1º grau no *site* do Tribunal de Justiça do Estado de São Paulo, buscou o entendimento dos julgados sobre a emissão de uma categoria específica de documentos falsificados - os atestados médicos.

Foram analisados 48 processos recuperados pelas buscas até a data de 11 de maio de 2017, e no que se referem à autoria do delito, os resultados mostraram que 96% foram praticados por não médicos; 2% por médicos e não médicos, conjuntamente, e apenas 2% por médicos. Dessa forma, apenas em dois (02) processos (4,16%) havia um médico como réu, evidenciando a que a prática ilícita da falsificação do referido documento parte de terceiros.

As informações contidas em um atestado médico-odontológico, até que se prove ao contrário, servem como declaração pública utilizadas como justificativa de ausência ao trabalho, conforme Artigo 6º da Lei 605/49, em seu parágrafo segundo.

Por se tratar de um documento de fé-pública, a sua falsificação é um ato proibido por lei, com punição por infração entre dois a seis anos de detenção, conforme artigos 297 e 304

do Código Penal Brasileiro, no entanto, a prática da sua falsificação ocorre facilmente a partir de terceiros.

Os resultados desse ato tanto tendem a trazer prejuízos socioeconômicos na esfera pública ou privada, quanto à possibilidade de recair sobre o médico ou cirurgião-dentista responder pelas informações contidas em um documento que não foi emitido por ele mas carrega seu nome, conforme artigo 80 do Código de Ética Médica (RESOLUÇÃO CFM nº 2.217/2018, Cap. X, Art.80).

Os mecanismos que se propõem a disciplinar, normatizar e dar as diretrizes necessárias à emissão desse tipo de documento prevê, em seus efeitos, a coibição desta prática, como é o caso do Código Penal Brasileiro e a norma expressa na Resolução CFM nº 1.658/2002.

A norma dessa Resolução fornece diretrizes para a emissão de atestados médicos, orientando o registro das informações em ficha própria e/ou em prontuário médico com as informações dos exames e tratamentos realizados (CFM, 2002, Art. 2º).

Segundo o mesmo artigo dessa Resolução, essas informações documentadas deverão atender o provisionamento de informações a médicos peritos de empresas ou órgãos públicos da Previdência Social e da Justiça, quando se fizer necessário.

Mesmo com a presença desses mecanismos, o afastamento indevido ao trabalho, amparado por atestados falsos, tem causado grandes prejuízos socioeconômicos e inúmeras disputas na justiça por demissões sem justa causa, além da obtenção indevida de outros benefícios.

Segundo uma pesquisa acessada pelo Fórum das Entidades e Federações (FEF)¹, somente no estado do Espírito Santo, cerca de 30 mil atestados médicos falsos são apresentados por mês, sendo que o prejuízo às empresas chega a R\$ 20 milhões por ano.

Atestados médicos falsificados foram utilizados para pedidos ilegais de auxílio-doença em Londrina-PR, causando um prejuízo de 1,1 milhão, podendo ultrapassar a 3 milhões após a apuração dos documentos, segundo informado pela Polícia Federal².

Nesse contexto, a falsidade de documentos é tema constante nos tribunais brasileiros. A partir de dados recuperados e analisados na base de dados JUSBRASIL (2019), no período de 2016 a 2018, a presente pesquisa obteve um número superior a 2 mil processos tramitando em Tribunais de Justiça e outras instâncias jurídicas.

¹ Fonte: Portal de Notícias G1 Espírito Santo, 2017. Disponível em: <https://glo.bo/2vO9rcH>. Acesso em: 10/10/2019.

² Fonte: Portal de Notícias G1 Norte e Noroeste. Disponível em: encurtador.com.br/oAUV8. Acesso em: 10/10/2019.

Nesse mesmo período observou-se na mesma base de dados um número superior a 5 mil processos tramitando em Tribunais Regionais do Trabalho, com número semelhante em Tribunais Regionais Federais, ultrapassando a 6 mil processos divulgados em Diários Oficiais (considerando Tribunais Regionais do Trabalho, Tribunais Regionais Federais e o Supremo Tribunal de Justiça), evidenciando prejuízos econômicos à classe empregadora (JUSBRASIL, 2019).

Diante do exposto, propõe-se a seguinte questão-problema para esse estudo: Como garantir o registro e a autenticidade de atestados médicos-odontológicos de forma unificada?

1.2 Justificativa

No Brasil, os únicos profissionais de saúde autorizados a emitir atestados médicos são o médico e o cirurgião-dentista, conforme Lei 605/49, art. 6º, parágrafo segundo; Lei 5.081/66, art. 6º, inciso III, e RESOLUÇÃO CFM nº 1.658/2002.

Segundo o CFM (Conselho Federal de Medicina), e o Conselho Federal de Odontologia (CFO), até 30 de novembro 2019, havia **477.022** médicos e **328.251** cirurgiões-dentistas ativos no Brasil.

De acordo informado pelo SEBRAE do Estado de São Paulo, em 2018 existiam no Brasil 6,4 milhões de pequenos negócios empresariais. Desse total, as micro e pequenas empresas (MPEs), correspondem a 99%, respondendo por 52% dos empregos com carteira assinada no setor privado (16,1 milhões)³.

Médicos, cirurgiões-dentistas e entidades empregadoras (empresas do setor público e privado), pacientes e órgãos reguladores, participam do cenário do ciclo de vida de um atestado médico-odontológico sendo estes os atores, as partes interessadas e também os que sofrem as maiores consequências advindas destes documentos falsificados.

De acordo com os dados da pesquisa de Braga, Ertler e Pereira (2018), os casos de atestados falsos oriundos de terceiros (que não médicos) estavam associados à situação de absenteísmo, sendo as faltas ao trabalho justificadas por atestados falsificados.

O Artigo 482 da Consolidação das Leis do Trabalho (CLT) trata a falsificação de atestado médico como infração grave, e categoriza a falsificação do documento como um ato de improbidade. Diante disso, a infração é passível de demissão por justa causa.

Assim sendo, e com base nos estudos de Braga, Ertler e Pereira (2018), supõe-se que

³ <http://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD> . Acesso em: 05/10/2019.

as entidades empregadoras tendem a ter prejuízos econômicos diante da possível perda de produtividade em função do afastamento indevido de mão de obra, além de possíveis custos com causas administrativas ou jurídicas deflagradas a partir da descoberta do documento falso.

De acordo Barazetti, Morandini e Bonamigo (2014), existem dificuldades em se comprovar de forma objetiva a falsidade do documento e, decorrente disso, a punição dos infratores se torna mais difícil. Para tanto os documentos suspeitos deveriam ser analisados um a um.

Por conta de desafios dessa natureza, novos mecanismos Governamentais para incentivar iniciativas que desenvolvam, executem, operem ou comercializem novas modalidades de produtos e serviços para atender demandas como essas estão cada vez mais iminentes.

Como exemplo, a Lei de Liberdade Econômica (Lei nº 13.874/2019), em seu Artigo 3º, Inciso VI, dispõe em seus termos, o incentivo ao desenvolvimento de soluções quando normas infralegais se tornarem obsoletas ou desatualizadas, por força de desenvolvimento tecnológico.

Do mesmo modo, a Lei 13.787/2018 dispõe sobre a utilização de sistemas informatizados para guardar, armazenar e manusear informações de pacientes, em prontuário de formato digital. De acordo com essa Lei, em seu Artigo 2º, a forma de realizar esse processo tecnológico-digital deve contemplar a seguridade e a integridade das informações, assim como a autenticidade e a confidencialidade do documento.

Em face dessas oportunidades, as tecnologias consideradas disruptivas, ligadas à Inteligência Artificial (AI), *Internet* das Coisas (IoT) e *Blockchain*, têm se tornado o alvo de pesquisas na tentativa de resolver problemas reais, cuja demanda exige o registro, autenticidade, tratamento e compartilhamento de dados de forma íntegra (CHRISTIDIS; DEVETSIKIOTIS, 2016; HUCKLE *et al.*, 2016; MILLER, 2018; SUN *et al.*, 2016; MOUGAYAR, 2018; TRAUTMAN, 2016).

Dentre elas, a *blockchain* se tornou uma das tecnologias emergentes que, devido a sua arquitetura, oferece suporte ao desenvolvimento de soluções confiáveis para a realização de transações que envolvem cenários onde não há confiança. Através dela é possível criar digitalmente um ambiente descentralizado e confiável, sem a necessidade de uma terceira parte para moderá-lo (CHRISTIDIS, 2016; CROSBY *et al.*, 2015; DEVETSIKIOTI, 2016; GREVE *et al.*, 2018; TRELEAVEN; BROWN; YANG, 2017).

Dentro desse viés, o Estado da Arte apresenta modelos de soluções tecnológicas que

visam registrar informações médicas através de *software*, proporcionando o gerenciamento particular desses dados (ANDROULAKI, 2017; AZARIA *et al.*, 2016).

O Estado da Técnica dispõe de soluções tecnológicas que se propõe a registrar atestados médicos ou o histórico médico de pacientes (prontuários) com modelos de negócio baseados em aplicações comerciais ou iniciativas de entidades específicas.

Diante da avaliação desse cenário, a presente pesquisa nasceu da constatação de oportunidades que surgiram a partir das lacunas deixadas por estas soluções tecnológicas, e que poderão ser preenchidas pelos resultados deste estudo, conforme a seguir.

Embora modelos propostos no Estado da Arte e as soluções já existentes no Estado da Técnica apresentem soluções que corroboram com o propósito deste estudo, seus modelos não estão voltados para a unificação, em rede distribuída, dos registros de atestados médico-odontológico.

Além disso, mesmo diante dos relevantes esforços legais já existentes no combate à falsificação desse tipo de documento, até o momento deste estudo, ainda não há um dado oficial da existência e utilização de um instrumento tecnológico institucionalizado que permita, além do registro em uma rede unificada, a sua rastreabilidade, a verificação da sua autenticidade e geração de dados estatísticos a partir dos dados informados no atestado.

Incentivos como o disposto na Lei de Liberdade Econômica e na Lei 13.787/2018 tendem a impulsionar o crescimento de pesquisas de soluções em inovação tecnológica, com o uso de tecnologias que favoreçam a criação de soluções digitais, a exemplo da *blockchain*, o que tende a favorecer os resultados deste estudo.

Os estudos de Androulaki (2017) apresentam o Modelo de Arquitetura *Blockchain* de Execução por Ordem de Validação do *Hyperledger Fabric* em seus resultados, e os fundamentos desse modelo lastreia a elaboração do modelo de registro proposto na presente pesquisa.

Do mesmo modo, os estudos de Azaria (2016) apresentam em seus resultados um modelo de registro de prontuário de pacientes em *blockchain*, reforçando a teoria de que a tecnologia pode ser utilizada para o registro de informações médicas.

Esses e os demais fundamentos teóricos do Estado da Arte reafirmam que a tecnologia *blockchain* tende a se tornar a mais viável para o controle seguro de todo o processo do atestado desde seu armazenamento, após sua geração, até a validação da sua autenticidade justificando, dessa forma, a escolha da tecnologia para os resultados desta pesquisa.

Diante do exposto, averiguou-se que havia uma brecha que consistia na necessidade da elaboração e implementação de um modelo de registro que orientasse todo o percurso de

registro e validação por meio tecnológico-digital do referido documento, desde a sua emissão até a sua utilização.

O modelo deveria responder à questão-problema dessa pesquisa, contemplando regras de negócio que envolve desde o credenciamento prévio dos possíveis participantes da rede de registro (médicos; cirurgiões-dentistas, empresas empregadoras e órgãos interessados, do setor público e privado), passando pelo processo de emissão e registro por meios tecnológicos, até a consulta eletrônica para a validação do documento.

As regras do modelo deveriam ser implementadas utilizando tecnologia *blockchain* e por ela contemplar a unificação registral de atestados médicos-odontológicos emitidos por outras soluções tecnológicas, sejam de iniciativa comercial, pública ou privada, garantindo a reunião dos registros em um só repositório.

O modelo proposto nesse trabalho aborda o processo de registro e a validação desse tipo de documento em esfera abrangente, contribuindo com a minimização de prejuízos socioeconômicos, além da preservação da autonomia e da credibilidade dos profissionais de saúde, supracitados.

1.3. Objetivo Geral

O objetivo geral desse trabalho foi propor um modelo de registro unificado para verificação de autenticidade de atestados médicos-odontológicos em rede *blockchain*, elencando as possibilidades de proteção intelectual e transferência de tecnologia.

1.4 Objetivos Específicos

Para alcançar o objetivo geral citado, foi necessário:

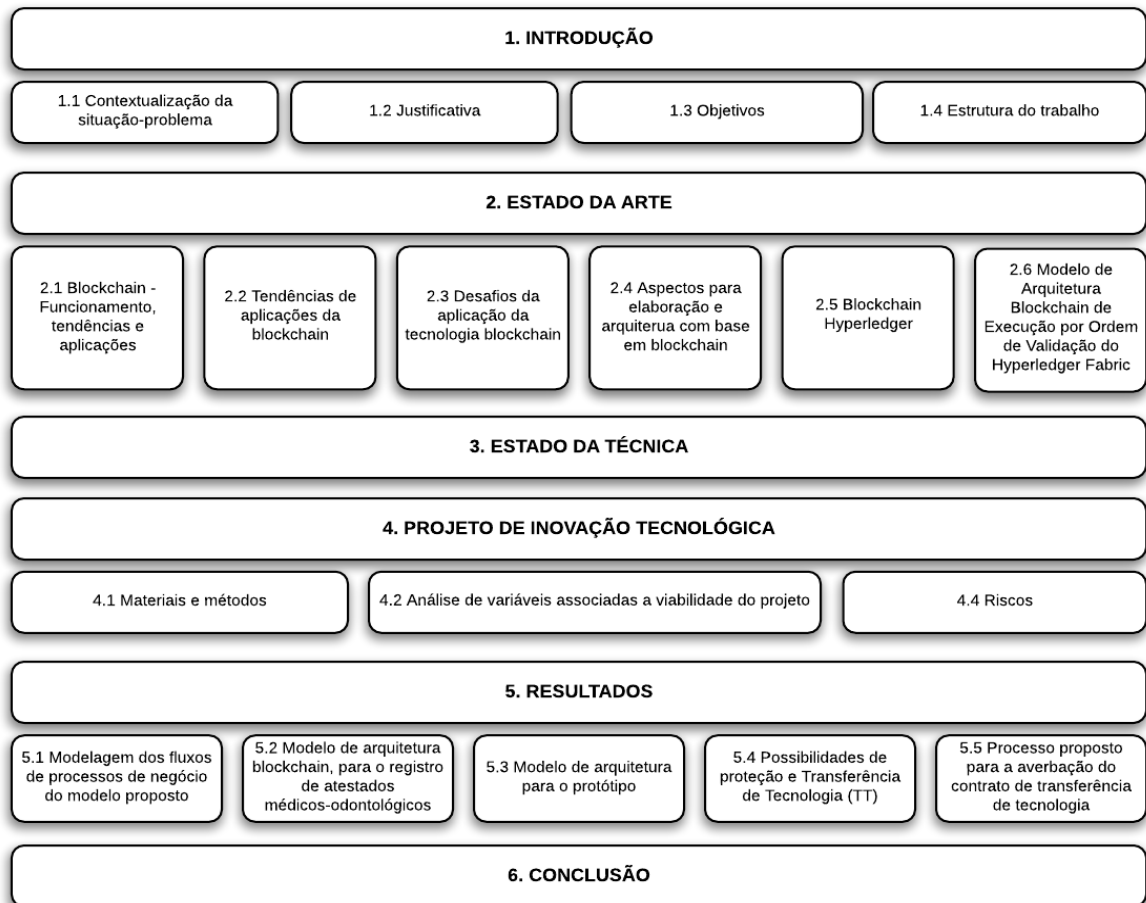
- Elaborar uma modelagem de processos de negócio envolvendo as operações de registro e validação de autenticidade do documento;
- Elaborar arquitetura tecnológica prevendo a sua modelagem, as regras de negócio e os casos de uso que serviram de diretrizes de desenvolvimento de um sistema em nível de protótipo para validar o modelo proposto nessa pesquisa.
- Apresentar um protótipo com base na arquitetura, visando testar e validar a viabilidade da proposta;
- Elencar as possibilidades de proteção intelectual e transferência de tecnologia,

avaliando o processo de averbação contratual junto ao INPI.

1.5 Estrutura do trabalho

A estrutura deste trabalho está dividida em seis capítulos que, além dessa introdução, pretendem apresentar desde a contextualização do problema até um projeto de inovação tecnológica que propõe em seus resultados uma possível solução à questão-problema da pesquisa. Conforme a **Figura 1**, a seguir.

Figura 1 - Estrutura do trabalho



Fonte: Autoria própria (2019).

A Introdução é o capítulo que apresenta o tema e expõe um panorama geral dos aspectos que envolvem a Transferência de Tecnologia (TT) e aborda-se a contextualização da situação-problema, justificando a escolha do tema estudado, além da apresentação dos objetivos a serem alcançados, e a estruturação do trabalho.

O Estado da Arte é o capítulo que apresenta as obras que fundamentam teoricamente

os resultados da pesquisa. Esse levantamento aborda conhecimentos relacionados à *blockchain*, e que fundamentam a elaboração do modelo proposto neste estudo.

No capítulo Estado da Técnica apresentam-se as soluções similares ou periféricas ao modelo proposto na presente pesquisa, expondo seus tipos de aplicação e objetivos, além da comparação entre elas e o modelo proposto nesse estudo.

O capítulo Projeto de Inovação Tecnológica apresenta os métodos da pesquisa e as etapas dos procedimentos utilizados para a obtenção dos resultados. Também é apresentado uma análise de variáveis técnicas, econômicas, de mecanismos de proteção intelectual e transferência de tecnologia e riscos, associados à viabilidade do projeto.

O capítulo Resultados apresenta o modelo teórico de registro proposto com base na tecnologia *blockchain*, com modelagens de fluxos de processo de negócio, exposição das regras de negócio, requisitos funcionais e Casos de Uso, utilizados no desenvolvimento de um protótipo para a validação da teoria.

Adicionalmente a esse capítulo, são apresentadas as possibilidades e recomendações para a proteção intelectual e de transferência de tecnologia que atendam a adequada proteção do produto gerado, seguida do processo de transferência ao mercado produtivo.

O capítulo Conclusão trata das considerações finais, considerando as respostas referentes à questão-problema dessa pesquisa, o alcance dos seus objetivos, os seus limites e, por fim, a proposição de estudos futuros para a continuidade do trabalho.

2 ESTADO DA ARTE

O presente capítulo apresenta o disposto no Estado da Arte levantado por essa pesquisa, fazendo referência ao que já se tem publicado sobre o assunto pesquisado, amparando o entendimento da elaboração e aplicação do modelo aqui proposto.

A revisão e sintetização das obras parte dos conceitos elementares que compreendem a *blockchain*, os conhecimentos basilares que envolvem as diversas aplicações da tecnologia, elementos da sua arquitetura, e modelos de arquitetura de sistemas de registros distribuídos.

2.1 *Blockchain – Funcionamento, Evolução e Aplicações*

Buscando entender o funcionamento, evolução e as aplicações elementares da *blockchain*, as primeiras obras apresentadas nesse trabalho incluem os conceitos gerais do tema (CROSBY, *et al.*, 2015; GREVE *et al.*, 2018; NAKAMOTO, 2008; SWAN, 2015); o histórico e o resultado da evolução da tecnologia (ZHAO, FAN; YAN, 2016); as plataformas oriundas dessa evolução: *Ethereum*, *R3 Corda* e *Hyperledger* (VALENTA; SANDNER, 2017); e a introdução às aplicações da tecnologia em novos modelos de negócio (MOUGAYAR, 2016; NOWIŃSKI e KOZMA, 2017; SILVA; BOVÉRIO, 2018).

A *blockchain* surgiu com o *Bitcoin* quando Satoshi Nakamoto (pseudônimo usado pelo autor) propõe, em seu famoso *paper* datado de 2008, uma tecnologia que funcione como um “livro-razão” capaz de armazenar todas as transações financeiras de todos os membros da rede *Bitcoin*, tornando visível todo o histórico de todas as transações já realizadas (NAKAMOTO, 2008).

Uma *blockchain*, portanto, é um tipo de banco de dados que armazena informações registradas de forma permanente e a prova de qualquer violação externa, (CROSBY, *et al.*, 2015; GREVE *et al.*, 2018).

O estudo de Crosby *et al.* (2015), traz o conceito da *blockchain* como essencialmente um banco de dados distribuído, com o registro de todas as transações ou eventos que foram executados e compartilhado entre as partes participantes.

Corroborando com esses autores, as características da tecnologia trazidas pelo estudo de Greve *et al.* (2018), descreve:

Blockchain é uma tecnologia emergente que oferece suporte distribuído confiável e seguro para realização de transações entre participantes que não necessariamente têm confiança entre si e que estão dispersos em larga escala numa rede P2P. É

considerada uma tecnologia disruptiva, pois cria digitalmente uma entidade de confiança descentralizada, eliminando a necessidade de uma terceira parte de confiança (GREVE *et al.*, 2018. p.2).

O estudo de Swan (2015), por sua vez, compara e define a *blockchain* como uma espécie de “livro-razão” público e expansível, contendo o registro de todas as transações que já foram executadas, as informações são adicionadas a ele de forma encriptada e protegida de possíveis adulterações (SWAN, 2015).

O trabalho de Mougayar (2016) aborda que, após servir como base tecnológica de criptomoedas, a *blockchain* passou a receber o interesse em pesquisas por instituições financeiras, empresas globais e organizações governamentais, desencadeando diversas evoluções e mudanças na tecnologia, de modo que diversas aplicações pudessem ser desenvolvidas com ela (MOUGAYAR, 2016).

Como resultado, tornou-se possível o desenvolvimento de soluções em vários setores e em diversos segmentos, dentre eles o setor automotivo, as seguradoras, o registro de notas, a cadeia de suprimentos, processos eleitorais, dentre outros (ARRUDA, 2017; NOWIŃSKI; KOZMA, 2017).

De acordo o estudo de Zhao, Fan e Yan (2016), três gerações de *blockchains* surgiram durante esse período de mudanças e evolução. A primeira denominada *Blockchain 1.0*, referindo-se às moedas digitais; a segunda denominada *Blockchain 2.0*, a serviços financeiros digitais; e, finalmente, a denominada *Blockchain 3.0*, referindo-se à sociedade digital.

Originalmente a primeira aplicação da tecnologia foi a criação de criptomoedas, porém a partir do ano de 2013 com o surgimento da “*Blockchain 2.0*” inicia-se um novo projeto no campo de banco de dados distribuído, dando assim início a novas arquiteturas capazes de atender outras aplicações para fins de transações financeiras (SWAN, 2015; ZHAO, FAN; YAN, 2016).

Os estudos de Gates (2017) e de Greve *et al.* (2018), abordam que a partir das evoluções implementadas nessa segunda geração, surgem novas plataformas *blockchains* com a possibilidade de implementação de políticas de consenso e execução de regras de negócios de forma automatizada.

O resultado deu início a redes *blockchains* capazes de suportar e responder a novos modelos de negócio, inaugurando a terceira geração da tecnologia (VALENTA; SANDNER, 2017).

Os estudos de Brown *et al.* (2016); Gates (2017); Greve *et al.* (2018); Swan (2015); Tasca, Thanabalasingham e Tessone (2017); Trautman (2016) e Valenta e Sandner (2017)

discutem as características principais destas redes, conforme a seguir:

I) *Ethereum*:

Em 1994, o Criptógrafo Nick Szabo⁴ propôs o conceito de contrato inteligente (*smart contract*) utilizando a tecnologia *blockchain* como base, e com funções de código capazes de interagir com outros contratos, tomando decisões, armazenando os dados e enviando pagamento para outras pessoas (SZABO, 1994).

Com base nesse conceito, a *Ethereum* é fundada em janeiro de 2014 por Vitalik Buterin com o propósito de executar acordos contratuais programados em código de linguagem de programação, sem a possibilidade de censura, fraudes ou interferência de terceiros (GATES, 2017).

De acordo Swan (2015), a plataforma permite que seus usuários criem contratos inteligentes (*smart contracts*) com regras de acordos contratuais programados em aplicações computacionais, de maneira que sejam executadas na íntegra através da *blockchain*.

Sendo assim, as transações concernentes aos acordos financeiros e regras de um negócio podem ser firmadas e automaticamente executadas por *smart contracts* que, por sua vez, desafiam as atuais formas de formalização, registro e execução dos acordos contratuais tradicionais (GATES, 2017; TASCA; THANABALASINGHAM; TESSONE, 2017).

II) *Hyperledger*

Projeto de esforço colaborativo iniciado em 2016 pela Linux Foundation⁵, tendo como objetivo evoluir a tecnologia de registro distribuindo *blockchain* em diversos segmentos da indústria (TASCA; THANABALASINGHAM; TESSONE, 2017).

Trata-se de uma estrutura básica de registro distribuído de código aberto de nível empresarial, transformando a forma como as transações comerciais são conduzidas globalmente (GREVE *et al.*, 2018).

Um maior aprofundamento das características dessa plataforma será passado mais adiante, ainda nessa revisão do Estado da Arte.

⁴ Disponível em:

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em 11/10/2019.

⁵ Disponível em: <https://www.hyperledger.org/>. Acesso em: 11/10/2019.

III) R3 Corda

Desenvolvida em 2016 pela R3⁶, empresa americana de *software blockchain*, a plataforma Corda foi projetada através de um estreito trabalho colaborativo que contou com a participação de instituições financeiras, reguladores, associações comerciais, empresas de tecnologia e de serviços (BROWN *et al.*, 2016).

Segundo Trautman, (2016), o propósito da iniciativa foi tornar a arquitetura da *blockchain* poderosa o suficiente para suportar desafios específicos da indústria e ter a sua aplicação ligada diretamente a todas as outras áreas de negócios.

Segundo Brown *et al.* (2016), a plataforma Corda é especializada em instituições financeiras regulamentadas, e dentre as suas principais características estão:

- O registro e a gestão dos acordos financeiros;
- Articular o fluxo de trabalho entre empresas sem um controlador central;
- Apoiar o consenso entre firmas em nível de negócio;
- Validar transações entre as partes;
- Apoiar uma variedade de mecanismos de consenso.

IV) Comparação entre *Ethereum*, *Hyperledger* e R3 Corda

Ethereum, *Hyperledger* e R3 Corda estão posicionados como *frameworks* para aplicações em *blockchain* em diferentes campos de atuação. A **Tabela 1**, a seguir, resume os três *frameworks*:

⁶ Disponível em: <https://www.r3.com/platform/>. Acesso em: 11/10/2019.

Tabela 1 - Resumo comparativo entre *Ethereum*, *Hyperledger* e R3 Corda

Características	Ethereum	Hyperledger	R3 Corda
Descrição da plataforma	Plataforma <i>blockchain</i> genérica	Plataforma <i>blockchain</i> modular	Plataforma especializada para o setor financeiro
Governança	Desenvolvedores <i>Ethereum</i>	<i>Linux Foundation</i>	R3
Modo de operação	Não permissionado, público ou privado	Permissionado, privado	Permissionado, privado
Consenso	- Mineração baseado em prova de trabalho (PoW) - Nível de “livro-razão”	- Compreensão ampla do consenso que permite múltiplas abordagens - Nível de transação	- Compreensão específica do consenso (ou seja, nós notários) - Nível de transação
Contrato inteligente	Código de contrato inteligente	Código de contrato inteligente (por exemplo, Go, Java)	Código de contrato inteligente (por exemplo, Kotlin, Java) Contrato legal inteligente (prosa legal)
Moeda digital	<i>Ether Tokens</i> via contrato inteligente	Nenhuma Moeda e <i>tokens</i> via lógica de negócio	Nenhuma

Fonte: Elaborado a partir de Brown et al. (2016); Gates (2017); Greve et al. (2018); Valenta e Sandner (2017); Swan (2015); Tasca, Thanabalasingham e Tessone (2017); Trautman (2016).

De acordo com Valenta e Sandner (2017), enquanto a principal aplicação do R3 Corda está voltada à serviços financeiros, o *Hyperledger* possui uma arquitetura modular e estendida que pode ser empregada em vários segmentos como indústria, áreas financeiras, saúde, e cadeia de suprimentos, dentre outras.

A *Ethereum*, diferente do *Hyperledger* cuja característica está na modularidade, se destaca como uma plataforma genérica, independente e aplicável a qualquer tipo transação (VALENTA; SANDNER, 2017).

Dois modos de operação determinam o tipo de participação no consenso nessas redes: “não-permissionado” e “permissionado”. No primeiro modo, qualquer pessoa participa da rede, como acontece na *Ethereum*, pois se trata de uma *blockchain* pública (GATES, 2017; VALENTA; SANDNER, 2017).

Por outro lado, de acordo aos autores, se o modo é “permissionado”, os participantes são selecionados previamente e o acesso à rede é restrito a apenas esses participantes, como ocorre na *Hyperledger* e Corda.

De acordo com Valenta e Sandner, (2017), os modos de participação “não-permissionado” ou “permissionado” promovem relevantes impactos na forma como o consenso é alcançado na rede.

Na *Ethereum* o consenso acontece com base em prova de trabalho (*Proof of Work* - PoW). Todos os participantes da rede precisam concordar com os dados registrados no “livro-

razão”. A desvantagem desse tipo de consenso é que o desempenho do processamento das transações é afetado desfavoravelmente (GATES, 2017).

Diferente da *Ethereum*, as redes *Hyperledger* e Corda possuem um consenso mais refinado, pois somente as partes que participam da transação precisam chegar ao consenso, podendo também ser executado pelas regras codificadas em um *smart contract* (GATES, 2017; VALENTA; SANDNER, 2017).

O **Quadro 1**, a seguir, expõe as obras até aqui apresentadas (em ordem cronológica decrescente) relacionadas aos conceitos gerais da *blockchain*, sua evolução, e conceitos básicos de aplicação.

Quadro 1 - Obras do tema “Blockchain”

Título da obra	Abordagem	Aplicação
<i>Blockchain e a Revolução do Consenso sob Demanda</i> (GREVE <i>et al.</i> , 2018)	Através de uma pesquisa explicativa e aplicada, os autores apresentam os principais elementos, propriedades, modelos e algoritmos da <i>blockchain</i> , e os desafios de aplicá-los.	Aplicado à área de Computação, mais especificamente à Engenharia de <i>Software</i> , o estudo propõe modelos de protocolos de consenso distribuído voltados à segurança, utilizados em contexto de redes de computadores, computação em nuvem e <i>Internet das Coisas</i> .
<i>Blockchain: uma tecnologia além da criptomoeda virtual</i> (SILVA; BOVÉRIO, 2018)	Através de uma revisão de literatura os autores investigam o que é a tecnologia <i>blockchain</i> e suas possíveis aplicações em nível de implementação em diversas áreas.	Aplicado à área de Computação, mais especificamente à Tecnologia em Informática, o estudo explica as características e limitações da tecnologia a serem consideradas, quando implementada em aplicações diversas.
<i>How Can Blockchain Technology Disrupt the Existing Business Models</i> (NOWIŃSKI; KOZMA, 2017)	Através de um trabalho de desenvolvimento de teoria baseado em revisão de literatura, os autores apresentam como a tecnologia <i>blockchain</i> pode atuar de forma disruptiva em relação aos modelos de negócios existentes e exploram os impactos disso.	Aplicado à área de Negócios e Economia, o estudo fornece uma breve visão geral sobre inovação de modelos de negócios impulsionados pela <i>blockchain</i> . Propõe maneiras cruciais pelas quais a tecnologia pode impactar os atuais modelos de negócios: autenticidade, desintermediação e melhoraria da eficiência operacional.
<i>Ethereum: Complete guide to understanding Ethereum Blockchain, Smart Contracts, ICOs, and Decentralized Apps</i> (GATES, 2017)	Através de uma revisão de literatura, os autores discutem conceitos gerais de contratos inteligentes aplicados à plataforma <i>Ethereum</i> .	Aplicado à área de Computação, a obra apresenta as bases para a configuração de contratos inteligentes (<i>smart contracts</i>), na rede <i>blockchain Ethereum</i> .
<i>Ontology of Blockchain Technologies: Principles of Identification and Classification</i> (TASCA; THANABALASINGHAM; TESSONE, 2017)	Através de um texto expositivo-argumentativo, o autor realiza um estudo comparativo entre as tecnologias de <i>blockchain</i> mais amplamente conhecidas, dando destaque a modelos de referência técnica padrão da <i>blockchain</i> .	Aplicado à área de Computação, mais especificamente à Engenharia de <i>Software</i> , o resultado é uma ontologia <i>blockchain</i> universal que agrupa, em uma estrutura hierárquica, os seus principais componentes, identificando sua relação funcional e possíveis padrões de <i>design</i> de arquiteturas para aplicação em sistemas.

Título da obra	Abordagem	Aplicação
<i>Comparison of Ethereum, Hyperledger Fabric and Corda</i> (VALENTA; SANDNER, 2017)	Através de um trabalho de desenvolvimento de teoria os autores fornecem uma breve análise das diferenças mais notáveis entre as tecnologias de <i>blockchain</i> distribuída, <i>Hyperledger</i> , R3 Corda e <i>Ethereum</i>	Aplicado à área de Computação, o estudo demonstra para quais casos de uso o <i>Hyperledger</i> , Corda e <i>Ethereum</i> são mais adequados.
<i>Corda: An Introduction</i> (BROWN <i>et al.</i> , 2016)	Através de um trabalho de desenvolvimento de teoria, este artigo fornece uma introdução de alto nível sobre a plataforma.	Aplicada à área de Computação, o estudo descreve os conceitos elementares, as regras de negócios e o modelo de transação da plataforma Corda.
<i>The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology</i> (MOUGAYAR, 2016)	A obra mapeia novas possibilidades no avanço da aplicação da <i>blockchain</i> no mundo, destrinchando elementos que possibilitarão a ascensão de novos modelos e ideias de negócios, baseados na tecnologia.	Aplicado à área de Negócios, a obra é um guia para nortear novos modelos de negócio baseados em <i>blockchain</i> , que podem ainda não ter visibilidade.
<i>Is Disruptive Blockchain Technology the Future of Financial Services</i> (TRAUTMAN, 2016)	Através de um trabalho de desenvolvimento de teoria, o autor examina algumas das mudanças disruptivas que provavelmente ocorrerão nos serviços financeiros devido aos rápidos avanços tecnológicos da <i>blockchain</i> .	Aplicado à área de Economia e Negócios, o trabalho apresenta resultados de estudos de validação de aplicações <i>blockchain</i> em mercados que necessitam articular fluxo de trabalho entre empresas sem um controlador central. Destaca também os desafios regulatórios para a adoção da tecnologia.
<i>New kid on the block: a strategic archetypes approach to understanding the Blockchain</i> (WALSH <i>et al.</i> , 2016)	Com base em uma revisão de literatura os autores identificam oito recursos principais da tecnologia <i>blockchain</i> dos quais emergem quatro arquétipos de sistema.	Aplicado à área de Computação, mais especificamente Sistemas de Informação, os resultados do estudo identificam quatro arquétipos de <i>blockchain</i> : 1) Descentralizado/Extensível, 2) Descentralizado/Inextensível, 3) Centralizado/Extensível 4) Centralizado / Inextensível. A identificação deles fornece uma base importante para pesquisas futuras, possibilitando a realização de pesquisas aprofundadas que delinearão os custos, benefícios, riscos e problemas associados a cada arquétipo que porventura seja aplicado a um sistema.
<i>Blockchain Technology Beyond Bitcoin</i> (CROSBY <i>et al.</i> , 2015)	O estudo discute como transações digitais na <i>internet</i> utilizam entidades para intermediar e garantir a efetivação destas transações, e mostra como a utilização da <i>blockchain</i> poderá eliminar o uso destes terceiros.	Aplicado à área de Economia e Negócios, o estudo apresenta e analisa as oportunidades de negócios nessa tecnologia aplicada a modelos que necessitam eliminar um terceiro para sua mediação.
<i>Blockchain: Blueprint for a new economy</i> (SWAN, 2015)	A obra discute aspectos conceituais das gerações evolutivas da tecnologia <i>Blockchain</i> .	Aplicado à área de Economia e Negócios, o estudo avalia as três gerações da <i>blockchain</i> cruzando os aspectos tecnológicos de cada geração com modelos de negócio.

Fonte: Autoria própria (2019).

Os objetivos, resultados e aplicações das obras demonstradas no quadro acima amparam o entendimento conceitual que envolve a tecnologia, ampliam a compreensão e dão o suporte inicial à solução proposta na presente pesquisa.

2.2 Tendências de aplicações da blockchain

Explorar como a *blockchain* pode ser aplicada a novos segmentos da indústria, economia e serviços também tem se tornado o alvo de pesquisadores.

As obras citadas neste tópico tratam sobre a aplicação da tecnologia em: modelos de segurança em sistemas e serviços financeiros (MOUGAYAR, 2018; TRAUTMAN, 2016; TRELEAVEN; BROWN; YANG, 2017), modelos de governança de serviços com base na tecnologia (YEMARCK, 2017), e modelos de negócios e serviços através da *Internet* das Coisas - IoT (CHRISTIDIS; DEVETSIKIOTIS, 2016; HUCKLE *et al.*, 2016; MILLER, 2018; SUN *et al.*, 2016).

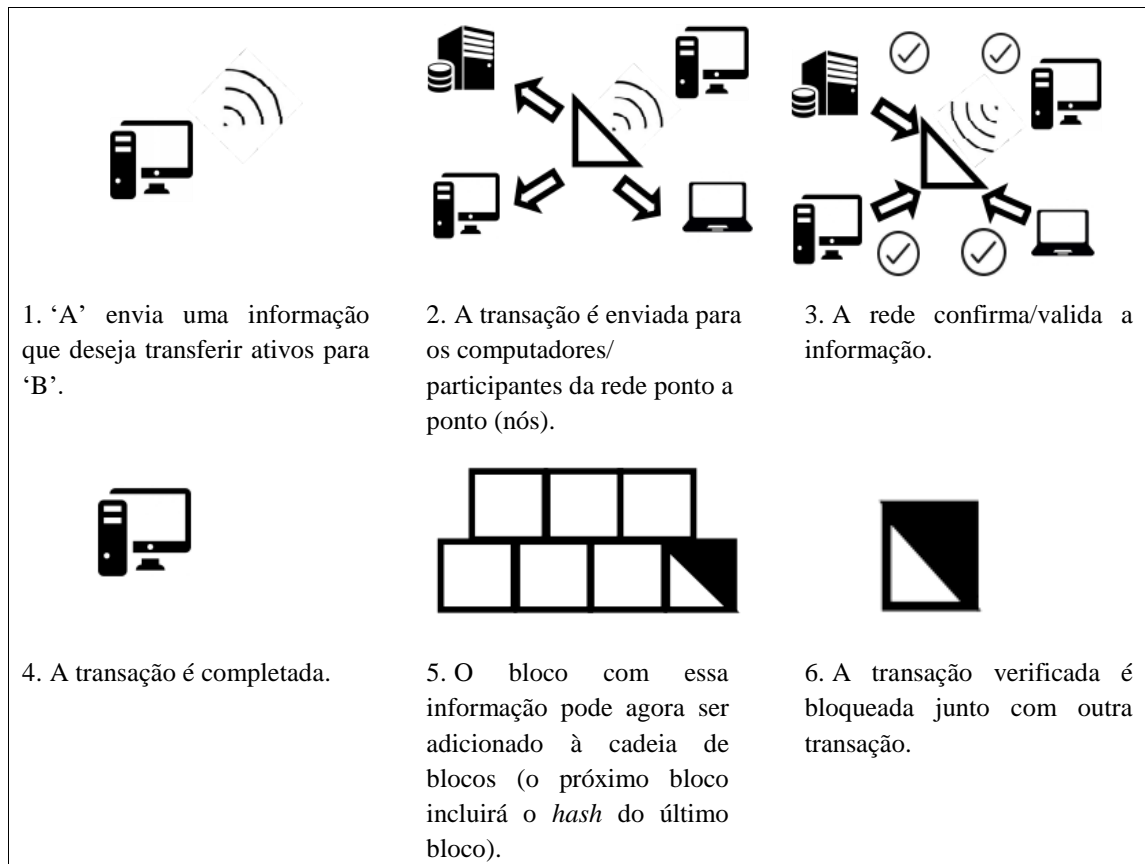
De acordo com os estudos de Mougayar (2018), dois caminhos paralelos apontam o futuro da *blockchain* em relação a serviços financeiros: um deles é o caminho das *Start ups Fintechs*, investindo cada vez mais na criação de serviços financeiros em plataformas digitais, sem precedentes.

O segundo caminho é o da simplificação de operações bancárias com uso da *blockchain* em serviços digitais inteligentes que detectam os comportamentos e preferências dos seus usuários (MOUGAYAR, 2018; TRAUTMAN, 2016; TRELEAVEN; BROWN; YANG, 2017).

De acordo com os estudos de Christidis e Devetsikioti (2016) e Treleaven, Brown e Yang (2017), o uso da tecnologia, portanto, resolve desafios em transações onde se faz necessário confiança e transparência eliminando a necessidade de um terceiro interventor, para que haja a garantia da execução dos acordos previamente estabelecidos.

Segundo Nowiński e Kozma (2017), por este princípio de funcionamento onde a autoridade centralizada é substituída por uma comunidade na forma de rede ponto a ponto, caracterizando-se em um contexto democratizado, as informações são validadas em conformidade com todos os participantes da rede, conforme exemplifica a **Figura 2** a seguir:

Figura 2 - Esquema simplificado de uma transação *Blockchain*



Fonte: Adaptado de Nowiński e Kozma, (2017, p. 174).

De acordo com o esquema de Nowiński e Kozma (2017) apresentado na **Figura 2**, nenhum dos participantes pode tomar ações unilateralmente eliminando possibilidades de governo, empresas ou outras autoridades induzirem resultados, quebrarem regras do sistema, ou manipularem indivíduos.

Os estudos de Zhao, Fan e Yan (2016) e Yemarck (2017) pontuam que o mesmo modelo aplicado a serviços financeiros podem ser utilizados em diversas áreas tradicionais (engenharias, saúde, negócios, economia etc.), ou a novos conceitos como: economia compartilhada, colaboração coletiva (*crowdsourcing*) e a processos de compartilhamento de negócios digitais e, por isso, a importância de estudá-los.

Segundo os estudos de Yermack (2017), os modelos de governança de negócios e serviços, baseados em *blockchain*, trazem mais transparência para a prática gerencial.

Uma vez munida de informações privilegiadas coletadas pelo mercado em tempo real e gravadas na cadeia de blocos, a prática gerencial terá a facilitação da antecipação na realização de negócios (YERMACK, 2017).

Outro aspecto apresentado pelos autores é que a manipulação e a adulteração de

informações gerenciais também tendem a se tornar mais difícil, pois os participantes da rede não poderão reescrever o histórico dos dados gravados, uma vez que a *blockchain* não permitiria (ZHAO; FAN; YAN, 2016; YERMACK, 2017).

As obras apresentadas até aqui elencam as aplicações da *blockchain* em sistemas e serviços que envolvem partes interessadas, porém sem a intermediação de um terceiro, e são apresentadas (em ordem cronológica decrescente) no **Quadro 2**, a seguir:

Quadro 2 - Obras do tema: *Blockchain* em Sistema Financeiros e Governança Corporativa

Título da obra	Abordagem	Aplicações
<i>Blockchain</i> para negócios: promessa, prática e aplicação da nova tecnologia na Internet (MOUGAYAR, 2018)	Através do desenvolvimento de teoria, o autor detalha os elementos da <i>blockchain</i> e discute suas aplicações relacionadas ao fluxo de valor, e como papéis da economia e modelos de governança poderão ser afetados.	Aplicado à área de Negócio e Economia, o estudo apresenta duas assertivas estratégicas. A primeira é que o <i>blockchain</i> possui características polimórficas, sua aplicação resultará em uma multiplicidade de efeitos. A segunda é que a <i>blockchain</i> possibilitará a ascensão de novos modelos e ideias de negócios que podem ainda não terem sido descobertos.
<i>Blockchain Technology in Finance</i> (TRELEAVEN; BROWN; YANG, 2017)	Através de uma narrativa, a obra discute impactos e desafios de implementação da tecnologia <i>blockchain</i> dentro da indústria bancária e de serviços financeiros.	Aplicado à área de Computação, os autores descrevem os desafios encontrados para a implementação de modelos de serviços que envolvem partes interessadas, porém sem a intermediação de um terceiro.
<i>Corporate Governance and Blockchains</i> (YERMACK, 2017)	A obra discute como a <i>blockchain</i> representa uma nova aplicação da criptografia e da tecnologia da informação a antigos problemas de manutenção de registros, podendo levar a mudanças de longo alcance na governança corporativa.	Aplicado às áreas de Computação, Economia e Negócios, avalia as implicações potenciais de modelos de governança de negócios e serviços, baseados em <i>blockchain</i> e os impactos dessas mudanças às partes envolvidas na governança corporativa.
<i>Overview of business innovations and research opportunities in blockchain and introduction to the special issue</i> (ZHAO; FAN; YAN, 2016).	Através da prospecção de estudos sobre <i>blockchain</i> publicados entre 2014 a 2016 e da revisão sistemática da literatura, os autores constroem um panorama da busca de oportunidades e inovação de negócios com tecnologia <i>blockchain</i> .	Aplicado à área de Negócios, o estudo apresenta uma visão geral sobre pesquisa e desenvolvimento de <i>blockchain</i> no mundo, mostrando sua ampla adoção em outros setores da economia, levando a muitas inovações de negócios, bem como a muitas oportunidades de pesquisa.
<i>Is Disruptive Blockchain Technology the Future of Financial Services</i> (TRAUTMAN, 2016)	Através de um trabalho de desenvolvimento de teoria, o autor examina algumas das mudanças disruptivas que provavelmente ocorrerão nos serviços financeiros devido aos rápidos avanços tecnológicos da <i>blockchain</i> .	Aplicado à área de Economia e Negócios, o trabalho apresenta resultados de estudos de validação de aplicações <i>blockchain</i> em mercados que necessitam articular fluxo de trabalho entre empresas sem um controlador central. Destaca também os desafios regulatórios para a adoção da tecnologia.

Fonte: Autoria própria (2019).

O quadro acima reúne obras que enfatizam a utilização da *blockchain* em ambientes sem confiança, tornando possível a transações entre duas ou mais partes sem a necessidade de um “controlador” central.

As discussões dos autores servem como referência conceitual para a idealização do modelo de registro de atestados proposto na presente pesquisa, que utiliza a mesma característica de operação descentralizada sem um controlador central. Compreender as tendências apresentadas por estes autores contribuiu na compreensão da robustez da tecnologia *blockchain* e o quanto ela já vem mostrando resultados em outros setores com complexidade.

Ainda nesse contexto, outro importante aspecto discutido pelos autores apresentados em seguida é o uso da *blockchain* com *Internet* das Coisas (IoT).

De acordo os estudos de Huckle *et al.* (2016), a evolução de periféricos, dispositivos digitais e sensores diversos apoiam transações automatizadas coletando, transmitindo e recebendo dados através da *internet*, de maneiras diversas e em qualquer lugar sem a necessidade de intervenção humana.

Segundo os estudos de Sun *et al.* (2016) e Trautman (2016), os sensores nos dispositivos diversos garantem qualidade, precisão e autonomia da entrada de informações na rede *blockchain*, que são traduzidas em códigos de computação para executar automaticamente serviços inteligentes ou as obrigações contratuais acordadas.

Um exemplo desse cenário são os sistemas cognitivos de Inteligência Artificial, como o *Watson*® desenvolvido pela IBM®, envolvendo uma *blockchain* que recebe as informações de dispositivos de identificação por rádio frequência (RFID), proporcionando o “aprendizado” das preferências e comportamentos para uso posterior (SUN *et al.*, 2016).

Além desses dispositivos, eventos de códigos de barras digitalizados ou dados coletados por dispositivos diversos são transmitidos para a *blockchain* para atualizar ou validar contratos inteligentes (HUCKLE *et al.*, 2016; SUN *et al.*, 2016).

Segundo o estudo de Miller (2018), a cadeia de suprimentos é outro exemplo dessa aplicação. De acordo o autor, a *blockchain* captura dados de remessa enviados por dispositivos IoT que estão conectados em produtos ou *containers* à medida em que eles se movem entre a origem e destino.

As informações das transações da remessa gravadas na *blockchain* garantem a comprovação de entrega de produtos sem que haja a necessidade de intermediários para a aprovação de documentação da remessa a cada ponto de coleta e envio (MILLER, 2018).

As obras discutidas nesse tópico são apresentadas no **Quadro 3**, a seguir:

Quadro 3 - Obras do Tema: Blockchain e Internet das Coisas (IoT)

Título da obra	Abordagem	Aplicação
<i>Blockchain and the Internet of Things in the Industrial Sector</i> (MILLER, 2018)	A obra propõe como IoT e <i>blockchain</i> , fornecerão novas oportunidades de negócios, atenderão aos requisitos regulamentares e melhorarão a transparência e a visibilidade nos próximos dez anos.	Aplicado à área de Computação, o estudo descreve modelos de aplicação da <i>blockchain</i> e IoT em áreas de serviços que necessitam de registro, autenticidade e rastreamento.
<i>Blockchains and Smart Contracts for the Internet of Things</i> (CHRISTIDIS; DEVETSIKIOTIS, 2016)	A obra fornece uma descrição detalhada de como a <i>blockchains</i> e contratos inteligentes funcionam, identificando os prós e contras em um sistema e destaca as maneiras como <i>blockchains</i> e IoT podem ser usados juntos.	Aplicado à área de Computação, o estudo permite que o leitor identifique casos de uso potencialmente novos para aplicações e projetos com <i>blockchain</i> e IoT. Os resultados podem ser utilizados em sistemas que necessitem de coleta de dados, registro e rastreamento de transações.
<i>Blockchain-based sharing services: What blockchain technology can contribute to smart cities</i> (SUN <i>et al.</i> , 2016)	Com base em revisão de literatura, esse estudo propõe uma estrutura conceitual explorando um conjunto de fatores fundamentais que tornam uma cidade inteligente do ponto de vista da economia compartilhada.	Aplicado à área de Inovação e Negócios, discute como os serviços de compartilhamento em cidades inteligentes, baseados em <i>blockchain</i> , podem contribuir para modelos de negócios de serviços inteligentes, em três dimensões: humana, tecnológica e organizacional.
<i>Internet of Things, blockchain and shared economy applications</i> (HUCKLE <i>et al.</i> , 2016)	Com base em revisão de literatura e simulação de cenários, o estudo discute como a <i>Internet</i> das Coisas e a <i>blockchain</i> poderiam ser utilizadas para construir aplicações distribuídas.	Aplicado à área de Inovação e Negócios, discute cenários de aplicações da <i>blockchain</i> e IoT em modelos de negócios distribuídos e compartilhados.

Fonte: Autoria própria (2019).

As obras apresentadas no quadro acima são utilizadas nessa pesquisa como suporte à compreensão de dispositivos IoT que poderiam ou tendem a ser utilizados nas operações de coleta de dados previstas no modelo proposto nos resultados dessa pesquisa.

2.3 Desafios da aplicação da tecnologia blockchain

Para muitos especialistas a *blockchain* já é uma tecnologia pronta para ser usada, porém ainda existem desafios a serem considerados e tratados no momento da sua aplicação.

As obras citadas neste tópico abordam desafios para a adoção da *blockchain* em caráter técnico e regulamentares (LIN; LIAO, 2017; ZHENG *et al.*, 2018), e de adequação à legislação vigente (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

As abordagens relacionadas aos desafios às adequações dos modelos de negócio atuais são discutidas de acordo a autores já citados em tópicos anteriores (CROSBY *et al.*, 2015; MOUGAYAR, 2018).

Inicialmente, os estudos de Lin e Liao (2017) e Zheng *et al.*, (2018), destacam

possíveis desafios técnicos que precisam ser considerados durante a implementação de um sistema em *blockchain*, conforme a seguir:

a) Ataque Majoritário: Em caso de redes que utilizem a mineração para o processo de consenso, um minerador que tenha um maior poder computacional acabará assumindo o controle da *blockchain*.

Nessa condição, caso alguém possua 51% do poder computacional da rede, poderá achar o valor do *nonce* (campo cujo valor é ajustado para que o *hash* do bloco, seja menor ou igual ao destino atual da rede) mais rapidamente que outros mineradores e, conseqüentemente, terá maior autoridade para decidir qual bloco entra na rede. As implicações disso é que a verificação dos blocos poderá ser monopolizada e paralisada (LIN; LIAO, 2017; ZHENG *et al.*, 2018).

b) Escalabilidade: À medida que a rede *blockchain* cresce, os dados se tornam cada vez maiores e mais lentos de serem carregados, e o poder computacional também fica cada vez mais difícil levando muito tempo para sincronizar os dados simultaneamente. Os dados ainda aumentam continuamente, o que pode trazer um grande problema para o “cliente” durante a execução do sistema (LIN; LIAO, 2017; ZHENG *et al.*, 2018).

Outro aspecto relevante trazido pelos estudos de Lin e Liao (2017), Mougayar (2018) e Zheng *et al.*, (2018) que precisam ser considerados como desafio da tecnologia é a inexistência de atos regulamentares especificamente definidos.

Segundo os autores, o uso da característica de sistema descentralizado no tocante a moedas digitais enfraquece a capacidade do banco central de controlar a política econômica e a quantidade de dinheiro, o que torna o governo cauteloso com a tecnologia *blockchain*.

As autoridades tendem a pesquisar esse novo problema e acelerar a formulação de novas políticas, caso contrário haverá riscos no mercado (LIN; LIAO, 2017; MOUGAYAR, 2018; ZHENG *et al.*, 2018).

Também segundo os autores, sendo a *blockchain* considerada uma tecnologia em ascensão, critérios precisos para intervenções jurídicas e a regulação da aplicação ainda estão em andamento e é um desafio diante da legislação vigente.

De acordo Mougayar (2018), são muitas as autoridades regulatórias ao redor do mundo e muitas delas já estão observando a *blockchain*, e pensando em atualizações regulatórias.

Porém, se cada uma delas iniciar a sua própria regulamentação sem coordenação ou sem a consideração para a completa implicação de tais políticas, não somente criará uma grande confusão, mas poderá fazer a indústria em torno da *blockchain* morrer (MOUGAYAR,

2018).

Os estudos Crosby *et al.* (2015) e Mougayar (2018) destacam que atualmente todos os segmentos da economia já estão amparados por algum tipo de sistema ou tecnologia de processamento e segurança, tornando-se praticamente impossível o declínio ou a substituição imediata por novas soluções baseadas em *blockchain*.

Esse cenário, portanto, exigirá a criação de estratégias para a integração de novos modelos e sistemas, a partir da tecnologia com os mais diversos sistemas já existentes (CROSBY *et al.*, 2015; MOUGAYAR, 2018).

Ainda de acordo Lin e Liao (2017) e Zheng *et al.*, (2018), os custos, incluindo tempo e dinheiro para alterar sistemas existentes, especialmente quando for uma infraestrutura, são altos.

Os autores destacam a importância de contrabalancear a utilização da tecnologia, criando benefícios econômicos para demandas inovadoras, assim como para os requisitos de supervisão da organização tradicional (LIN; LIAO, 2017; ZHENG *et al.*, 2018).

Os estudos de Finck (2017), Ramsay (2018) e Rebelo (2019) destacam outro importante desafio a considerar diante da implementação de sistemas em *blockchain*: a adequação à Lei Geral de Proteção de Dados (LGPD).

No Brasil, a LGPD é a Lei Federal 13.709/2018, sancionada em agosto de 2018 e que entrará em vigor em 2020, estabelecendo as regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

A Lei dispõe sobre a coleta e o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos de liberdade e de privacidade, e o livre desenvolvimento da personalidade de pessoa comum (BRASIL, 2018. Art. 1º).

Para efeitos de discussão das abordagens dos estudos de Finck (2017), Ramsay (2018) e Rebelo (2019), se faz necessário destacar os seguintes pontos da Lei:

- 1) Qualquer tipo de informação associada a uma pessoa identificada/identificável é considerado um dado pessoal (BRASIL, 2018. Art. 5º).
- 2) De acordo o Artigo 5, Inciso II, um dado pessoal é considerado um dado sensível quando estão sujeitos à condições de tratamento específicas como: dado pessoal que revele a origem racial ou étnica, convicção ou opinião religiosa, política ou filosófica; filiação sindical; dado genético ou biométrico, tratados para identificação de um ser humano; dado relacionado à saúde; dados relativos à vida ou orientação sexual da pessoa.
- 3) Ainda segundo o Artigo 5, Inciso III, um dado anonimizado é aquele relativo à

titular que não possa ser identificado.

- 4) Os incisos de I a III do Artigo 4º dessa Lei dispõe as exceções da sua aplicação no tocante a tratamento de dados, que são: quando realizado por pessoa natural para fins particulares e não comerciais; para fins exclusivamente jornalísticos, artísticos ou acadêmicos; para fins exclusivos de segurança pública, nacional ou do Estado ou atividades de investigação e repressão de infrações penais.
- 5) O inciso IV do Artigo 4º ainda acrescenta a sua não aplicação quando os dados forem,

[...] provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018. Art. 4º, Inciso IV).

Dentro deste disposto, para saber se a *blockchain* lida com dados pessoais, o estudo de Finck (2017) aborda os dois tipos de dados que nela interagem: chaves públicas e os chamados dados transacionais.

De acordo Finck (2017) e Rebelo (2019), consideram-se dados transacionais aqueles que podem ser movimentados por transações *online*. A exemplo disso estão: dados médicos, financeiros, comportamento do consumidor e dados de identificação.

As autoras abordam que a arquitetura de uma *blockchain* armazena dados de três maneiras: texto, criptografia ou *hashing*. É importante considerar que o armazenamento por texto simples é a forma mais frágil e com a maior possibilidade de identificar o “proprietário” do dado.

O armazenamento por criptografia também pode não preservar o anonimato, pois seu acesso ocorre através de uma chave privada tornando possível o rastreamento até seus titulares.

Por fim, se os dados transacionais forem transformados em *hashes* o nível de privacidade é consideravelmente maior que na criptografia comum, pois não podem ser projetados reversamente (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

Entretanto, de acordo Rebelo (2019), tanto a criptografia ou *hashing* são formas de pseudonimização e não necessariamente uma anonimização de dados pessoais, e esse fato tende a um potencial conflito com o Artigo 5º, Inciso III da Lei, que versa sobre dado anonimizado (relativo a titular que não possa ser identificado na utilização de meios técnicos para o seu tratamento).

Por sua vez as chaves públicas não são identificadas como dados transacionáveis, mas um conjunto alfanumérico que identifica um usuário que pretende fazer transações, de forma pseudonimizada (RAMSAY, 2018).

Segundo o Artigo 13, parágrafo 4, da LGPD, a pseudonimização é o tratamento pelo qual um dado perde a sua correlação (direta ou indireta) com um indivíduo, a não ser pelo uso de informação adicional guardada de forma separada, em ambiente seguro e controlado, pelo controlador (BRASIL, 2018, Art .4, §4º).

Nesse ponto, os estudos de Finck (2017), Ramsay (2018) e Rebelo (2019) destacam que a possibilidade de conflito com a norma está no fato que as transações que ocorrem em uma *blockchain*, através da publicação de uma chave pública, estão associadas a uma *Internet Protocol Address* (endereço IP).

Se por um lado uma chave pública é criptografada para que se alcance determinado anonimato na transação *online*, do outro é possível identificar a “entidade” que representa aquele usuário pela reutilização da chave pública, e a correspondente correlação com o endereço IP (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

Desse modo, por essa correlação, pode-se concluir que as chaves públicas se qualificam como um dado pessoal que poderá estar sob os efeitos da Lei.

Os autores destacam também o tratamento de dados como outro aspecto a observar na relação da lei com aplicações da *blockchain*. Nos termos da Lei, o tratamento de dados é considerado como qualquer operação executada com dados pessoais.

Nos termos do Artigo 6º dessa Lei, algumas dessas operações qualificadas compreendem: coleta, registro, organização, estruturação, conservação, alteração ou adaptação, consulta ou recuperação, transmissão, difusão ou disponibilização, comparação, interconexão, remoção ou destruição (BRASIL, 2018; REBELO, 2019).

Nesse contexto, os estudos de Finck (2017), Ramsay (2018) e Rebelo (2019) mais uma vez analisam as ações que são executadas nos dados carregados para a *blockchain* como dados pessoais, ponderando as chaves públicas, os dados transacionais e os *nodes*, conforme a seguir.

Cada chave pública corresponde a uma chave privada que por sua vez pertence aos usuários da cadeia de blocos. Por este motivo é possível a todos os usuários verificar mutuamente a autorização de novas transações.

As verificações de validade são automatizadas através de um algoritmo da *blockchain*. No entanto, considerando a amplitude da LGPD em relação ao tratamento dos dados, mesmo que o tratamento seja automatizado por um algoritmo matemático, ainda seria possível

qualificar a operação de verificação da validade da transação através das chaves públicas (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

No tocante aos dados transacionais, algoritmos validam os dados da transação. A operação compreende em armazenar esses dados em um bloco, anexá-lo à *blockchain* e distribuí-lo por todos os usuários.

O significado disso é que essas operações de uso e armazenamento de dados são realizadas, considerando-se a existência de tratamento de dados mediante os termos do Artigo 6º dessa Lei.

No que se refere aos *nodes*, também podem ser qualificados como tratamento de dados nos termos da Lei, pois cada um deles mantém cópia e registro de todos os outros *nodes* com os quais teve comunicação, mantendo uma rede de armazenamento de dados pessoais (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

Por fim, os estudos de Finck (2017), Ramsay (2018) e Rebelo (2019), abordam questões de potenciais conflitos com a norma, conforme a seguir.

Uma *blockchain* recebe e armazena dados indistintamente e se revela através de códigos alfanuméricos (*hashes*), e por isso na maior parte do tempo, seus administradores não controlam e não conhecem que dados pessoais estão sendo inseridos na rede, além de não saberem se estes são dados sensíveis, ou não.

Os maiores desafios conflitantes, nesse caso, estão presentes em *blockchains* públicas dadas a diversidade de possíveis usos em redes dessa natureza, dificultando a elaboração de medidas legais de proteção.

Outra questão analisada frente à Norma é que a arquitetura da *blockchain*, de caráter descentralizado e com ausência de controle através de uma entidade centralizadora, dificulta a adequação às regras previstas na lei, assim como a apuração de responsabilidades e a aplicação das respectivas sanções.

Os estudos de Rebelo (2019) destacam que a característica descentralizada da tecnologia também promove um conflito de objetivos quando confrontada, de um lado, a necessidade de proteger dados pessoais e garantir o direito de seus titulares, e do outro, impulsionar a inovação tecnológica.

Outro aspecto que pode representar um problema sob a ótica da LGPD é que, em princípio, dados lançados em uma *blockchain* não podem ser modificados ou deletados.

Em sistemas como a *blockchain* as transações são registradas em um bloco que faz referência ao bloco anterior através de um *hash* criptográfico, o que torna praticamente impossível a remoção de uma informação da cadeia de blocos (FINCK, 2017; RAMSAY,

2018; REBELO, 2019).

Esse aspecto deve ser analisado nos termos do Artigo 18, Inciso IV e VI da Lei, que dispõe sobre os direitos do titular, quanto à eliminação e portabilidade de seus dados mediante seu consentimento.

A transferência de dados é outro aspecto a observar nos termos que dispõe a Lei. Alguns dos aspectos legais a considerar para a realização dessa operação em uma *blockchain*, são:

- O disposto no Artigo 33, Inciso II, itens “a” e “b”, que abrange sobre a oferta de garantias da observância e cumprimento dos princípios da Lei sob cláusulas contratuais por parte do responsável pelo tratamento.
- O disposto no Artigo 34, Inciso III, que abrange a observância dos princípios gerais de proteção de dados pessoais previstos na Lei brasileira, mesmo que o responsável esteja fora do território nacional.
- O disposto nos Artigos 33 e 34, Incisos VIII e III, respectivamente, que em seus termos determina que uma das possibilidades da transferência de dados para países de terceiros só é possível quando respeitadas as condições de nível de proteção e autorizados especificamente pelo titular dos dados.

Dentro desses aspectos, os estudos de Rebelo (2019) levantam as seguintes questões que devem ser consideradas ao se estabelecer um modelo de governança em sistemas implementados em *blockchain*:

- Como determinar a origem geográfica de um *node* (computadores/usuários)?
- Como garantir níveis adequados de proteção no que se refere à transferência de dados em uma *blockchain*?
- Diante de acordos contratuais, será possível elaborar cláusulas que salvaguardem esses direitos na *blockchain*?

Outro desafio levantando pelos estudos de Ramsay (2018) e Rebelo (2019) é a identificação do Controlador (responsável pelo tratamento), e do subcontratante (a entidade que realiza o tratamento dos dados sob as diretrizes do Controlador).

Os autores abordam que no contexto digital que envolve a *blockchain*, esse aspecto pode se tornar complexo se for considerado que as mesmas entidades podem assumir um papel diferente, além do que lhe é atribuído.

Embora ambos os papéis tenham responsabilidades claras estabelecidas pela Norma, ainda é necessário que se determine precisamente o papel de cada um (RAMSAY, 2018;

REBELO, 2019).

Esse desafio se resolve mais facilmente no caso das *blockchains* privadas (redes permissionadas), pois se qualifica como Controlador – aquele que se assume como destinatário dos dados enviados pelo titular.

No entanto, no caso das *blockchains* públicas (redes não permissionadas onde não há um controlador central), descentralizadas em um indeterminado número de *nodes* (computadores/usuários), todos os participantes da rede podem realizar as operações de carregar e tratar dados de terceiros (RAMSAY, 2018; REBELO, 2019).

Diante disso, e segundo os estudos de Finck (2017), *a priori* conclui-se que nenhum dos participantes da rede podem se qualificar como responsável pelo tratamento, pois não existe uma entidade autônoma e específica com a finalidade de processamento.

Outra possibilidade é concluir que nenhum desses participantes agem com o objetivo de tratamento das informações distribuídas na rede por terceiros, ou todos podem ser qualificados já que nenhum está sujeito a instruções de terceiros no momento em que carregam dados para o “livro-razão” (FINCK, 2017; RAMSAY, 2018; REBELO, 2019).

As obras discutidas neste tópico e que amparam as considerações mais relevantes para esta pesquisa, no tocante aos desafios da aplicação da *blockchain*, são apresentadas no **Quadro 4**, a seguir.

Quadro 4 - Obras do Tema: *Blockchain* e os desafios de aplicação da tecnologia

Título da obra	Abordagem	Aplicação
Os desafios do RGPD perante as novas tecnologias <i>blockchain</i> . (REBELO, 2019).	Através de um estudo exploratório e analítico, o artigo analisa e confronta as questões do funcionamento da arquitetura da <i>blockchain</i> diante dos termos da Lei Geral de Proteção de Dados.	Aplicado a áreas interdisciplinares, o estudo analisa as questões conflitantes entre a aplicação da <i>blockchain</i> frente à Lei Geral de Proteção de Dados.
<i>Blockchains and Data Protection in the European Union</i> (FINCK, 2018)	Através de um estudo exploratório e analítico, o artigo examina a proteção de dados em <i>blockchain</i> frente a iminente entrada e vigor da Lei Geral de Proteção de Dados.	Aplicado a áreas interdisciplinares, o estudo apresenta questões legais a serem consideradas diante da <i>blockchain</i> como o novo paradigma de armazenamento de dados.
<i>The General Data Protection Regulation vs. The Blockchain - A legal study on the compatibility between blockchain technology and the GDPR</i> (RAMSAY, 2018)	Através de um estudo dogmático, o objetivo desta tese é investigar até que ponto o GDPR e as obrigações que ele cria podem ser aplicados ao <i>blockchain</i> .	Aplicado às áreas de Direito e Informática, a tese prepara o terreno para uma nova área da tecnologia sob uma perspectiva jurídica, resultando em uma análise que não emerja em concepções específicas, mas crie uma base ampla para entender e conceituar os problemas jurídicos que cercam a tecnologia.
<i>A Survey of Blockchain</i>	Através de um estudo de análise	Aplicado à área de Computação, o

Título da obra	Abordagem	Aplicação
<i>Security Issues and Challenges</i> (LIN; LIAO, 2017)	técnica, o artigo discute problemas de segurança e os desafios a serem superados em implementações de sistemas em <i>blockchain</i> .	estudo apresenta questões técnicas que devem ser observadas e contrabalanceadas com as vantagens oferecidas pela arquitetura da <i>blockchain</i> .
<i>Blockchain challenges and opportunities: a survey</i> (ZHENG <i>et al.</i> , 2018)	O objetivo do trabalho é apresentar uma pesquisa abrangente, analisando aplicações da <i>blockchain</i> e discutindo desafios técnicos a serem superados.	Aplicado à área de Computação, este estudo fornece a taxonomia da <i>blockchain</i> , apresentando algoritmos típicos de consenso, analisando aplicações e desafios técnicos, bem como avanços recentes na solução dos desafios.

Fonte: Autoria própria (2019).

As obras apresentadas no quadro acima trazem as questões que devem ser levadas em consideração na proposição de minimização dos riscos frente à implementação do modelo proposto nos resultados desta pesquisa.

2.4 Aspectos para elaboração de arquitetura com base em *blockchain*

Sendo uma área relacionada com a Engenharia de *Software*, a arquitetura de sistemas foca nos aspectos, componentes, propriedades internas e externas do desenvolvimento e da evolução de sistemas complexos (SOMMERVILLE, 2011).

As obras citadas neste tópico discutem elementos chaves para uma arquitetura de sistema baseada em *blockchain* e servem como bases norteadoras para a elaboração do modelo de processo de negócio, além da arquitetura proposta nos resultados desta pesquisa e podem ser compreendidos em três dimensões, quais sejam: componentes e design; métodos de consenso; e aspectos de segurança em redes *blockchain*.

Em relação a dimensão componentes e *design* de arquitetura para aplicação em sistemas *blockchain*, pode-se destacar os estudos de Walsh *et al.*, (2016); Prieto-Castrillo; Kushch; Corchado, (2017); Salimitari; Chatterjee, (2019); Zheng *et al.*, (2017); Lucena; Henriques, (2016). Métodos de consenso, destacam-se os estudos de Salimitari; Chatterjee, (2019); Swanson, (2015). Aspectos de segurança em redes *blockchain*, os estudos de Park; Park, (2017; Gopichand *et al.*, (2018); Pires, (2017); Christidis; Devetsiokiotis, (2016).

Segundo os estudos de Prieto-Castrillo, Kushch e Corchado (2017), as *blockchains*, além de serem concebidas como bancos de dados dinâmicos distribuídos, têm seus constituintes (blocos) construídos colaborativamente e incrementalmente por um conjunto de agentes.

Os blocos são adicionados a *blockchain* em ordem cronológica linear. Cada “nó” (computador) conectado à rede usando um cliente que executa a tarefa de validar e retransmitir transações tem uma cópia da *blockchain*, que é baixada automaticamente quando o usuário se une à rede (PRIETO-CASTRILLO; KUSHCH; CORCHADO, 2017; SWAN, 2015).

Para que haja esse funcionamento, Lucena e Henriques (2016) explicam os cinco princípios que norteiam essa operação na *blockchain*:

- Funções de mão única ou *hashs*: elementos que tornam improvável a adulteração do “livro-razão”, pois trabalham com funções computacionais que realizam operações em um único sentido sendo praticamente improvável conhecer o seu valor de entrada, sendo conhecido apenas o valor da saída;
- O registro de tempo: elemento que impede fraudes temporais na *blockchain* armazenando o momento em que qualquer alteração ocorreu;
- Assinatura digital: recurso que garante que as alterações de algum elemento que pertença a um nó da rede sejam realizadas apenas pelo proprietário das chaves públicas e privadas daquele nó.
- Rede descentralizada ponto a ponto: elemento indispensável para o funcionamento da *blockchain*, pois todas as novas informações ou alterações poderão ser aceitas ou rejeitadas pelos “pontos” da rede garantindo a integridade das informações que trafegam nela.

Os estudos de Salimitari e Chatterjee (2019) e de Zheng *et al.* (2017) pontuam que a característica da arquitetura da *blockchain* está baseada na comunicação entre dois ou mais computadores (chamados “nós”), que compõem uma rede ponto a ponto e compartilham todas as transações existentes.

Quando uma nova informação surge na rede, automaticamente é criptografada e partilhada entre esses “nós”, garantindo assim a segurança e o conhecimento “público” da informação partilhada (SALIMITARI; CHATTERJEE, 2019; ZHENG *et al.*, 2017).

Esse resultado é possível porque a rede *blockchain* opera como uma lista estruturada que grava informações com um formato semelhante em um banco de dados distribuído, projetado para dificultar uma provável manipulação (PARK; PARK, 2017; SALIMITARI; CHATTERJEE, 2019).

Os estudos de Christidis e Devetsiokiotis (2016) e de Lima (2015) destacam que em aspectos de segurança por criptografia o conceito de *hashes* é outro importante recurso

utilizado pela *blockchain*.

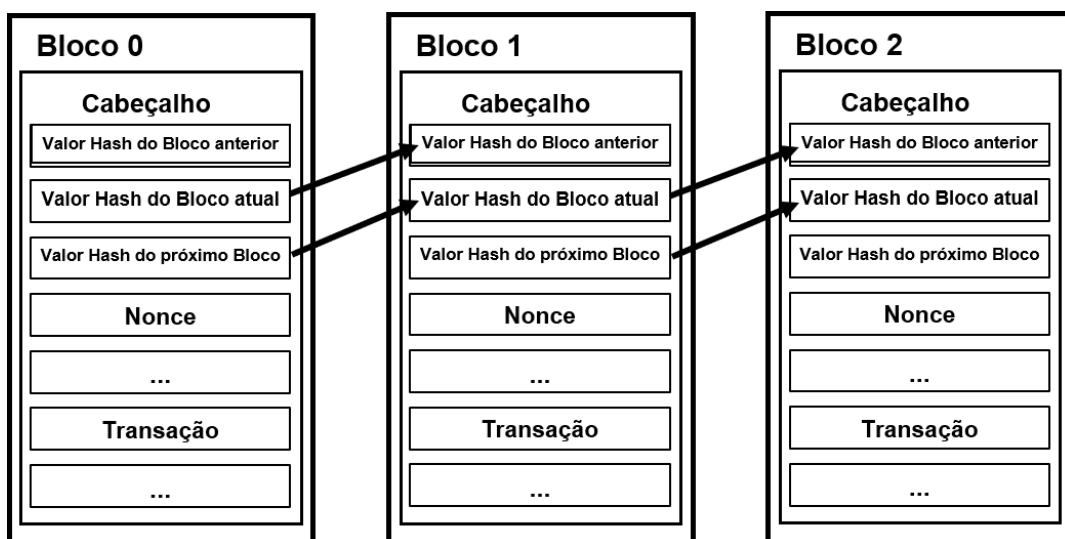
De forma simples, Lima (2015) explica que uma função *hash* é um tipo muito específico de função matemática que aceita como entrada qualquer dado digital (um texto, uma foto, um arquivo de outro conteúdo qualquer), e só aceita uma entrada de dados de um tamanho arbitrário, devolvendo um valor de tamanho fixo também chamado *hash*.

Portanto, uma função *hash* criptográfica tem como característica facilitar o cálculo do resultado da sua aplicação em alguma informação, porém torna extremamente difícil deduzir tal informação conhecendo apenas a função *hash* resultante (CHRISTIDIS; DEVETSIOKIOTIS, 2016; LIMA 2015).

Os estudos de Park e Park (2017) complementam destacando que a verificação pública baseada em chave e função *hash* na *blockchain* utiliza o algoritmo de assinatura eletrônica ECDSA (*Eliptic Curve Digital Signature Algorithm*) para verificar a assinatura digital gerada durante uma transação entre indivíduos, e é usado para provar que os dados da transação não foram alterados.

Os mesmos autores ainda ampliam o entendimento da arquitetura da *blockchain* abordando que os dados são salvos em blocos, os quais possuem uma estrutura que contém um cabeçalho e um corpo conforme a **Figura 3**, a seguir:

Figura 3 - Estrutura de conexão *blockchain*



Fonte: Adaptado de Park e Park, (2017, p. 13).

De acordo com a figura acima, o cabeçalho de um bloco contém os valores de *hash* dos blocos anteriores e também o *nonce* anteriores e atuais (campo cujo valor é ajustado para que o *hash* do bloco seja menor ou igual ao destino atual da rede).

A leitura dos dados desses blocos ocorre no banco de dados através de um método de índices e, embora o bloco já contenha o valor de *hash* do próximo, por padrão ele é adicionado (PARK; PARK, 2017).

Além disso, os estudos de Gopichand *et al.* (2018) e Zheng *et al.* (2017) reforçam que a segurança, forte característica considerável na arquitetura da *blockchain*, está baseada também em características inerentes à sua própria “natureza”, conforme descritas a seguir:

A) descentralização – fator que preserva a consistência dos registros na rede através do consenso dos seus participantes;

B) persistência – característica que torna quase impossível excluir ou reverter as transações depois que elas são protegidas na cadeia de blocos, além da rápida identificação de transações inválidas;

C) anonimato – cada usuário da rede pode interagir com a *blockchain* sem necessitar da sua real identificação;

D) auditabilidade – no caso do modelo da *blockchain* do *bitcoin*, o armazenamento dos dados acontece baseado no modelo de Saída de Transações não Utilizadas. Qualquer transação deve se referir a alguma transação anteriormente não utilizada.

Uma vez que a transação atual é registrada, o estado dessas transações não usadas passa de “não-utilizada” para “utilizada”, facilitando sua a verificação e rastreo (GOPICHAND *et al.*, 2018).

Em se tratando de aspectos técnicos, parte da segurança está baseada em um dos conceitos fundamentais da criptografia moderna: a verificação de pares de chave, uma pública e outra privada (CHRISTIDIS; DEVETSIOKIOTIS, 2016).

Segundo Christidis e Devetsiokiotis (2016) e Gopichand *et al.* (2018), um algoritmo gera um par de chaves: uma pública, cujo conhecimento de sua existência poderá ser divulgado livremente, e uma privada que deve ser guardada em segredo pelo seu dono.

A mensagem codificada com a chave pública só poderá ser decodificada com a chave privada correspondente garantindo, assim, a segurança da transação (CHRISTIDIS; DEVETSIOKIOTIS, 2016; GOPICHAND *et al.*, 2018).

Em termos práticos, os autores explicam que um indivíduo “A” codifica uma mensagem para um indivíduo “B” usando a chave pública desse indivíduo que está disponível livremente na *internet*. A mensagem é enviada para seu destinatário, o qual utiliza a sua chave privada para lê-la. Para responder à mensagem o indivíduo “B” deverá proceder da mesma maneira utilizando a chave pública do indivíduo “A”, o qual utilizará a sua chave privada para lê-la (CHRISTIDIS; DEVETSIOKIOTIS, 2016; GOPICHAND *et al.*, 2018).

Ainda segundo os autores, na *blockchain* a chave pública é anônima e garante que as informações relativas ao proprietário não sejam encontradas, mesmo sendo possível saber a origem e o destino da transação.

Os estudos de Prieto-Castrillo, Kushch e Corchado (2017), Salimitari e Chatterjee (2019), Sun *et al.* (2016) e de Swanson (2015) apontam outro aspecto de alta relevância a ser considerado no quesito de segurança e na implementação da arquitetura da *blockchain*: a confiança através do consenso.

De acordo Sun *et al.* (2016), a dinâmica das pessoas em relação à confiança quanto ao uso das transações em *blockchain* está baseada na transparência e na privacidade da relação de serviços entre seres humanos e tecnologia.

Por registrar de forma permanente o histórico das transações em cada “nó” da *blockchain*, a tecnologia permite que as pessoas acessem os registros de cada transação que fazem promovendo a confiabilidade compartilhada e distribuída entre eles, democratizando assim os serviços (SUN *et al.* 2016).

Os estudos de Salimitari e Chatterjee (2019) ressaltam que todo o processo de implementação de uma rede *blockchain* está diretamente ligado com o tipo de consenso utilizado. Isso significa que o resultado de todo o desempenho da rede implementada dependerá diretamente do método de consenso adotado (PRIETO-CASTRILLO, KUSHCH; CORCHADO, 2017; SALIMITARI; CHATTERJEE, 2019).

Em seu trabalho, Salimitari e Chatterjee (2019) apresentam dois métodos de consenso que criam as bases para modelos onde a confiança se baseia em regras pré-estabelecidas. São eles:

- *Practical Byzantine Fault Tolerance* – PBFT (Tolerância Prática a Falhas Bizantinas);
- *Delegated Byzantine Fault Tolerance* – DBFT (Tolerância a Falhas Bizantinas Delegadas).

O **Quadro 5**, a seguir, reúne os principais aspectos que envolve o método PBFT.

Quadro 5 - Método de consenso: Tolerância Prática a Falhas Bizantinas (PBFT)

Principal característica requerida:	Todos os “nós” da rede devem participar do processo de consenso para adicionar o próximo bloco.
Condição mínima para o alcance do consenso:	Mais de um terço dos “nós” participantes.
Tolerância a falhas:	Tolera até um terço de todos os “nós” com comportamento malicioso.
Vantagens:	Mais rápido e econômico se comparado a outros métodos por não exigir grande poder computacional.
Restrições:	Não aplicável a redes públicas “não-permissionadas”, devido à sua baixa

	tolerância a atividades maliciosas.
Indicação do método:	Adequado para <i>blockchains</i> particulares, como <i>Hyperledger</i> , que são controlados por terceiros.

Fonte: Elaborado a partir dos estudos de Salimitari e Chatterjee, (2019).

Os aspectos mostrados no **Quadro 5**, acima, e segundo os estudos de Salimitari e Chatterjee (2019) e Sukhwani *et al.* (2017), no método PBFT um próximo bloco só é adicionado à *blockchain* com a participação de todos os nós da rede. Esse é o principal requisito do método, no entanto, não restringe a continuidade do processo de consenso.

O consenso já é alcançado quando mais de dois terços dos “nós” que participam da rede concordam com o novo bloco, dando a condição necessária para que o novo bloco já seja adicionado à rede (SALIMITARI; CHATTERJEE, 2019; SUKHWANI, 2017).

Ainda segundo os autores, embora as possibilidades de atividades não confiáveis em redes privadas, de caráter “permissionado”, sejam quase improváveis, o PBFT prevê uma tolerância de atividades não confiáveis na rede de até um terço dos “nós”.

Em seus estudos, Sukhwani *et al.* (2017) complementa que a principal vantagem desse tipo de método é que o consenso é atingido mais rapidamente e mais economicamente se comparado a outros métodos como a Prova de Trabalho (PoW) presentes em redes *Bitcoins*.

Isso ocorre devido à baixa exigência de poder computacional, uma vez que o consenso é realizado por regras pré-estabelecidas e não por “mineração”, como ocorre em redes *Bitcoins* (SUKHWANI *et al.*, 2017).

Segundo os estudos de Salimitari e Chatterjee (2019), o método não deve ser usado para redes *blockchain* públicas, de acesso “não-permissionado”, pois nesse contexto demonstraria baixa tolerância a atividades maliciosas ameaçando a integridade do consenso da rede.

Ainda de acordo com os autores, o segundo método mencionado – Tolerância a Falhas Bizantinas Delegas (DBFT), possui as mesmas regras que o PBFT, a exceção está apenas na não exigência da participação de todos os “nós” da rede para que um novo bloco seja adicionado.

Isso significa que somente os participantes envolvidos naquela transação já são necessários para o consenso, o que facilita a sua adoção em modelos dinâmicos destinados a apenas registro e validação de autenticidade de dados em redes *blockchain* com IoT (SALIMITARI; CHATTERJEE, 2019; SUKHWANI, 2017).

As discussões abordadas pelas obras que fundamentam esse tópico dão suporte à elaboração dos requisitos que compõem o modelo da arquitetura apresentada nessa pesquisa,

pois abrangem aspectos de segurança e proteção de dados e método de consenso, adotados para a solução proposta nesse estudo. O **Quadro 6**, a seguir, resume as obras selecionadas com esse propósito.

Quadro 6 - Obras do tema: Arquitetura e segurança na *blockchain*

Título da obra	Abordagem	Aplicação do estudo
<i>A detailed study and advancement of blockchain</i> (GOPICHAND <i>et al.</i> , 2018)	Através de revisão de literatura, os autores realizam um amplo estudo da arquitetura da <i>blockchain</i> incluindo questões de desafios de segurança.	Aplicado à área de Engenharia de <i>Software</i> , apresenta um diagrama da arquitetura da <i>blockchain</i> e modelos padrões para aplicações em futuras arquiteturas.
<i>Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions</i> (PARK; PARK, 2017).	Através de revisão de literatura, os autores discutem o conceito da tecnologia <i>blockchain</i> e suas tendências de pesquisa e fornecem estudos de casos para demonstrar a adaptação da segurança da <i>blockchain</i> à sistemas de computação em nuvem.	Aplicado à área de Ciência da Computação, apresenta resultados de estudos de caso e propostas de modelos de segurança em <i>blockchain</i> que podem ser implementados em sistemas em nuvem.
<i>Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum</i> (LUCENAS; HENRIQUES, 2018)	Através de revisão de literatura, os autores apresentam os principais problemas enfrentados pelos <i>blockchains</i> de <i>Bitcoin</i> e <i>Ethereum</i> , e as diretrizes para o que, dentro da conclusão dos estudos dos autores, seria considerada uma <i>blockchain</i> eficiente.	Aplicado à área de Engenharia da Computação, a obra discute modelos simplificados para a construção de uma rede <i>blockchain</i> eficiente.
<i>Distributed Sequential Consensus in Networks: Analysis of Partially Connected Blockchains with Uncertainty</i> (PRIETO-CASTRILLO; KUSHCH; CORCHADO, 2017)	Apresenta uma análise teórica e numérica das condições sob as quais o consenso sequencial distribuído é possível quando o estado de uma porção de nós em uma rede é instável.	Aplicado à área de Computação, especificamente examina o nível de consenso de <i>blockchains</i> parcialmente conectados em eventos de falha / ataque. Os resultados propõem modelos de consenso que levam as redes a tolerarem um ataque.
<i>A Survey on Consensus Protocols in Blockchain for IoT Networks</i> (SALIMITARI; CHATTERJEE, 2019)	Através de uma revisão de literatura, evidenciando métodos de consenso existentes que foram implementados, os autores discutem o funcionamento da <i>blockchain</i> , suas aplicações e formas de implementações.	Aplicado à área de Computação, o estudo descreve vários métodos de consenso baseados em <i>blockchain</i> que são aplicáveis a dispositivos e redes de IoT, visando reduzir o poder computacional e o tempo de convergência.
<i>Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems</i> (SWANSON, 2015)	Estudo comparativo que descreve a divergência entre sistemas de criptomoedas "não permissionados" (como <i>Bitcoin</i> , <i>Ethereum</i> e <i>Peercoin</i>) e distribuições "permissionadas" (como <i>Ripple</i> e <i>Hyperledger</i>).	Aplicado à área de Computação, o estudo esclarece, comparativamente, através de casos de uso, os aspectos a serem considerados em arquiteturas de consenso em redes permissionadas e não-permissionadas.
<i>An Overview of Blockchain Technology:</i>	Pesquisa abrangente que aborda desafios técnicos e avanços recentes e	Aplicado à área de Computação, este artigo fornece uma visão geral da

Título da obra	Abordagem	Aplicação do estudo
<i>Architecture, Consensus, and Future Trends</i> (ZHENG <i>et al.</i> , 2017)	possíveis tendências da arquitetura da <i>blockchain</i> .	arquitetura de <i>blockchain</i> comparando alguns algoritmos de consenso típicos usados em diferentes cadeias de blocos.

Fonte: Autoria própria (2019).

As obras reunidas no quadro acima trazem discussões que abordam a arquitetura de proteção e consenso existente na *blockchain*, destacando como os dados são registrados, não permitindo que sejam apagados.

Os autores abordam também a rastreabilidade dos dados registrados, outro aspecto destacado como ponto forte de uma rede *blockchain* devido a seus “blocos” ficarem espalhados em diversos computadores distribuídos pelo mundo.

Essa topologia acaba forçando que uma mudança em um registro de informação só ocorra quando aceita por todos os sistemas pertencentes a esta rede.

As informações levantadas nos temas se tornam relevantes para o presente estudo no sentido de elucidar o dimensionamento dos esforços e a compreensão da melhor abordagem de implementação da segurança necessária à arquitetura da solução proposta nessa pesquisa.

2.5 Blockchain Hyperledger

As obras apresentadas dentro desse tópico têm o propósito de apoiar os estudos da distribuição *Hyperledger* que é utilizado na elaboração da arquitetura da solução proposta nesse trabalho.

Do mesmo modo, ampara o aprendizado dos fundamentos do *framework Hyperledger Fabric* usado no desenvolvimento do protótipo que comprova a hipótese do modelo proposto nessa pesquisa.

Os estudos abordam os fundamentos conceituais do *Hyperledger* e suas camadas de arquitetura, os elementos do processo de consenso no *Hyperledger*, e os fundamentos do *framework Hyperledger Fabric* (ANDROULAKI *et al.*, 2018; CACHIN, 2016; LINUX FOUNDATION, 2019; SUKHWANI *et al.*, 2017; SWANSON, 2015).

De acordo a *Linux Foundation* (2019), que atualmente coordena o projeto, o *Hyperledger* é um esforço colaborativo de código aberto criado para promover as tecnologias de *blockchain* de vários setores.

Trata-se de uma colaboração global, que reúne várias empresas de tecnologia no

mundo como a IBM, Intel, Cisco e muitas outras de grande relevância, incluindo líderes em finanças, serviços bancários, *Internet* das Coisas (IoT), cadeias de suprimento, manufatura e tecnologia, e demais (ANDROULAKI *et al.*, 2018; CACHIN, 2016; LINUX FOUNDATION, 2019; SWANSON, 2015).

De acordo os estudos de Cachin (2016), o *Hyperledger* é conhecido como a *Blockchain* para Negócios, pois compreende uma variedade de recursos e tecnologias para desenvolvimento de aplicações para este fim.

Segundo a *Linux Foundation* (2019), sua arquitetura é formada por diversas “camadas” com regras de negócio conforme o **Quadro 7**, a seguir:

Quadro 7 - Camadas da arquitetura do *Hyperledger*

Camada	Função
Consenso	Gerar um acordo sobre o pedido e confirmando a exatidão do conjunto de transações que constituem um bloco.
Contrato Inteligente (<i>smart contract</i>):	Processamento de solicitações de transação e determinar se as transações são válidas executando a lógica de negócios.
Comunicação	Transportar mensagens <i>peer-to-peer</i> (ponto a ponto) entre os nós que participam de uma instância do “livro-razão” compartilhado.
Abstração de armazenamento de dados	Permitir que diferentes armazenamentos de dados sejam usados por outros módulos.
Abstração de criptografia	Permitir que diferentes algoritmos de criptografia ou módulos sejam trocados sem afetar outros módulos.
Serviços de identidade	Estabelecer, de uma raiz de confiança durante a configuração de uma instância <i>blockchain</i> , o registro de identidades ou entidades do sistema durante a operação da rede, e o gerenciamento de alterações, acréscimos e revogações na rede. Além disso, fornece autenticação e autorização.
Serviços de Política	Gerenciar várias políticas especificadas no sistema, como a política de endosso, a de consenso ou a de gerenciamento.
Interface de Programação de Aplicações (API)	Permitir que clientes e aplicativos se comuniquem com a <i>blockchain</i> .
Interoperação	Suportar a interoperabilidade entre diferentes instâncias de <i>blockchain</i> .

Fonte: Elaborado a partir das informações disponibilizadas pelo site oficial da *Linux Foundation* (2019).

As camadas mostradas no quadro acima reúnem os aspectos críticos de uma arquitetura modular que fornece componentes funcionais em camadas, e módulos que padronizam a interface e interoperabilidade entre os componentes, incluindo o consenso para a validação das transações (LINUX FOUNDATION, 2019).

De acordo com Cachin (2016) e Swanson (2015), consenso é o processo pelo qual uma rede de nós fornece um ordenamento garantido de transações e valida o bloco de transações.

Segundo os estudos de Androulaki *et al.* (2018) e de Sukhwani *et al.* (2017), no caso da *blockchain* para criptomoedas, o consenso ocorre pelo processo de “mineração” através do

princípio de *Proof-of-Work* (prova de trabalho).

No *Hyperledger*, por sua vez, o consenso ocorre através de regras introduzidas em algoritmos e políticas de consenso que são executadas por *smart-contracts* durante o processo de validação da transação (ANDROULAKI *et al.*, 2018; SUKHWANI *et al.*, 2017).

De acordo a *Linux Foundation* (2019), para otimizar o processo de desenvolvimento de aplicações o Projeto *Hyperledger* disponibiliza diversos *frameworks*, de modo a proporcionar diferentes mecanismos de consenso na rede bem como várias abordagens de implementação. São eles: *Hyperledger Indy*; *Hyperledger Iroha*; *Hyperledger Sawtooth* e *Hyperledger Fabric*. Cada um deles utiliza algoritmos, políticas e propriedades específicas visando o consenso na rede.

Em conformidade aos objetivos da presente pesquisa, a seguir serão apresentadas as características apenas do *Hyperledger Fabric*, amparado pelos estudos dos autores selecionados.

Segundo os estudos de Cachin (2016), o *framework Hyperledger Fabric* é uma implementação de uma plataforma distribuída para executar contratos inteligentes, alavancando tecnologias conhecidas e comprovadas, com uma arquitetura modular que permite implementações conectáveis de várias funções.

Ainda segundo o mesmo autor, algumas características estão presentes na plataforma:

- Possui um *blockchain* autorizado com finalização imediata;
- Executa *smart-contracts* de forma arbitrária;
- Utiliza protocolo de consenso “plugável”, possibilitando a implementação de outros protocolos de consenso;
- Suporte de segurança por meio de autoridades de certificação (certificado da camada de segurança de transporte – TLS; certificados de registro e transação);
- Estado persistente usando uma interface de armazenamento de valor-chave;
- Possui uma estrutura de eventos que suporta eventos predefinidos e personalizados;
- Possui uma interface de cliente *Node.js*;
- Suporte para Interface de Programação de Aplicações (API) e Interface de Linhas de Comando (CLI)

De acordo a *Linux Foundation* (2019), o consenso no *Hyperledger Fabric* se divide em três fases:

- Endosso – fase em que as transações são endossadas através da verificação das políticas de endosso.

- Solicitação – fase de aceitação das transações endossadas, e as solicitações de gravação no “livro-razão”.
- Validação – fase de aceitação de um bloco de transações ordenadas e validadas pela exatidão dos resultados, incluindo a verificação da política de endosso.

De acordo com os estudos elencados, a plataforma além de código aberto, se baseia em padrões de execução de contratos inteligentes definidos pelo usuário, suportando recursos de segurança e identidade altamente confiáveis, utilizando uma arquitetura modular que possibilita a conexão de protocolos de consenso.

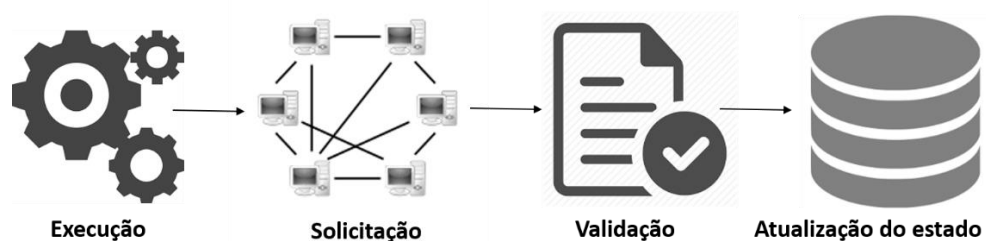
2.6 Modelo de Arquitetura Blockchain de Execução por Ordem de Validação do Hyperledger Fabric

Os estudos de Androulaki (2017) apresentam o Modelo de Arquitetura *Blockchain* de Execução por Ordem de Validação do *Hyperledger Fabric*, que se divide em duas partes:

- Contrato Inteligente (*smart contract*), chamado “*chaincode*”: código do programa que implementa a lógica do aplicativo executado na fase de execução.
- Política de Endosso: “biblioteca” com regras estáticas utilizadas na fase de validação para que a transação seja validada. (Somente administradores designados tem permissão para alterar políticas de endosso, através de sistemas de gerenciamento).

O Modelo é ilustrado pela **Figura 4**, a seguir:

Figura 4 - Modelo de Arquitetura *Blockchain* de Execução por Ordem de Validação do *Hyperledger Fabric*



Fonte: Adaptado de Androulaki *et al.*, (2018, p. 5).

As fases mostradas na **Figura 4** acima, serão discutidas a seguir de acordo com o modelo apresentado nos estudos dos autores.

Na fase de execução ocorre a identificação do “cliente” e o envio da proposta de

transação para que os endossantes da rede possam executar na fase seguinte.

A proposta de transação deve conter a ID (identidade) do “cliente” que está enviando a operação a ser executada, os parâmetros (condições), o identificador do *chaincode* (política de endosso que será utilizada) e um identificador de transação derivado do ID do “cliente”.

A fase de solicitação vem em seguida, quando ocorre a transmissão atômica de endossos na rede, estabelecendo o consenso sobre as transações. Nessa fase, as solicitações são agrupadas em várias transações gerando uma sequência de blocos contendo transações com *hash* encadeada.

O agrupamento ou lote de transações em blocos melhora a taxa de transferência do protocolo de transmissão, que é uma técnica bem conhecida na área de computação usada em transmissões Tolerantes a Falhas Bizantinas (PBFT).

Na sequência, um novo bloco entra na fase de validação, quando o sistema de validação “*chaincode*”, com a política de endosso, é “invocado”. Caso a transação não satisfaça as regras da política, será marcada como “inválida” e será descartada.

Por último, a fase de atualização do “livro-razão” é executada. Nessa fase, caso todas as regras da política de endosso sejam atendidas, o bloco é anexado e o estado da cadeia de blocos é atualizado.

As obras que amparam os fundamentos e modelos estudados do *Hyperledger Fabric* aplicados à arquitetura da solução da presente pesquisa estão reunidas no **Quadro 8**, a seguir.

Quadro 8 - Obras do Tema: Blockchain e Hyperledger

Título da obra	Abordagem	Aplicação
<i>HYPERLEDGER Blockchain Technologies for Business: Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus</i> (LINUX FOUNDATION, 2019)	Artigo técnico de texto dissertativo-informativo que tem como objetivo apresentar aplicações para <i>blockchain</i> corporativo em diferentes setores, descrevendo as estruturas e ferramentas de código aberto da <i>Hyperledger</i> .	Aplicado à área de Computação, mais especificamente à Engenharia de <i>Software</i> , descreve uma arquitetura de referência generalizada para redes de <i>blockchain</i> permissionadas e, através da sua discussão, orienta sobre o desenvolvimento de projetos modulares com base na Arquitetura <i>Hyperledger</i> .
<i>Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains</i> (ANDROULAKI <i>et al.</i> , 2018)	Artigo técnico de texto dissertativo-explicativo que tem como objetivo apresentar e descrever as características funcionais do <i>framework Hyperledger Fabric</i> .	Aplicado à área de Computação, descreve a arquitetura do <i>Hyperledger Fabric</i> , a lógica por trás de várias decisões de <i>design</i> de arquitetura, seus aspectos de implementação mais proeminentes, bem como seu modelo de programação de aplicativos distribuídos.
<i>Architecture of the Hyperledger Blockchain Fabric</i> (CACHIN, 2016)	Artigo técnico de texto dissertativo-explicativo que apresenta um <i>overview</i> da documentação do <i>framework Hyperledger Fabric</i> .	Aplicado à área de Computação, o trabalho discute os padrões de recursos de segurança e identidade da arquitetura modular, e dos protocolos de consenso conectáveis.
<i>Performance Modeling of</i>	Artigo técnico que propõe um	Aplicado à área de Computação, o

Título da obra	Abordagem	Aplicação
<i>PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)</i> (SUKHWANI <i>et al.</i> , 2017)	modelo de Processo de Consenso, baseado no modelo de Tolerância a Falhas Bizantinas (PBFT), para redes permissionadas <i>blockchain Hyperledger Fabric</i> .	artigo apresenta um modelo de confiança de consenso para redes <i>blockchain</i> construídas em <i>Hyperledger Fabric</i> .

Fonte: Autoria própria (2019).

As obras apresentadas no quadro acima reúnem estudos que amparam os resultados da presente pesquisa. Os fundamentos apresentados pelos autores dão suporte aos aspectos técnicos a serem considerados na elaboração de arquiteturas de sistemas baseado em *blockchain*, corroborando com os objetivos dessa pesquisa.

3 ESTADO DA TÉCNICA

O estudo do Estado da Técnica realizado nessa pesquisa tem a finalidade de prospectar e identificar, de forma antecipada, soluções tecnológicas cujo modelo de negócio apresente proposta de registro de atestados médicos ou outras informações relacionadas a registros médicos de pacientes. A finalidade é evitar investigações redundantes e até desnecessárias dentro do avanço do presente estudo.

Os resultados encontrados são demonstrados no **Quadro 9**, a seguir:

Quadro 9 - Estado da Técnica de soluções similares ou periféricas ao presente estudo

Nome da solução	Tipo da Aplicação	Objetivo	Similaridade / Diferenças
Atestados.MED.br	<i>Software</i> comercial para o registro de atestados médicos já emitidos.	O objetivo é assegurar a autenticidade dos documentos médicos para as empresas, e para os profissionais e instituições de saúde. Médicos ou empresas podem licenciá-lo para criar um controle particular dos documentos emitidos ⁷ .	Cadastra atestados em base de dados própria, mas não se propõe a unificar o registro em rede distribuída nacionalmente.
Atestado Médico Digital	<i>Software</i> desenvolvido pela Associação Paulista de Medicina para emissão de atestados médicos digitais, disponível também em versão <i>mobile</i> .	O objetivo é a emissão de atestado médico digital, assegurando a autenticidade dos documentos, evitando falsificações ⁸ .	Cadastra atestados em base de dados própria, mas não se propõe a unificar o registro em rede distribuída nacionalmente. Atende uma iniciativa isolada da Associação Paulista de Medicina
Cartão Prescrição Digital	Cartão Magnético que centraliza o histórico e as informações do paciente, e que poderão ser utilizadas por outros médicos em procedimentos posteriores.	O objetivo é centralizar todo o histórico médico de um paciente em um cartão digital magnético. O próprio paciente será o portador deste cartão ⁹ .	Foca em armazenar informações de prontuário de paciente em cartões magnéticos individuais, sendo os dados centralizados nesse dispositivo. Embora tenha de forma geral o mesmo conceito de registro de informações de pacientes geradas por um médico, não utiliza um modelo descentralizado e distribuído de registro de informações.
Memed	<i>Software</i> comercial, integrado com base de dados de farmácias, para prescrição médica	O objetivo é dar ao médico a possibilidade de registrar, eletronicamente, todo o histórico de prescrições de medicamentos do seu paciente utilizando uma base de dados atualizada	Embora também possua o conceito de armazenamento de dados de pacientes, limita-se a registrar e a gerar um histórico de informações referentes a prescrição de medicamentos.

⁷ Atestados.MED.br. Disponível em: <https://atestados.med.br/>

⁸ Atestado Médico Digital. Associação Paulista de Medicina. Disponível em: <http://www.apm.org.br/atestadodigital>. Acesso em: 15/10/2019.

⁹ CryptoID Portal de Conteúdo de Identificação Digital. Disponível em: <https://cryptoid.com.br/banco-de-noticias/prescricao-digital-uma-revolucao-em-andamento-na-relacao-medico-paciente/>. Acesso em: 15/10/2019.

Nome da solução	Tipo da Aplicação	Objetivo	Similaridade / Diferenças
	digital.	diariamente, com milhares de medicamentos ¹⁰ .	
MEDREC	Plataforma <i>web</i> que fornece ao paciente um registro abrangente e credível do seu histórico médico, utilizando tecnologia <i>blockchain</i> .	O objetivo é registrar, distribuir e compartilhar, através de uma plataforma, as informações do histórico do paciente registrada pelo médico, permitindo a troca de dados iniciada pelo paciente entre jurisdições médicas. ¹¹ .	Possui o mesmo conceito de registro de informações de pacientes de forma descentralizada e distribuída, em rede <i>blockchain</i> , porém com o propósito de compartilhar informações entre jurisdições médicas através do mundo.
FINEP Saúde	CIM- Projeto que propõe a utilização de chaves públicas/privadas, com utilização de <i>smartcards</i> ou <i>tokens</i> em dispositivos (computadores, celulares, <i>tablets</i>), para que médicos possam assinar seus documentos digitalmente.	O objetivo é desenvolver uma estratégia que permita ao médico assinar, eletronicamente e com segurança, e de qualquer lugar, documentos emitidos por eles ¹² .	Assemelha-se apenas na intenção de proporcionar segurança na validação da veracidade de documentos médicos.

Fonte: Autoria própria (2019).

O quadro acima mostra as atuais soluções encontradas que apontam para uma direção similar ou periférica ao presente estudo, e serão discutidas a seguir.

As duas primeiras soluções apresentadas no **Quadro 9**, são *softwares* desenvolvidos em plataforma *web*, destinados a emitir ou registrar atestados médicos (Atestados.MED.br e Atestado Médico Digital).

A primeira solução – Atestados.MED.br – de caráter comercial, atende médicos ou empresas que desejam licenciar o *software* e criar uma rede de administração privada para gerenciar os atestados emitidos ou registrados nela.

Do mesmo modo a solução Atestado Médico Digital, desenvolvida pela Associação de Médicos Paulista, assegura a autenticidade nas emissões evitando falsificações, além de racionalizar custos na gestão da medicina do trabalho e na emissão dos atestados médicos digitais.

Os atestados médicos digitais desta solução estão disponíveis nas opções com ou sem o uso do e-CPF, e versão *móvil*.

As duas soluções, embora sejam isoladas em seus propósitos, apoiam os esforços da

¹⁰ Memed Prescrição Digital. Disponível em: <https://memed.com.br/>. Acesso em: 10/10/2019.

¹¹ MedRec. Disponível em: <http://medrec.io/>. Acesso em: 10/10/2019.

¹² Artigo publicado em Radiologia Brasileira. Dez/2011. DOI: 10.1590/S0100-39842011000600001

presente pesquisa em preencher a lacuna para um modelo de registro unificado em rede *blockchain*, institucionalizado, e de caráter governamental no que se refere ao registro geral de atestados médico-odontológico.

A proposta da solução FINEP CIM-Saúde fornece insumos para o presente estudo no que se refere a meios de identificação do médico, em caso da implementação tecnológica do modelo proposto na presente pesquisa.

As soluções, Cartão Prescrição Digital, Memed e MedRec, embora tenham propostas de funcionamento tecnológico diferentes, têm em comum a proposição de integração de informações, o que favorece os estudos da presente pesquisa.

O MedRec, em particular, apresenta proposta de modelo de registro de prontuário de pacientes utilizando *blockchain*, e ampara a presente pesquisa reforçando a teoria de que informações médicas podem ser registradas utilizando essa tecnologia.

O **Quadro 10** a seguir resume as principais características comparativas entre as soluções apresentadas e o modelo proposto na presente pesquisa.

Quadro 10 - Resumo comparativo das características gerais das soluções e o modelo proposto nesta pesquisa

	Estado da Técnica	Modelo proposto
Modelo de negócio	Comercial/Pesquisa	Público/Governamental
Tipo de iniciativa	Local / específica	Abrangente / Institucionalizada
Tipo de Governança	Privada	Entidade Pública Reguladora
Processo de negócio	Gestão de dados, desde a entrada (digitação/leitura) até a saída (transmissão/visualização/impressão) da informação.	Rastreabilidade de um atestado médico-odontológico, desde a geração do registro até sua utilização.
Proposta tecnológica	Sistemas para armazenamento de informações de pacientes e assinatura digital de documentos.	Rede distribuída <i>blockchain</i> e sistema de interfaceamento e integração, para a unificação de registro e verificação de autenticidade de atestado médico-odontológico, no País.
Funcionamento	Controle e gestão de registros médicos.	Integração e validação de registros em <i>blockchain</i> , de atestados médico-odontológico gerados por <i>softwares</i> clientes.

Fonte: A autoria própria (2019)

Conforme o quadro acima, as soluções apresentadas, embora tenham modelos de negócio com finalidade comercial, corroboram para o objetivo dessa pesquisa, pois as suas propostas tecnológicas estão voltadas para o armazenamento e a gestão segura de informações médicas.

O tipo de iniciativa e o tipo de governança das soluções apresentadas são de cunho privado (Atestados.MED.br; Cartão Prescrição Digital; Memed e MedRec) e/ou demandados por uma iniciativa específica local (Atestado Médico Digital; FINEP CIM-Saúde), enquanto esses aspectos são de cunho abrangente e institucionalizado no caso do modelo proposto nesta pesquisa.

O processo de negócio das soluções apresentadas está voltado à entrada de dados, tratamento, armazenamento e saída de informações através de suas propostas tecnológicas que abrangem sistemas (*softwares*, cartões magnéticos e *tokens*) de gestão de informações de pacientes.

Em comparação, o processo de negócio da proposta da presente pesquisa está modelado para a rastreabilidade de um atestado médico-odontológico, desde a sua geração até a sua utilização.

Este processo poderá ser implementado através da proposta tecnológica que abrange uma rede *blockchain* distribuída, abastecida por dados passados para ela por um sistema de interfaceamento e integração com as demais soluções.

Os aspectos comparativos demonstram primeiramente, um hiato deixado entre as propostas, modelos de funcionamento, iniciativas e demais características do Estado da Técnica se comparados ao objetivo deste estudo.

Em comparação, o modelo de funcionamento proposto na presente pesquisa seria institucionalizado, regulado por autarquia ou entidade governamental, integrando todas as outras soluções tecnológicas apresentadas.

Entretanto, ao mesmo tempo, os modelos de processo e propostas tecnológicas do Estado da Técnica apoiam a presente pesquisa pelos resultados já obtidos em suas soluções, promovendo fonte indireta de estudo.

Esses resultados promovem complementariedade e confirmam o objetivo deste estudo, pois seus esforços estão voltados ao controle e à gestão das informações de pacientes geradas por um médico, proporcionando a saída dos dados que abasteceriam a rede distribuída proposta nessa pesquisa.

4. PROJETO DE INOVAÇÃO TECNOLÓGICA

Esse capítulo apresenta os procedimentos utilizados para alcançar os resultados desse trabalho. Demonstra também os estudos de viabilidade da implementação do projeto, bem como os riscos de sua execução.

Como já destacado na introdução, essa pesquisa objetivou propor um modelo de registro unificado para verificação de autenticidade de atestados médicos-odontológicos em rede *blockchain*, elencando as possibilidades de proteção intelectual e transferência de tecnologia. Para o alcance desse objetivo, de forma específica, foi necessário:

- Elaborar uma modelagem de processos de negócio envolvendo as operações de registro e validação de autenticidade do documento
- Elaborar uma arquitetura prevendo o modelo, as regras de negócio e os casos de uso para que servissem de diretrizes de desenvolvimento de um protótipo para a validação do modelo proposto nessa pesquisa.
- Apresentar um protótipo com base na arquitetura elaborada, visando testar e validar a viabilidade da proposta
- Elencar as possibilidades de proteção intelectual e transferência de tecnologia, avaliando o processo de averbação contratual junto ao INPI.

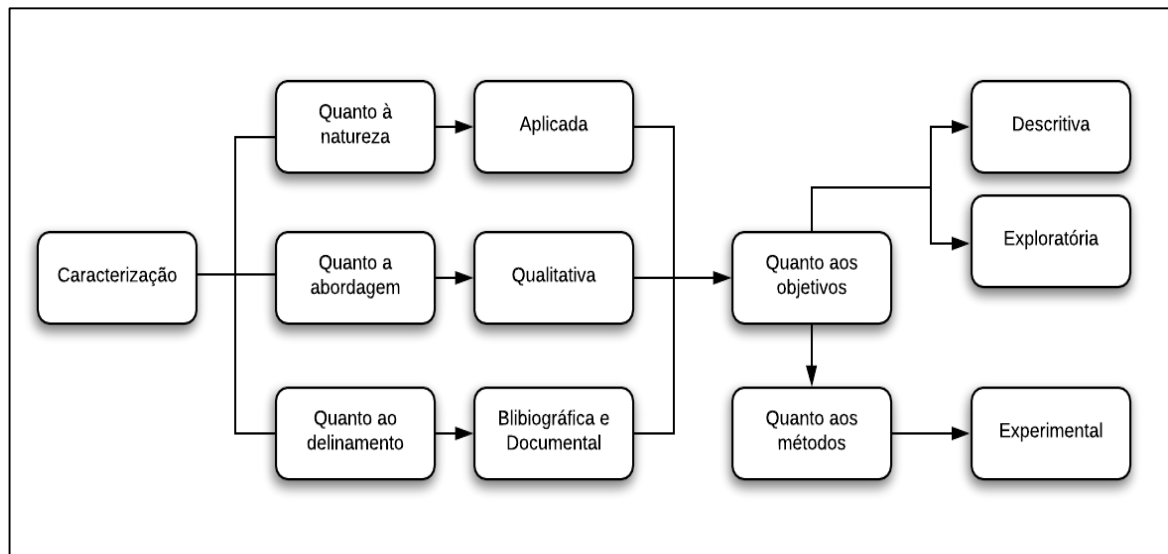
4.1 Métodos

O propósito desse tópico é apresentar a sequência lógica das etapas pelas quais foi possível alcançar os resultados da pesquisa. Os procedimentos dispostos partem da oportunidade do problema percebido de modo a apresentar as estratégias adotadas para o alinhamento do contexto da problemática aos objetivos, e dos procedimentos utilizados para a obtenção dos resultados.

4.1.1 Caracterização da Pesquisa

De acordo Marconi e Lakatos (2010), a caracterização de uma pesquisa varia de acordo a interesses, condições, objetivos, objetos de estudo, dentre outros critérios. Portanto, a presente pesquisa é caracterizada conforme apresentado na **Figura 2**, a seguir:

Figura 5 - Caracterização da pesquisa



Fonte: Autoria própria (2019).

Quanto à sua natureza, a pesquisa é do tipo aplicada, pois os conhecimentos podem ser aplicados efetivamente na vida real com o propósito de solucionar problemas (PRODANOV E FREITAS, 2013).

Quanto aos objetivos, adotou-se os métodos descritivo, para que houvesse o aprofundamento bibliográfico e documental necessário para se evidenciar e fundamentar a proposta desse projeto, e exploratório, para que houvesse o aprimoramento da ideia através de uma maior aproximação e familiaridade com o problema. (GIL, 2010).

Quanto à sua abordagem a pesquisa é do tipo qualitativa, pois os dados coletados e analisados são descritivos e não há preocupação em comprovar hipóteses anteriores utilizando métodos estatísticos. (PRODANOV E FREITAS, 2013).

Dentro dessa abordagem, a pesquisa se dividiu em duas partes: a primeira, consistindo na coleta e análise de informações para obter-se uma leitura real dos fatos do cenário. A segunda, em uma análise subjetiva da problemática visando avaliar os impactos da solução proposta diante dos aspectos socioeconômicos, norteando assim seu ciclo de vida.

Quanto aos métodos, a pesquisa é experimental, uma vez que consistiu na investigação para descobrir novos materiais, métodos, técnicas, protótipos de *software*, e estudos de laboratório (ensaios, modelagem e sistemas).

Quanto ao delineamento, trata-se de uma pesquisa bibliográfica e documental, consistindo no levantamento e coleta de informações em livros, artigos e demais documentos de caráter científico, legislativo, informativo e técnico.

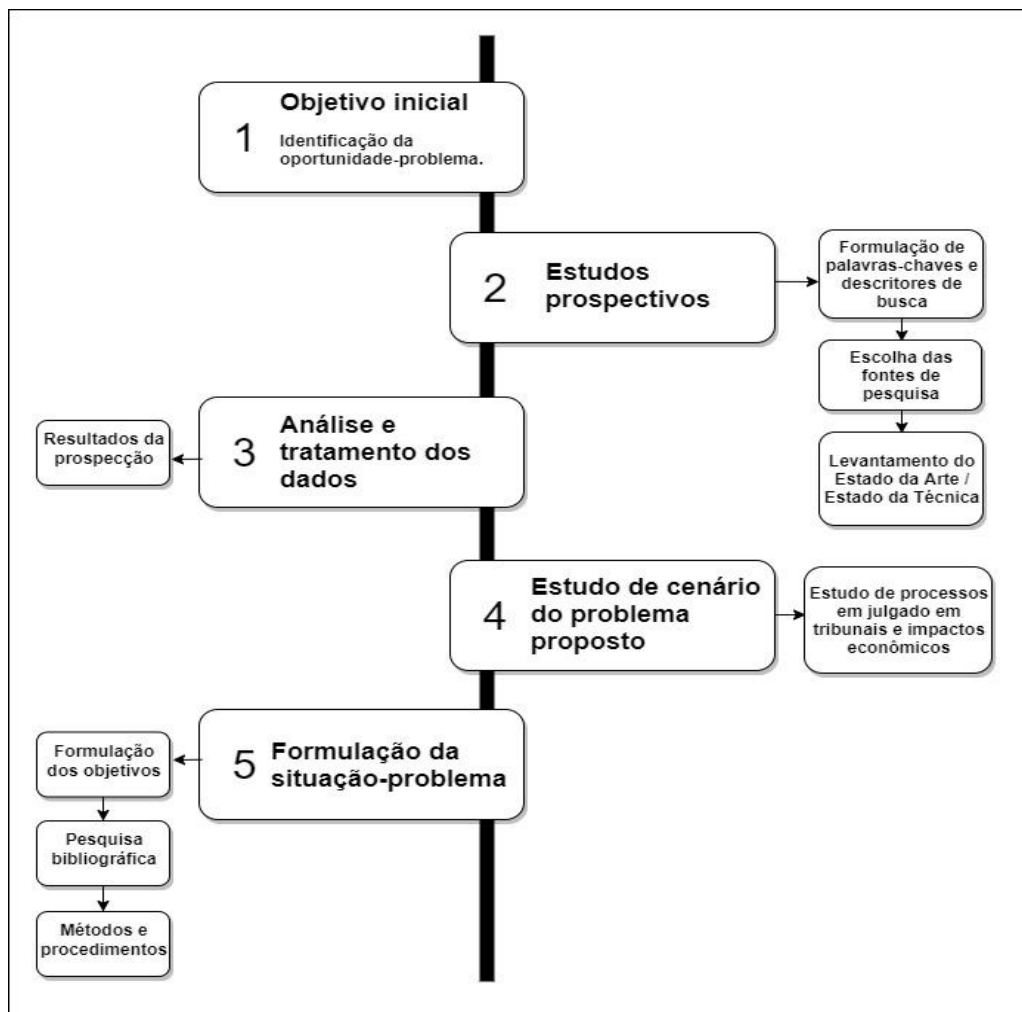
O ponto de partida inicial foram os estudos prospectivos em bases de dados e repositórios científicos para o levantamento dos Estados da Arte e do Estado da Técnica, sendo estas as etapas iniciais para a elaboração da situação-problema proposta.

As obras investigadas que sustentam esse trabalho foram selecionadas em pesquisa realizada em 2018 e 2019, nas bases de dados: Scielo, Periódicos Capes, *Google Scholar*, Base de Teses e Dissertações, Biblioteca Digital Brasileira de Teses e Dissertações, *Scopus* e *IEEE Xplore Digital Library*. O critério utilizado foi a relevância dos temas e dos resultados apresentados, considerando o diálogo que exercem com o tema central dessa pesquisa.

O passo seguinte foi a formulação da situação-problema a partir do estudo dos aspectos do cenário que a envolve, seguido da elaboração dos objetivos que foram desenvolvidos a partir do estudo exploratório baseado na pesquisa bibliográfica.

A **Figura 6**, a seguir, demonstra a sequência adotada no esboço da primeira fase da pesquisa:

Figura 6 - Delineamento da pesquisa - Fase 1

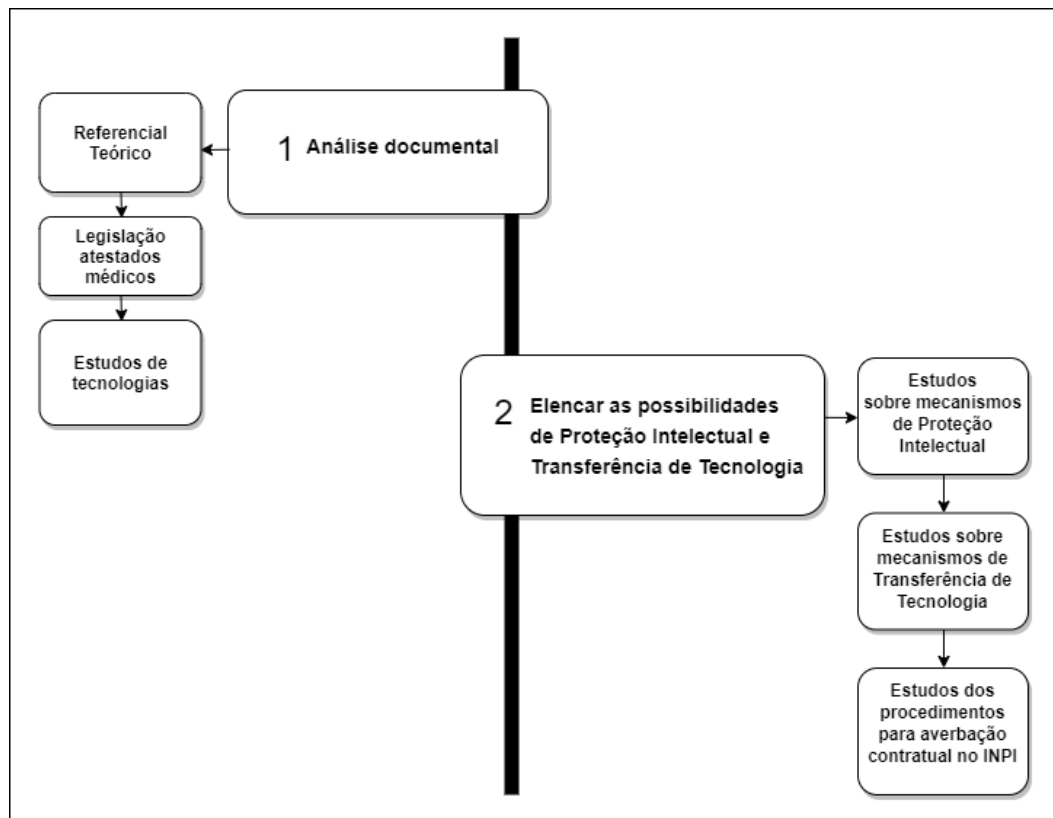


Fonte: Autoria própria (2019).

A sequência apresentada na **Figura 6**, acima, demonstra que elementos gerados por estudos precedentes foram necessários para subsidiar a elaboração da situação-problema da pesquisa dando-lhe amparo para as próximas fases.

A fase seguinte teve a sua elaboração baseada no referencial teórico e na análise documental, conforme mostrado na **Figura 7**, a seguir:

Figura 7 - Delineamento da pesquisa - Fase 2



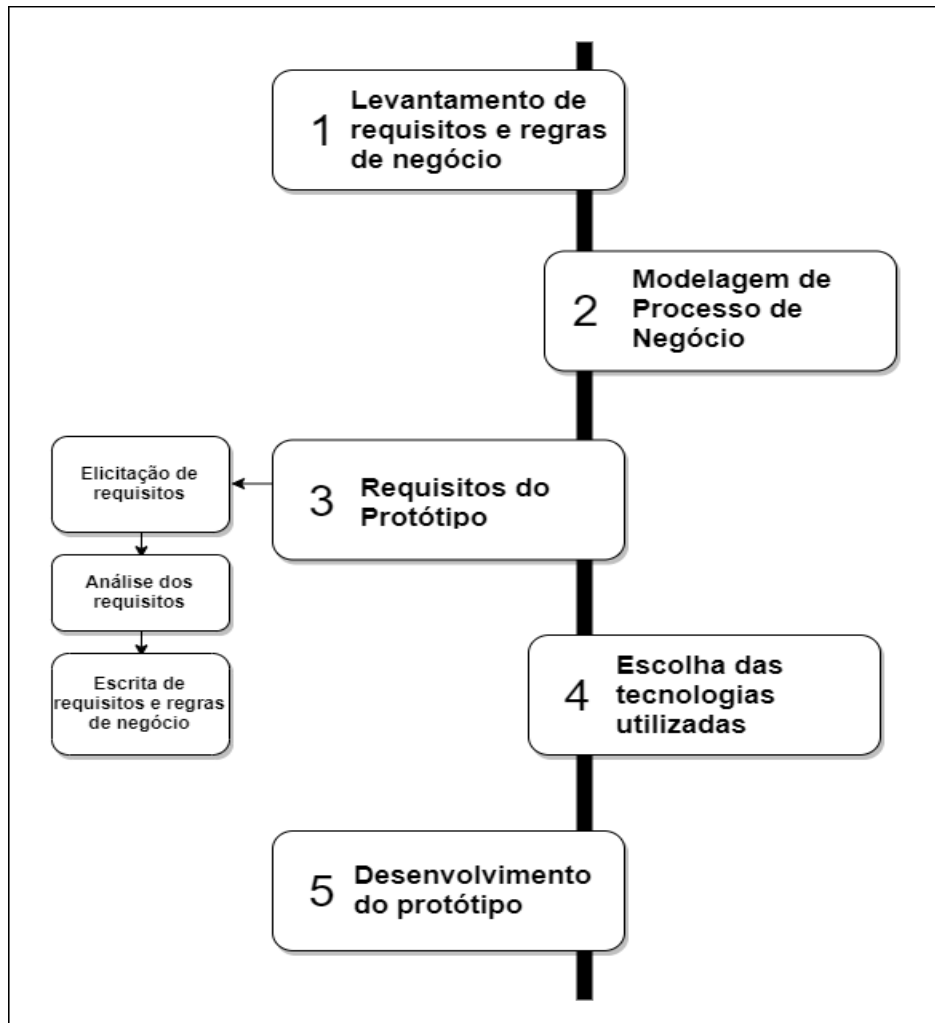
Fonte: Autoria própria (2019).

Segundo a **Figura 7**, acima, os documentos analisados envolveram as regras e legislação para emissão de atestados médicos-odontológicos e estudos das tecnologias envolvidas na elaboração do modelo proposto.

Nessa fase também foram realizados estudos para o levantamento das possibilidades de proteção intelectual e transferência de tecnologia, e os estudos dos procedimentos para averbação contratual junto ao INPI.

A terceira fase da pesquisa se concentrou na construção do modelo proposto nesse trabalho, tendo a sua elaboração baseada a partir da avaliação dos requisitos e regras de negócio necessárias à sua aplicação, seguido do desenvolvimento de um protótipo para a sua validação, conforme apresentado na **Figura 8**, a seguir:

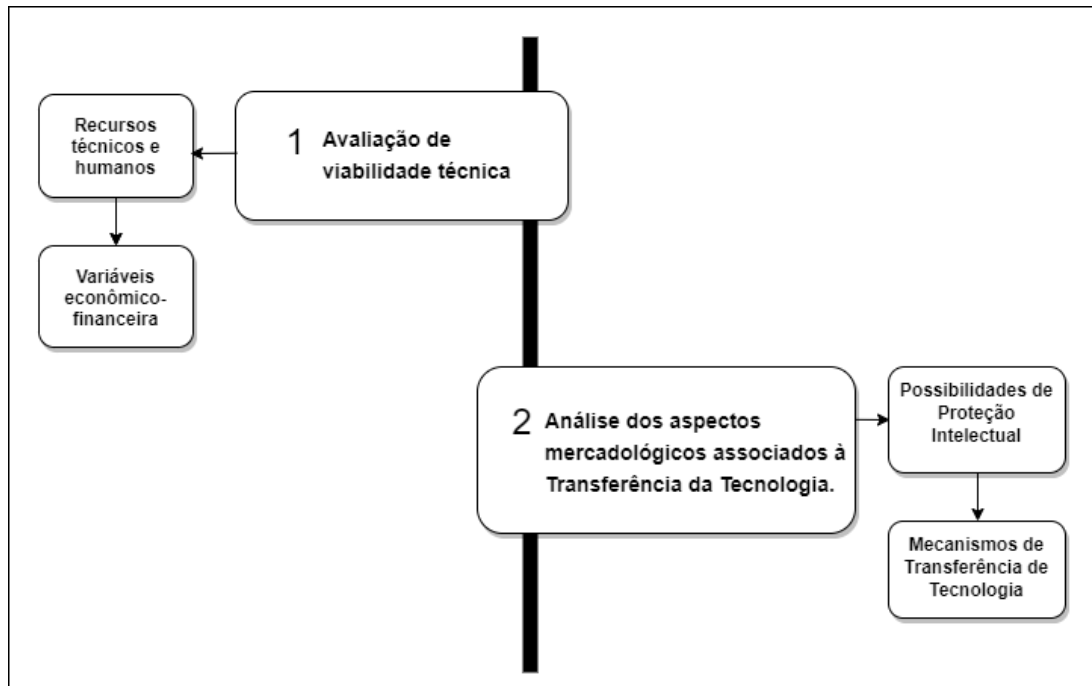
Figura 8 - Delineamento da pesquisa - Fase 3



Fonte: Autoria própria (2019).

Além da etapa de elaboração de levantamento de requisitos e regras de negócio necessárias ao modelo proposto, a **Figura 8** (acima) demonstra os passos que se seguiram após essa etapa, consistindo na elicitacão, análise e escrita de requisitos e regras de negócio para o protótipo; escolha da linguagem de programação e demais tecnologias e, finalmente, o desenvolvimento do protótipo.

A quarta e última fase da pesquisa foi destinada à análise de variáveis associadas à viabilidade do projeto, conforme a **Figura 9**, a seguir:

Figura 9 - Delineamento da pesquisa - Fase 4

Fonte: Autoria própria (2019).

De acordo com a **Figura 9** (acima) foram avaliados os recursos técnicos que compreendem a infraestrutura e ferramentas tecnológicas necessárias ao desenvolvimento da solução tecnológica, e os recursos humanos que compreendem as especialidades dos possíveis integrantes da equipe técnica.

A segunda etapa dessa fase analisou os aspectos mercadológicos associados à Transferência de Tecnologia (TT) avaliando as possibilidades de proteção da produção intelectual por registro de *software*, e através de patente de invenção implementada por programa de computador.

Também foram analisados, nessa etapa, os mecanismos de Transferência de Tecnologia (TT) previstos em lei que possibilitem a transferência do produto dessa pesquisa ao mercado produtivo.

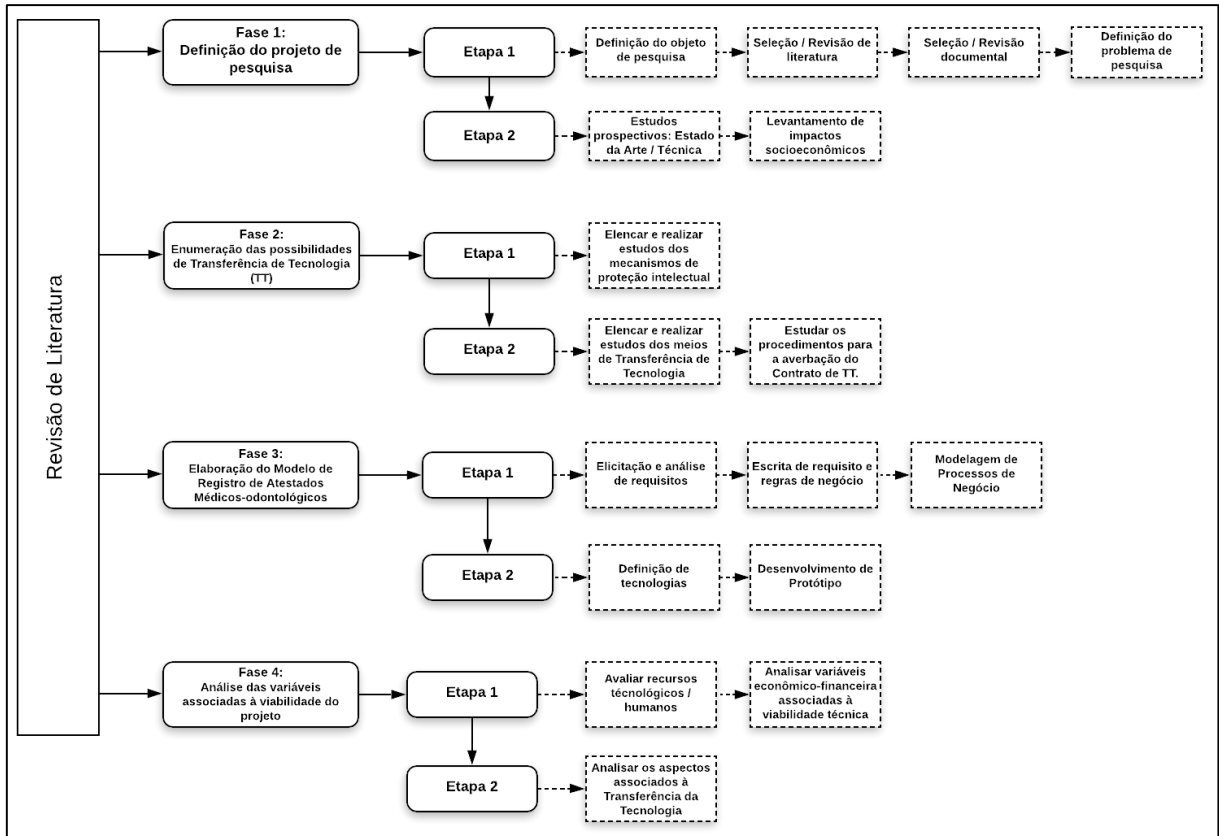
Para uma melhor compreensão das fases do delineamento e suas etapas, os procedimentos da pesquisa estão detalhados a seguir.

4.1.2 Etapas e Procedimentos da Pesquisa

Para se chegar à proposta desse trabalho, foi necessário estruturar a pesquisa em ações que permitiram, no decorrer do tempo, uma maior aproximação com o conhecimento requerido para a sua elaboração.

A **Figura 10**, abaixo, apresenta essas ações dentro do percurso metodológico seguido para a obtenção dos resultados.

Figura 10 - Percurso metodológico



Fonte: Autoria própria (2019).

Como demonstrado na **Figura 10**, didaticamente, as ações são apresentadas em quatro fases específicas com suas respectivas etapas: Fase 1 – Definição do projeto de pesquisa; Fase 2 – Enumeração das possibilidades de Transferência de Tecnologia; Fase 3 – Elaboração do Modelo de Registro de Atestados Médicos-odontológicos; e Fase 4 – Análise das variáveis associadas à viabilidade do projeto. A seguir, o detalhamento de cada fase:

1) Fase 1 – Definição do Projeto de Pesquisa

O propósito da primeira fase foi estabelecer uma maior aproximação com a situação-problema de modo a definir o objeto do projeto de pesquisa, conforme mostrado no **Quadro 11**, a seguir:

Quadro 11 - Etapas e atividade metodológicas da Fase 1

FASE 1 Definição do Projeto de Pesquisa	ETAPAS	ATIVIDADES METODOLÓGICAS
	1. Definição do Objeto de Pesquisa	a) Revisão de literatura e análise documental; b) Definição do problema.
2. Obtenção de informações através de estudos prospectivos – levantamento do Estado da Arte e da Técnica, e impactos socioeconômicos.	a) Prospecção junto a bases de dados, INPI, e levantamento documental (técnico/legal); b) Estudos dos impactos socioeconômicos sobre as fraudes do documento.	

Fonte: Autoria própria (2019).

a) Etapa 1/Fase 1: Definição do Objeto de Pesquisa

A revisão de literatura e a definição do problema foram atividades metodológicas que demandaram uma maior atenção para chegar ao conhecimento do objeto da pesquisa.

Por ser ainda incipiente, o número ainda pequeno de publicações de cunho científico sobre a tecnologia *blockchain* em comparação a outros temas, tornou-se um desafio a ser superado para a fundamentação teórica desse trabalho, sendo também necessário analisar documentos e obras de cunho técnico para se chegar à sua completude.

Para tanto, inicialmente, foi realizado o levantamento de fontes teóricas para fundamentar os conceitos desenvolvidos no tema, consistindo em: levantamento bibliográfico preliminar de acordo ao tema; busca das fontes; leitura do material; fichamento; organização lógica do assunto.

Essa etapa teve também o propósito de levantar o Estado da Arte de modo a identificar as obras basilares publicadas com maior aproximação do tema proposto. A finalidade foi procurar fontes que aumentassem a relevância dos esforços em descobrir conceitos e juízos de valores já manifestados. Desta forma, os resultados e as conclusões de outros autores passaram a apoiar o direcionamento da pesquisa, confirmando as suas conclusões.

Na revisão de literatura foram utilizadas fontes teóricas diversas, oriundas de fontes nacionais e internacionais, de informação específica ou mais genérica sobre o tema, escrita e qualificadamente publicada.

Na análise documental, houve a consulta de documentos e informativos que ainda não foram elaborados, escritos ou não, mas que serviram para a pesquisa, assim como a legislação vigente que regula as atividades de Transferência de Tecnologia (TT) e a averbação de contratos de TT.

Um estudo sobre os atos regulatórios e implicações legais quanto à emissão de

atestados médicos junto ao Conselho Federal de Medicina e órgãos responsáveis foi também realizado com a finalidade da maior elucidação e aproximação com o objeto da pesquisa.

O passo seguinte foi realizar um levantamento de fontes técnicas que proporcionaram estudos comparativos sobre a evolução da tecnologia *blockchain* e a sua aplicabilidade dentro e fora do contexto das moedas digitais. Para isso, foram consultados livros e artigos de cunho técnico, e *sites web* de conteúdo específico.

Para a definição do problema foi necessário delimitar o tema em torno dos relevantes impactos socioeconômicos causados pela prática da falsificação de atestados médicos-odontológicos, devido à fragilidade de registro, autenticidade e rastreabilidade do documento.

Embora a solução final desse trabalho, hipoteticamente, possa atender a um universo maior quanto ao registro e à autenticidade de documentos médicos, o “recorte” se tornou, nesse estudo, o fator orientador para o desenvolvimento da problemática.

Para criar um maior embasamento no percurso do desenvolvimento do problema, um estudo foi realizado para levantar o número de processos criminais, e trabalhistas em diversas dimensões processuais, e em variadas instâncias jurídicas, visando tornar relevante a proposta que responde ao problema dessa pesquisa.

Esse estudo teve como fonte de coleta de dados a base de dados JUSBRASIL, e utilizou-se das expressões de busca para a aplicação de filtros de pesquisa: “atestados médicos falsos”; “atestados médicos falsificados”, e “falsificação de atestados médicos”.

Em adição às expressões de busca foi utilizado o período entre os anos de 2016 e 2018, e a seleção da instância jurídica desejada (Diários Oficiais, Diários de Justiça, Tribunais Regionais do Trabalho, Tribunais Regionais Federais e Supremo Tribunal Federal).

Os dados foram tabulados e tratados no *software Microsoft® Excel®*, sendo os gráficos gerados a partir dele.

b) Etapa 2/Fase 1: Obtenção de informações prévias através de estudos prospectivos

O propósito dessa etapa foi identificar o Estado da Técnica, elencando soluções tecnológicas já desenvolvidas, sob proteção de propriedade intelectual ou não, no intuito de averiguar a novidade do modelo proposto nesse estudo.

Nessa atividade foram realizados estudos de prospecção tecnológica em bases de dados *online* e mecanismos de busca na *internet*. As buscas iniciais foram realizadas entre os meses de agosto e setembro de 2018, tendo a sua revisão entre os meses de abril e maio, e também entre os meses de julho e agosto de 2019.

As fontes de base de dados utilizadas foram: Base gratuita de patentes e registro de *software* do INPI; Base de dados gratuita ESPACENET e PUBMED; Base de dados licenciada Questel ORBIT^(TM), esta última com acesso cedido através do Instituto Federal de Ciência e Tecnologia do Estado da Bahia – IFBA.

Para o levantamento dos dados foi elaborada uma estratégia de pesquisa que teve como base a formulação de palavras-chaves e descritores de busca. Os idiomas utilizados foram o português e o inglês, conforme o **Quadro 12**, a seguir.

Quadro 12 - Palavras-chaves e descritores utilizados em estratégias de busca

Palavras-chaves	Descritores de busca
Idioma: Português	
atestados médicos <i>online</i>	documentos médicos
atestados médicos <i>blockchain</i>	atestados médicos
atestados <i>blockchain</i>	emissão de atestados médicos
sistema atestado médico	atestados médicos automação
software atestado médico	atestados médicos regras
	atestados médicos <i>online</i>
Idioma: Inglês	
<i>online medical certificate</i>	
<i>medical certificate blockchain</i>	
<i>medical certificate system</i>	
<i>software medical certificate</i>	

Fonte: Autoria própria (2019).

Os operadores lógicos AND, OR, e NOT foram utilizados em todas as combinações das palavras-chaves mostradas no **Quadro 12**, acima, no intuito de tornar o resultado da pesquisa ainda mais amplo e mais preciso. Os resultados dessa atividade são mostrados na seção Estado da Técnica na primeira parte desse trabalho.

A atividade de estudos dos impactos socioeconômicos sobre as fraudes dos documentos teve como propósito realizar um levantamento dos impactos e prejuízos decorrentes da falsificação de atestados médicos. A intenção foi entender as motivações para a realização da pesquisa, ter uma maior aproximação com o problema estudado, e a elaboração do modelo proposto nesse estudo.

A finalidade foi enumerar e avaliar uma amostra de processos em julgado em tribunais de justiça, em diversas instâncias entre os anos de 2016 a 2018, oriundos de variadas decorrências da prática examinando o conteúdo, a origem e o estado atual do processo e a sentença deferida.

Além dessas fontes, foram também observadas diversas matérias em portais de notícias, com relatos de prejuízos instaurados em diversos contextos, apoiando a percepção

dos impactos socioeconômicos em outras instâncias.

O levantamento foi realizado através de mecanismos de busca na *internet*, em Diários Oficiais, em base de dados de Tribunais Regionais e Superior do Trabalho; Tribunal Regional Federal por Região; Supremo Tribunal Federal; e a base de dados de processos em julgado – JUSBRASIL.

As pesquisas ocorreram no período de agosto a setembro de 2018, tendo a sua revisão nos períodos de março a maio de 2019, utilizando-se de descritores de busca e palavras-chaves, conforme mostrados no **Quadro 13** a seguir:

Quadro 13 - Descritores e palavras-chaves dos impactos socioeconômicos utilizadas nos motores de busca

Descritores	Palavras-chaves
Atestado médico	prejuízos atestado médico falso
Falsidade atestado médico	prejuízos falsidade atestado médico
Atestado médico falso	consequências atestado médico falso
	consequências falsidade atestado médico
	impactos atestados médicos falsos
	Impactos falsidade atestado médico

Fonte: Autoria própria (2019).

2) Fase 2 – Enumeração das Possibilidades de Transferência da Tecnologia (TT)

A segunda fase do percurso metodológico compreende a aproximação com o eixo central da linha de pesquisa abordada nesse estudo – Transferência de Tecnologia – de modo a elaborar as proposições para a transferência da solução tecnológica desenvolvida em resposta ao problema dessa pesquisa, conforme o **Quadro 14**, a seguir:

Quadro 14 - Etapas e atividades metodológicas da segunda fase da pesquisa

FASE 2 Enumeração das possibilidades de TT	ETAPAS	ATIVIDADES METODOLÓGICAS
	1. Elencar e realizar estudos dos mecanismos de proteção intelectual.	a) Estudos sobre proteção por patente de invenção implementada por <i>software</i> ; b) Estudos sobre proteção por registro de <i>software</i> .
2. Elencar e realizar estudos dos meios de transferência de tecnologia.	a) Estudos das possibilidades contratuais e normas para a TT, e dos procedimentos para a averbação contratual junto ao INPI.	

Fonte: Autoria própria (2019).

A legislação utilizada nas atividades metodológicas da Fase 2 foi: Lei da Propriedade Industrial (Lei nº 9.279/96); Lei do *Software* (Lei nº 9.609/98); Lei de Direito Autoral (Lei nº

9.610/98); Lei da Inovação (Lei nº 10.973/04); Decreto nº. 5.563/05; Decreto nº 9.283/18; Instrução Normativa nº 031/2013; Resolução INPI/PR nº 158/2016; Resolução nº 170/2016; Resolução nº 199/2017; Instrução Normativa nº 70/2017; Instrução Normativa INPI/PR nº 099/2019.

A finalidade das etapas dessa fase foi elencar os mecanismos possíveis, previstos na atual legislação em vigor referente aos Direitos de Propriedade Intelectual para a devida proteção da solução proposta nesse estudo.

Para tanto, foram necessários estudos sistemáticos da legislação correspondente, com maior enfoque na proteção por patente de invenção implementada por programa de computador, e na proteção por registro de *software*.

Do mesmo modo, os estudos deram enfoque à avaliação das possibilidades para a Transferência da Tecnologia (TT) e os mecanismos para a averbação do instrumento contratual junto ao INPI.

Os resultados referentes a essas atividades metodológicas são apresentados na análise dos aspectos mercadológicos, associados à transferência da proposta, no tópico 4.4 - Análise de Variáveis Associadas à Viabilidade do Projeto, e no capítulo de resultados e discussões desse trabalho.

3) Fase 3 – Elaboração do Modelo de Registro de Atestados Médicos-odontológicos

A terceira fase do percurso metodológico compreende a elaboração e validação do modelo de registro de atestados médicos-odontológicos, com base em arquitetura *blockchain*, conforme mostrado no **Quadro 15**, a seguir.

Quadro 15 - Etapas e atividades metodológicas da terceira fase da pesquisa

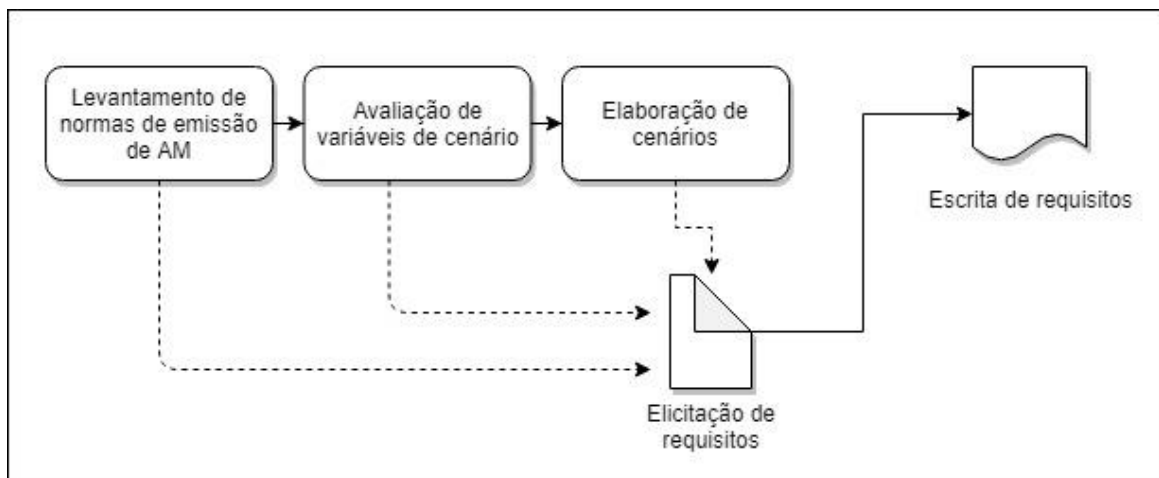
	ETAPAS	ATIVIDADES METODOLÓGICAS
FASE 3 Elaboração do modelo de Registro de Atestados Médicos-odontológicos	1. Elaboração do Modelo de Registro de atestados, com base em arquitetura <i>blockchain</i> .	a) Levantamento de requisitos e regras de negócio; b) Modelagem dos fluxos de processo de negócio.
	2. Desenvolvimento de um protótipo.	a) Elicitação, análise e escrita de requisitos, regras de negócio e diagramas de caso de uso; b) Seleção de tecnologias para o desenvolvimento do protótipo.

Fonte: Autoria própria (2019).

a) Etapa 1 da Fase 3 – Elaboração do Modelo de Registro de atestados, com base em arquitetura *blockchain*

A finalidade dessa etapa foi compor os requisitos que fazem parte do modelo proposto. Para tanto, foi necessário realizar um estudo preliminar para obter-se a primeira visão do modelo, alcançada através dos seguintes passos:

Figura 11 - Passos para a obtenção da primeira visão do modelo



Fonte: Autoria própria (2019).

O levantamento das normas de emissão de atestados médicos se deu pelo meio da avaliação da Resolução CFM nº 1.658/2002 e a Resolução CFM nº 1.851/2008 do Conselho Federal de Medicina, visando identificar os parâmetros e pré-requisitos obrigatórios que envolvem o fluxo da emissão do documento.

A avaliação das variáveis teve como objetivo prever as possibilidades não controladas que podem ocorrer no cenário que envolve a emissão do documento (quando o documento é emitido por outro “ator” e assinado posteriormente pelo médico, por exemplo).

A elaboração de cenários se deu com a construção de diferentes fluxos dentro do processo prático que envolve a emissão do documento, visando identificar a forma mais otimizada e segura do procedimento de emissão e possíveis gargalos.

O passo seguinte foi a especificação do fluxo lógico utilizando a modelagem de processos de negócios (BPM), metodologia utilizada para a elaboração das operações que envolvem os atores que interagem com o modelo (demonstrada no tópico 5.1 Modelagem dos Fluxos de Processo de Negócio do Modelo Proposto).

b) Etapa 2 da Fase 3: Desenvolvimento de um sistema protótipo

A atividade inicial dessa etapa foi a escrita das regras de negócio e dos requisitos funcionais que compõe o protótipo, além da seleção das tecnologias para o seu desenvolvimento.

Os requisitos foram escritos utilizando o método “história de usuário” que visa detectar “quem”, “o quê” e “o porquê” de um requisito, obtendo principalmente o que o “usuário” deseja ou necessita fazer. A finalidade da utilização desse método foi definir o escopo do protótipo a ser desenvolvido.

Além disso, para auxiliar essa atividade, foram elaborados diagramas de casos de uso para descrever a sequência de eventos que os “atores”, relacionados ao protótipo, fazem para completar o processo.

A apresentação dessas histórias foi realizada através de representações gráficas que mostram legivelmente o percurso de cada regra de negócio implementada no protótipo, dispostas nos resultados desse estudo.

Em seguida, iniciou-se o estudo para a escolha da plataforma *blockchain* utilizada como base arquitetural para o protótipo. Inicialmente, foram analisadas as plataformas privadas: *Ethereum*, R3 Corda e *Hyperledger Fabric*, avaliando as características que poderiam melhor apoiar o desenvolvimento do protótipo proposto.

Foi selecionada a plataforma *Hyperledger Fabric* devido aos fundamentos de sua arquitetura utilizados na elaboração do modelo desse estudo e aos aspectos técnicos que a envolve. Os itens avaliados e que justificaram a escolha foram:

- a) Modelo de execução por ordem de validação: utiliza protocolos que descentralizam a validação dos dados baseada na “aprovação” final mediante regras de consenso estabelecidas previamente pelos participantes da rede;
- b) A segurança da informação inserida na cadeia de blocos é combinada com a informação do bloco anterior, tornando a falsificação dos dados praticamente impossível;
- c) Nenhum custo de licenciamento envolvido.

O desenvolvimento do protótipo implementado com base no modelo de registro proposto utilizou as seguintes ferramentas e tecnologias:

Hyperledger Fabric: plataforma para *blockchains* permissionadas que executa aplicativos distribuídos escritos em linguagens de programação geral (por exemplo: Go, Java, *Node.js*).

Node.js: interpretador de código *JavaScript* com código aberto focado em migrar o *Javascript* do lado do cliente para servidores, utilizado para a criação do *node* (nó) da rede *blockchain*.

Visual Studio Code: editor de código-fonte desenvolvido pela *Microsoft*® para *Windows*®, *Linux* e *macOS*®, utilizado como a IDE (Ambiente Integral de Desenvolvimento) do desenvolvimento.

Yeoman: ferramenta de *software* de código aberto para aplicativos da *web*, utilizada como uma interface de linha de comando escrito para *Node.js* combinando em um só lugar, as seguintes funções: geração de um modelo de entrada; gerenciamento de dependências; execução dos testes de unidade proporcionando um servidor de desenvolvimento local, e otimizando o código de produção para implantação.

Docker: plataforma de código aberto escrito em *Go* (linguagem de programação de alto desempenho desenvolvida pela *Google*), utilizada para facilitar a criação e administração de ambientes virtualizados.

Git: sistema de controle de versões distribuído, utilizado para o controle de versionamento de *software*.

Oauth2.0: protocolo de autorização para API's *web* (Interface de Programação de Aplicativos), utilizado para permitir que a aplicação cliente acesse o ambiente *web*.

Mongodb: *software* de banco de dados orientado a documentos livres, de código aberto e multiplataforma.

Hyperledger Fabric Development: *framework* de estrutura de código aberto para redes de negócios permissionadas.

4) Fase 4 – Análise das variáveis associadas à viabilidade do projeto

A quarta fase do percurso metodológico compreende analisar as variáveis mais elementares necessárias à execução técnica do projeto.

Essa fase teve o suporte dos elementos elencados nas fases anteriores para a sua completude, conforme o **Quadro 16**, a seguir:

Quadro 16 - Etapas e atividades metodológicas da quarta fase da pesquisa

FASE 4 Análise de variáveis da viabilidade técnica	ETAPAS	ATIVIDADES METODOLÓGICAS
	1. Avaliação da viabilidade técnica.	a) Avaliar os recursos, técnicos e humanos elementares, necessários à viabilidade do projeto; b) Analisar as variáveis econômico-financeiras associadas à viabilidade técnica.
2. Avaliação dos aspectos mercadológicos associados à Transferência da Tecnologia (TT).	a) Analisar os mecanismos legais, elencados na Fase 2, para a proteção da criação e a transferência da tecnologia ao mercado produtivo.	

Fonte: Autoria própria (2019).

A finalidade das etapas dessa fase foi realizar a avaliação da viabilidade técnica do projeto; analisar as variáveis econômico-financeiras associadas à viabilidade técnica; e avaliar os aspectos associados à viabilidade de proteção intelectual e Transferência da Tecnologia (TT). Para isso, como parâmetro, foi necessário tomar como base os recursos utilizados no desenvolvimento do sistema protótipo para as avaliações e análises.

a) Etapa 1 da Fase 4: Avaliação da viabilidade técnica

A finalidade dessa etapa foi elencar os recursos, técnicos e humanos, elementares ao desenvolvimento e funcionamento da solução tecnológica, e estimar os custos envolvidos associados a essas variáveis.

As tecnologias essenciais recomendadas e os sistemas e serviços necessários ao funcionamento das máquinas foram selecionadas pelo critério de serem ferramentas de código aberto, sem custo, seguras, de alto desempenho e satisfatória disseminação de conhecimento.

A escolha da infraestrutura recomendada tomou como base a configuração intermediária de computadores, atualmente no mercado, e que pudessem ter poder computacional necessário às atividades de programação.

Em termos de recursos que demandam custos, as estimativas se basearam em valores de serviço de servidor em nuvem, e o dimensionamento da equipe técnica necessária ao desenvolvimento e manutenção da solução.

A equipe técnica necessária ao desenvolvimento e manutenção da solução foi elencada tomando como base o modelo proposto, a arquitetura de requisitos por Casos de Uso, as regras de negócio projetadas para o sistema protótipo, a manutenibilidade posterior (caso supostamente houvesse), e as recomendações do Projeto *Hyperledger* da *Linux Foundation*.

Para o dimensionamento dos custos com a equipe técnica do projeto foram tomados:

- Média salarial de um Programador de Computador em uma jornada de trabalho de 42 horas semanais, informada pelo Cadastro Geral de Empregados e Desempregados (CAGED) do Ministério do Trabalho no exercício de 2019: **R\$ 3.812,78.**
- Valor do Fundo de Garantia por Tempo de Serviço (FGTS), calculado pela alíquota de 8%, (Fonte: Caixa Econômica Federal), sobre esse salário: $R\$ 3.812,78 \times 0,08 = \mathbf{R\$ 305,02.}$
- Um terço de férias: $R\$ 3.812,78 / 3 = \mathbf{R\$ R\$1.270,93.}$
- Período base: **12 meses.**
- Valor do 13º Salário, obtido pelo incremento de mais 01 mês, ao do período base.

O Custo total de salários é calculado pela seguinte fórmula:

$$Ts = ((P+1) \times S) \times n$$

Onde:

Ts = Total de salários ao ano.

P = Período.

S = Salário base.

n = Número de integrantes da equipe técnica.

O custo total com FGTS é calculado pela formula a seguir:

$$Tf = ((P+1) \times (S \times i) \times n)$$

Onde:

Tf = Total de FGTS ao ano.

P = Período.

S = Salário base.

i = Alíquota de FGTS.

n = Número de integrantes da equipe técnica.

O custo total com 1/3 de férias é calculado pela seguinte fórmula:

$$F = \left(\frac{S}{3}\right) \times n$$

Onde:

F = Total de 1/3 de Férias.

S = Salário base.

n = Número de integrantes da equipe técnica.

Para o dimensionamento dos custos com servidor, primeiramente elegeu-se um serviço de servidor em nuvem para a cotação dos valores.

O critério da escolha foi a confiabilidade e a possibilidade de contratar processamento e armazenamento sob demanda, baseada em horas.

Diante disso, o servidor *Amazon® Web Service (AWS)* foi selecionado por dispor desse recurso, possuindo também uma ferramenta que auxilia o dimensionamento de demanda *versus* recursos de processamento e armazenamento disponibilizados em seu site, reforçando a escolha desse servidor.

Os Custos estimados com servidor levaram em consideração:

- Valor hora de um servidor *Amazon®* de 04 núcleos, com processamento sob demanda e sistema operacional *Linux*: **R\$ 0,8452 / hora.**
- Valor hora de uma Aplicação de balanceamento de carga: **R\$ 0,0956 / hora.**
- Total de horas no período de um ano: 24h x 30 dias x 12 meses = **8.640 horas.**

Os cálculos são baseados na seguinte fórmula:

$$Tps = ((hS + hA) \times h)$$

Onde:

Tps = Total de custos com recursos de processamento de servidor.

hS = Valor hora Servidor sob demanda.

hA = Valor hora Aplicação de balanceamento de carga.

h = Total de horas no período.

A partir desses primeiros resultados, realizaram-se as projeções estimadas dos custos associados à viabilidade técnica, tendo como base o crescimento da adesão dos médicos e cirurgiões-dentistas à solução, de modo a estimar a escalabilidade dos custos com servidor e equipe técnica.

Para tanto foram adotados os seguintes fatores e variáveis de crescimento:

a) A indicação do número de atendimentos realizados por um médico, por turno de quatro horas que, segundo o Artigo 2º da Resolução CREMERS nº 007/2011, é no máximo **14 (quatorze)** pacientes.

Adotou-se esse número como uma constante do quantitativo de atestados emitidos ao dia, por não haver um número regulamentado como limite para a emissão de atestados dentro de um período.

b) Dias úteis no ano de 2019 = **255 dias**.

c) O tamanho de **500 (quinhentos) Bytes**, em medida computacional, de um atestado em formato de arquivo texto (tamanho estimado a partir do protótipo);

d) A população total de médicos e cirurgiões-dentistas em atividade no país até o momento desse estudo (resultado do somatório das principais inscrições ativas em todas as Unidades da Federação): **805.273 (oitocentos e cinco mil, duzentos e setenta e três)**, sendo **477.022** médicos¹³, e **328.251** cirurgiões-dentistas¹⁴.

e) Quatro diferentes amostras do número total da população de profissionais;

f) Quantidade estimada de atestados emitidos por cada amostra;

g) Período base: **12 meses**.

As amostras obtidas do total da população de Médicos e Cirurgiões-dentistas foram extraídas em quatro partes iguais, através do método estatístico - **Quartil**, com cada amostra representando 1/4 da população.

Os quartis ficaram assim representados:

- Primeiro quartil (designado por $Q_{1/4}$) = **201.318** (25% da amostra);
- Segundo quartil (designado por $Q_{2/4}$) = **402.637** (50% da amostra);
- Terceiro quartil (designado por $Q_{3/4}$) = **603.955** (75% da amostra).

O número estimado da quantidade de atestados emitidos por amostra de profissionais, dentro do período base, foi obtido dentro das projeções, pela fórmula a seguir:

$$Ta = ((14 \times dU) \times n)$$

Onde:

Ta = Total de atestados emitidos no período de 12 meses.

dU = Número de dias úteis.

n = Número da amostra do Quartil.

¹³ Fonte: Conselho Federal de Medicina.

Disponível em: http://portal.cfm.org.br/?option=com_estatistica. Acesso em 30/11/2019.

¹⁴ Fonte: Conselho Federal de Odontologia. Disponível em: <http://cfo.org.br/website/estatisticas/quantidade-geral-de-entidades-e-profissionais-ativos/>. Acesso em 30/11/ 2019.

A fórmula acima foi utilizada em todas as projeções para estimar o número de atestados emitidos por cada amostra dentro dos 255 dias úteis do período base.

Os totais de atestados obtidos pela fórmula acima foram considerados para o dimensionamento do consumo de armazenamento e armazenamento adicional para *backup* no servidor. As estimativas dos custos totais com armazenamento levaram em consideração o Valor Unitário por Medida de Consumo (VMC), cotados no servidor:

- Valor de 1 *Gigabyte*/mês de armazenamento: **R\$ 0,4247.**
- Valor de 1 *Gigabyte* de armazenamento adicional para *backup*: **R\$ 0,4035.**

Os totais de consumo utilizados no armazenamento são determinados pela relação de medida computacional *Gigabyte* que, segundo os prefixos do Sistema Internacional de Unidades do INMETRO (2006), equivalem a 1.000.000.000 (um bilhão) ou ainda 10^9 de seu originário, nesse caso 1 (um) *Byte*.

Um *Byte* é uma medida equivalente a um caractere qualquer armazenado no servidor. Portanto, considerando que um atestado em formato de arquivo texto tenha aproximadamente 500 *Bytes*, os custos totais de armazenamento e armazenamento adicional para *backup* foram dimensionados utilizando a seguinte fórmula:

$$Ca = \left(\frac{tA \times 500}{10^9} \right) \times n$$

Onde:

Ca = Total de custos com armazenamento.

tA = Total de atestados emitidos pela amostra.

n = VMC de Armazenamento ou Armazenamento adicional para *backup*.

As projeções de custos foram escaladas aplicando as mesmas fórmulas de cálculo sobre cada amostra de profissionais, sendo também acrescentado custos com um novo integrante na equipe técnica a cada projeção.

b) Etapa 2 da Fase 4: Avaliação dos aspectos associados à Proteção Intelectual e a Transferência da Tecnologia (TT)

Os aspectos levados em consideração para essa avaliação foram:

- A natureza dos produtos gerados nesse trabalho: modelo de registro, fluxo de processos de negócio, arquitetura de requisitos e um *software* protótipo.

- A análise dos meios legais dos mecanismos de proteção intelectual que poderiam atender à proteção das criações intelectuais geradas nessa pesquisa;
- Os mecanismos legais de transferência da tecnologia que poderiam atender aos meios de proteção avaliados;
- Os direitos e obrigações dos Cedentes e Cessionários, e requisitos mínimos esperados nos acordos dos contratos de Transferência de Tecnologia (TT).

Para essa etapa utilizou-se elementos associados à revisão integrativa, pois o método permite a reunião, a avaliação e sintetização dos resultados de estudos, possibilitando novas perspectivas sobre o tema revisado (MARCONI; LAKATOS, 2010).

Para isso, os estudos elencados na Fase 2 dessa pesquisa foram primeiramente organizados de forma a explorar e analisar os dados coletados.

O **Quadro 17**, a seguir, apresenta a estrutura utilizada para essa organização:

Quadro 17 - Forma de organização dos estudos para revisão integrativa

Legislação estudada	Leis; Resoluções; Decretos.
Tema da legislação	Tema tratado pela legislação estudada.
Classificação	Proteção Intelectual; Transferência de Tecnologia (TT).
Ano	Ano da publicação da legislação.
Onde encontrar	Sites; Bases de dados.
Palavras-chaves	Resumo dos temas principais do texto; Identificação de ideias importantes para pesquisa complementar.
Recomendações	Destaques e aspectos centrais relevantes.
Considerações	Reflexões após análise mais aprofundada.
Conclusões	Atendimento dos meios de proteção aos produtos gerados; Direitos e obrigações contratuais.

Fonte: Autoria própria (2019).

O **Quadro 17**, acima, demonstra um exemplo da estrutura de tabela utilizada para classificar e ordenar os estudos elencados.

Cada documento referente a uma Lei, Resolução ou Instrução Normativa foram adicionados a essa tabela com a sua identificação no campo “Legislação Estudada”, e com o respectivo tema e as disposições tratadas por ele no campo “Tema da Legislação”.

Em seguida, nos campos “Classificação” e “Ano”, foi identificado se o tema estava relacionado à Proteção Intelectual ou Transferência de Tecnologia (TT), seguido do ano da sua publicação.

Nos campos “Onde encontrar” e “Palavras-chaves”, foi informado o *site* ou base de dados onde é possível encontrar a documentação e o resumo dos temas principais do texto

com a identificação de ideias importantes para pesquisas complementares, respectivamente.

Finalmente, nos campos “Recomendações”, “Considerações” e “Conclusões”, foi informado os destaques e aspectos centrais do texto, reflexões e pensamentos após análise mais aprofundada do texto, e se os aspectos dispostos atendiam aos meios de proteção e transferência dos produtos gerados nesse trabalho.

A partir da interpretação e síntese dos dados evidenciados na análise da legislação foi possível apresentar o texto que analisa os aspectos associados à viabilidade de proteção intelectual e a Transferência de Tecnologia (TT), e que dialogam com os aspectos considerados, dispostos no tópico 4.4.3 desse trabalho.

4.2 Estudos de viabilidade da inovação

Esse tópico avalia como a solução proposta nesse projeto poderá ser exequível e atingir resultados dentro de perspectivas técnicas minimamente desejáveis.

O propósito é apresentar requisitos preliminares de viabilidade técnica, diante da possibilidade de implementação futura do modelo proposto, através de um *software*, avaliando as variáveis econômico-financeiras minimamente desejáveis para essa implementação.

Estende-se também a avaliar aspectos de viabilidade associados à proteção intelectual e Transferência de Tecnologia (TT), uma vez que a completude do projeto só será possível após a transferência do modelo proposto para o mercado produtivo.

Vale salientar que um estudo de viabilidade econômico-financeira é altamente recomendado adicionalmente a esse trabalho, de forma a dimensionar e estimar mais amplamente o retorno sobre o investimento e as variáveis econômicas que poderão impactar nos riscos de sua produção e distribuição posterior.

4.2.1 Viabilidade técnica

A avaliação de viabilidade técnica visa analisar as alternativas dos recursos técnicos (tecnologias, *softwares* e equipamentos) e conhecimentos da equipe técnica necessários para tornar o projeto implementável em um *software*.

As premissas estabelecidas para analisar esses elementos são: disponibilidade (tecnologia presente no mercado e disponível para utilização ou aquisição); maturidade (tempo de vida, presença e resultados em várias outras aplicações); e conhecimento técnico

dos Desenvolvedores e Equipe de Projeto (nível de conhecimento *versus* tempo de aprendizado).

Os aspectos técnicos preliminares, considerados até o momento desse estudo, tomam como base os recursos e tecnologias utilizadas na arquitetura do protótipo apresentado nessa pesquisa e estão descritos a seguir.

a) Tecnologias essenciais recomendadas

As tecnologias essenciais recomendadas a seguir são apenas uma referência de um arcabouço de ferramentas possíveis dentro de uma estratégia de desenvolvimento de um *software* que implemente o modelo.

A escolha das ferramentas apontadas no **Quadro 18**, a seguir, se baseia nos requisitos necessários ao atendimento dos resultados da arquitetura proposta nesse trabalho.

Quadro 18 - Tecnologias necessárias para a fase do desenvolvimento de um *software*

Tecnologias essenciais	Finalidade
<i>Hiperledger Fabric</i>	Rede <i>blockchain</i> permissionada, utilizada como o “ambiente” de desenvolvimento e execução de um <i>software</i> .
<i>Docker</i>	Plataforma de código aberto para possibilitar que os Desenvolvedores e Administradores do Sistema desenvolvam, enviem e executem a aplicação.
<i>Docker compose</i>	Ferramenta utilizada para facilitar a configuração dos <i>containers</i> (espécie de máquinas virtuais) na plataforma <i>Docker</i> .
<i>Docker Engine</i>	Componente do <i>Docker</i> para facilitar a criação e administração dos ambientes virtualizados durante o desenvolvimento.
<i>Github</i>	Sistema de controle de versões distribuído, utilizado para controlar o versionamento do <i>software</i> .
<i>Cli tools</i>	Interface de linha de comando utilizada para emitir comandos para o programa em forma de linha de texto, para a realização de configurações de servidores através de <i>scripts</i> .
<i>PostgreSQL</i>	Sistema gerenciador de banco de dados relacional.

Fonte: Autoria própria (2019).

As tecnologias descritas no quadro acima estão baseadas em ferramentas de código aberto, de baixo ou nenhum custo, segurança, alto desempenho e vasta disseminação de conhecimento, o que as tornam mais acessíveis e plausíveis para a aplicação.

Na maioria dos casos, a escolha dos recursos de tecnologia parte de profissionais ligados à Arquitetura ou Engenharia de *Software* com base em sua estratégia para o desenvolvimento da aplicação.

É considerada também por eles, no momento da escolha, a familiaridade da equipe de desenvolvimento (analistas e programadores) com os recursos escolhidos.

Portanto, uma vez transferido para o mercado produtivo, os recursos de tecnologias apontados no quadro acima tenderão a ser substituídos por outros que atendam ao mesmo propósito, já que se trata de ferramentas para desenvolvimento de sistemas.

b) Infraestrutura recomendada

A infraestrutura contempla os recursos físicos, serviços e ferramentas tecnológicas necessárias para as fases de desenvolvimento, execução e manutenção do sistema, e compreendem os requisitos mínimos que abrangem todas essas fases.

Os recursos mínimos recomendados para a execução desse projeto são descritos a seguir.

Quadro 19 - Equipamentos e serviços recomendados à infraestrutura

Equipamento / Serviço	Configuração
Estações de trabalho (computadores)	Processadores Intel® Core i7 ou superior, memória RAM de 8GB ou superior.
<i>Link</i> de <i>internet</i> dedicado	Velocidade de 20MB ou superior.
Servidores de serviço de processamento e hospedagem em nuvem (<i>Datacenter</i>).	Servidor <i>OnDemand Linux</i> c4.xlarge, 1000GB SSD, <i>backup storage</i> , aplicação de carga balanceada.

Fonte: Autoria própria (2019).

As estações de trabalho compreendem os computadores utilizados pela Equipe de Desenvolvimento durante a fase de construção e posterior manutenção do *software*.

O *Link* de *internet* dedicado é um serviço oferecido por empresas de telefonia ou provedores de *internet*, com uma velocidade e estabilidade muito superior se comparados aos serviços de *internet* de banda larga.

Os Servidores de Serviço de processamento e hospedagem em nuvem são serviços que abrigam *hardwares* essenciais para alto poder de processamento e armazenamento de dados,

reunidos em um só lugar, com um custo de investimento relativamente baixo se comparados a estruturas de servidores locais.

Os benefícios da utilização de servidores em nuvem se mostram muito maiores se comparados aos servidores locais, pois dispensam custos tradicionais (manutenção de equipamento, equipe de manutenção dentre outros), possibilitando ao seu utilizador focar maiores esforços econômicos no negócio.

O **Quadro 20**, a seguir, mostra um comparativo entre as duas modalidades de servidores, destacando os benefícios da utilização do servidor em nuvem *versus* um servidor local.

Quadro 20 - Comparativo entre as duas modalidades de servidores

Servidor em nuvem	Servidor local
<ul style="list-style-type: none"> • Elasticidade: fácil aumento da capacidade de hospedagem sob a demanda de crescimento da aplicação; • Baixo custo: pagamento proporcional a apenas os recursos utilizados; • Desempenho e escalabilidade: fácil aumento de poder de processamento, memória e armazenamento; <i>internet</i> dedicada e compatibilidade com aplicações levadas para “nuvem”; • Suporte e atendimento: garantia de funcionamento 24 horas por dia; • Segurança física: garantia e resolução de incidentes como incêndios, desastres naturais, disfunção elétrica etc.; • Segurança da informação: altos padrões de segurança de dados. 	<ul style="list-style-type: none"> • Complexidade na manutenção do <i>hardware</i>; • Elevados custos com serviços (redundância, internet e energia); • Custo com equipes especialistas em manutenção, segurança física e lógica.

Fonte: Autoria própria (2019).

Os servidores de processamento e hospedagem em nuvem recomendados por este estudo são: *Microsoft® Azure; Amazon® AWS; Google® Cloud, Hetzner Online ou Oracle® Cloud*, por se tratarem de empresas de alto renome e com alto potencial e competência tecnológica, com a melhor relação custo-benefício.

Dentro de uma das análises das variáveis econômico-financeiras associadas a essa proposta, descritas na sequência desse estudo, o serviço da *Amazon®* foi o selecionado com o intuito de demonstrar prováveis custos com um servidor de hospedagem.

Os sistemas e serviços instalados, necessários ao funcionamento das máquinas (estações de trabalho e servidor em nuvem) são descritos no **Quadro 21**, a seguir:

Quadro 21 - Sistemas e serviços instalados necessários ao funcionamento das máquinas

Sistema operacional	<i>Ubuntu Linux</i> 14.04 / 16.04 LTS (ambos 64-bit), ou Mac OS 10.12.
Ferramentas <i>Docker</i>	<i>Docker Engine</i> : Versão 17.03 ou superior. <i>Docker-Compose</i> : Versão 1.8 ou superior.
Interpretador de código aberto para migrar a programação do <i>Javascript</i> do cliente para o servidor.	<i>Node.js</i> . Versão 8.9 ou superior.
Gerenciador de pacotes para linguagem de programação <i>Javascript</i>	<i>Node Package Manager</i> (NPM). Versão 5.x.
Repositório do código fonte com controlador de versão	<i>Github</i> Versão 2.9.x ou superior.
Linguagem de programação	<i>Python</i> . Versão 2.7.x.

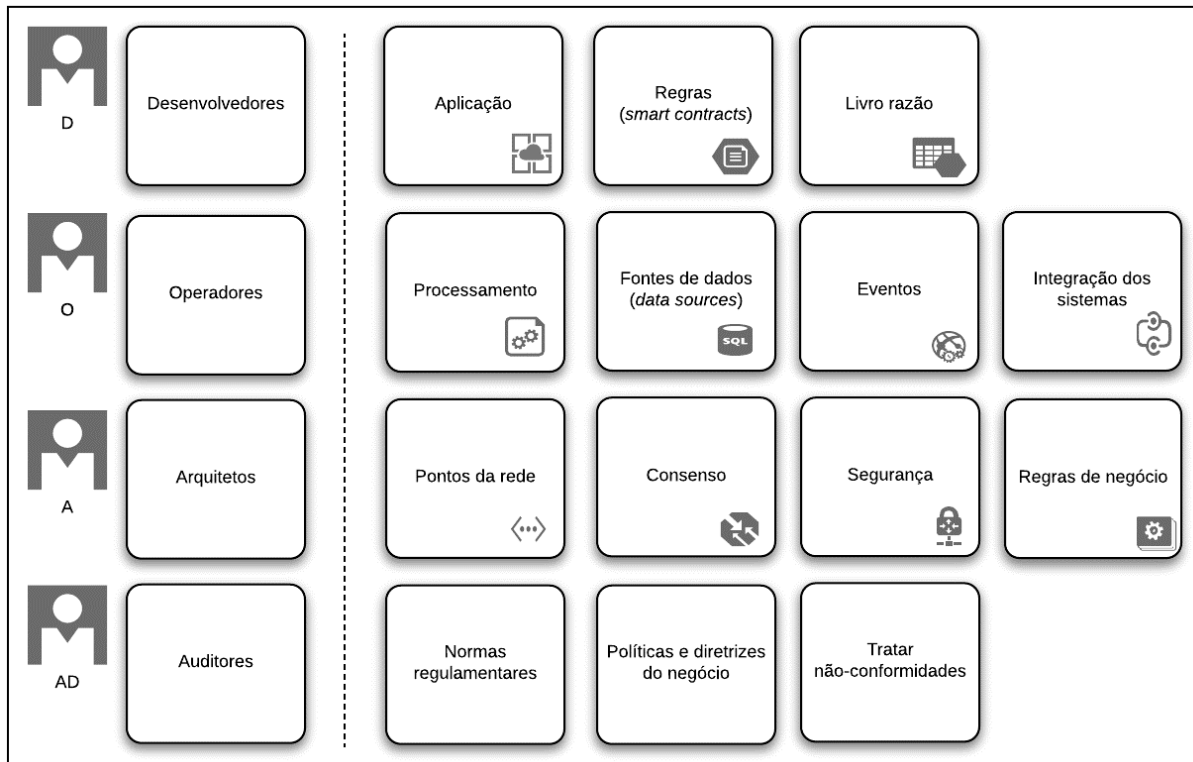
Fonte: A autoria própria (2019).

c) Configuração da equipe necessária para o desenvolvimento

A equipe necessária para a execução do projeto compreende especialistas com conhecimento aprofundado em tecnologia *blockchain*, desenvolvimento de sistemas em “nuvem”, banco de dados relacional, linguagem de programação orientada a objetos, ferramentas para ambientes de programação, segurança de dados e regras de negócio.

Os atores devem possuir habilidades multidisciplinares para o exercício dos seguintes papéis:

Figura 12 - Configuração da equipe especialista



Fonte: Autoria própria (2019).

Os Desenvolvedores *Blockchain* são os responsáveis pela criação da aplicação e desenvolver as regras (*smart contracts*) que vão interagir com a *blockchain* e serão utilizadas para iniciar as transações do usuário com a rede.

Os Arquitetos *Blockchain* realizam atividades administrativas como o desdobramento e a configuração da aplicação ou da rede *blockchain*.

Os Operadores *Blockchain* têm a função de definir, criar, gerenciar e monitorar a rede *blockchain* e a aplicação.

Os Auditores são os responsáveis por revisar e fazer cumprir as normas legais e regulamentares, as políticas e diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, assim como tratar as não conformidades e desvios que possam existir.

4.2.2 Análise das variáveis econômico-financeiras associadas à viabilidade técnica

A finalidade desse tópico é analisar variáveis minimamente desejáveis dentro do aspecto econômico-financeiro e que estão associados à viabilidade técnica do projeto.

O propósito é elencar os custos básicos e a projeção destes custos associados aos recursos técnicos, uma vez que o objeto desse estudo se encontra ainda em fase de proposta,

limitando-se ao limiar da Transferência da Tecnologia (TT).

1) Custos básicos do projeto

Dentro dessa perspectiva é minimamente desejável considerar duas variáveis centrais para a viabilização técnica do projeto: a) Custos com a Equipe de Desenvolvimento e Manutenção e b) Custos com o Servidor em Nuvem.

Recursos Humanos das áreas administrativas não foram considerados nas estimativas e projeções por não se tratar de uma avaliação organizacional, já que esse estudo não contempla a estruturação de uma organização empresarial em si para a execução do projeto.

a) Custos com Equipe de Desenvolvimento e Manutenção

De acordo ao Cadastro Geral de Empregados e Desempregados (CAGED) do Ministério do Trabalho, um Programador de Computador – Código Brasileiro de Ocupação (CBO 3171-10), ganha em média **R\$ 3.812,78** no mercado de trabalho brasileiro, em uma jornada de 42 horas semanais.

A faixa salarial varia entre R\$ 2.000,00 e R\$ 5.761,99 levando-se em consideração a média do piso salarial 2019 de convenções coletivas e dissídios, salário mediana da amostragem e o teto salarial da categoria.

Tendo como referência a configuração da equipe necessária à execução desse projeto (02 Desenvolvedores, 01 Operador, 01 Arquiteto e 01 Auditor), perfazendo um total de 05 integrantes, e considerando o salário médio de R\$ 3.812,78, estima-se os **custos para um ano** de projeto, aplicando-se ainda custos adicionais com 13º Salário e Férias, conforme a **Tabela 2** a seguir:

Tabela 2 - Custos com equipe de projeto no período de um ano

Custos individuais por membro da equipe		Custo anual com toda equipe
Salário base	R\$ 3.812,78	R\$ 228.766,80
FGTS	R\$ 305,02	R\$ 19.826,46
Décimo terceiro	R\$ 3.812,78	R\$ 19.063,90
1/2 das férias	R\$ 1.270,93	R\$ 6.354,63
Total	R\$ 9.201,51	R\$ 274.011,79

Fonte: Autoria própria a partir dos dados levantados no CAGED e Caixa Econômica Federal (2019).

A **Tabela 2**, acima, demonstra nas colunas da esquerda os custos individuais por membro da equipe, tendo a projeção total desses custos na coluna da direita.

Como ponto de partida, foi considerado, para a obtenção do custo anual, o total de 05 (cinco) integrantes dentro de um período de 12 meses (somando a este período, mais um mês referente ao 13º salário), para o salário base e para o recolhimento de FGTS.

Em adição, é acrescentado o valor total de 13º Salário e mais 1/3 de Férias, proventos que ocorrem apenas uma vez ao ano, obtendo a projeção total desses custos considerando os 05 (cinco) integrantes da equipe.

A estimativa de custos com recursos humanos associados à viabilidade técnica do projeto estaria dentro de uma perspectiva inicial de **R\$ 274.011,79** (Duzentos e setenta e quatro mil, onze reais e setenta e nove centavos) num período de **12 meses**.

Para essa estimativa foram considerados proventos dentro dos direitos trabalhistas, não considerando outros benefícios agregados.

b) Custos com Servidor em Nuvem

Os custos envolvidos com o Servidor em Nuvem, mostrados a seguir, têm como referência os valores dos serviços de servidores da *Amazon*®.

Esse servidor foi escolhido por dispor de um simulador de investimento sobre recursos a contratar (Calculadora de Custo Total de Propriedade (TCO) da AWS *Amazon*®)¹⁵ no próprio *site* do fornecedor dos serviços.

Os valores foram calculados com o auxílio dessa ferramenta e são demonstrados a seguir:

Quadro 22 - Demonstrativo de custos com servidor da *Amazon*®

Recursos do servidor AWS <i>Amazon</i> ®	Medida de consumo	Valor por medida de consumo
Servidor <i>OnDemand Linux c4.xlarge</i>	Hora	US\$0,199
Aplicação de balanceamento de carga	Hora / hora parcial	US\$0,0225
Armazenamento	<i>Gigabyte</i> / mês	US\$0,10
Armazenamento adicional para <i>backup</i>	<i>Gigabyte</i> adicional / mês	US\$0,095

Fonte: Autoria própria a partir dos dados coletados (2019).

¹⁵ Calculadora de Custo Total de Propriedade (TCO). Disponível em: <https://awstccalculator.com/>. Acesso em: 15/10/2019.

A configuração do servidor que poderia ser contratado compreende múltiplos processadores de 04 (quatro) núcleos que trabalham sob demanda com o investimento de US\$0,199 por hora de consumo.

Conta também com uma aplicação de balanceamento de carga com investimento de US\$0,0225 por hora de consumo.

A capacidade de armazenamento de dados demanda um custo de US\$0,10 por *Gigabytes* consumidos ao mês, assim como o armazenamento adicional para gerar as cópias de segurança (*backup*), demandando um custo de US\$0,095 por *Gigabyte* adicional consumido no mês.

Considerando que a plataforma *blockchain* para registro e validação de autenticidade de atestados médicos-odontológicos necessitaria de funcionamento 24 horas por dia, e 30 dias por mês, o valor do custo com servidor, referente a apenas o processamento de máquina, poderia ser estimado com base no consumo de horas, conforme **Tabela 3**, a seguir:

Tabela 3 - Custos com recursos de processamento/hora de servidor

Recursos do servidor	Custo anual	Conversão
Servidor <i>OnDemand Linux c4.xlarge</i>	US\$1.719,36	R\$ 7.302,81
Aplicação de balanceamento de carga	US\$194,40	R\$ 825,69
Total dos custos iniciais	US\$1.913,75	R\$ 8.128,51

Fonte: Autoria própria a partir dos dados da pesquisa (2019).

A conversão monetária dos valores demonstrados na **Tabela 3**, acima, foi realizada considerando a taxa de câmbio do Dólar dos Estados Unidos (USD)¹⁶

Os valores referentes aos recursos, Servidor *OnDemand Linux c4.xlarge* e a Aplicação de balanceamento de carga, estão estimados considerando o valor unitário da hora (US\$0,199) e seu funcionamento 24 horas por dia, durante 12 meses, totalizando **8.640 horas**.

Os custos de Armazenamento e de Armazenamento Adicional para *backup* do servidor não são considerados nessa primeira estimativa, pois se referem ao consumo para a gravação dos atestados emitidos, porém serão consideradas em seguida, nas projeções de custos por amostra de profissionais.

Os custos com processamento e balanceamento de carga do servidor estariam,

¹⁶ Conversão com base na taxa de câmbio do Dólar Americano do dia 28/11/2019. Dólar do dia US\$4,2474. Fonte: Banco Central do Brasil. Disponível em: <https://www.bcb.gov.br/conversao>. Acesso em: 29/11/2019.

portanto, dentro de uma perspectiva inicial de **R\$8.128,51** (Oito mil, cento e vinte e oito reais e cinquenta e um centavos), ao final de um período de **12 meses**.

2) Projeções dos custos associados a viabilidade técnica do projeto

A seguir são apresentadas projeções dos custos associados à viabilidade técnica tendo como base a adesão escalável dos médicos e cirurgiões-dentistas à solução proposta. As projeções consideram:

- A indicação do número de atendimentos que, segundo o Artigo 2º da Resolução CREMERS nº 007/2011, é no máximo **14 (quatorze) pacientes** por turno de quatro horas;
- O tamanho de **500 (quinhentos) Bytes**, em medida computacional de um atestado em formato de arquivo texto;
- A população total de médicos e cirurgiões-dentistas em atividade no país até o momento desse estudo, sendo o resultado do somatório das principais inscrições ativas em todas as Unidades da Federação:

a) **Médicos = 477.022** (Quatrocentos e setenta e sete mil e vinte e dois) profissionais ativos¹⁷.

b) **Cirurgiões-dentistas = 328.251** (Trezentos e vinte e oito mil duzentos e cinquenta e um) profissionais ativos¹⁸

Sendo o total da população de Profissionais ativos igual a **805.273** (Oitocentos e cinco mil duzentos e setenta e três).

As projeções de custos apresentadas a seguir, utilizam como variáveis: 04 (quatro) diferentes amostras do número total da população de profissionais, e a quantidade estimada de atestados emitidos por cada amostra considerando o consumo de armazenamento gerado por essa demanda no servidor em nuvem. A primeira projeção é mostrada pela **Tabela 4**, a seguir:

¹⁷ Fonte: Conselho Federal de Medicina.

Disponível em: http://portal.cfm.org.br/?option=com_estatistica. Acesso em: 30/11/2019.

¹⁸ Fonte: Conselho Federal de Odontologia. Disponível em: <http://cfo.org.br/website/estatisticas/quantidade-geral-de-entidades-e-profissionais-ativos/>. Acesso em: 30/11/2019.

Tabela 4 - Primeira projeção de custos de viabilidade técnica

Quantidade da amostra: 201.318 profissionais (25%)	
Atestados emitidos	718.705.260
Consumo de armazenamento no servidor	359,35GB
Equipe técnica necessária	05 integrantes
Total dos custos em 12 meses	R\$ 274.309,42

Fonte: Autoria própria (2019)

A tabela acima utiliza uma amostra de **201.318** profissionais em sua projeção, equivalente a **25% da população total** de médicos e cirurgiões-dentistas. Dentro dessa perspectiva de custos, considera-se:

- A quantidade de atestados emitidos por esses profissionais estimada em aproximadamente **718.705.260** documentos dentro do período de **255 dias úteis em 12 meses**, sendo consumido cerca de **359,35GB** de armazenamento no servidor, gerando um custo de **R\$ 297,63** por esse consumo.
- A equipe técnica utilizada é de **cinco (05) especialistas**, gerando um custo de **R\$ 274.011,79**, com recursos humanos.

O total de custos dessa projeção, ao final do período, é de: **R\$ 274.309,42**.

Para a segunda projeção de custos de viabilidade técnica, considera-se uma amostra de **50% da população de profissionais**, e seus resultados são apresentados na **Tabela 5**, a seguir:

Tabela 5 - Segunda projeção de custos de viabilidade técnica

Quantidade da amostra: 402.637 profissionais (50%)	
Atestados emitidos	1.437.414.090
Consumo de armazenamento no servidor	718,71GB
Equipe técnica necessária	06 integrantes
Total dos custos em 12 meses	R\$ 329.143,58

Fonte: Autoria própria (2019)

A tabela acima demonstra a projeção sobre uma amostra de **402.637** profissionais, equivalendo a **50% da população total** de médicos e cirurgiões-dentistas. Nessa projeção

considera-se:

- A quantidade de atestados emitidos por esses profissionais estimada em aproximadamente **1.437.414.090 documentos** dentro do período de **255 dias úteis** em **12 meses**, sendo necessário o consumo aproximado de **718,71GB** de armazenamento no servidor, gerando um custo de **R\$329,43** por esse consumo.
- Além do aumento dos custos com servidor, para essa amostra é necessária à adição de mais um Desenvolvedor de *Software* devido ao aumento da demanda, totalizando **seis (06) especialistas** na equipe técnica, gerando um custo de **R\$ 328.814,15** com recursos humanos.

O custo total dessa projeção é de **R\$ 329.143,58** no final de 12 meses.

A terceira projeção de custos de viabilidade técnica ocorre sobre uma amostra de **75% da população de profissionais**. A **Tabela 6**, a seguir, apresenta esses resultados:

Tabela 6 - Terceira projeção de custos de viabilidade técnica

Quantidade da amostra: 603.955 profissionais (75%)	
Atestados emitidos	2.156.119.350
Consumo de armazenamento no servidor	1.078,06GB
Equipe técnica necessária	07 integrantes
Total dos custos em 12 meses	R\$ 384.110,65

Fonte: Autoria própria (2019)

A amostra de **603.955** profissionais apresentada na terceira projeção na tabela acima, equivale a **75% da população total** de médicos e cirurgiões-dentistas. Nela considera-se:

- A quantidade de atestados emitidos por esses profissionais estimada em aproximadamente **2.156.119.350 documentos** em um período de **255 dias úteis** em **12 meses**, sendo necessário o consumo aproximado de **1.078,06GB** de armazenamento no servidor, totalizando um custo de **R\$494,15** com esse consumo.
- Para essa amostra, além do aumento dos custos com servidor, é necessária a adição de mais um Desenvolvedor de *Software* em relação à projeção anterior, totalizando **sete (07) especialistas** na equipe técnica, perfazendo um custo total de **R\$ 383.616,51** com recursos humanos.

O total de custos dessa projeção, ao final de 12 meses, é de **R\$ 384.110,65**.

A última projeção de custos de viabilidade técnica considera os **100% da população de profissionais**. A **Tabela 7**, a seguir apresenta os resultados:

Tabela 7 - Quarta projeção de custos de viabilidade técnica

Quantidade da amostra: 805.273 profissionais (100%)	
Atestados emitidos	2.874.824.610
Consumo de armazenamento no servidor	1.437,41GB
Equipe técnica necessária	08 integrantes
Total dos custos em 12 meses	R\$ 439.077,72

Fonte: Autoria própria (2019)

A projeção demonstrada na tabela acima considera a hipótese de **100% de adesão** da população de profissionais, ou seja, **805.273** médicos e cirurgiões-dentistas utilizarem a solução.

A quantidade de atestados emitidos por esses profissionais dentro de **255 dias** úteis em **12 meses** é estimada em aproximadamente **2.874.824.610 documentos**, sendo necessário um consumo aproximado de **1.437,41GB** de armazenamento no servidor, gerando um custo de **R\$ 658,56** por esse consumo.

Para essa amostra, além do aumento dos custos com servidor, é necessária uma **equipe técnica de oito (08) integrantes**, sendo que cinco (05) deles Desenvolvedores de *Software*. O custo total com recursos humanos, portanto, é estimado em: **R\$ 438.418,86**.

O custo total dessa projeção é de **R\$ 439.077,72** no final de **12 meses**.

Para a obtenção de uma visão geral das projeções acima, a **Tabela 8**, a seguir, apresenta a totalização dos números estimados em todas as projeções.

Tabela 8 - Totalização dos custos estimados em todas as projeções

Amostra	Integrantes Equipe	Custo Recursos Humanos	Consumo Servidor	Custo Servidor	Total
(25%) 201.318	5	R\$ 274.011,79	359,35GB	R\$297,63	R\$ 274.309,42
(50%) 402.637	6	R\$ 328.814,15	718,71GB	R\$329,43	R\$ 329.143,58
(75%) 603.955	7	R\$ 383.616,51	1.078,06GB	R\$494,15	R\$ 384.110,65
(100%) 805.273	8	R\$ 438.418,86	1.437,41GB	R\$658,56	R\$ 439.077,72

Fonte: Autoria própria (2019)

A **Tabela 8**, acima, reúne o total de custos estimados para viabilizar o projeto por 12 meses, associados aos aspectos técnicos que envolvem equipe técnica de projeto e serviço de servidor em nuvem, diante da perspectiva de amostras de profissionais que aderirem a solução.

As projeções estimam os custos de acordo com a demanda de consumo de processamento e armazenagem em servidor em nuvem, à medida que houver o aumento gradativo da emissão de atestados utilizando a solução tecnológica.

Também estimam a demanda de recursos humanos diante da mesma proporção de crescimento, de maneira a incrementar e dar manutenção à estrutura da solução, caso haja uma crescente demanda.

É importante salientar que as projeções estimadas se baseiam em números apenas indicativos e que podem variar conforme a dinâmica e aspectos de empregabilidade que envolve o mercado de tecnologia, além do serviço de servidor escolhido e outros custos com infraestrutura, que não foram considerados por serem altamente variantes.

4.2.3 Aspectos associados à viabilidade de Proteção Intelectual e Transferência de Tecnologia (TT)

A solução tecnológica poderá ser viabilizada para a produção mediante ao atendimento prévio de requisitos que atendam: a) a proteção intelectual da criação; b) o processo de transferência ao mercado produtivo.

As possíveis possibilidades de proteção propostas para os produtos gerados por esse projeto são:

1) Proteção por registro de *software*

O Artigo 7 da Lei de Direito Autoral (Lei nº 9.610, de 19 de fevereiro de 1998), define quais as obras intelectuais são protegidas por meio da criação do espírito.

O Inciso XII desse artigo insere também os programas de computador como obras protegidas, sendo que seu parágrafo primeiro rege que programa de computador é objeto de legislação específica.

A Lei nº 9.609, de 19 de fevereiro de 1998, conhecida como “Lei do *Software*”, estabelece a proteção à propriedade intelectual dos programas de computador.

O Artigo 1º dessa Lei define um programa de computador como um conjunto de

instruções escritas em linguagem própria a serem utilizadas de forma direta ou indireta por dispositivo computacional, a fim de obter um resultado.

A Lei de *Software*, diferentemente da Lei da Propriedade Industrial (LPI), abrange apenas as expressões contidas no código, não os procedimentos ou métodos, estes últimos poderão ser protegidos pela LPI, considerada uma proteção mais abrangente.

Conforme a Lei nº 9.609/98, a proteção de *software* oferece:

- a) Maior rapidez na obtenção da propriedade;
- b) Proteção automática para 176 países;
- c) Garantia da propriedade no ato da sua criação;
- d) Registro independente de exame;
- e) Vigência maior que a Lei de Patente.

Considerando-se a proteção dos direitos de autor, todas as expressões (ou partes delas) no programa de computador estão protegidas e não depende de registro.

Portanto, a motivação para o registro junto ao INPI está na garantia de uma maior segurança jurídica para os detentores da tecnologia descrita nesse projeto, caso haja demanda jurídica para comprovar a autoria ou a titularidade de um *software*.

Partindo desses princípios, e considerando que os próprios detentores desenvolvam um *software*, implementando o modelo proposto nesse trabalho, o registro de proteção para programa de computador deverá ser primeiramente obtido para então ser transferido ao mercado produtivo.

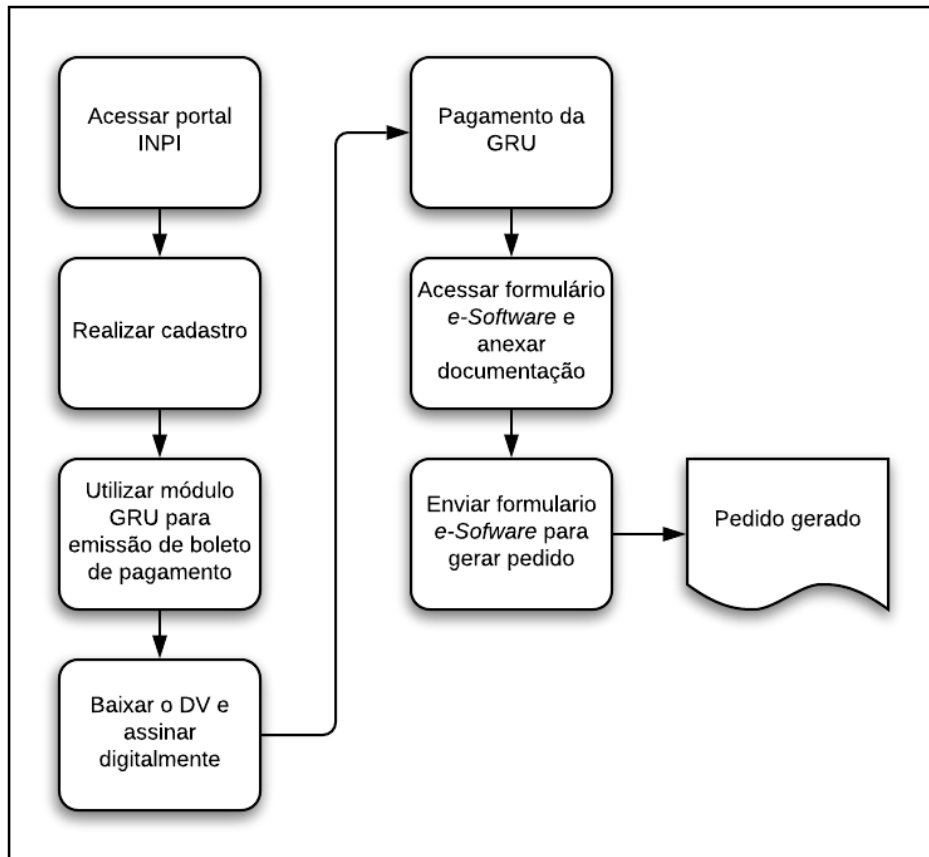
Essa obtenção ocorrerá através do Núcleo de Inovação Tecnologia – NIT do Instituto Federal de Ciência e Tecnologia do Estado da Bahia (IFBA) em conformidade à Instrução Normativa INPI/PR nº 099, de 08 de fevereiro de 2019, e observando o Manual do Usuário para o Registro Eletrônico de Programas de Computador, de 2019, que disciplinam o processo de registro eletrônico de programas de computador.

O pedido do registro do *software* proposto será apresentado exclusivamente por meio do formulário eletrônico *e-Software* e conterà três elementos essenciais:

- Taxa de depósito (não reembolsável);
- Declaração de veracidade;
- Formulário Eletrônico para o pedido de registro do *software* disponibilizado pela plataforma *e-Software*.

De acordo com o Manual do Usuário para o Registro Eletrônico de Programas de Computador (2019), e em conformidade com a Resolução INPI/PR nº 099/2019, o registro de um programa de computador ocorre em sete passos, demonstrados na **Figura 13** a seguir:

Figura 13 - Registro de Programa de Computador (RPC) em 7 passos



Fonte: Autoria própria (2019).

A figura acima demonstra o percurso padrão para a realização de um registro de programa de computador em sete (07) etapas. Após percorrer todas as etapas, se não existirem não-conformidades no pedido, o Certificado de Registro será disponibilizado para ser baixado no Portal do INPI.

O primeiro passo será realizar o cadastramento no “e-INPI”, direto no portal. Se for o próprio interessado, deverá selecionar o perfil correspondente à natureza do cliente – Pessoa Física ou Jurídica, sem procurador e domiciliado no país.

O termo de adesão deverá ser aceito para, então, seguir com o cadastramento. Os dados informados nessa etapa serão migrados automaticamente para o formulário eletrônico “e-Software”.

A emissão do Guia de Recolhimento da União (GRU) virá em seguida e deverá ser, obrigatoriamente, efetuada pelo titular do direito ou procurador. O passo seguinte será baixar a Declaração de Veracidade (DV) e assiná-la digitalmente, seguindo-se do pagamento obrigatório da GRU.

A documentação, então, deverá ser anexada ao formulário eletrônico e enviada para que o pedido seja gerado e, em caso de aprovação, a concessão será anunciada através de

publicação na edição seguinte disponível da Revista de Propriedade Industrial (RPI).

2) Proteção por patente envolvendo a invenção implementada por Programa de Computador

Outra possibilidade entre os mecanismos propostos para a proteção do produto apresentado nesse trabalho está baseada na busca do amparo das duas legislações.

A primeira assegurando a posse exclusiva do modelo proposto pelo sistema de patentes, e a segunda garantindo a autoria dos trechos relevantes do código pelo registro de *software*, sendo ambos os pedidos depositados junto ao INPI através do NIT.

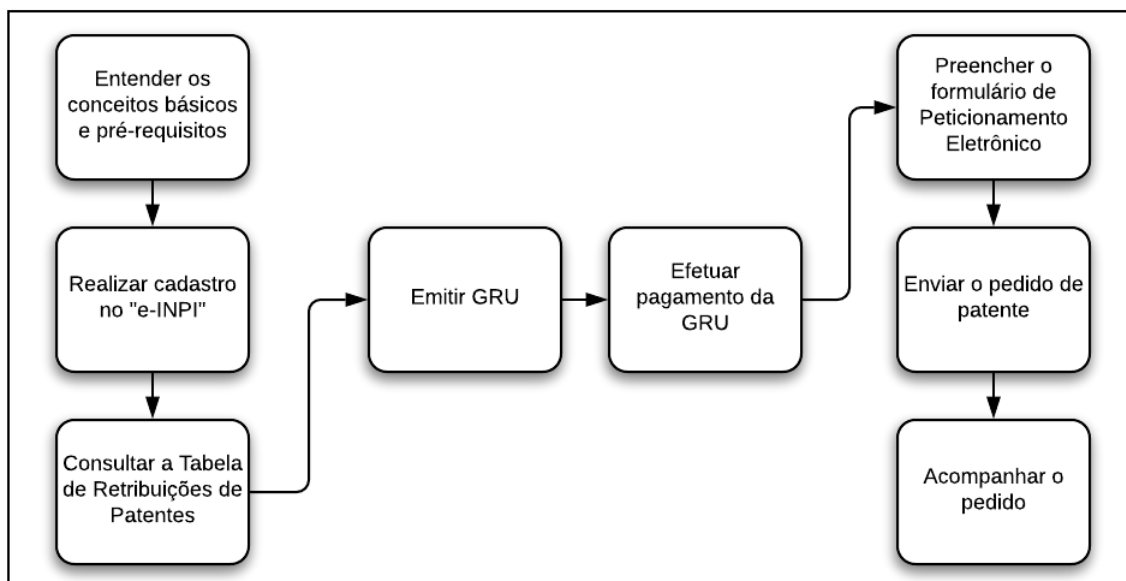
Nesse caso, em conformidade à Resolução INPI/PR nº 158, de 28 de novembro de 2016, a patente de invenção poderá ser usada para proteger o EFEITO TÉCNICO do programa de computador e não ele em si, desde que este cumpra os requisitos de patenteabilidade: novidade, atividade inventiva, aplicabilidade industrial e suficiência descritiva (LPI 9.279/96) caracterizando, nesse caso, uma invenção implementada por um *software*.

Partindo desse princípio, o pedido da patente envolvendo o modelo de registro, implementado por programa de computador (protótipo) para o registro e validação de atestados médicos poderia ocorrer pela proteção do efeito técnico.

O processo de proteção poderia ocorrer por meio do Núcleo de Inovação Tecnologia (NIT) do Instituto Federal de Ciência e Tecnologia do Estado da Bahia (IFBA) em conformidade à Resolução INPI/PR nº 158, de 28 de novembro de 2016, que norteia o processo de pedido de patente dessa natureza.

De acordo ao Guia Básico de Patentes, o Manual do Usuário do Módulo de Patentes do Peticionamento Eletrônico do INPI e em conformidade à Lei nº 9.279/96, em linhas gerais, o pedido de uma patente ocorre em oito passos, demonstrados na **Figura 14**, a seguir:

Figura 14 - Procedimentos para efetuar o peticionamento de Patente (em 8 passos)



Fonte: Autoria própria (2019).

As etapas necessárias para a realização de um pedido de patente perpassam pelos passos demonstrados na **Figura 14** (acima). O requerente poderá realizar o peticionamento através de meio eletrônico visando gerar o protocolo digital para o acompanhamento do pedido.

O primeiro passo compreende a leitura da legislação vigente que dispõe sobre o depósito de patentes, o entendimento do Manual do Usuário e a compreensão da Lei da Propriedade Industrial – LPI (Lei nº 9.279/96), com o propósito de conhecer os processamentos e prazos concernentes a um pedido de patente.

O passo seguinte é efetuar um cadastro no “*e-INPI*” com o objetivo de obter um *login* e uma senha e, em seguida, a Tabela de Retribuições de Patentes disponível no *site* do INPI, deverá ser consultada com o propósito de validar o valor e o tipo de serviço que deseja protocolar.

A etapa seguinte é a emissão do Guia de Recolhimento da União (GRU) de acordo ao serviço escolhido, seguido do próximo passo que é o pagamento desse documento.

A próxima etapa é o preenchimento do formulário eletrônico através do *link* “Peticionamento Eletrônico” no *site* do INPI, seguido do envio do Pedido de Patente, o que proporcionará o acompanhamento do pedido na Revista da Propriedade Industrial (RPI).

No que se refere à Transferência da Tecnologia (TT), as possibilidades de transferência do objeto proposto serão tratadas através de contrato de transferência de tecnologia, sendo que os mecanismos aqui avaliados tiveram como base a seguinte legislação:

- **Lei nº 9.609/98** – Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
- **Lei nº 10.973/04** – Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.
- **Decreto nº. 5.563/05** – Regulamenta a Lei nº 10.973/04.
- **Decreto nº. 9.283/18** – Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004; a Lei nº 13.243, de 11 de janeiro de 2016; o art. 24, § 3º, e o art. 32, § 7º da Lei nº 8.666, de 21 de junho de 1993; o art. 1º da Lei nº 8.010, de 29 de março de 1990; e o art. 2º, *caput*, Inciso I, alínea "g" da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional.
- **Instrução Normativa nº 31/2013** – Estabelece normas gerais de procedimentos para explicitar e cumprir dispositivos da Lei de Propriedade Industrial – Lei nº 9.279, de 14 de maio de 1996, no que se refere às especificações formais dos pedidos de patente.
- **Resolução nº 170/2016** – Disciplina o Peticionamento Eletrônico do Sistema *e-CONTRATOS*, denominado Formulário Eletrônico, regido pela presente Resolução e pelas regras que disciplinam o sistema *e-INPI*, fixadas na Resolução nº 25, de 18 de março de 2016.
- **Resolução nº 199/2017** – Dispõe sobre as Diretrizes de exame para averbação ou registro de contratos de licença de direito de Propriedade Industrial e de registro de topografia de circuito integrado, Transferência de Tecnologia (TT) e franquia.
- **Instrução Normativa nº 070/2017** – Dispõe sobre o procedimento administrativo de averbação de licenças e cessões de direitos de propriedade industrial e de registro de contratos de transferência de tecnologia e de franquia.
- **Instrução Normativa INPI/PR nº 099, de 08 de fevereiro de 2019** – Disciplina o processo de registro eletrônico de programas de computador.

Partindo desse pressuposto, a seguir, são apresentadas as possibilidades pautadas nas seguintes modalidades: Fornecimento de Conhecimento Tecnológico (Transferência de *know-how*); Licença para uso e exploração; e Cessão dos direitos do registro.

3) Fornecimento de Conhecimento Tecnológico (Transferência de *know-how*).

Considerando a transferência de *know-how*, seriam analisados os conhecimentos construídos a partir da: criação, pesquisa, e dos estudos tecnológicos gerados nesse trabalho resultando na elaboração de uma arquitetura composta dos requisitos e regras de negócio.

Essa arquitetura servirá como base para o desenvolvimento posterior de um sistema para registro e validação de autenticidade de atestados médicos.

Para essa possibilidade, a modalidade de contrato utilizada seria: Fornecimento de Tecnologia que, segundo a Resolução INPI/PR nº 199/2017, compreende a aquisição dos conhecimentos e das técnicas não amparadas por direitos de propriedade industrial ou fornecimento de informações tecnológicas.

Todas as diretrizes e discussões a seguir estão fundamentadas na referida Resolução.

a) as partes previstas nessa modalidade de contrato seriam:

- Os cedentes, representado por pessoa física (os detentores do conhecimento);
- A empresa cessionária ou adquirente, sendo a receptora do *know-how* que servirá de escopo para o desenvolvimento das competências produtivas.

b) previamente ao firmamento do acordo de transferência mediante instrumento contratual, se faria necessário um acordo de confidencialidade e sigilo.

Nessa fase, ainda não coberta por contrato, são compartilhadas informações importantes que poderão ser utilizadas, caso não seja assinado previamente um acordo dessa natureza, que coíba qualquer tentativa de uso de informações confidenciais.

c) os ganhos avaliados mediante esse mecanismo de transferência estariam no interesse da empresa em ter a garantia da exclusividade (não amparada pela lei), e no fato de poucos terem acesso à informação, e o sigilo, nesse processo, é fator fundamental, pois torna o conhecimento transferido, nesse contexto, tão valioso quanto uma patente.

Por ser um bem imaterial não protegido por direitos de propriedade intelectual devido a ser um conhecimento técnico, os riscos inerentes a este tipo de transferência poderiam ocorrer por conta da ausência dos requisitos de proteção não estabelecidos, limitando os recursos para a proteção efetiva apenas por meio do sigilo acordado.

Outros fatores de risco dessa modalidade estariam por conta de limites e características ligadas ao tempo e a geografia, e da obrigatoriedade de revelar informações, podendo ocorrer o desinteresse pela proteção de produtos futuros oriundos desse conhecimento.

Outro aspecto limitante está no fato de não gerar exclusividade jurídica de mercado,

ou seja, quem detiver o segredo não poderia impedir que outros, baseados no conceito, cheguem ao mesmo tipo de conhecimento e o explorem.

Portanto, a proteção jurídica é limitada e ocorreria apenas através de normas de concorrência desleal, acontecendo apenas quando o acesso ao segredo ocorrer de forma ilícita.

3.1) Recomendações aos termos basilares do acordo contratual

Os termos basilares do acordo contratual para esta modalidade iniciam-se no objeto do instrumento contratual descrevendo a transferência do *kow-how* para a cessionária, com a finalidade de que esta venha a desenvolver e comercializar o produto final resultante dos conhecimentos transferidos.

Os termos do acordo preveem a transferência do modelo de registro, a arquitetura e a descrição dos requisitos de todo o protótipo que envolve a base de dados em *blockchain* com a API de integração.

Os ganhos aferidos ocorreriam mediante o pagamento da cessionária ao cedente, de importância previamente acordada partindo da prévia valoração da tecnologia, dentro de um prazo antecipadamente estabelecido no acordo contratual.

Na eventual hipótese de a cessionária transferir a totalidade dos direitos sobre o produto para outra pessoa ou instituição, a cessionária pagaria ao cedente um percentual sobre o valor da cessão dos direitos. Ainda nesse caso, a cessão de direitos deveria ser condicionada ao pagamento pelo adquirente de *royalties*, ao cedente.

Caso a cessionária comercializasse ou obtivesse faturamento sobre a tecnologia desenvolvida posteriormente por ela, pagaria ao cedente uma quantia com base em percentual denominado: *royalties*.

Estes seriam calculados sobre o faturamento líquido (faturamento bruto total, deduzidas as despesas e impostos incidentes sobre faturamento bruto), e pagos a título de remuneração relativa à produção e exploração a partir do conhecimento tecnológico proposto nesse trabalho.

Estariam previstos também o pagamento de *royalties* pelo uso eventual de ajustes, ou melhorias componentes gerados na tecnologia pagos dentro de determinado período em que ocorresse o faturamento líquido.

No caso da adoção dessa modalidade de transferência, o início efetivo de produção e comercialização do produto desenvolvido pela cessionária deverá ser comunicado por escrito aos cedentes.

No caso de quebra contratual e ofensa à boa-fé entre as partes, os cedentes poderão rescindir o acordo e proceder a um novo licenciamento, além de exigir pagamento de perdas e danos e demais cominações legais, caso a cessionária inicie a produção e comercialização da solução sem a efetiva comunicação aos cedentes.

O prazo para início da utilização com fins comerciais da solução desenvolvida, só devem ser contados a partir da averbação junto ao INPI, ressalvados casos de força maior, os quais devem ser devidamente fundamentados e notificados aos cedentes sob pena de incidência do §3º do Art. 6º da Lei de Inovação.

Entre as obrigações previstas nesse tipo de transferência para os cedentes estariam à entrega da documentação da arquitetura, memoriais técnicos e demais documentos relacionados ao conhecimento tecnológico necessário à fiel execução do objeto do contrato.

As obrigações também preveem serviços de assessoria à cessionária, no que se refere ao esclarecimento de dúvidas sobre o conhecimento tecnológico.

Ainda nesse contexto, deverá fornecer à cessionária, durante a vigência do contrato, todas as inovações, melhoramentos ou aperfeiçoamentos do conhecimento tecnológico, se houver. Do mesmo modo, supervisionar a implementação do produto a ser desenvolvido pela cessionária objetivando seu perfeito funcionamento.

Em se tratando de obrigações da cessionária, a informação contínua para os cedentes quanto à produção e início da comercialização após seu desenvolvimento, deve ser mantida, assim como deverá assegurar sua regularidade jurídica e fiscal, a sua qualificação técnica e econômico-financeira, caracterizando estas como requisitos para sua qualificação como parte no acordo.

O sigilo e a responsabilidade serão a cargo de ambas as partes, não podendo revelar para qualquer pessoa, física ou jurídica, os aspectos técnicos do CONHECIMENTO TECNOLÓGICO ou da produção do sistema, exceto se exigido por lei, sem a autorização prévia por escrito da outra parte.

4) Licença para uso e exploração

Nesse contexto, os titulares concederiam ao licenciado a permissão de usar e explorar a tecnologia e, como não haveria a transferência da titularidade, as negociações das obrigações de manutenção estariam baseadas na manutenção do registro.

Partindo desses princípios, além da doutrina geral de contratos prevista na legislação brasileira, os termos do acordo para o licenciamento e/ou exploração do *software*

desenvolvido deverão observar os seguintes aspectos basilares:

- Poderá se tornar alvo do objeto do contrato qualquer produto ou serviço desenvolvido a partir dos conhecimentos gerados nesse projeto, composto pelo modelo de registro e a arquitetura da solução tecnológica proposta;
- Tornar-se-ia objeto do contrato de licenciamento para uso e exploração um possível pedido de patente ou registro de programa de computador, depositado junto ao INPI, e a eventual patente ou registro resultante da concessão desse pedido.
- A remuneração pela licença de uso e exploração deveria ser calculada como porcentagem da receita líquida obtida pela venda dos produtos/serviços.
- As condições para a renovação contratual, caso as partes entendessem como necessária, poderia ocorrer até o limite da vigência do registro do *software* e não haveria ônus algum para ambas as partes, caso decidissem pela renovação.

Essa última condição poderia não ocorrer caso a licenciada estivesse em débito com o pagamento dos *royalties* ou qualquer outra pendência financeira.

5) Cessão dos direitos

Em caso de cessão de direitos, os cedentes transfeririam a titularidade dos direitos de propriedade intelectual concedida ou depositada aos cessionários.

No caso da patente, os direitos para produzir, vender etc., seriam determinados pelo acordo contratual.

No caso do registro de *software*, haveria a transferência da titularidade sobre o conhecimento tecnológico (*know-how*) protegido por registro, assim como envolveria a transferência do conhecimento acumulado para que o cessionário viesse fazer uso adequado da tecnologia.

As condições desse acordo estariam na aquisição dos ativos protegidos dos seus detentores, sendo que a título de remuneração pela licença de uso e exploração da solução protegida, a “licenciada” pagaria ao “licenciante” um percentual a negociar referente ao pagamento de *royalties* e ao valor da aquisição dos direitos.

Considerações sobre os direitos, obrigações e responsabilidades das partes:

Do licenciante:

- Respeitar os termos do contrato;

- Colocar à disposição da licenciada todas as informações relacionadas ao programa de computador registrado, de modo a viabilizar a transferência da tecnologia e a exploração do seu uso;
- Disponibilizar todos os documentos necessários para alcançar o objetivo proposto.

Seria excluído dessas obrigações o desempenho, o atributo, a qualidade, a característica, o volume de vendas e funcionamento dentro de qualquer parâmetro ou critério do programa de computador protegido a ser comercializado ou explorado pela LICENCIADA.

Da licenciada:

- Respeitar os termos do contrato;
- Utilizar o programa de computador protegido, no Brasil, para exploração econômica;
- Arcar com todos os investimentos de promoção e *marketing*, publicidade, comercialização e distribuição;
- Assumir as responsabilidades por toda a operação de desenvolvimento e comercialização do *software* produzido;
- Pagar as remunerações no prazo determinado.

Os procedimentos para a execução das possibilidades relatadas nesse tópico serão demonstrados como resultados esperados desse estudo.

4.4 Riscos

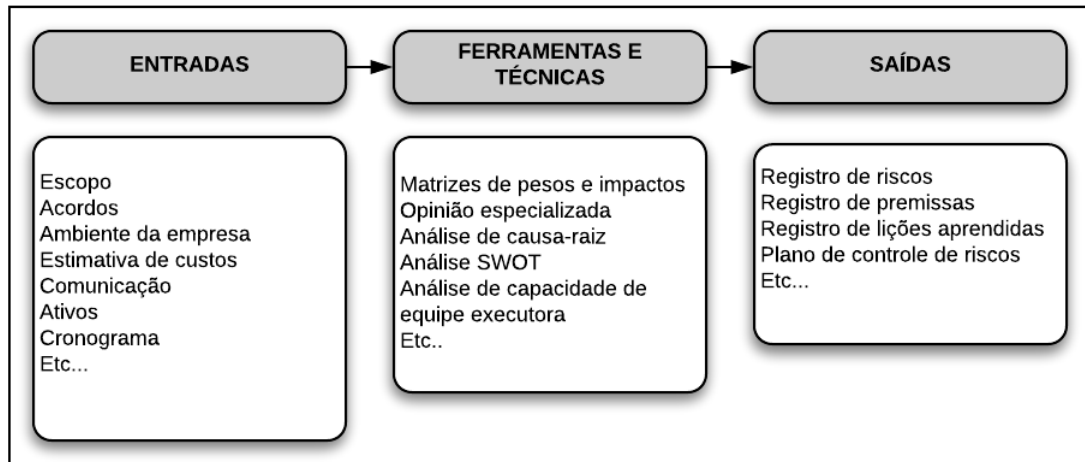
Qualquer alteração no ambiente que cerca um projeto pode ser considerado um risco e poderá ameaçar a execução do projeto, mesmo quando as variáveis são conhecidas.

As principais fontes de riscos são: os relacionados com recursos orçamentais, pois a situação econômica do setor pode sofrer alterações no decorrer da execução do projeto; os relacionados com tecnologia, podendo causar dificuldades na entrega do projeto devido a falhas com recursos tecnológicos; e os planejados, ou seja, aqueles que foram identificados e planejados previamente de acordo o maior número de cenários elaborados possíveis.

De acordo o Guia de Conhecimento em Gerenciamento de Projetos (GUIA PMBOK, 2017), a planificação deve seguir um processo de identificação dos riscos individuais, assim como as fontes dos riscos gerais do projeto, documentando as suas características. A **Figura**

15, a seguir, demonstra esse processo.

Figura 15 - Processo de identificação de riscos



Fonte: Autoria própria (2019),
Adaptado de Project Management Institute, (2017, p. 396).

Os procedimentos demonstrados na figura acima se iniciam pelos *inputs* (entradas), que são as fontes de informações iniciais que abastecem o processo. Dentre elas estão o escopo, os acordos entre as partes interessadas, o ambiente no qual a empresa ou detentora do projeto está inserida, os custos que envolverão as etapas de execução, cronograma dentre outros.

Esses dados deverão ser analisados através de ferramentas e técnicas que possibilitarão identificar as informações que serão registradas (saídas) para o monitoramento e controle dos riscos.

De forma preliminar e de modo a alcançar as primeiras identificações dos riscos da solução proposta nesse projeto, foi considerado o aspecto da não aceitação ao modelo proposto, falta de interesse na aquisição dos direitos de Propriedade Intelectual, a inabilidade da equipe executora, e o não atendimento às normas legais vigentes, conforme o **Quadro 23**, a seguir.

Quadro 23 - Identificação de riscos atuais do projeto

Riscos	Descrição	Probabilidade de ocorrência	Impacto
Não aceitação pelo Conselho Federal de Medicina ou outro órgão governamental.	A maior possibilidade de êxito desse projeto está atrelada a aceitação de uma entidade reguladora, como o CFM. No caso da não aceitação, a probabilidade de adesão da solução pelo mercado diminui consideravelmente.	Média	Alto
Falta de interesse na aquisição dos direitos da PI.	A ausência de um adquirente dos direitos da proteção intelectual poderá impossibilitar a transferência da tecnologia para a sua produção.	Médio	Alto
Inabilidade da equipe executora.	A falta de conhecimento de desenvolvedores de <i>software</i> nas tecnologias envolvidas para a execução do projeto poderá impossibilitar o seu desenvolvimento.	Baixo	Alto
Não atendimento às normativas atuais de uso dos dados.	Implicações pelo não atendimento às normas da nova Lei Geral de Proteção de Dados (LGPD) que demanda uma governança clara sobre a transmissão de dados tratados no Brasil.	Alta	Alta

Fonte: Autoria própria (2019).

Conforme demonstrado no **Quadro 23**, acima, a severidade do risco inerente ao tratamento de dados sob as tratativas das normas da nova Lei Geral de Proteção de Dados (LGPD) será um dos mais iminentes riscos a serem abordados na gestão de riscos do projeto, quando ocorrer a sua execução.

Publicada em 15 de agosto de 2018, com prazo para entrar em vigor em 2020, a Lei nº 13.709, tem o intuito de permitir que os cidadãos tenham maior controle sobre seus dados, e regular o tratamento de dados pessoais gerenciados por organizações. A lei é aplicada a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica de natureza pública ou privada.

A abrangência da legislação se estende desde órgãos públicos, além de todas as empresas estabelecidas no país e outras com sede no exterior, esse último grupo são as que prestam serviços ou possuem operações que envolvam dados no Brasil.

O novo padrão de proteção de dados não está limitado apenas às formas de registro de informações de consentimento individual, mas percorre por outros diversos aspectos jurídicos que necessitam atenção.

De acordo ao Art. 6º dessa Lei, as atividades de tratamento dos dados deverão observar os seguintes princípios:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma

incompatível com essas finalidades;

- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre acesso:** garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos dados:** garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência:** garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O descumprimento dessas regras trará desde advertências, bloqueios e suspensões parciais ou totais das atividades até multas gigantescas que poderão atingir milhões de reais.

Portanto, para a gestão adequada desse risco, que poderá afetar a exequibilidade do presente projeto, é recomendado que se previna nos Planos de Gestão de Riscos, após o processo de transferência de tecnologia, a adoção de medidas de segurança da informação através de práticas de Governança, Riscos e *Compliance* (conjunto de disciplinas que direcionam o cumprimento de normas legais e regulamentares, e políticas internas estabelecidas para a gestão dos dados).

5. RESULTADOS

Esse projeto visa contribuir com a minimização dos impactos advindos dos prejuízos causados à sociedade pela falsificação de atestados médicos-odontológicos.

Os resultados iniciais, através do modelo proposto, trazem melhorias ao processo de emissão do documento, criando critérios que deverão ser obrigatoriamente atendidos desde a sua emissão até a sua utilização no que se referem ao registro, a rastreabilidade e a verificação de autenticidade do documento.

O modelo de registro baseado em arquitetura *blockchain*, apresentado em seguida, validado por um sistema protótipo poderá criar uma base para o desenvolvimento de uma plataforma futura no momento em que ocorrer a transferência da tecnologia para o mercado produtivo.

Finalmente, a proposição das possibilidades de proteção e Transferência da Tecnologia cria um arcabouço que norteia as possibilidades da “passagem” do conhecimento tecnológico de forma segura, visando à produção e implementação da solução proposta pelo mercado produtivo.

Os resultados desse projeto apresentam: a modelagem dos processos de negócio relacionados com as estruturas das operações principais, incluindo em seus fluxos a interação com *Softwares* Clientes (*softwares* de terceiros) que farão as requisições de gravação e validação da autenticidade de atestados emitidos por eles em uma rede *blockchain*.

Em seguida, a arquitetura básica do protótipo que visa comprovar o modelo proposto demonstrando as regras de negócio e a arquitetura de requisitos por Casos de Uso que modelam a sua implementação.

Finalmente, elencam-se os mecanismos possíveis de proteção e Transferência da Tecnologia considerando as normas legais vigentes, os possíveis atores envolvidos no processo e os procedimentos para a efetivação do instrumento contratual, através de sua averbação.

5.1 Modelagem dos fluxos de processos de negócio do modelo proposto

O modelo consiste em controlar a trajetória de um atestado médico desde a sua emissão, passando pelo registro e verificação de autenticidade até a sua utilização final.

Para que haja efetividade da proposta, o modelo deverá ser institucionalizado por uma entidade reguladora superior como o Conselho Federal de Medicina (CFM), Ministério da

Saúde ou Secretarias de Saúde do Estado ou Municipais, de modo a manter e administrar seu uso e normatizar o processo de emissão de atestados médicos-odontológicos de forma automatizada.

No entanto, levar essa proposta a uma autarquia está além do propósito desse trabalho restringindo-se a apenas modelar e propor uma solução tecnológica para minimização do problema apresentado nesse estudo.

Os fluxos de processos de negócio que envolve o modelo são modelados em duas categorias distintas: 1) processo de negócio das operações de usabilidade dos Atores-usuários, e 2) processo de negócio das operações que compõem o conjunto da solução tecnológica, conforme a seguir.

1) **Processo das Operações de usabilidade dos Atores-usuários**

As operações dos Atores-usuários envolvem os seguintes atores:

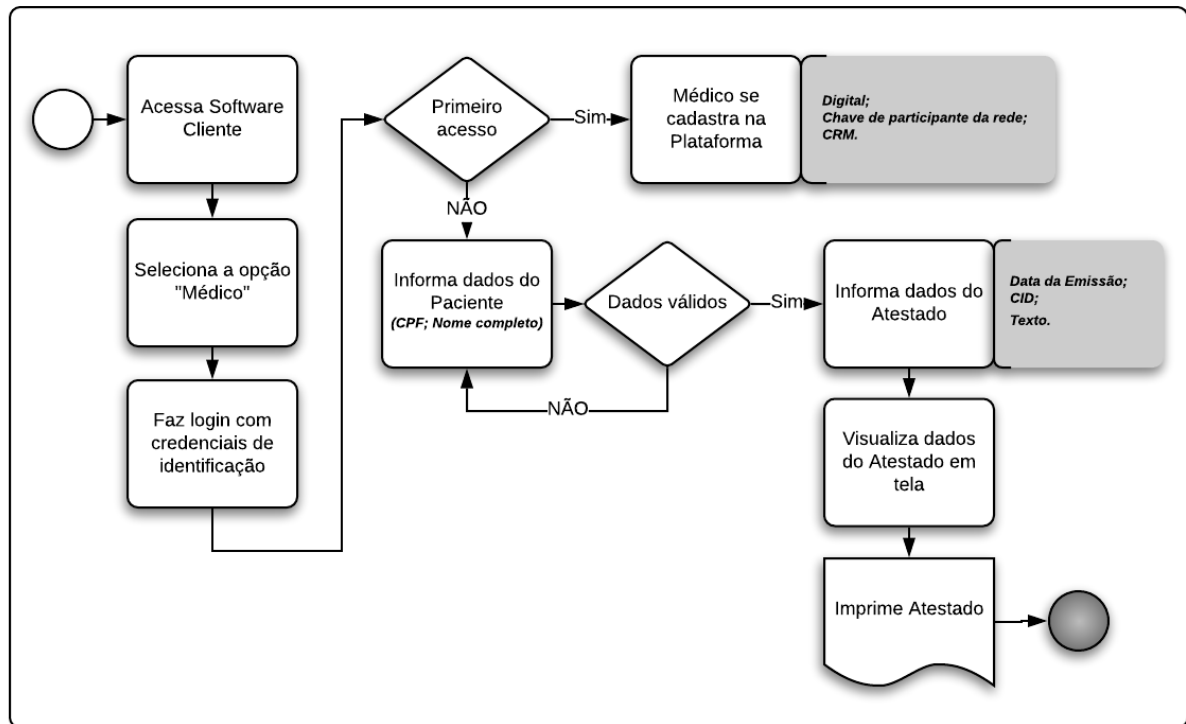
- **Profissional de Saúde** – Neste caso, o Médico ou Cirurgião-dentista responsável por avaliar o quadro do paciente, inserir e atestar as informações que comporão o documento final;
- **Paciente** – requerente ou o objeto central do documento, objeto das informações atestadas pelo médico no documento final;
- **Entidade Utilizadora** – órgão ou instituição privada ou pública que recebe e utiliza o documento final com o intento de comprovar a solicitação destinada ao paciente mediante a justificativa explicitada pelo médico no documento.
- **Entidade Reguladora** – órgão ou autarquia responsável por implementar, institucionalizar e regular o modelo proposto.

Como pré-requisito, todos os atores devem estar devidamente credenciados pela “Entidade Reguladora Superior” a participar de uma rede *blockchain* privada utilizando uma “Chave de Identificação de Participante da Rede”.

A finalidade é a realização do consenso da informação depositada na rede assegurando, assim, a sua veracidade como pré-requisito para a gravação dos dados.

A **Figura 16**, a seguir, demonstra o fluxo da operação de usabilidade do Profissional de Saúde.

Figura 16 - Fluxo do processo da operação de usabilidade do Profissional de Saúde



Fonte: Autoria própria (2019).

Conforme a **Figura 16**, acima, o primeiro passo para o Médico ou Cirurgião-dentista emitir o atestado é acessar um *Software* Cliente já habilitado a realizar essa operação.

Os passos seguintes envolvem informar o tipo de usuário que está acessando o sistema, selecionando a opção “Médico/Cirurgião-dentista”, e informar as credenciais de identificação para realizar o “*login*” na rede. As credenciais envolvem as seguintes informações: Registro Médico/Odontológico CRM/CRO, Chave de Participante de Rede, seguido da leitura biométrica da digital.

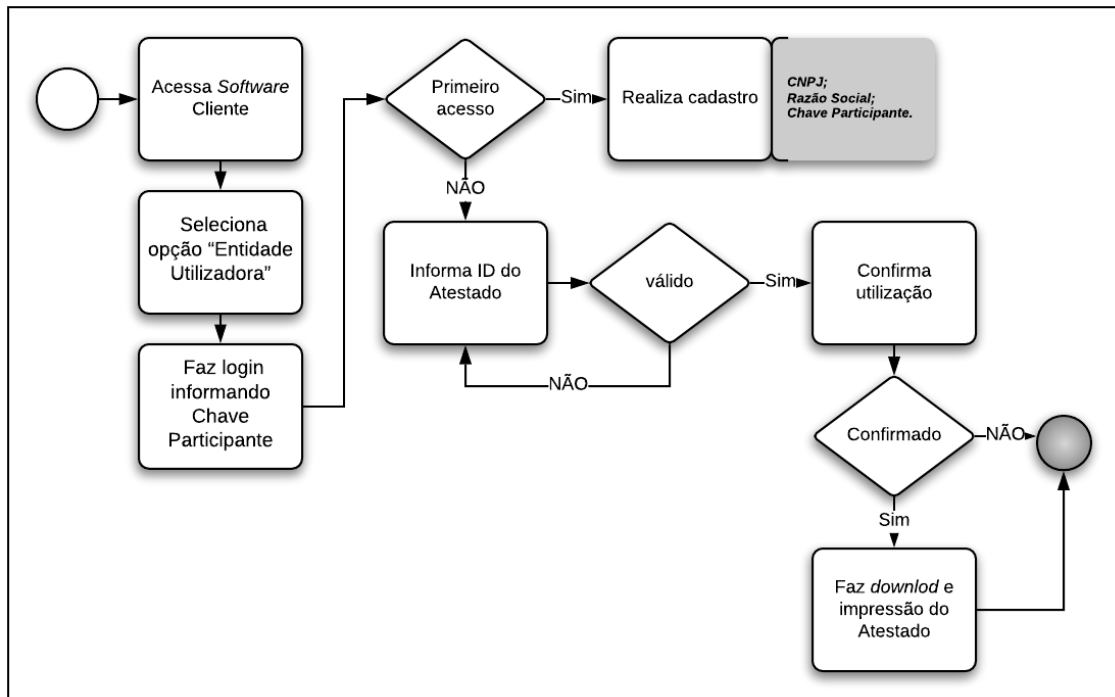
Caso seja o primeiro acesso do Profissional de Saúde à rede, o sistema solicitará que ele se cadastre pedindo o nome completo em adição aos dados anteriores.

O passo seguinte será informar os dados do paciente: CPF e Nome completo. Uma vez validado pelo sistema, as informações do atestado (Data de Emissão; Classificação Internacional de Doenças – CID; Texto do corpo do atestado) deverão ser inseridas no sistema.

Ao finalizar o documento digital, será exibido em tela com os dados informados, podendo ser impresso logo em seguida mediante confirmação.

A **Figura 17**, a seguir, demonstra o fluxo da operação de usabilidade da Entidade Utilizadora.

Figura 17 - Fluxo do processo da operação de usabilidade da Entidade Utilizadora



Fonte: Autoria própria (2019).

De acordo com a **Figura 17** acima, o primeiro passo para que uma Entidade Utilizadora verifique a autenticidade de um atestado que fará uso é acessar o *Software* Cliente e selecionar a opção tipo de usuário: “Entidade Utilizadora”.

O passo seguinte será fazer o “*login*” (entrada no sistema), informando a sua Chave de Participante da Rede.

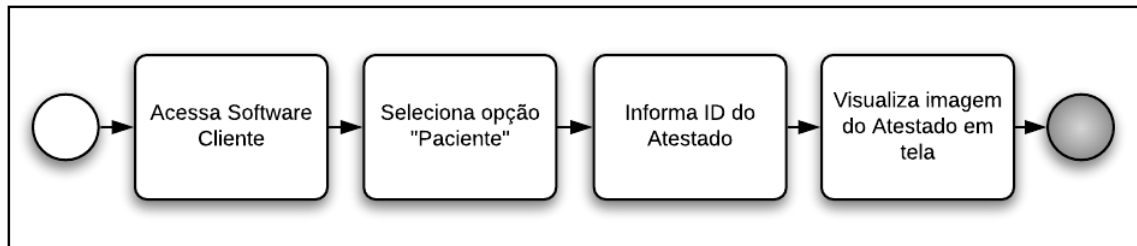
Caso seja o primeiro acesso, o sistema solicitará para que a Entidade Utilizadora realize o seu cadastramento na rede. Os dados solicitados para esse procedimento, além da chave de participante, serão o número de CNPJ e mais a Razão Social.

Em seguida a ID (Código de Identificação) do atestado deverá ser informado para que o sistema o localize na rede *blockchain*.

Caso o documento seja válido, a Entidade Utilizadora deverá confirmar que utilizará o atestado, fazendo o *download* da imagem e a sua impressão em seguida.

A **Figura 18**, a seguir, demonstra o fluxo da operação de usabilidade do Paciente.

Figura 18 - Fluxo do processo da operação de usabilidade do Paciente



Fonte: Autoria própria (2019).

Conforme a **Figura 18**, acima, o Paciente também poderá realizar a consulta do Atestado. Para isso ele deverá acessar um *Software* Cliente e selecionar a opção de tipo de usuário: “Paciente”.

O passo seguinte será informar a ID (Código de Identificação) do atestado, para que o sistema verifique a sua autenticidade. Uma vez identificado, o paciente visualizará o conteúdo do documento em tela.

2) Processo das Operações que compõem o conjunto da solução tecnológica

Os elementos que compõem o conjunto da solução tecnológica serão assim designados desse ponto em diante:

Blockchain – Rede de registro distribuído que registrará um atestado médico-odontológico de forma definitiva;

Banco de dados – Sistema de Banco de Dados que terá a função de registrar dados voláteis. Trata-se de informações que serão utilizadas nos procedimentos prévios ao registro definitivo/consulta na *blockchain*;

API – Sistema que fará a interface entre os mecanismos de registro (*blockchain*/Banco de Dados) e as aplicações clientes de terceiros (*Software* Cliente).

Esses três elementos compõem a “Plataforma” que fará o registro e auditabilidade desse tipo de documento.

A modelagem também contempla outro elemento indireto: o **Software Cliente**, que consiste em soluções do Estado da Técnica desenvolvidas por terceiros, já existentes ou a serem desenvolvidos no mercado, destinados a automatizar as operações de usabilidade dos atores envolvidos nos processos apresentados anteriormente.

Esses *softwares* poderão ser de arquiteturas e tecnologias diferentes (aplicações *web*, *desktop* ou aplicativos de celular etc.), e também com propósitos diversos (programas de

consultórios, gestão de clínicas, emissores específicos de atestados médicos etc.).

Deverão ser credenciados a participar da rede de registro de atestados pela “Entidade Reguladora” obtendo previamente, a partir dela, uma “Chave de Participante da Rede”.

Para que haja o correto envio e consulta das informações dos registros na rede, será necessário a implementação do protocolo de integração que permitirá a correta comunicação dos dados com a API por parte dos programadores do *Software* Cliente.

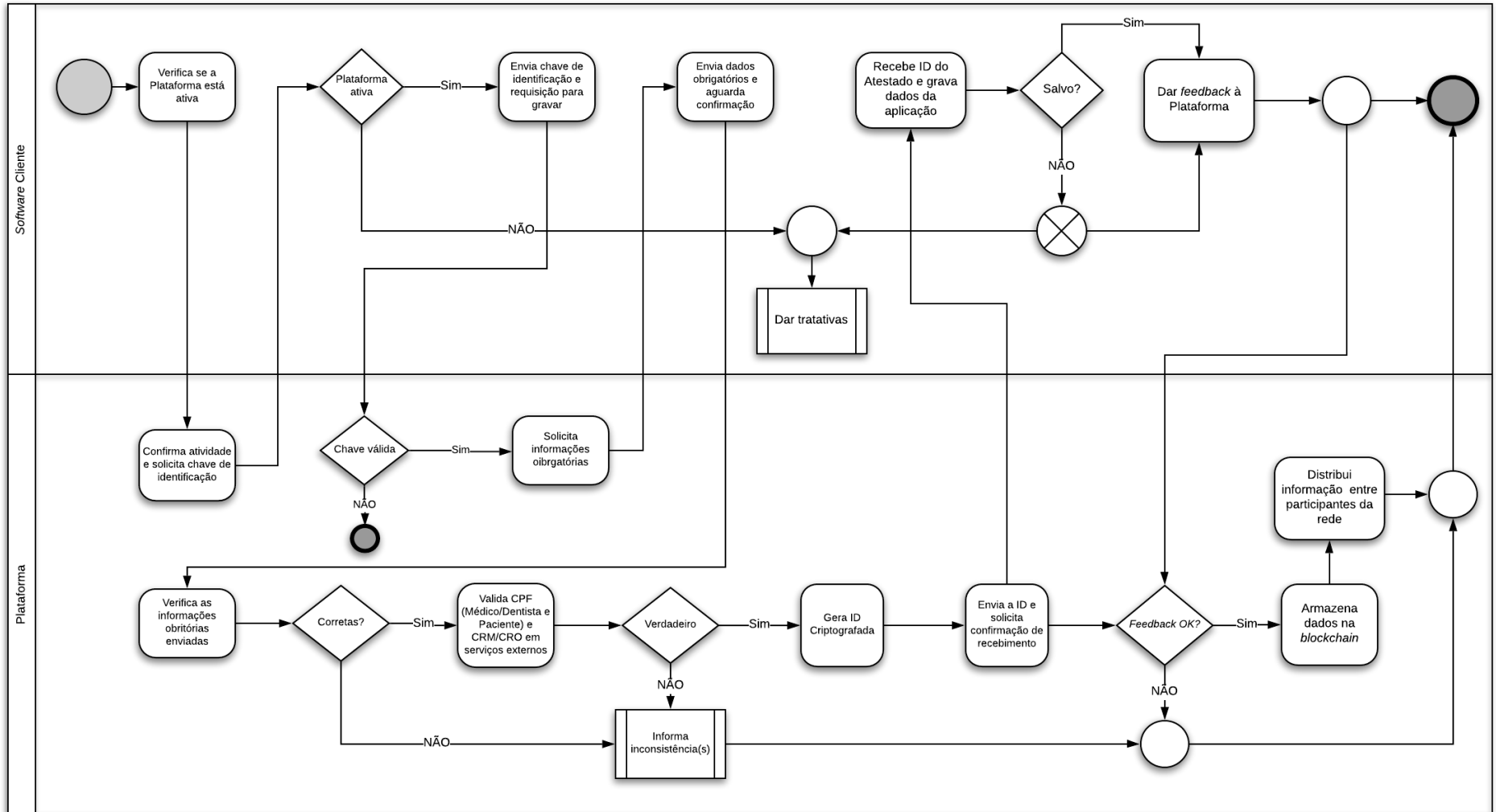
A modelagem do processo de negócio que compõe o conjunto da solução tecnológica se divide em dois níveis de operação:

- a) Requisição para a gravação de um novo documento.
- b) Requisição para a validação da autenticidade do atestado médico-odontológico.

As requisições são enviadas pelo *Software* Cliente para que a API realize as operações junto à rede *blockchain*.

O fluxo do item (a) é apresentado a seguir, na **Figura 19**:

Figura 19 - Modelagem do Processo de Negócio (Requisição para a gravação do atestado)



Fonte: Autoria própria (2019).

De acordo com a **Figura 19**, o processo inicia-se quando o *Software* Cliente verifica se a Plataforma se encontra ativa.

Com a confirmação da atividade, o *Software* Cliente envia para a Plataforma a Chave de Identificação do participante da rede, seguida da requisição para gravar um registro.

Uma vez o *Software* Cliente reconhecido como participante da rede, a Plataforma solicita as informações obrigatórias que deverá compor o registro do documento:

- Data de emissão;
- CRM/CRO do Médico ou Cirurgião-dentista;
- CPF do Médico/Cirurgião-dentista e do Paciente;
- CID da doença;
- Texto descrito no documento.

O *Software* Cliente envia as informações em resposta à solicitação e a Plataforma verifica a consistência dos dados.

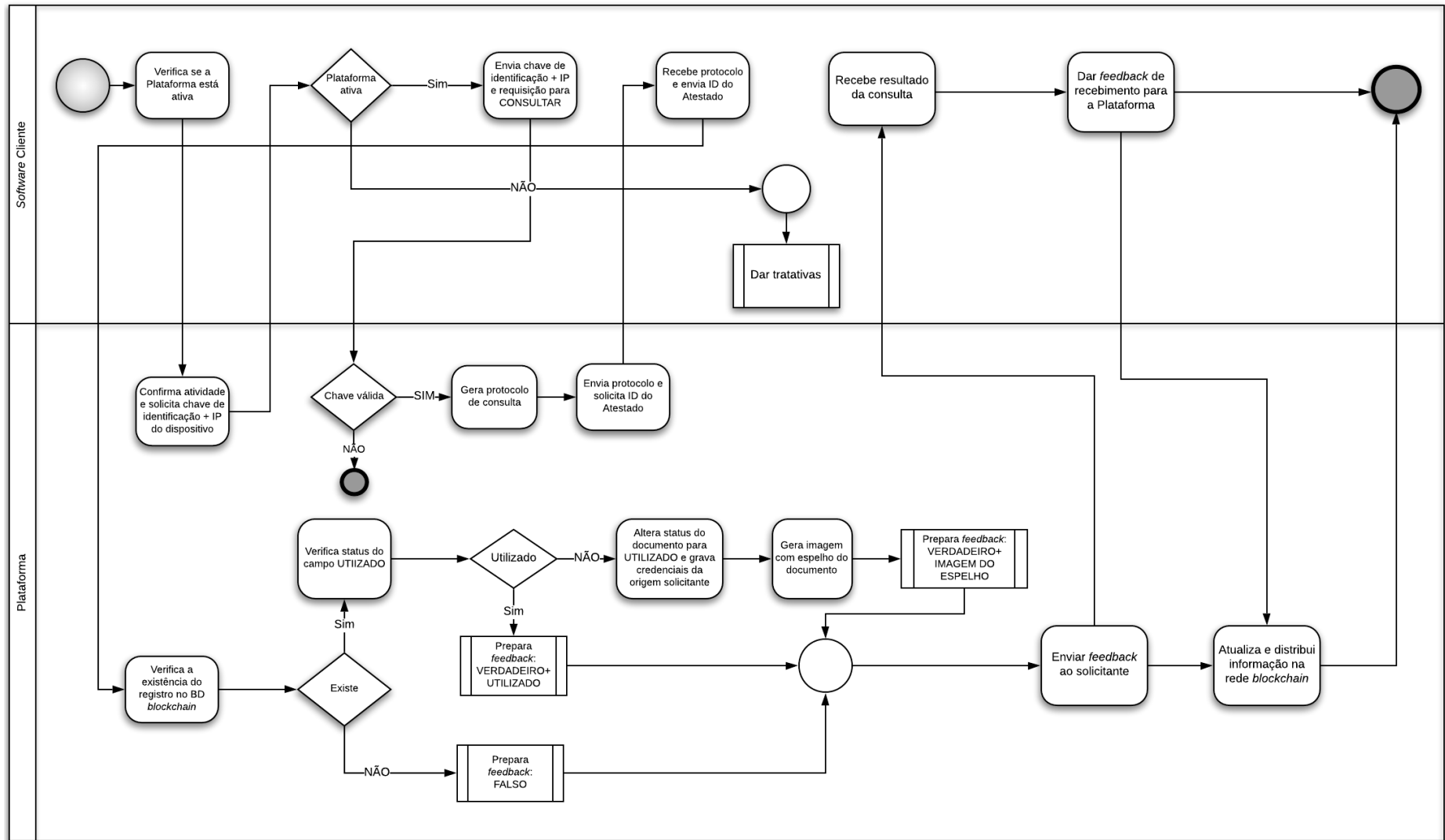
Uma vez validadas, a Plataforma gera um Código de Identificação – ID (*Hash* criptografada) enviando para o *Software* Cliente solicitante, e requiere a confirmação do recebimento.

Quando o registro é gravado no Banco de Dados ou repositório do *Software* Cliente, o *feedback* de confirmação de gravação é enviado à Plataforma.

O registro é então armazenado pela Plataforma no banco de dados em rede *blockchain*, mediante as regras de consenso, distribuindo a informação entre os participantes da rede.

O fluxo do item (b), referente à operação de consulta para a validação da existência e autenticidade do documento à Plataforma, é a segunda operação representada pelo fluxograma apresentado na **Figura 20**, a seguir.

Figura 20 - Modelagem do Processo de Negócio (Requisição para a validação de autenticidade do atestado)



Fonte: Autoria própria (2019).

Conforme a **Figura 20**, após o processo de verificação da identidade do participante da rede, a plataforma gera um protocolo de consulta e envia para a origem (*Software Cliente*) solicitando o Código de Identificação do documento (ID).

O *Software Cliente* recebe o protocolo e envia a ID (Código de Identificação) do documento a ser consultado.

O processo de verificação do documento, então, ocorre com a busca do registro no banco de dados da rede *blockchain*. A Plataforma informa que o documento não foi identificado na rede, caso o registro não seja encontrado.

Mediante a identificação do documento na rede, o *status* do campo “UTILIZADO” é verificado no Banco de Dados auxiliar (demonstrado na arquitetura do Protótipo) consistindo nos seguintes *feedbacks*:

- **Documento Utilizado:** Existente na rede *blockchain*, porém já utilizado por uma entidade consumidora;
- **Documento Não Utilizado:** Existente na rede *blockchain*, porém ainda não utilizado por uma entidade consumidora.

Caso o documento ainda não tenha sido utilizado por nenhuma Entidade Utilizadora, a Plataforma altera o conteúdo do campo “UTILIZADO” do registro para “VERDADEIRO” e gera o “espelho” do documento (imagem com o conteúdo do atestado) enviando como *feedback* para a origem (*Software Cliente*) solicitante.

Por fim, o *Software Cliente* recebe o resultado da consulta e confirma o recebimento. A Plataforma, então, atualiza os participantes da rede sobre a ocorrência.

5.2 Modelo de arquitetura *blockchain*, para o registro de atestados médicos-odontológicos

A arquitetura proposta nesse estudo envolve, em termos tecnológicos, a interatividade entre algumas entidades, de modo a cumprir a aplicabilidade do modelo proposto. Essas entidades são: *Software Cliente*, API e rede *blockchain*.

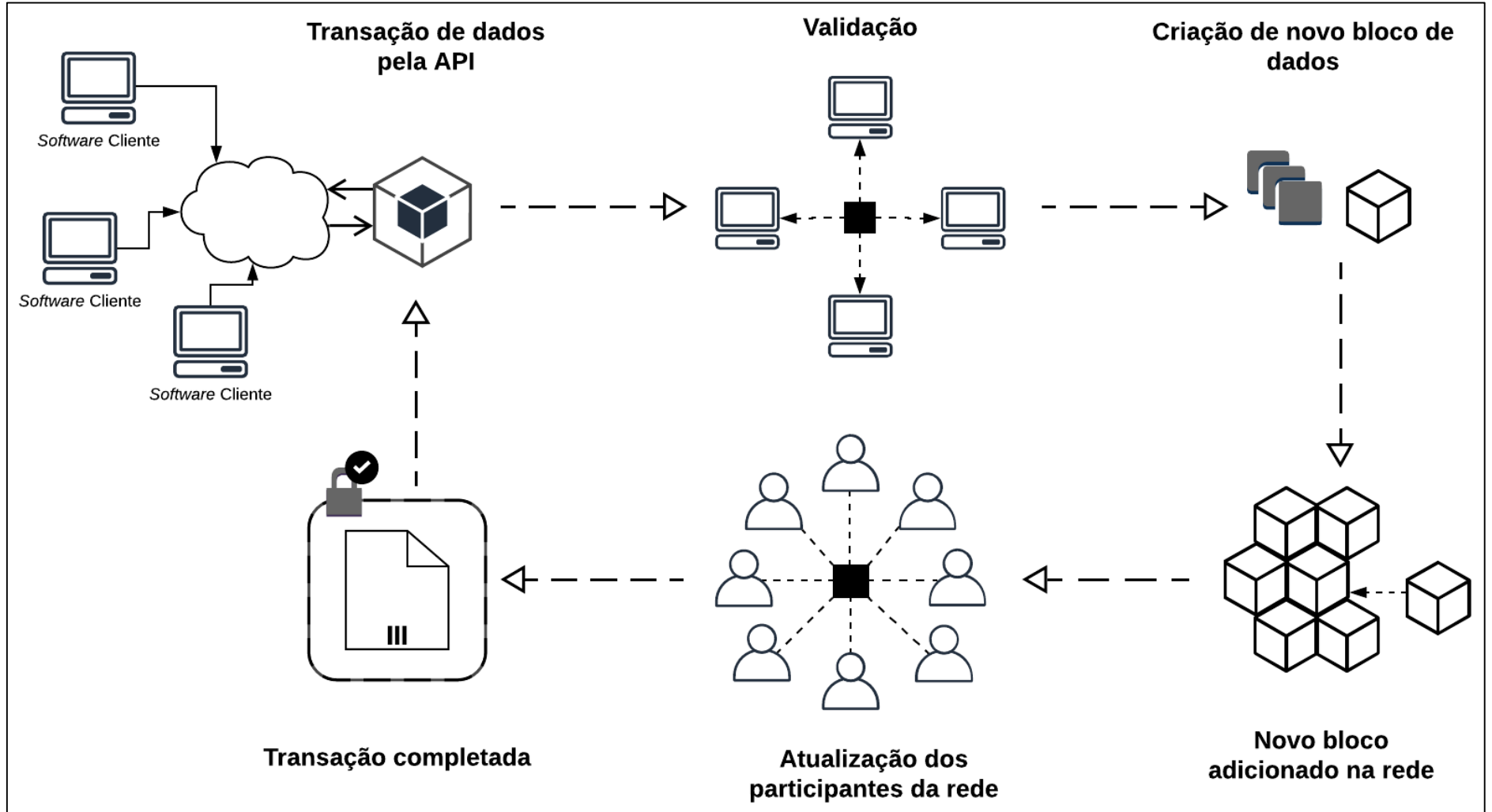
O funcionamento das operações que envolvem a interatividade dessas entidades está enfatizado nos Diagramas de Casos de Uso apresentados na sequência, no modelo de arquitetura para o protótipo.

Para uma maior compreensão da interatividade das operações que envolvem a rede *blockchain*, esse tópico foca em seu ciclo de execução. Os elementos centrais necessários ao ciclo de execução do modelo de arquitetura da rede *blockchain* para o registro de atestados, apresentado na sequência, são:

- **API** – uma Interface de Programação de Aplicações que realiza a integração de *Softwares* Clientes com a rede *blockchain*;
- **Chaincode** – código do sistema que implementa as regras da política de consenso (endosso da transação);
- **Política de Consenso** – “biblioteca” contida em um Contrato Inteligente (*smart contract*), com as regras utilizadas pelos participantes da rede para que um atestado seja gravado na rede *blockchain*, ou consultado a partir dela.
- **Participantes da rede** – Atores que estão ligados ao processo de emissão e recepção do documento (Médicos ou Cirurgiões-dentistas; Empresas Empregadoras, públicas ou privadas; órgãos ligados à saúde, públicos ou privados).

O Modelo é ilustrado pela **Figura 21**, a seguir:

Figura 21 - Modelo de arquitetura *blockchain* para registro de atestados médicos-odontológicos.



Fonte: Autoria própria (2019).

A **Figura 21** (acima) apresenta um modelo de arquitetura *blockchain* elaborada com a finalidade de registrar atestados médicos-odontológicos.

A sua elaboração se baseia na premissa de execução por ordem de validação, atendendo aos fundamentos previstos no Modelo de Arquitetura *Blockchain* de Execução por Ordem de Validação, do *Hyperledger Fabric*.

Esses fundamentos se traduzem em fases do ciclo de funcionamento da rede e são apresentados pelos resultados dos estudos de Androulaki (2018), conforme a seguir:

- **Execução** – fase que ocorre a identificação do “cliente” e a recepção da solicitação de transação, disparando as próximas etapas dentro da rede *blockchain*.
- **Solicitação** – fase de agrupamento das solicitações em grupos de transações encadeadas;
- **Validação** – fase onde a política de endosso é invocada para validar o bloco que será validado;
- **Atualização do estado** – fase em que o “livro-razão” é atualizado caso as regras da política de endosso tenham sido todas atendidas.

A elaboração de uma arquitetura *blockchain* baseada no *Hyperledger Fabric* deve atender a esses fundamentos em sua concepção e construção. Portanto, a seguir, são explanados como o modelo elaborado por esse trabalho atende a esses fundamentos.

Fase de Execução: para atender essa fase, o modelo apresentado acima propõe a integração entre *Softwares* Clientes (aplicações de qualquer natureza que emita um atestado médico-odontológico) e a rede *blockchain* através de uma API que executará as solicitações de transação vindas destes *softwares* externos.

Essa fase será disparada pela intervenção prévia de uma “entidade” – Médico, Cirurgião-dentista – realizando a sua identificação e inserindo um atestado na aplicação cliente.

Para atender a essa fase o modelo apresentado proporciona duas possibilidades:

- a) Solicitações de transação direta através de uma interface própria que poderia ser desenvolvida com essa finalidade (não contemplado por esse estudo);
- b) Através de outros *softwares* do mercado que poderão consumir os recursos da API, conforme é demonstrado na sequência, dentro da arquitetura desenhada para o sistema protótipo.

As **Fases de Solicitação e Validação** são atendidas no modelo operacionalizando as

duas fases conjuntamente. Para isso, as solicitações de transação são transformadas em *hashes*, ordenadas por ordem de solicitação, e transmitidas para uma rede ponto a ponto composta por “nós” (participantes da rede).

Os “nós” da rede validam (Fase de Validação) as informações do atestado, as informações de identificação da “entidade” e as condições para a aceitação do novo bloco na rede por meio das instruções da *chaincode*.

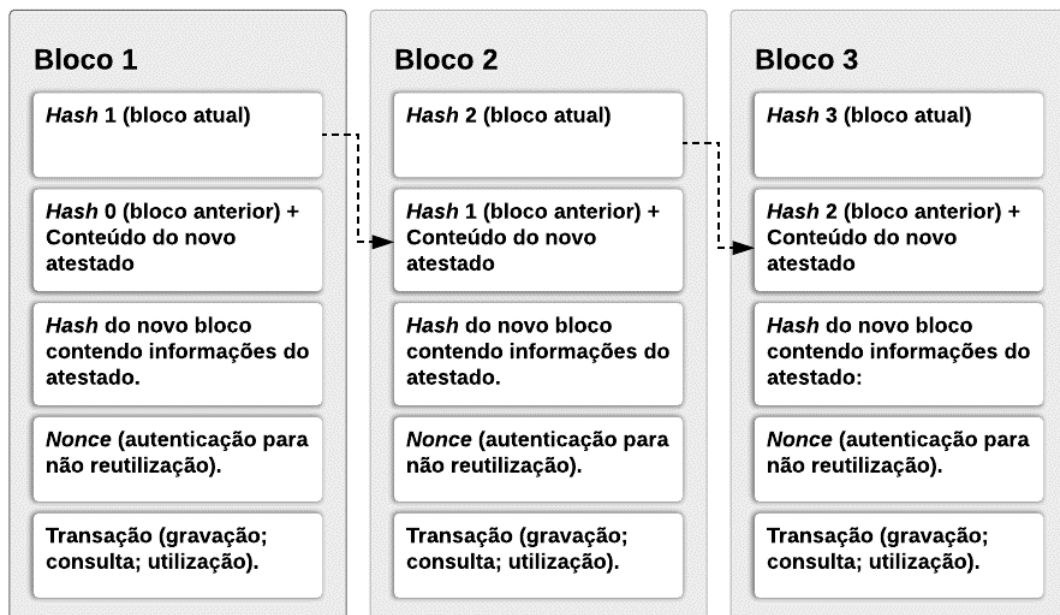
A *chaincode* possui todo o código de programação que carrega (invoca) a política de endosso contidas em um *smart contract*, com as regras de validação estabelecidas pelos participantes da rede.

Uma vez validada, a transação é combinada com outras transações para criar um novo bloco de dados para o “livro-razão”, iniciando a **Fase de Atualização dos Dados**.

Nessa última fase, o novo bloco é adicionado à rede *blockchain* de forma permanente e inalterável, completando a transação e atendendo assim a premissa dessa fase.

A visão da estrutura de dado dentro dos blocos do modelo proposto tem a seguinte modelagem:

Figura 22 - Visão da estrutura dos dados nos blocos da *blockchain* para registro de atestados



Fonte: Autoria própria (2019).

Na **Figura 22** (acima), se observa que o “cabeçalho” do bloco contém um *Hash* criptografado abrangendo as informações do bloco atual. Se esse bloco for o bloco 0 (zero), o *hash* terá a utilidade de identificar o bloco “gênese”, que marcará o início da rede de blocos.

O Cabeçalho ainda conterá o *hash* do bloco anterior com todo o seu conteúdo criptografado, e ainda associando nele o conteúdo do novo atestado. Isso garantirá a segurança de toda a cadeia de blocos, pois cada novo bloco terá a “herança” dos dados criptografados dos blocos anteriores.

Além do cabeçalho, o bloco conterá o *hash* com o conteúdo do atestado corrente, o *nonce* (um número aleatório que fará a autenticação da transação atual não ser mais utilizada posteriormente) e a transação solicitada.

Ao finalizar toda a transação, os participantes da rede são notificados, podendo atualizar a cadeia de blocos (*blockchain*) em seus “nós”.

Comparativamente, as principais características que envolvem o processo atual de emissão e registros de atestados médicos-odontológicos, e o modelo proposto, é mostrado no **Quadro 24**, a seguir:

Quadro 24 - Comparativo entre processo atual de emissão de atestados e o modelo proposto

	Processo atual	Modelo proposto
Forma de emissão	Escrito a punho, ou impresso por meio de <i>softwares</i> de consultórios.	Sempre por uma Aplicação cliente (<i>software</i> de consultório, aplicativos de celular, plataformas <i>web</i> etc.).
Forma de registro	Em ficha própria ou receituário médico. (RESOLUÇÃO CFM N° 1.658/2002).	Dados registrados em rede <i>blockchain</i> .
Rastreabilidade	Localizada e limitada à busca em armazenamento físico; Avaliação um a um.	Registrado em rede distribuída <i>blockchain</i> ; Distribuído entre os participantes da rede.
Autenticidade	Difícil de comprovar de forma objetiva.	Identificação do documento (ID) por <i>Hash</i> criptografado, com todas as informações do atestado e do profissional que o emitiu.
Segurança	Difícil de assegurar a veracidade; Frágil por ser fácil de falsificar.	Registro inviolável em rede <i>blockchain</i> .
Meio de leitura	Física.	Digital.
Modo de consulta	Leitura em documento físico.	Leitura por meio digital.
Modo de acesso	Busca e coleta de documento físico ou registro em banco de dados local (digitação posterior à emissão manual).	Acesso à rede de registros <i>blockchain</i> por meio de aplicação cliente.
Meio de recepção	Através do paciente, portador do documento.	Pelo paciente; Consulta pelo ID do Atestado / <i>download</i> da imagem espelho do documento direto na rede <i>blockchain</i> através de uma aplicação cliente.
Pontos fortes	Praticidade na emissão; Não depende de meios tecnológicos	Minimiza a exposição de médicos e cirurgiões-dentistas em documentos

	Processo atual	Modelo proposto
	para ser emitido; Normatizado e regulamentado.	falsificados; Ajuda no combate aos prejuízos de entidades empregadoras; Oferece um modelo regulador para a emissão e uso do documento, por meio de tecnologia.
Pontos fracos	Alta facilidade de falsificação; Difícil validação de autenticidade; Difícil rastreabilidade.	Dependem 100% de infraestrutura e meios tecnológicos; Em caso de falha de tecnologia ou infraestrutura, deverá ser emitido em contingência; Não regulamentado.

Fonte: Autoria própria (2019).

O **Quadro 24** (acima) demonstra que o processo atual de emissão de atestados limita-se a meios físicos, mesmo quando são utilizados *softwares* de consultórios para emitilos de forma impressa.

Por esse motivo, características como a forma de registro, acesso, leitura, consulta e meio de recepção do documento tendem a se tornar frágeis.

Pelo mesmo motivo, as características relacionadas à rastreabilidade, autenticidade e segurança tendem a ser vulneráveis facilitando a falsificação do documento. No entanto, se trata de um processo regulamentado com normas legais previstas assegurando a sua regulação.

No caso do modelo proposto por essa pesquisa, toda relevância da sua característica está ligada e assegurada por aspectos tecnológicos, oferecendo um modelo regulador para a emissão e uso do documento por meio de tecnologia.

5.3 Modelo de arquitetura para o protótipo

Um protótipo é um modelo criado com a finalidade de testar uma hipótese, um produto, um serviço ou modelo. Geralmente é construído em fase de testes ou planejamento de um projeto quando ainda não se sabe se o objeto proposto pode dar certo.

A finalidade do protótipo desenvolvido nesse projeto é realizar um teste de conceito e aprendizado diante de um cenário de incertezas e a validação dos modelos de processos de negócio proposto nessa pesquisa, limitando-se a um sistema mínimo viável sem grandes funcionalidades inteligentes.

No entanto, o modelo, regras e arquitetura propostas a seguir poderão dar suporte ao

desenvolvimento futuro de um sistema completo que se proponha a atender a demanda.

5.3.1 Regras de negócio e requisitos funcionais

As regras de negócio elencadas a seguir refletem as premissas, critérios e restrições que envolvem a operação de funcionamento do protótipo desenvolvido para validar o modelo proposto nesse estudo.

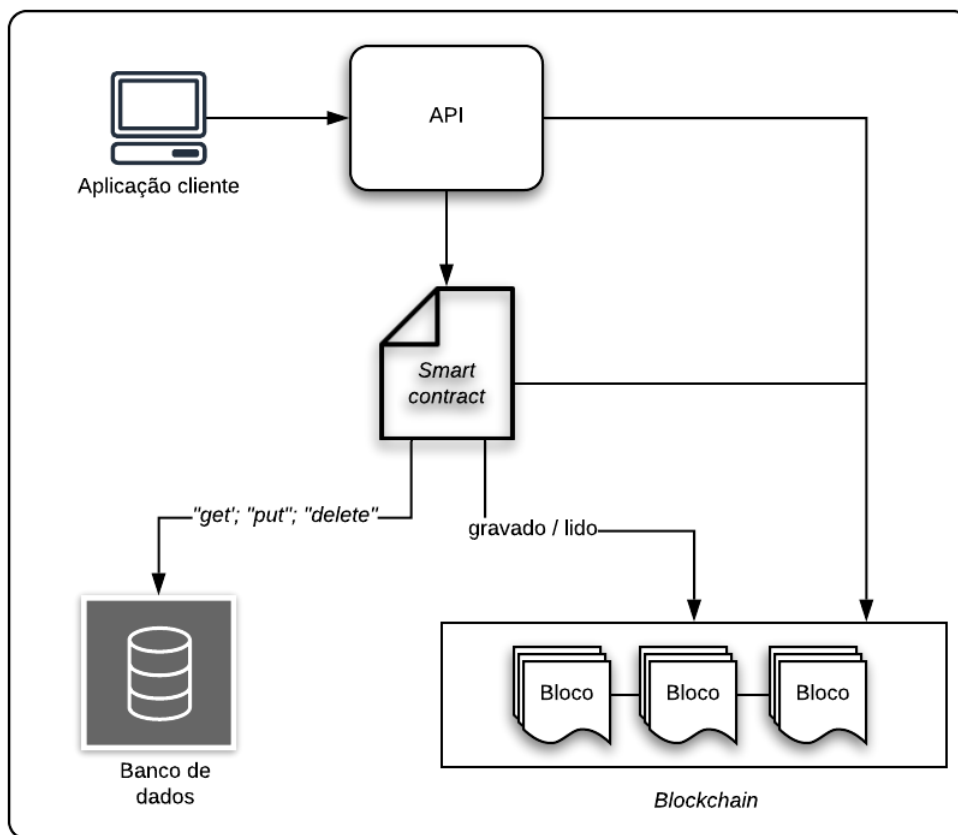
Compreendem o que o sistema fará para atender as necessidades e exigências definidas, e como um requisito funcional se comportará. Estes, são elencados de forma a descrever as ações que, uma vez implementadas, comporão as funcionalidades do protótipo.

As premissas iniciais dos requisitos do Protótipo estão baseadas em cinco elementos fundamentais:

- a) **API** – responsável pela integração entre o *Software* Cliente e a plataforma.
- b) **Smart contract** – *chaincode* contendo todas as regras de consenso para a validação do registro que estiver sendo gravado ou consultado;
- c) **Banco de dados relacional** – repositório de apoio à *blockchain*, utilizado para armazenar os dados de identificação dos participantes da rede (Médico/Cirurgião-dentista, e Entidade Utilizadora), o ID (Identificador) e o *status* do atestado.
- d) **Blockchain** – utilizada para criar uma rede de registros, armazenando os dados do Atestado Médico-Odontológico emitido por *hash* criptográfico de forma definitiva.
- e) **Aplicação Cliente** – *Software* Cliente utilizado pelo usuário para interagir com a rede de registros de atestados.

Essas premissas estão representadas na **Figura 23**, a seguir:

Figura 23 - Fundamentos da arquitetura do Protótipo



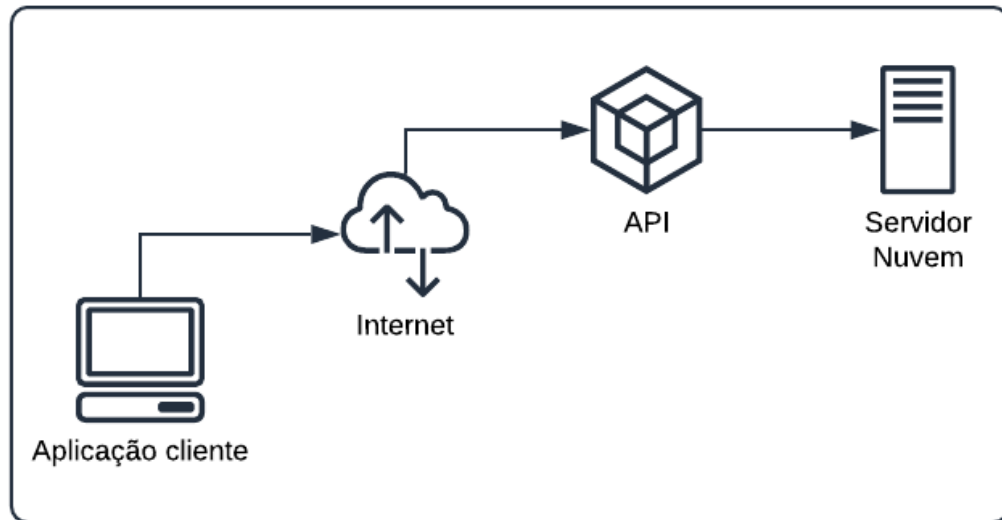
Fonte: Autoria própria (2019).

Conforme mostrado na figura acima, uma aplicação cliente se comunicará com a plataforma através de uma API.

As requisições da aplicação cliente serão verificadas e validadas pelas regras contidas no *Smart contract*. Se as requisições estiverem em conformidade com as regras, as operações serão disparadas para atender à requisição da aplicação (consultar ou gravar).

Entretanto, previamente a qualquer tipo de conexão para requisição, a aplicação cliente deverá primeiramente checar a atividade da plataforma de modo a retroalimentar o usuário quanto à disponibilidade do serviço, conforme mostrada na **Figura 24**, a seguir:

Figura 24 - Verificação de atividade da Plataforma



Fonte: Autoria própria (2019).

A figura acima mostra as etapas dessa operação sendo disparada a partir da aplicação cliente através da *internet*. A API será a responsável por receber a solicitação, obtendo o estado do serviço no servidor em nuvem, realizando o *feedback* em seguida, para a aplicação cliente.

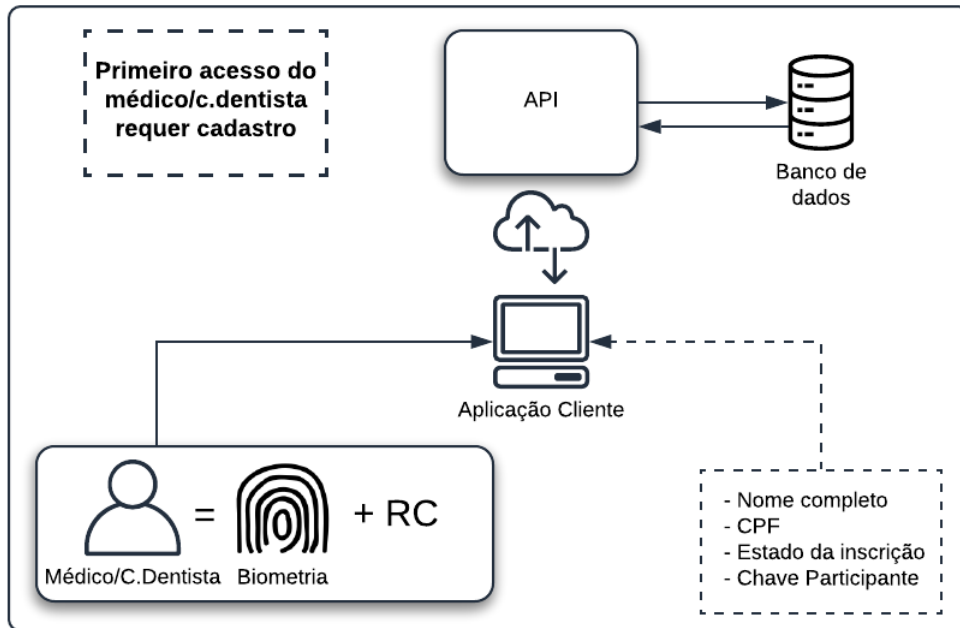
Caso a plataforma não esteja disponível, a aplicação cliente tratará a exceção informando ao cliente sobre o ocorrido.

A) Operações de gravação na plataforma

Uma vez disponível, a aplicação cliente solicitará do médico/cirurgião-dentista os caracteres do seu Registro junto ao Conselho Regional (RC) e coletará a sua digital através de um leitor biométrico, enviando os dados para a plataforma.

Caso o médico/cirurgião-dentista esteja acessando pela primeira vez, o sistema solicitará os dados cadastrais para registrá-lo em sua Base de Dados, conforme mostrado a seguir:

Figura 25 - Primeiro acesso: Cadastramento do médico/cirurgião dentista



Fonte: Autoria própria (2019)

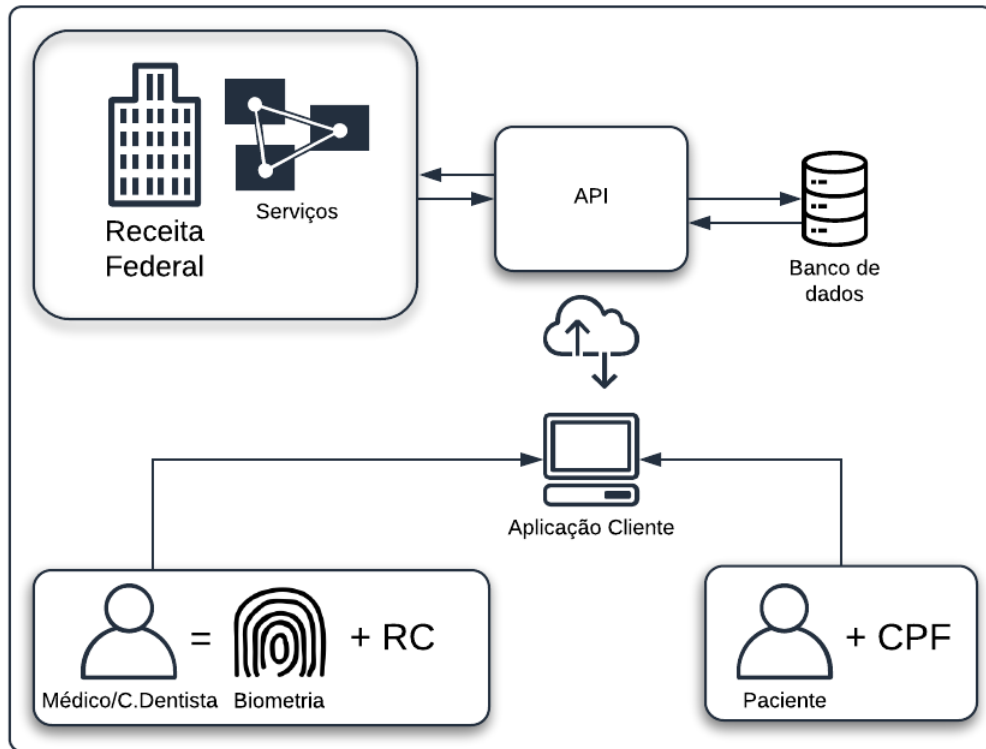
Para garantir que o documento (atestado) contenha um médico associado, a plataforma precisa identificá-lo. Esse procedimento acontecerá toda vez em que um atestado for emitido pelo profissional de medicina através da aplicação cliente, que enviará os dados coletados para a plataforma.

Caso a identificação do médico ou cirurgião-dentista ainda não exista no Banco de Dados, a plataforma exigirá seu cadastramento sendo que esse procedimento só ocorrerá uma vez, no momento em que houver o primeiro acesso para emissão do primeiro atestado na plataforma.

Em um momento seguinte, quando outro documento for emitido pelo médico/cirurgião-dentista, a plataforma apenas o identificará através do seu RC e da sua chave de participante da rede, verificando a existência dessas informações no Banco de Dados da plataforma. Uma vez validadas, essas informações serão associadas ao atestado.

Em ambas as situações, o passo seguinte será solicitar o CPF do paciente para que também seja associado ao documento, conforme mostrado na **Figura 26**, a seguir:

Figura 26 - Identificação do médico/cirurgião-dentista e paciente, e recepção dos dados obrigatórios



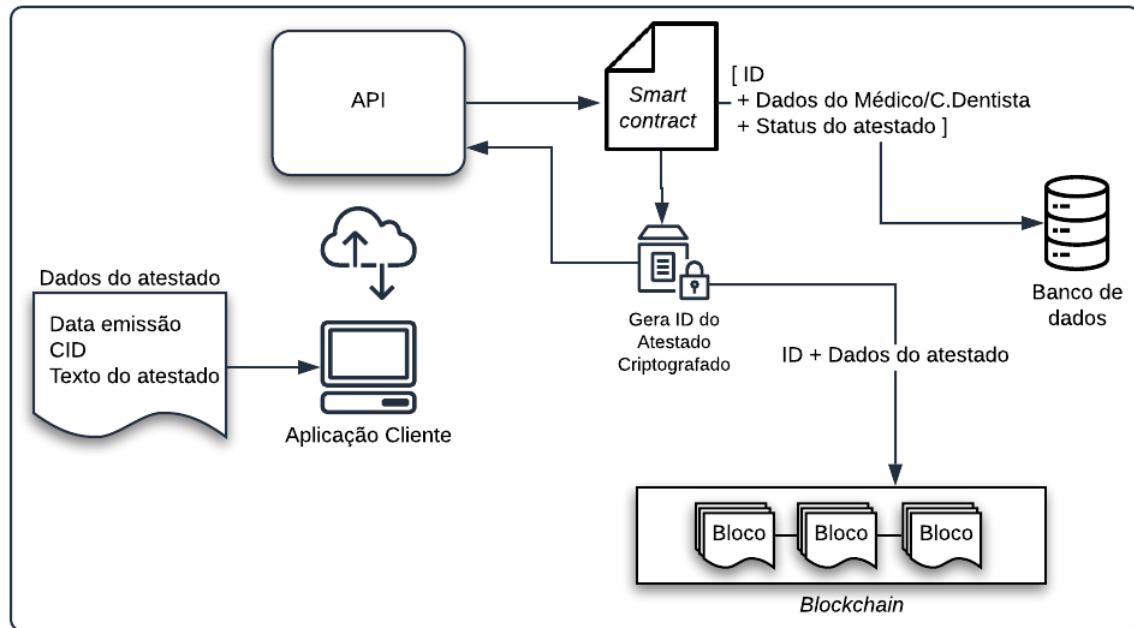
Fonte: Autoria própria (2019).

Pode-se observar, conforme a figura acima, que após a coleta das informações para a identificação do médico/cirurgião-dentista, o CPF do paciente será verificado junto à Receita Federal, validando a sua existência e autenticidade.

Uma vez validado, a plataforma solicitará os dados obrigatórios que compõem um atestado médico-odontológico:

- Data de Emissão;
- Código de Identificação da Doença – CID
- Texto escrito pelo médico ou cirurgião-dentista para o corpo do atestado.

A **Figura 27**, a seguir, demonstra essa e as demais operações para a gravação do documento.

Figura 27 - Operação de registro do atestado

Fonte: Autoria própria (2019).

Ao coletar os dados obrigatórios do atestado, a aplicação cliente envia-os para a plataforma que procederá com execução das regras de consenso contidas no *Smart contract*.

Uma vez em conformidade com as regras de consenso, a sistema (protótipo) gerará um Identificador (ID) criptografado que será associado ao atestado como seu registro de identificação única. Esse registro (ID) será utilizado posteriormente para a consulta da existência do documento.

O procedimento seguinte será a gravação de todos os dados coletados na *blockchain*, sendo gravado no banco de dados de apoio apenas a ID do documento acrescido dos dados de verificação do médico/cirurgião-dentista e o *status* de “NÃO UTILIZADO”, significando que o atestado ainda não foi utilizado por nenhuma Entidade Utilizadora.

A plataforma informará a ID do atestado à aplicação cliente, finalizando a operação.

B) Operação de consulta e utilização do atestado

A operação de utilização consiste em consultar a existência e a utilização do atestado. Essa operação será solicitada por uma Entidade Utilizadora que poderá ser qualquer entidade pública ou privada que necessite comprovar a emissão e autenticidade do atestado apresentado por um indivíduo à entidade.

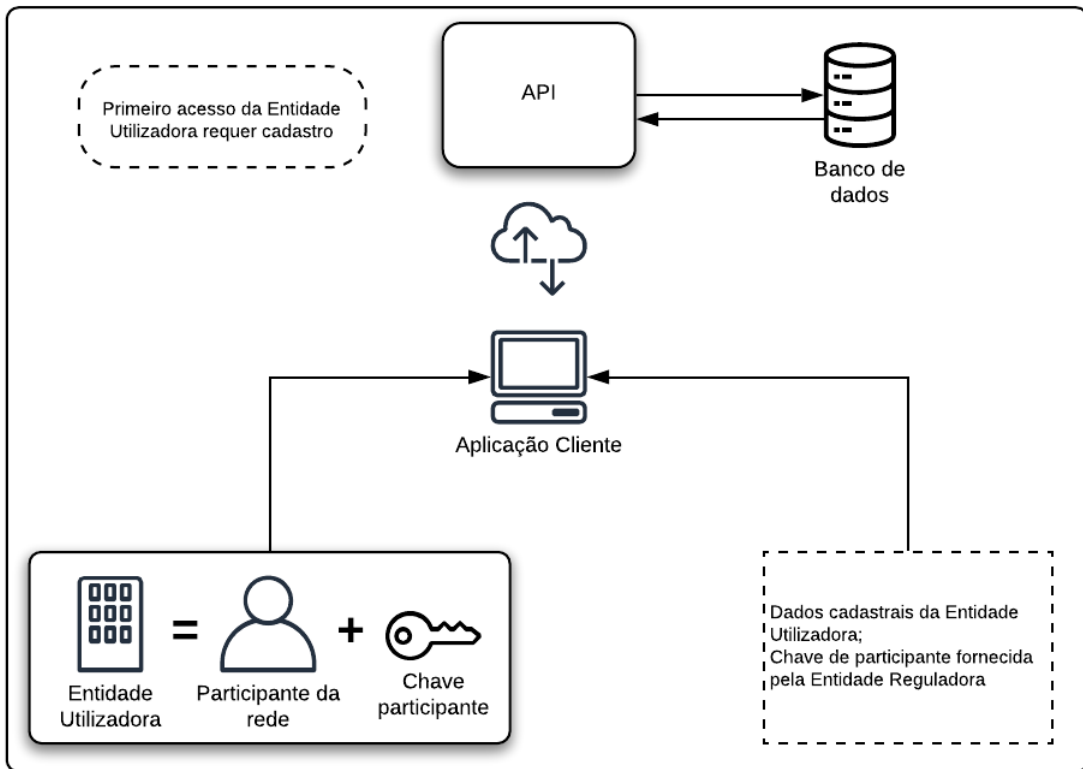
As Entidades Utilizadoras são identificadas como participantes da rede *blockchain*, e

deverão ser credenciadas previamente para ingressar na rede através da Entidade Reguladora.

Os procedimentos e pré-requisitos para esse credenciamento estão fora do escopo desse projeto, porém é recomendada a emissão de uma Chave ou Certificado de Participante da Rede como identificação única que comprove e identifique a Entidade Utilizadora como devidamente credenciada e apta a participar da rede.

De posse dessa Chave de Participante da Rede, a Entidade Utilizadora poderá realizar o seu cadastramento na rede na primeira vez em que acessar a plataforma. A **Figura 28**, a seguir, mostra essa operação.

Figura 28 - Primeiro acesso e cadastramento da Entidade Consumidora



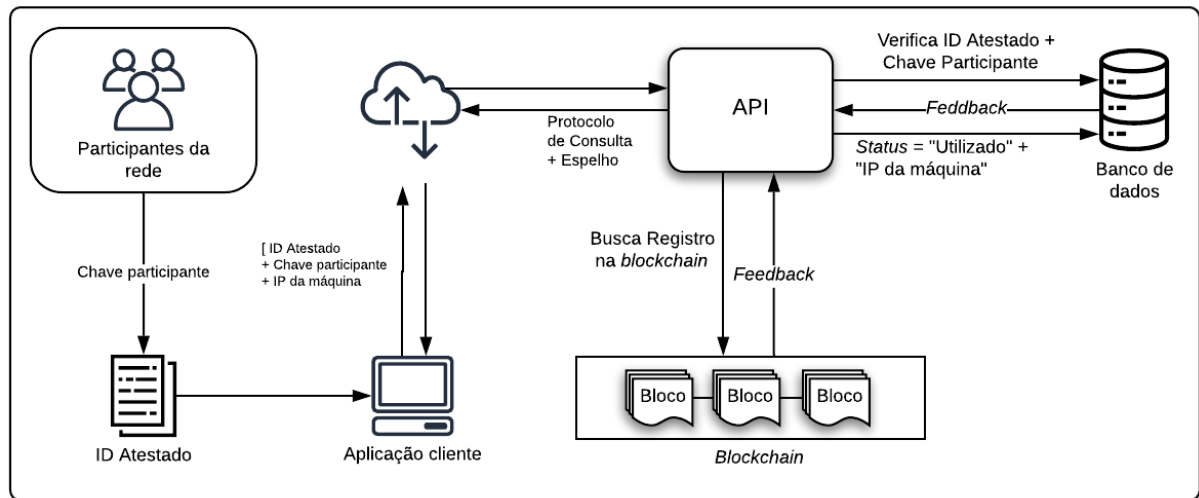
Fonte: Autoria própria (2019)

Como mostrado na **Figura 28**, acima, quando uma Entidade Utilizadora fizer um acesso para a consulta/utilização de um atestado pela primeira vez, a plataforma exigirá os seus dados cadastrais e a Chave de Participante da Rede.

Esses dados serão devidamente registrados no banco de dados de apoio da solução, de modo a serem utilizados posteriormente para consultas futuras.

Para consultar e utilizar um atestado, a Entidade Utilizadora, após a sua identificação ou cadastramento, deverá informar a ID do atestado. Essa operação é mostrada na **Figura 29**, a seguir:

Figura 29 - Consulta e utilização do atestado médico



Fonte: Autoria própria (2019)

Nessa operação, a plataforma também coletará o endereço de IP (Protocolo de *Internet*) da máquina ou dispositivo de onde saiu a requisição de modo a garantir a comprovação da sua origem, caso haja necessidades futuras.

De posse das informações (Chave + ID Atestado + IP), a API fará a busca no banco de dados realizando, primeiramente, a identificação da Entidade Utilizadora através da Chave de Participante informada.

Em seguida, fará a busca da ID do atestado, realizando a gravação do endereço de IP acrescido da Chave de Participante no registro, associando essas informações ao atestado. Por fim, a plataforma mudará o conteúdo do campo “*status*” do documento para UTILIZADO.

O passo seguinte será buscar e coletar o conteúdo do atestado na *blockchain*, construindo um “espelho” do documento, retornando essas informações.

Ao final da operação, a plataforma gerará um protocolo de consulta e informará a Aplicação Cliente junto com o “espelho” do documento consultado/consumido.

5.3.2 Modelo de arquitetura de requisitos por casos de uso

Para a compreensão do comportamento do protótipo no que concerne à arquitetura de requisitos, são demonstrados a seguir casos de uso representados por Diagramas de Casos de Uso.

Os Casos de Uso e os Diagramas de Casos de Uso incorporam a Linguagem Unificada de Modelagem – UML, tratando-se de uma linguagem gráfica utilizada para especificação, elaboração e documentação de artefatos de sistemas complexos de *software* (BOOCH;

RUMBAUGH; JACOBSON, 2006; GUEDES, 2011).


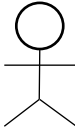



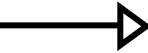


Um Caso de Uso especifica o comportamento de um sistema ou de parte dele, e descreve uma série de sequências de ações que serão realizadas por ele através da interação dos atores que o compõe (BOOCH; RUMBAUGH; JACOBSON, 2006).

Os Atores são os elementos que interagem com o sistema, podendo ser um ator humano ou, eventualmente, um dispositivo ou sistema automatizado, ou até mesmo outro *software* externo (GUEDES, 2011).

Todo o comportamento pretendido do protótipo pode ser interpretado por meio dos diagramas, sem que haja a necessidade da especificação de como esse comportamento será implementado tecnicamente.

Para uma maior compreensão dos Diagramas de Caso de Uso do protótipo, que serão apresentados na sequência, o **Quadro 25** explana os elementos que fazem parte da sua notação e que são utilizados na sua construção.

Quadro 25 - Elementos da notação gráfica de um Diagrama de Caso de Uso

Elemento gráfico	Significado
	Caso de uso.
	Ator.
	Fronteira.
	Nota explicativa (elemento opcional).
	Associação.
	Generalização.
	Extensão
	Conector de nota explicativa.

Fonte: Elaborado a partir de (GUEDES, 2011, p. 53 a 100).

Conforme o quadro acima, os elementos que compõe a notação gráfica são descritos a seguir:

O **Caso de Uso** é representado graficamente pela **elipse**, que contém o texto descrevendo a que funcionalidade o caso de uso se refere, enquanto que o “**bonequinho de palito**” representa um **Ator** – uma pessoa ou um autômato (sistema ou dispositivo) que interage com o protótipo através de uma ação.

O elemento de **Fronteira** é representado pelo **retângulo**, e faz a separação do que é interno e externo ao sistema. Dentro da fronteira, há a representação do cenário do que se está modelando por meio dos casos de uso, além do assunto relacionado ao cenário.

A **Nota Explicativa (retângulo em formato de documento)** contém um texto que explica a razão do uso de uma extensão de um caso de uso.

Os elementos de relacionamento se dividem em:

Associação – representado por uma **linha sólida**, relaciona o Caso de Uso ao Ator que o representa.

Generalização – representado por uma **seta sólida com ponta vazada**, aponta a relação de um Caso de Uso específico com um Caso de Uso geral.

Extensão – representado pela **seta pontilhada com ponta sólida**, aponta uma relação que estende (agrega opcionalmente uma funcionalidade) ou inclui (agrega uma funcionalidade obrigatória) de um Caso de Uso com outro qualquer.

Conector de nota explicativa – representado pela **linha pontilhada**, liga uma nota explicativa a outro elemento de relacionamento.

Os atores que integrantes dos Casos de Uso são:

Médico – Esse ator representa um profissional Médico ou Cirurgião-Dentista que emite o atestado médico-odontológico a partir de um *Software* cliente.

Entidade Utilizadora – Esse ator representa uma empresa ou órgão do setor público ou privado que recebe e utiliza o atestado emitido, e consulta sua autenticidade através de um *Software* cliente.

Paciente – Esse ator representa a pessoa que é o objeto do atestado, e consulta o documento através de um *Software* cliente.

API – Sistema Protótipo que executa as operações solicitadas pelos atores externos, em nível computacional, integrando os *Software* clientes com a rede *blockchain*.

Software cliente – Sistema externo de terceiros que interage com a API, enviando e recebendo os dados de gravação e consulta de atestados da rede *blockchain*.

A metodologia UML recomenda que a documentação explicativa de um Diagrama de

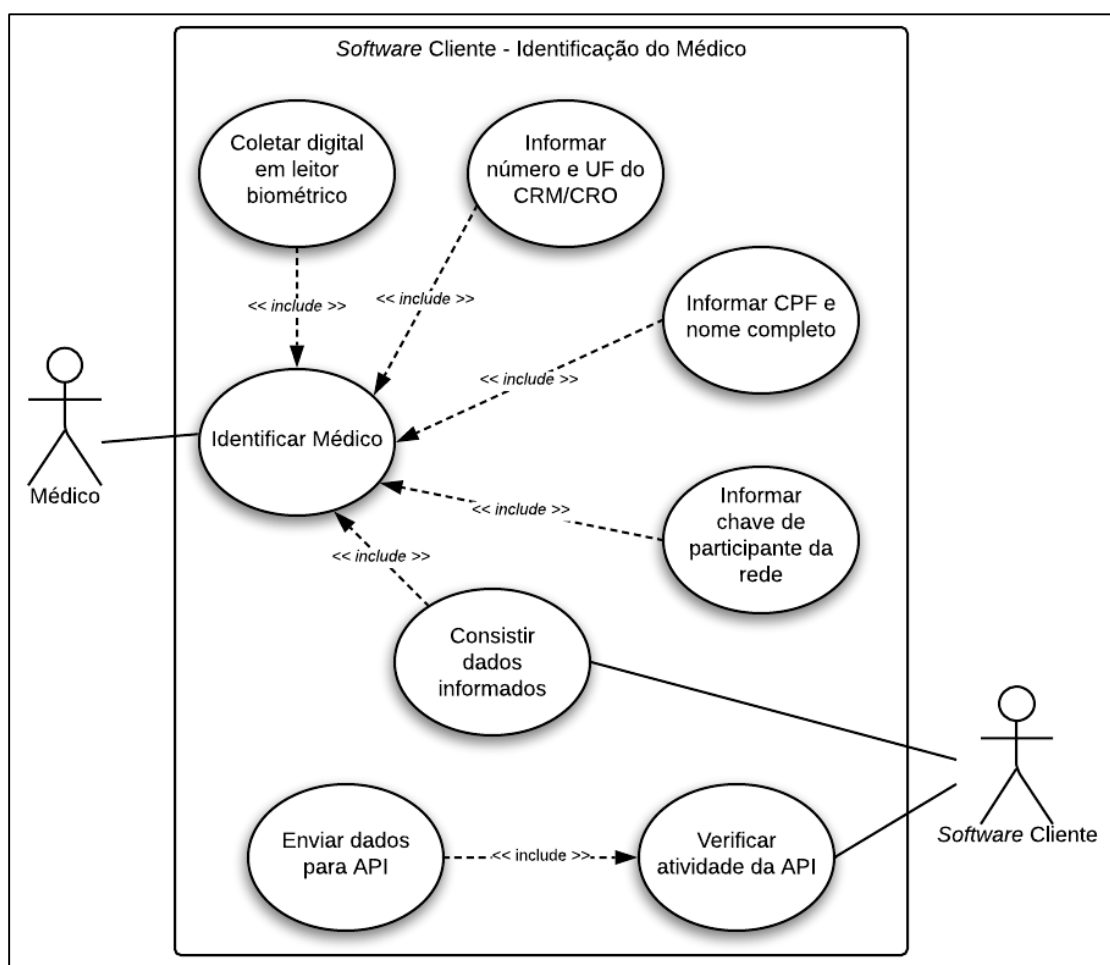
Caso de Uso seja apresentada através de tabelas, contendo essencialmente em seus campos a descrição do Caso de Uso representado pelo diagrama, a especificação dos atores principal e secundários, o resumo descritivo, as pré e pós-condições das ações e a descrição do fluxo principal e alternativos que envolvem a interação dos atores.

No entanto, para esse trabalho, adotou-se o meio textual para a descrição explicativa dos Diagramas apresentados nessa sessão.

Para maior entendimento da integração da API com *Software* Cliente, adotou-se como critério a apresentação de diagramas representando as ações dos Atores dentro do *Software* Cliente, sempre precedendo os Diagramas que envolvem o comportamento da API.

Na sequência são apresentados os Diagramas de Caso de Uso que representam graficamente o comportamento do protótipo e suas respectivas documentações explicativas.

Figura 30 - Diagrama do Caso de Uso Acesso e Identificação do Médico no *Software* cliente



Fonte: Autoria própria (2019).

A **Figura 30**, acima, demonstra o Diagrama do Caso de Uso que descreve as etapas percorridas pelo Médico no *Software* Cliente para realizar a sua identificação à rede de registro de atestados *blockchain*.

Os Atores participantes desse fluxo de comportamento são: o Médico, como Ator Principal que interage com o *Software* Cliente, e o Caso de Uso que, nesse caso, comporta-se como Ator Secundário respondendo às interações do Médico.

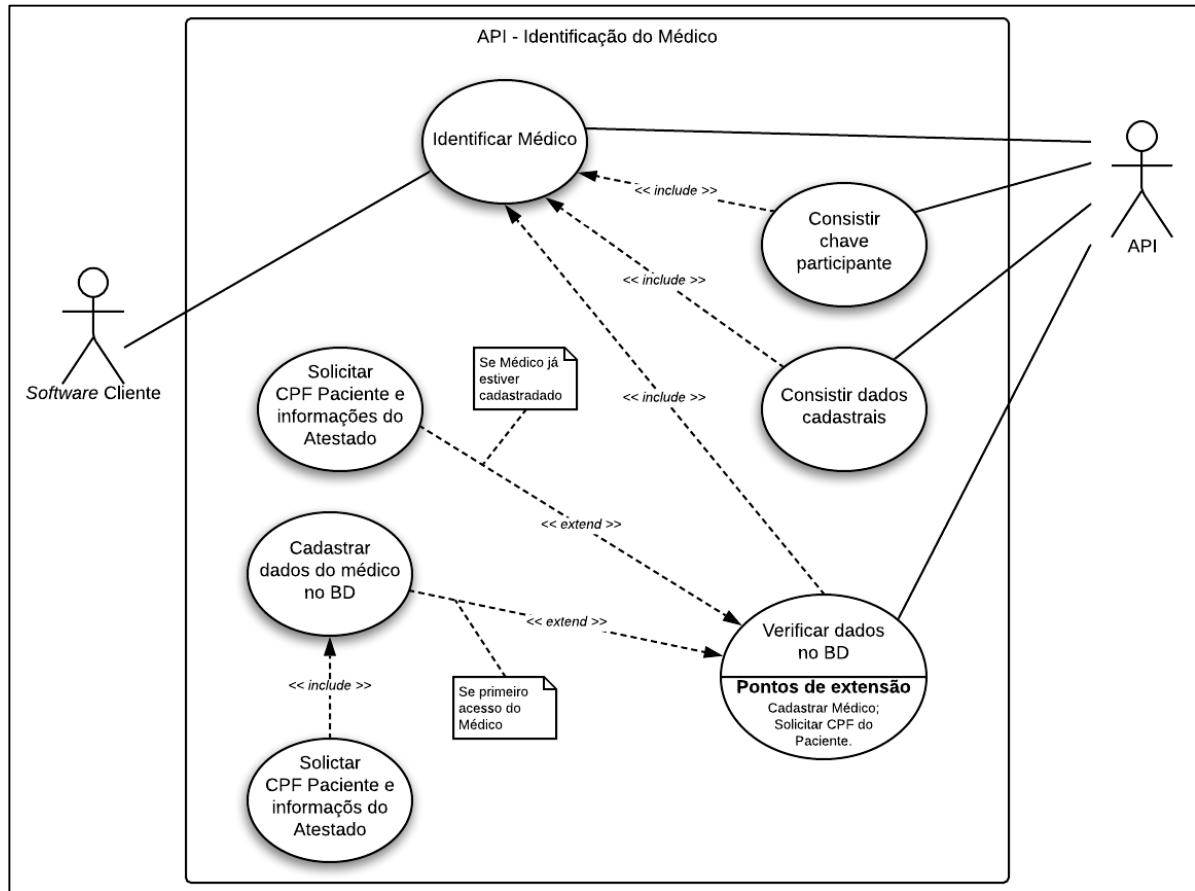
A pré e pós-condição para a execução desse Caso de Uso é que o Médico já possua uma chave de participante da rede e que se cadastre no sistema, caso seja o primeiro acesso à rede, respectivamente.

O fluxo principal ocorre com o Médico realizando a ação de identificar-se no sistema. Essa ação inclui coletar a sua digital em dispositivo biométrico; informar seu registro junto ao Conselho (CRM/CRO) e a Unidade Federativa correspondente ao Registro do Conselho; informar seu CPF e nome completo e, finalmente, informar a sua chave de participante da rede.

Em seguida, o *Software* Cliente deve consistir nos dados informados verificando se os campos estão preenchidos, se estão no formato correto e, finalmente, verificar se a API está ativa. Esta última ação inclui enviar todos os dados para a API.

Na sequência, é demonstrado o fluxo correspondente à identificação do Médico realizado pela API através do Diagrama representado pela **Figura 31**.

Figura 31 - Diagrama do Caso de Uso Identificação do Médico na API



Fonte: Autoria própria (2019).

Conforme a **Figura 31** acima, os Atores envolvidos nesse fluxo de comportamento são o *Software Cliente* como Ator Principal, e a API como Ator Secundário.

O Caso de Uso descreve as etapas percorridas pela API para verificar as informações de identificação do Médico enviadas pelo *Software Cliente* e, na sequência, solicita o CPF do Paciente e as informações do Atestado.

A pré-condição para a execução são os dados enviados pelo *Software Cliente*, enquanto que a pós-condição é solicitar o CPF do Paciente e as ações previstas no Caso de Uso de Inclusão do Atestado, mostrados na sequência.

O fluxo principal prevê que os atores devem identificar o Médico conjuntamente. O Ator Principal (*Software Cliente*) provisionando os dados coletados, e o Ator Secundário (API) realizando as ações de identificação que incluem:

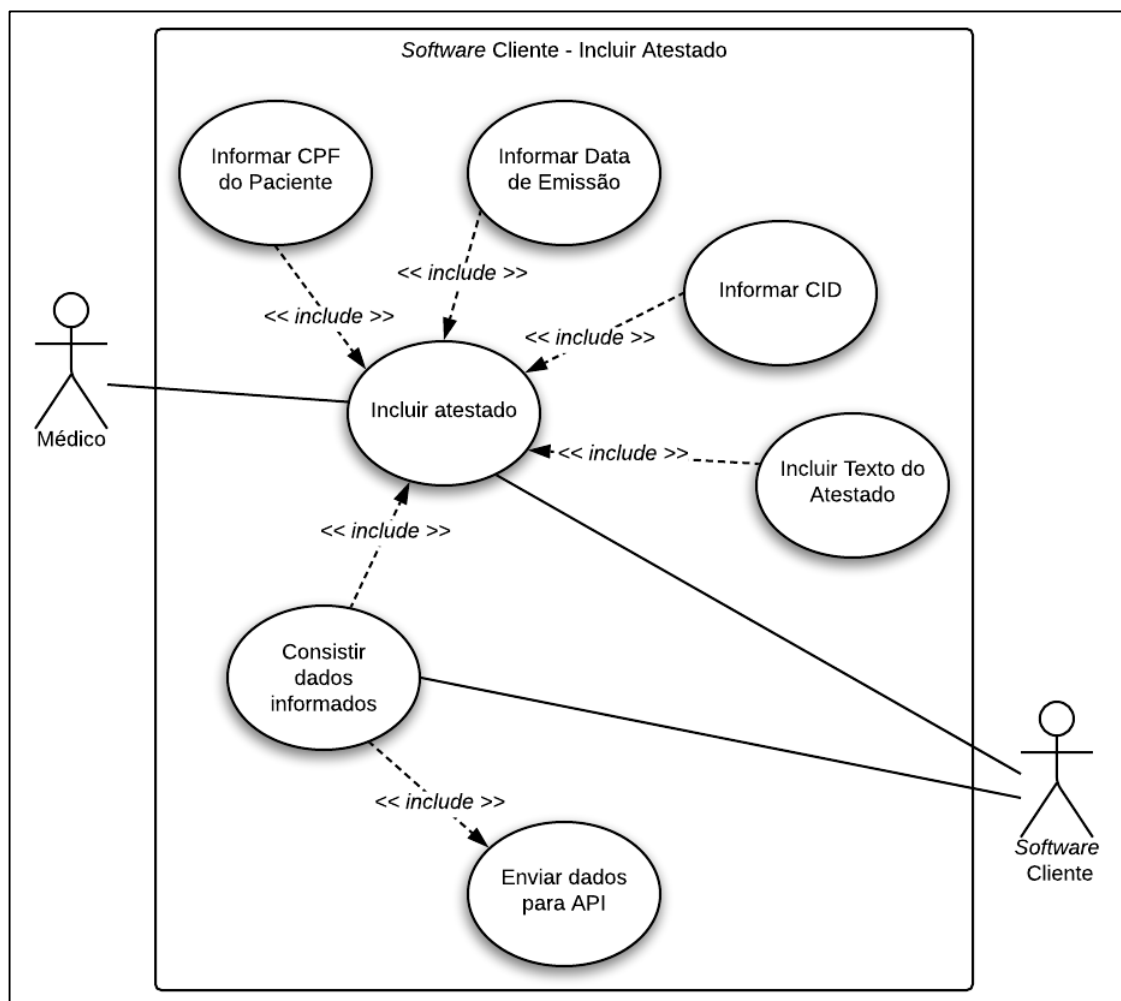
- Consistir na chave do participante verificando se está no formato válido;
- Consistir nos dados cadastrais verificando se estão em formato válido, e se todos os dados necessários para seguir com a próxima ação foram

informados.

Em seguida, a API verifica a existência dos dados informados no Banco de Dados (BD) auxiliar. Caso o Médico não esteja cadastrado, deverá ser cadastrado antes do CPF do Paciente e as informações do atestado serem solicitadas, caracterizando um fluxo alternativo de comportamento do Caso de Uso.

A seguir, a **Figura 32** apresenta o Diagrama de Caso de Uso Inclusão do Atestado, referente ao fluxo de comportamento dentro do *Software* Cliente.

Figura 32 - Diagrama do Caso de Uso Inclusão do Atestado no *Software* Cliente



Fonte: A autoria própria (2019).

De acordo a **Figura 32** acima, o Diagrama de Caso de Uso descreve as etapas percorridas pelo Médico no *Software* Cliente para incluir um novo Atestado que será enviado para a rede *blockchain*.

Os Atores envolvidos nesse fluxo de comportamento são o Médico, como Ator

Principal, e o *Software* Cliente como Ator Secundário.

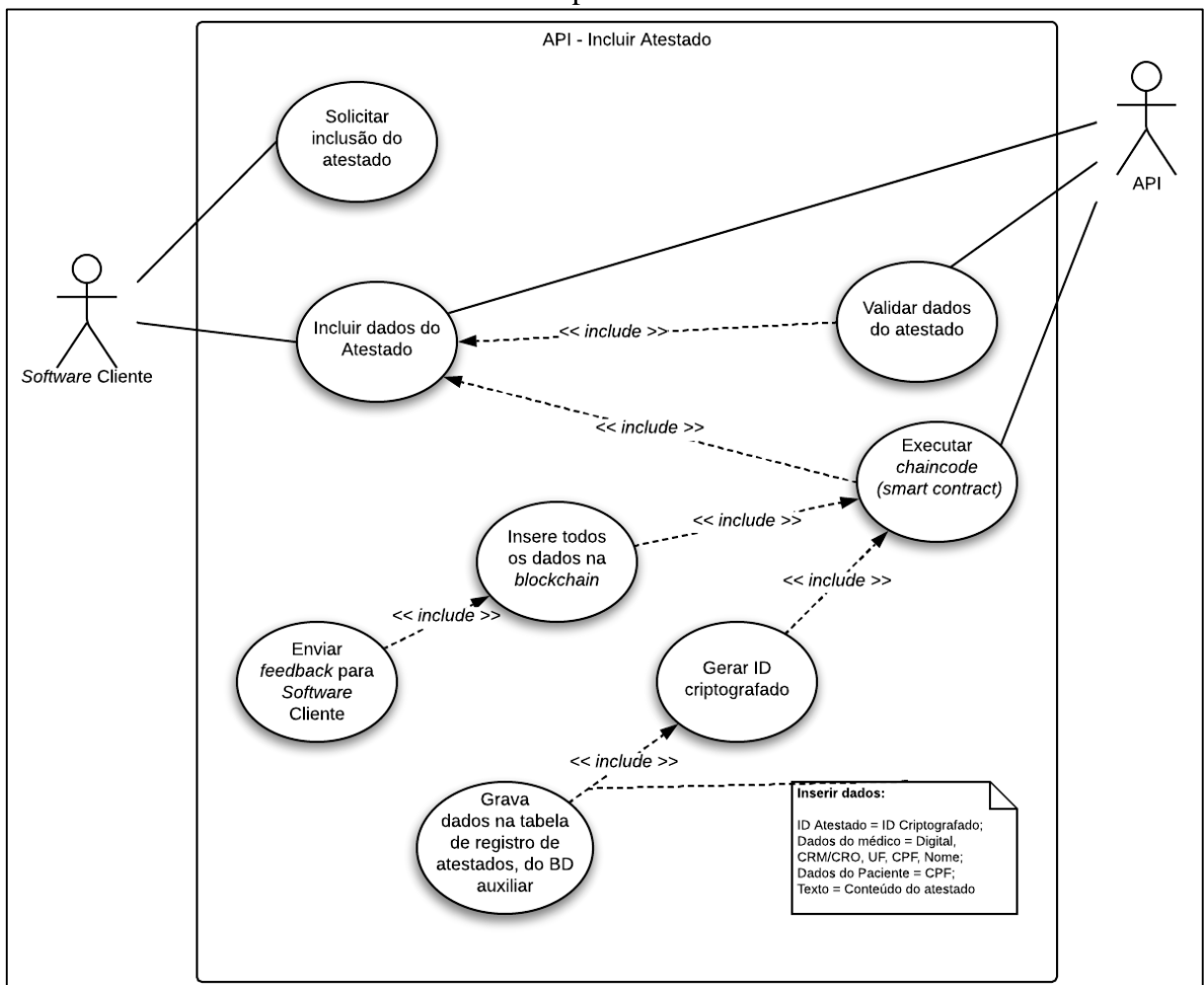
A pré-condição é a execução prévia dos Casos de Uso: Identificação do Médico no *Software* Cliente; Identificação do Médico na API. A pós-condição é expor o resultado da operação para o Ator Principal após o retorno dado pela API.

O fluxo principal prevê que o Ator Principal insira as informações do atestado. Essa ação inclui: informar o CPF do Paciente, a Data de Emissão do documento, a Classificação Internacional de Doenças (CID), e o Texto do Atestado.

Em seguida, o Ator Secundário envia os dados para a API. Essa ação inclui consistir, previamente, nos dados informados pelo médico, verificando se o formato e as informações necessárias estão em conformidade.

A **Figura 33**, a seguir, apresenta o Diagrama de Caso de Uso Inclusão do Atestado: Fluxo de Comportamento na API.

Figura 33 - Diagrama do Caso de Uso Inclusão do Atestado:
Fluxo de Comportamento na API



Fonte: Autoria própria (2019).

O Diagrama apresentado na **Figura 33**, acima, demonstra as etapas percorridas pela API para incluir um novo atestado na rede *blockchain*. Nessa representação, os Atores Principal e Secundário são: o *Software* Cliente e a API, respectivamente.

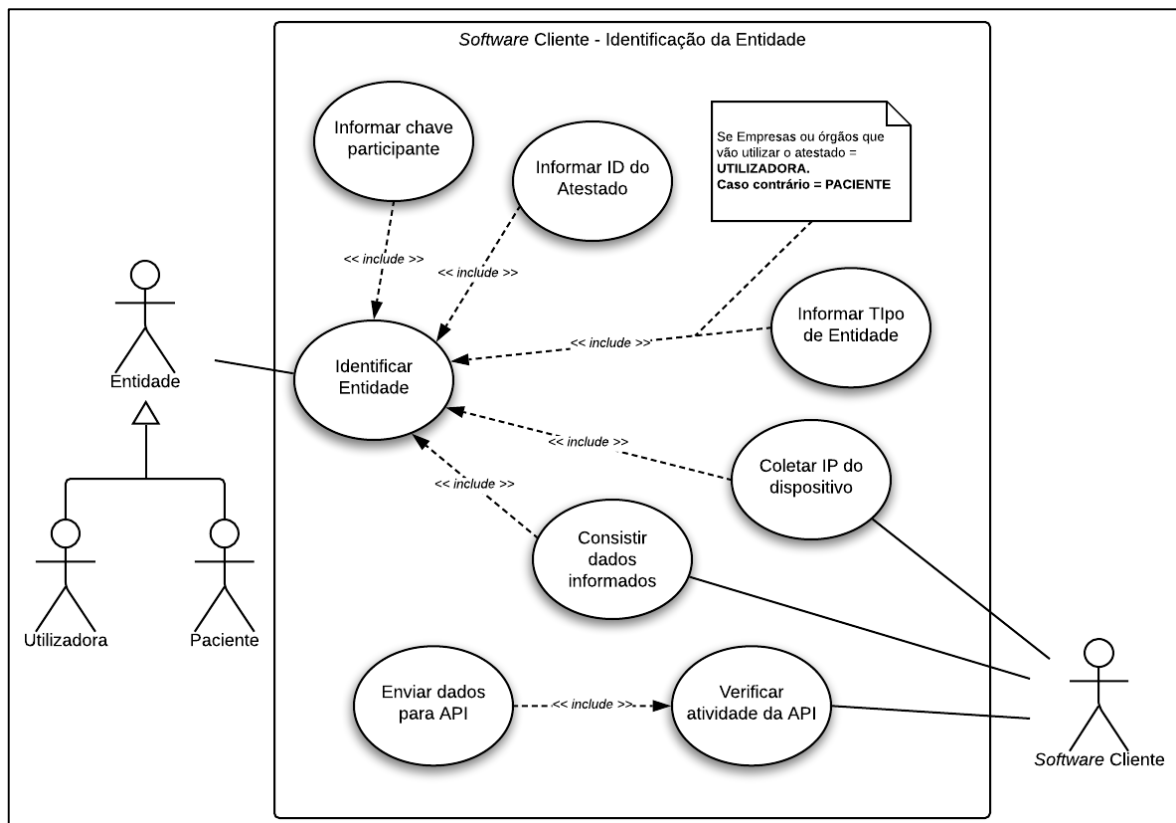
As pré e pós-condições são: ter executado previamente o comportamento do Caso de Uso Inclusão do Atestado no *Software* Cliente, e a API receber o retorno do *Software* Cliente para dar a transação como finalizada.

As ações do Ator Principal no fluxo principal envolvem: solicitar a inclusão do atestado na rede *blockchain* e incluir os dados do atestado. Enquanto que as ações do Ator Secundário envolvem: validar dados do atestado e executar as regras de consenso contidas na *chaincode* (*smart contract*).

Esta última ação inclui ações posteriores: gerar ID criptografada para o atestado; gravar dados da tabela de registros de atestados no BD auxiliar; inserir dados na rede *blockchain*; e enviar retorno para o *Software* cliente.

A **Figura 34**, a seguir, apresenta o Diagrama do Caso de Uso com o fluxo de comportamento no *Software* Cliente que envolve a identificação da Entidade que consulta/utiliza o atestado médico-odontológico digital.

Figura 34 - Diagrama do Caso de Uso Identificação da Entidade no *Software* Cliente.



De acordo a **Figura 34**, acima, o Diagrama de Caso de Uso descreve as etapas percorridas pela Entidade (empresas e órgãos públicos ou privados, e pacientes) que consultam/utilizam um atestado previamente inserido na rede *blockchain*.

Nesse Caso de Uso o Ator Principal compreende dois tipos de Entidade. Uma pode ser do tipo “Utilizadora” (empresas e órgãos públicos ou privados) com permissão para verificarem a autenticidade do atestado e utilizá-lo (consumi-lo administrativamente), ou do tipo “Paciente” (pessoa cuja chave de participante possui apenas permissão para a consulta do atestado).

As pré-condições desse Caso de Uso é que os Casos de Uso de nome: Inclusão do Atestado no *Software* Cliente, e Inclusão do Atestado - Fluxo de Comportamento na API já tenha sido executado.

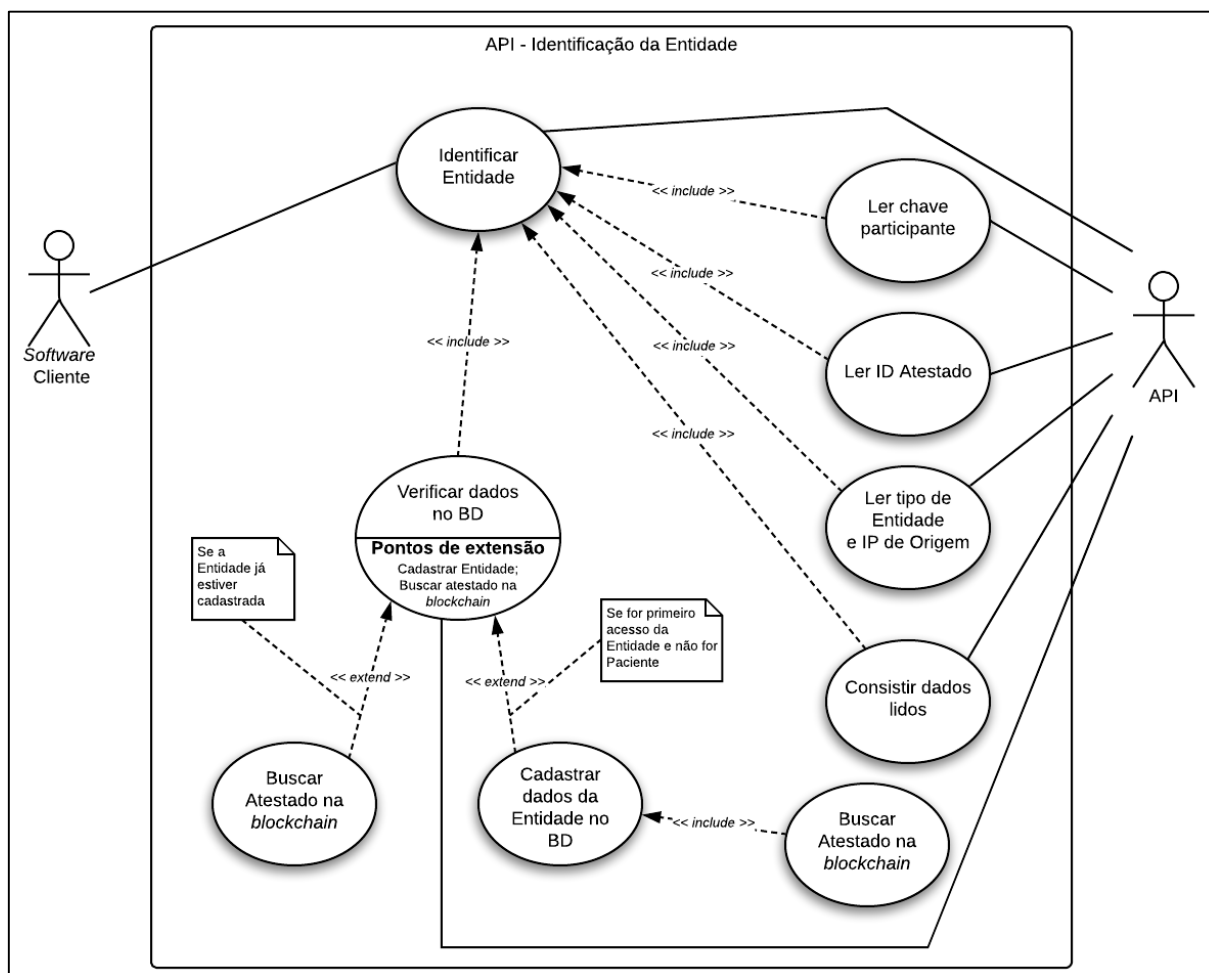
A pós-condição é executar o Caso de Uso Consultar [...], ou “Utilizar” o atestado: operação na API.

No fluxo principal, o Ator Principal deve primeiramente identificar-se no *Software* Cliente. Essa ação inclui informar a Chave de Participante da Rede, o Tipo de Entidade (UTILIZADORA ou PACIENTE), e a ID do Atestado a ser consultado/utilizado.

Em seguida, o Ator Secundário deve coletar todos os dados informados pelo Ator Principal e o IP do dispositivo de onde se origina a solicitação. Na sequência, deve consistir nos dados lidos/coletados para validar se está nos formatos corretos e, finalmente, verificar a atividade da API. Esta última ação inclui enviar dados para a API.

A **Figura 35**, a seguir, apresenta o Diagrama do Caso de Uso Identificação da Entidade: Operação na API.

Figura 35 - Diagrama do Caso de Uso Identificação da Entidade: Operação na API



Fonte: Autoria própria (2019).

O Caso de Uso referente ao Diagrama apresentado na **Figura 35** (acima) descreve as etapas percorridas pela API para consultar/utilizar um atestado, previamente inserido na rede *blockchain* e solicitado pelo *Software Cliente*.

Os Atores Principal e Secundário são o *Software Cliente* e a API, respectivamente. A pré-condição é ter executado o Caso de Uso: Identificação da Entidade no *Software Cliente*. A pós-condição é executar o Caso de Uso Consultar ou o Caso de Uso Utilizar, o atestado: Operação na API.

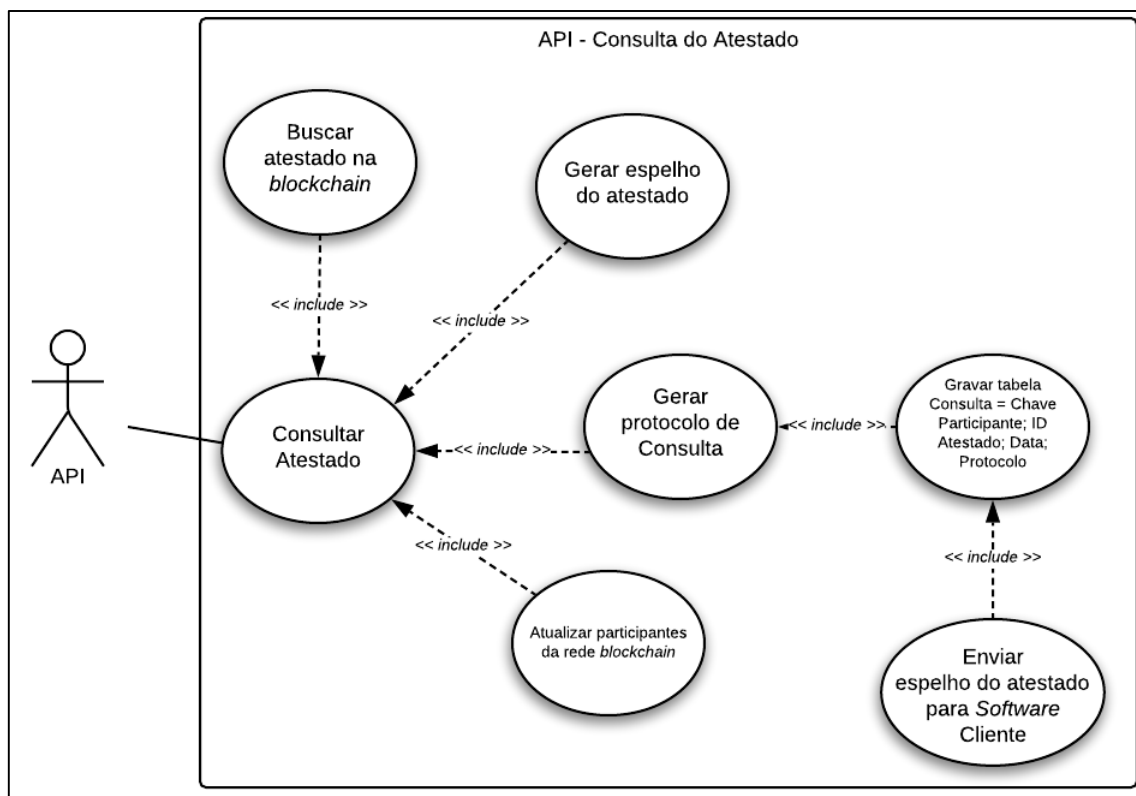
A ação do Ator Principal no fluxo principal é identificar a Entidade passando informações para a API. Em seguida o Ator Secundário deve realizar as leituras da Chave do Participante, do ID do Atestado, do Tipo da Entidade e o IP da Origem.

O passo seguinte do Ator Secundário é consistir nos dados para verificação de irregularidades, verificando os dados no Banco de Dados (BD) auxiliar em seguida. Esta última ação inclui buscar os dados do Atestado na *blockchain*.

Como fluxo alternativo, o Ator Secundário verifica os dados no Banco de Dados auxiliar e cadastra a Entidade, caso seja seu primeiro acesso. O passo seguinte inclui buscar os dados do Atestado na *blockchain*.

O Diagrama do Caso de Uso Consultar Atestado: Operação na API será apresentado na **Figura 36**, em seguida.

Figura 36 - Diagrama do Caso de Uso Consultar atestado: Operação na API



Fonte: Autoria própria (2019).

A **Figura 36**, acima, apresenta o Caso de Uso que descreve os procedimentos internos realizados pela API para recuperar as informações de um atestado, previamente inseridas na *blockchain*.

Nesse Caso de Uso o Ator é a própria API, pois o Diagrama descreve o comportamento da operação interna de busca dos dados realizada por ela.

O fluxo principal compreende o procedimento de consultar o atestado e inclui: Buscar os dados do atestado na *blockchain*; gerar o “espelho” com imagem do atestado construída a partir dos dados; e gerar um protocolo de consulta.

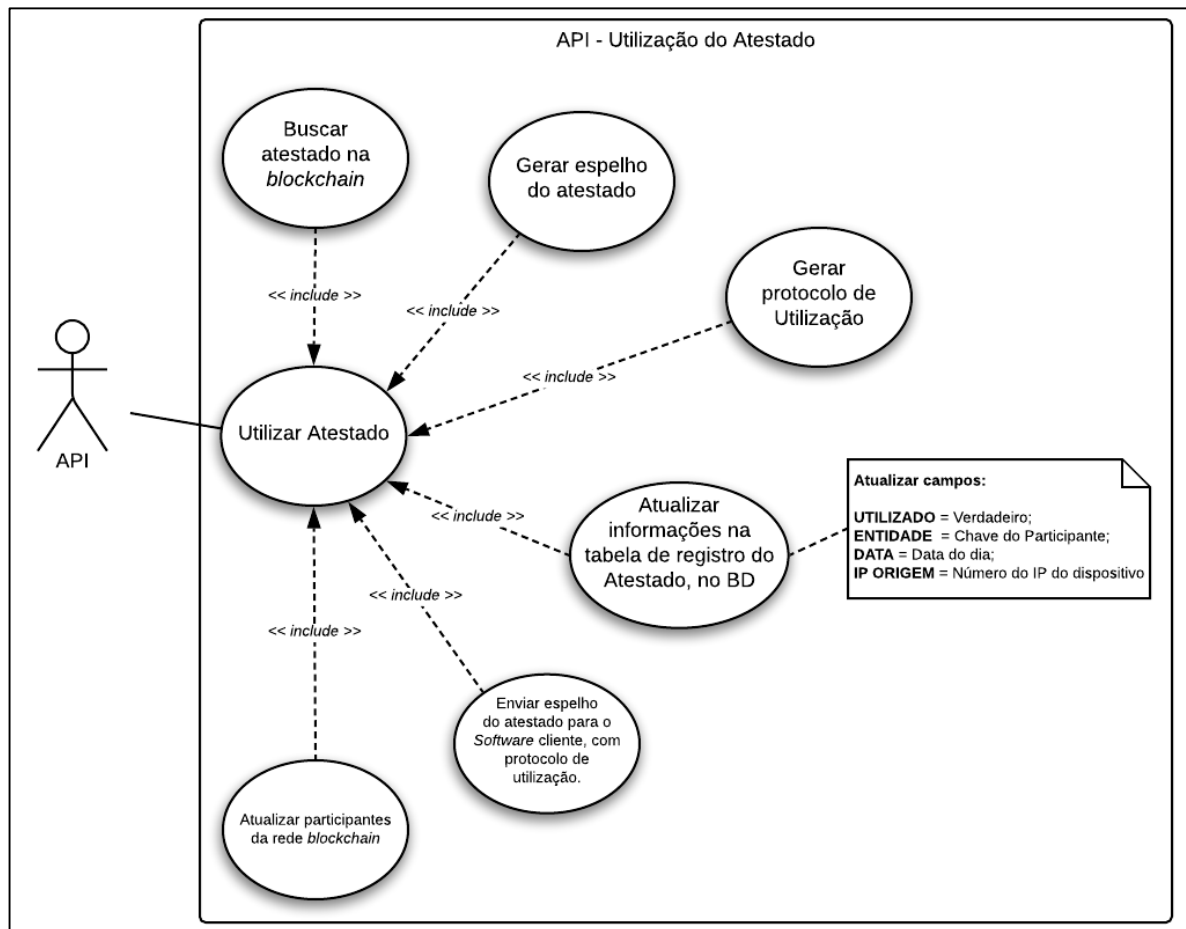
Este último procedimento inclui gravar na tabela “Consulta” os seguintes dados: Chave de Participante; ID do Atestado; Data da Consulta; e Protocolo. Inclui também enviar o

Espelho de Atestado para o *Software* Cliente.

A pré-condição é a execução do Caso de Uso Identificação da Entidade tanto no *Software* Cliente quanto na API. As pós-condições são: obter o retorno do *Software* Cliente e atualizar os participantes da rede sobre a ocorrência.

A **Figura 37**, a seguir, apresenta o Diagrama do Caso de Uso Utilizar Atestado: Operação na API.

Figura 37 - Diagrama do Caso de Uso Utilizar Atestado – operação na API



Fonte: Autoria própria (2019).

Conforme a **Figura 37** (acima), o Caso de Uso descreve os procedimentos internos realizados pela API para recuperar as informações de um atestado, previamente inserido na *blockchain*, e “marcá-lo” como “Utilizado”.

A própria API é o Ator Principal desse Caso de Uso, pois o Diagrama descreve o comportamento internamente realizado por ela para buscar e atualizar o “*status*” do atestado.

As pré-condições são a execução do Caso de Uso Identificação da Entidade, tanto no *Software* Cliente quanto na API e o tipo da Entidade ser obrigatoriamente “UTILIZADORA”.

As pós-condições são: obter o retorno do *Software* Cliente e atualizar os participantes da rede sobre a ocorrência.

O procedimento do fluxo principal é “Utilizar o Atestado” e essa ação inclui: Buscar dados do atestado na *blockchain*; gerar espelho do atestado; atualizar campos da tabela de registro de atestados, conforme a seguir:

- UTILIZADO = VERDADEIRO;
- ENTIDADE = Chave Participante;
- DATA = Data do dia;
- IP Origem = Número do IP do dispositivo que originou a solicitação.

Em seguida, enviar o “Espelho” do atestado e o protocolo de utilização para o *Software* Cliente e atualizar os participantes da rede *blockchain* sobre a ocorrência.

Os Casos de Uso descritos acima apresentam, em linhas gerais, o funcionamento, as atividades executadas, e os eventos de integração com *Softwares* Clientes que disparam a execução de eventos da API.

A finalidade é descrever os passos percorridos diante das requisições de inclusão e verificação de autenticidade de um atestado médico-odontológico em uma rede *blockchain*.

O documento também demonstra Casos de Uso que descrevem os passos que os Atores “humanos” (Médicos e/ou Cirurgiões-dentistas) deverão percorrer em *Softwares* Clientes desenvolvidos por outros programadores, que usufruirão os recursos da API para a complementação de suas aplicações com o mesmo propósito.

No entanto, como o formato de documentação de Casos Usos definido pela UML é bastante flexível, recomenda-se aos programadores que utilizarão os recursos da API, e que farão implementações em suas aplicações clientes com base nesses comportamentos, que a documentação seja complementada por meio de outros diagramas como o de sequência, o de máquina de estados ou de atividade.

5.4 Possibilidades de proteção e Transferência de Tecnologia (TT)

Para a obtenção de uma proteção intelectual é preciso observar as particularidades e os diversos procedimentos que envolvem o processo da realização do pedido.

Esse esforço é necessário para que haja a perfeita compreensão dos mecanismos e possibilidades para a proteção, e de forma que o requerimento contemple todos os elementos legislativos obrigatórios.

Em se tratando do modelo de registro proposto nessa pesquisa, e diante das possibilidades de proteção e transferência da tecnologia fundamentadas no estudo de viabilidade mercadológica (Tópico 4.4.3), os atores envolvidos seriam:

- **Autores:** Inventores da solução proposta nesse estudo;
- **NIT/ICT ou Empresa do setor produtivo:** Entidade encarregada de realizar o processo de proteção junto ao INPI;
- **Empresa do setor produtivo:** Entidade que poderá adquirir os direitos da propriedade intelectual. Exemplo: empresa do mercado produtivo de *software*.

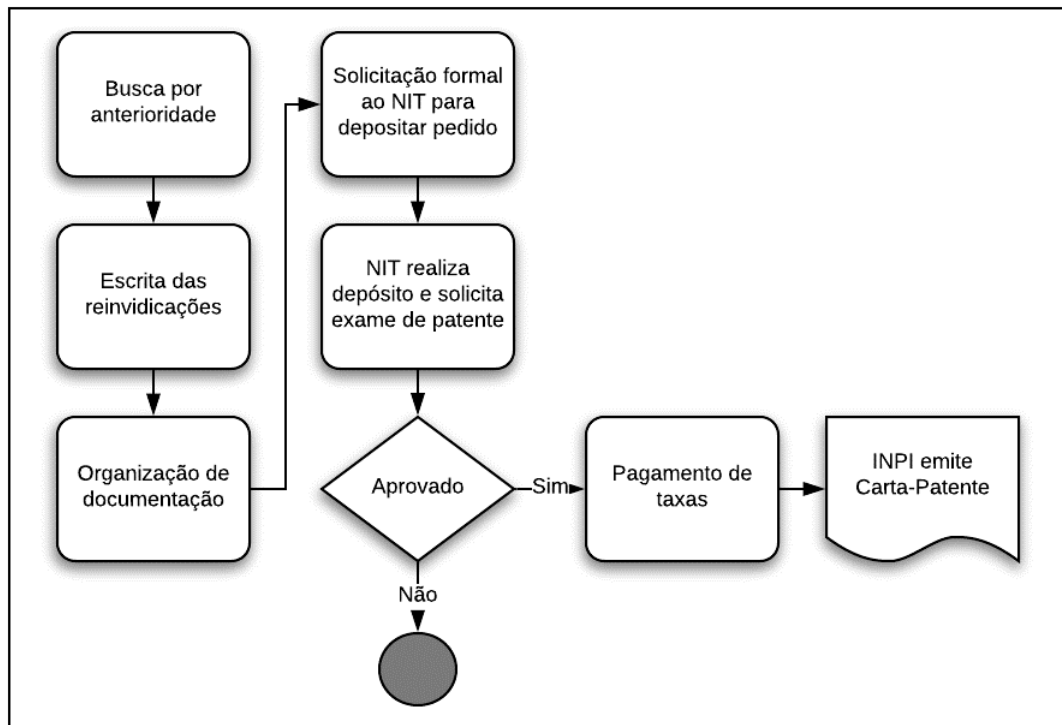
5.4.1 Proteção por patente de invenção implementada por Programa de Computador

A modalidade de Patente de invenção implementada por programa de computador é tratada pela Resolução INPI/PR nº158/2016, que versa:

Processo que utiliza grandezas abstratas para gerar um produto virtual. [...] e que proporcionem efeitos técnicos tais como métodos que otimizam recursos de *hardware* ou que confirmam maior confiabilidade e segurança (Resolução INPI/PR nº158/2016, Tópico 3, Inciso III).

Portanto, a proteção do presente modelo de registro proposto nessa pesquisa poderá seguir a modalidade de Patente de invenção implementada por programa de computador e a sua obtenção poderá ocorrer através do NIT.

Nessa possibilidade, os Atores envolvidos seriam: os Autores, o Núcleo de Inovação Tecnológica (NIT), e o Instituto Nacional de Propriedade Industrial (INPI), conforme a **Figura 38**, a seguir.

Figura 38 - Etapas envolvendo Autores - NIT/ICT - INPI

Fonte: Autoria própria (2019).

Conforme a figura acima, as etapas que perpassam para a obtenção dessa modalidade de patente iniciam-se nos Autores realizando uma busca de anterioridade com o propósito de identificarem no Estado da Arte e no Estado da Técnica o ineditismo do modelo de processo de negócio.

O passo seguinte é a escrita do pedido com o detalhamento da invenção e suas reivindicações para que, em seguida, seja encaminhado formalmente para o NIT/ICT para a realização do depósito e a solicitação do exame da patente junto ao INPI.

Após o exame, caso haja a aprovação, haverá o pagamento das taxas inerentes à solicitação seguida da obtenção da carta de patente ao final do processo, caso não exista irregularidades e não-conformidades.

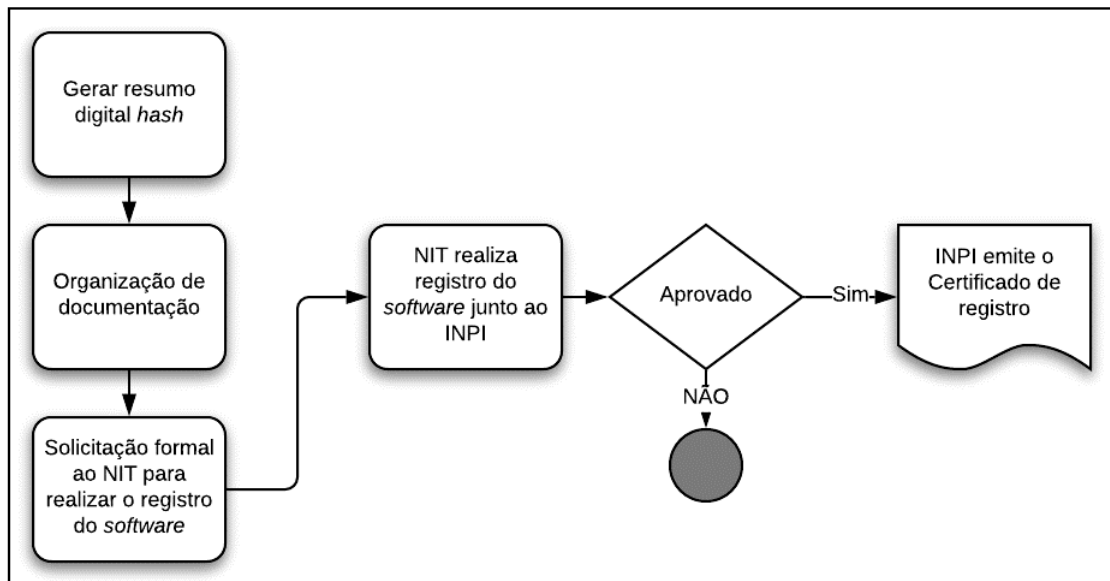
5.4.2 Processo para proteção por Registro de Programa de Computador (RPC)

A seguir são mostradas as duas possibilidades de registro do protótipo desenvolvido (Programa de Computador) que implementa o modelo de registro de Atestados proposto nessa pesquisa.

a) Possibilidade 1: Registro de Programa de Computador (RPC) através do NIT

Nessa possibilidade os Atores envolvidos serão: Os Autores, o Núcleo de Inovação Tecnológica (NIT) e o Instituto Nacional de Propriedade Industrial (INPI).

Figura 39 - RPC: Etapas envolvendo Autores - NIT/ICT - INPI



Fonte: Autoria própria (2019).

Conforme a figura acima, as etapas do registro iniciam-se pela geração do resumo digital *hash*¹⁹, dos trechos do *software* e demais dados considerados suficientes para identificação e caracterização da sua originalidade (código-fonte) que serão objeto do registro.

O passo seguinte será organizar toda a documentação para ser encaminhada ao NIT com a solicitação formal para que o procedimento do registro seja realizado junto ao INPI, através do portal *e-Software*. Caso seja aprovado, o certificado de registro será emitido.

b) Possibilidade 2: Registro de Programa de Computador (RPC) pela Empresa detentora dos direitos

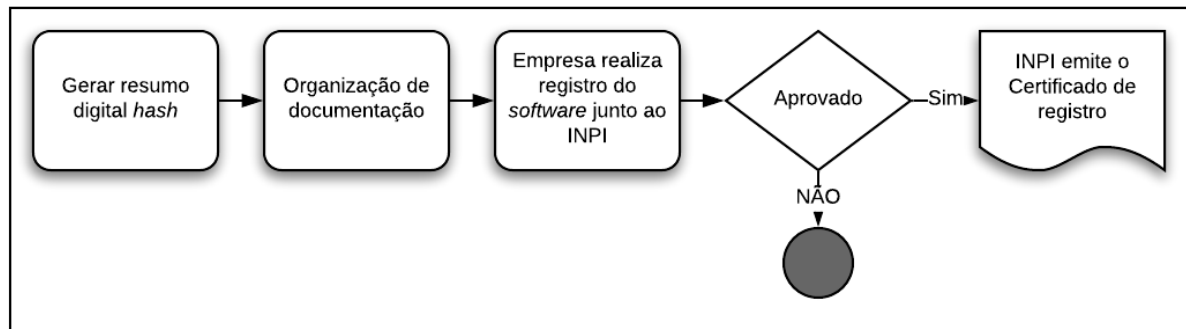
Essa possibilidade já considera uma empresa que tenha adquirido os direitos para uso e exploração da Patente de invenção do modelo de registro implementado por programa de

¹⁹ Segundo o Manual do Usuário para o Registro Eletrônico de Programas de Computador (2019), o *hash* é uma prova eletrônica que pode ser obtida a partir de um único arquivo de entrada, transformado em um arquivo de saída, com extensão “.PDF”, “.TXT”, “.ZIP”, “.RAR”, etc., com um resumo digital (*hash*). É fundamental que este resumo digital *hash* possa ser conferido pelo perito do juiz (em caso de comprovação de autoria/titularidade, por exemplo) tendo como base o código-fonte (arquivo de entrada) guardado em sigilo pelo titular do direito.

computador, através de negociação por contrato de transferência de tecnologia, mas sem que o *software* ainda esteja protegido.

Nessa possibilidade os Atores envolvidos são: A Empresa detentora dos direitos e o Instituto Nacional de Propriedade Industrial (INPI).

Figura 40 - RPC: Etapas envolvendo Empresa - INPI



Fonte: Autoria própria (2019).

Conforme demonstrado na figura acima, a empresa detentora dos direitos gera o resumo digital *hash*, organizando toda a documentação. O passo seguinte será realizar o registro através do portal *e-Software*, gerando o pedido junto ao INPI.

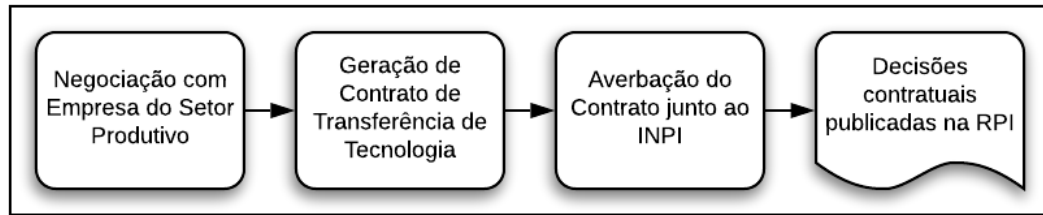
Caso não haja irregularidades, uma vez aprovado, o INPI emitirá o certificado e registro.

5.4.3 Processo para Transferência da Tecnologia

A transferência de tecnologia está prevista, nesse estudo, como uma negociação econômica e comercial que, dessa maneira, atenda a determinados preceitos legais e promova o progresso da empresa receptora e o desenvolvimento econômico do país. Essa negociação envolve a parceria entre as partes envolvidas que se estabelecem através de contrato de transferência de tecnologia.

Por esse instrumento o conjunto de conhecimentos, habilidades e procedimentos aplicáveis ao problema contextualizado são transferidos por transação de caráter econômico de uma pessoa física/instituição a outra, ampliando a capacidade de inovação da organização adquirente.

Em linhas gerais e em todas as possibilidades de Transferência de Tecnologia (TT), demonstradas a seguir, o processo de negociação e transferência passam pelos seguintes passos:

Figura 41 - Etapas da negociação e a transferência da tecnologia

Fonte: Autoria própria (2019).

Como demonstrado na **Figura 41** (acima), o processo de transferência da tecnologia inicia-se pela negociação com uma empresa legítima do setor produtivo que atenda aos requisitos de capacidade técnica e econômica para a produção do objeto da negociação.

Nessa etapa, todos os pré-requisitos, acordos e condições que comporão o instrumento contratual deverão ser negociados.

A etapa seguinte é a geração do documento contratual descrevendo todos os itens negociados na etapa anterior. Deverá também compor o contrato documentos anexos para expressar, determinar e atestar itens relevantes de caráter técnico que se façam necessários para a perfeita elucidação do objeto negociado.

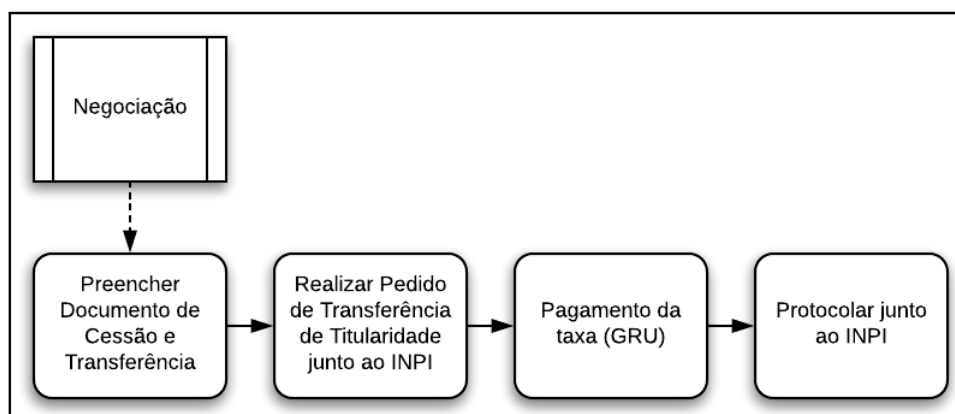
As partes acordadas deverão, então, dar entrada ao processo de averbação do contrato junto ao INPI. Essa etapa formaliza e protocola o instrumento contratual fazendo valer os direitos acordados.

Ao finalizar o processo de averbação, caso todos os requisitos sejam atendidos, o INPI publicará as decisões contratuais da Revista de Propriedade Industrial (RPI) para que o acordo, uma vez formalizado, se torne público.

Diante dessas premissas, as possibilidades de negociação propostas para a transferência da tecnologia desenvolvida nesse estudo são: Cessão dos direitos; Transferência de *know-how*; Licença de uso e exploração. A seguir, o detalhamento das possibilidades:

1) Possibilidade 1: Cessão da titularidade dos direitos

Nessa possibilidade, os Atores envolvidos são: Autores e Empresa do setor produtivo. A **Figura 42**, a seguir, mostra as etapas para esse processo.

Figura 42 - Etapas para a cessão da titularidade dos direitos de proteção

Fonte: A autoria própria (2019).

Conforme demonstrado na figura acima, as etapas de um processo para a cessão de titularidade da proteção são precedidas pela etapa de negociação quando as partes interessadas estabelecem as regras do instrumento de compra e venda, e os acordos econômicos que formalizarão a transferência da titularidade.

Os demais procedimentos são simples e compreendem o preenchimento de um Documento de Cessão de Transferência²⁰ assinado pelo cedente, pelo cessionário e por duas testemunhas.

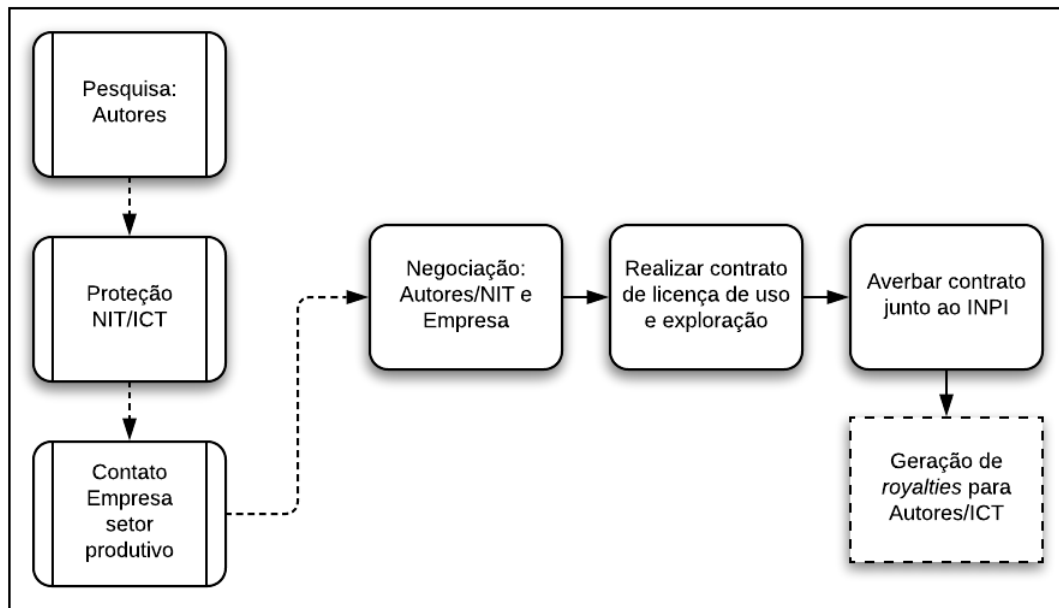
Caso o cessionário seja representado por um procurador, uma procuração em nome do Cessionário deverá fazer parte da documentação.

As etapas finais reúnem o pagamento da taxa (GRU), conforme “TABELA DE RETRIBUIÇÕES DOS SERVIÇOS PRESTADOS PELO INPI” e o protocolo de todos os documentos digitalizados no portal PETICIONAMENTO ELETRÔNICO do INPI.

2) Possibilidade 2: Licença de uso e exploração

Nessa possibilidade os Atores envolvidos são: Autores, NIT/ICT, Empresa do setor produtivo e INPI. A **Figura 43**, a seguir, mostra as etapas para esse processo:

²⁰ Modelo disponível para *download* em: <http://bit.ly/2M5rSDB>.

Figura 43 - Etapas para o licenciamento de uso e exploração dos direitos

Fonte: Autoria própria (2019).

A figura acima demonstra as etapas prévias necessárias para que o processo de transferência de tecnologia através da licença de uso e exploração dos direitos seja realizado.

Ou seja: A pesquisa, realizada pelos Autores; a proteção, realizada pelos Autores e o NIT/ICT; e o contato com a Empresa pleiteante do setor produtivo.

A etapa seguinte é a da livre negociação entre as partes para que sejam determinados os requisitos, termos contratuais e jurídicos, e acordo econômico que comporão o instrumento contratual, sendo a etapa seguinte.

Uma vez o contrato assinado entre as partes, o documento contratual é averbado junto ao INPI para que haja efeito legal dos seus termos, gerando os efeitos acordados de recolhimento de *royalties* para os Autores e ICT.

3) Possibilidade 3: Transferência de *know-how*

Essa possibilidade considera a aquisição do conjunto de informações técnicas que permitam o desenvolvimento de um *software* pela empresa receptora do mercado produtivo, que implemente o modelo de registro de Atestados proposto nesse estudo.

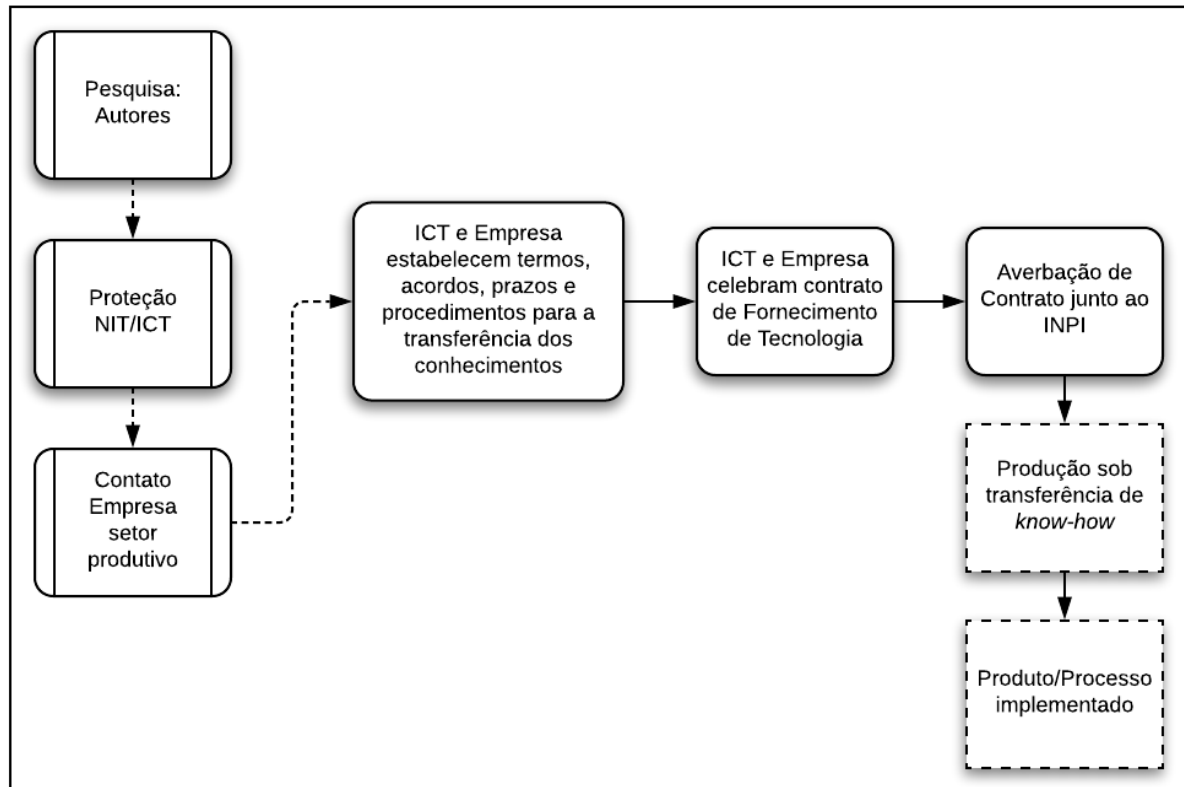
Os Atores envolvidos são: Autores e Empresa do setor produtivo, e poderá ocorrer sob dois possíveis cenários:

1. Transferência de *know-how* pura e simples, envolvendo apenas o “modo de fazer”;
2. Conjugada, quando ocorrer junto a outros fornecimentos de direitos, como a

Cessão de Titularidade ou Licença de Uso e Exploração.

A **Figura 44**, a seguir, demonstra as etapas para a formalização do contrato de Fornecimento de Tecnologia, como instrumento de transferência de *know-how*.

Figura 44 - Etapas para o fornecimento de tecnologia por transferência de *know-how*



Fonte: Autoria própria (2019).

Conforme demonstrado na figura acima, as etapas para a transferência de *know-how* são antecedidas pelas etapas de pesquisa, proteção e contato com empresa do setor produtivo.

As etapas seguintes são iniciadas pela fase onde a ICT e a Empresa estabelecem os termos, prazos e acordos econômicos que comporão o instrumento contratual.

Nessa fase também é elaborado um planejamento e cronograma de atividades para que haja o devido fornecimento do conhecimento tecnológico na fase de produção.

A averbação do contrato finaliza os passos para que haja a formalização dos termos do acordo.

5.5 Processo proposto para a averbação do contrato de transferência de tecnologia

De acordo ao INPI (2019), a Transferência de Tecnologia ocorre através do registro ou averbação de contratos que tratam acordos de direitos de propriedade industrial (marcas, patentes, desenho industriais e topografias de circuitos integrados), e fornecimento de tecnologia, serviços de assistência técnica e franquia.

Partindo desse princípio, o processo para a averbação do contrato da tecnologia proposta nesse trabalho está baseado na Resolução INPI/PR nº 199, de 07 de julho de 2017, que dispõe das diretrizes de exame para averbação ou registro de contratos de transferência de tecnologia dentre outros.

Conforme estabelecido pela Lei de Propriedade Industrial nº 9.279/96, os seguintes tipos de contratos de transferência de tecnologia são previstos:

- Exploração de patentes;
- Desenho industrial;
- Fornecimento de tecnologia;
- Prestação de serviço de assistência técnica e científica;
- Uso de marcas;
- Franquias.

Desse modo, o contrato inerente a esse estudo poderá ser formalizado de três formas:

1. Transferência da titularidade do direito da propriedade intelectual;
2. Contrato de licenciamento, que se refere ao licenciamento, uso do direito de propriedade intelectual de forma exclusiva ou não;
3. Contrato de transferência de tecnologia, que se refere ao fornecimento de conhecimentos não amparados por direitos de propriedade industrial (transferência de *know-how*).

O contrato ligado ao licenciamento de direitos (Exploração de Patentes, considerando o objeto desse estudo) refere-se ao conhecimento oriundo de diversas pesquisas do projeto já executadas.

O contrato que se refere à transferência de conhecimentos é o fornecimento de tecnologia e a prestação de serviços de assistência técnica, caso seja de interesse das partes.

No caso desse estudo, o Contrato de Fornecimento de Tecnologia será o celebrado para a transferência do *know-how* envolvendo os conhecimentos referentes à arquitetura da

base de dados em *blockchain* com a API de integração.

Compreenderá a aquisição de conhecimentos e de técnicas não amparadas por direitos de propriedade industrial ou o fornecimento de informações tecnológicas destinadas à produção do programa de computador pelo adquirente.

Em se tratando de Contrato de Licença, poderá ser celebrado sob duas perspectivas:

Primeira: Permissão de exploração de patente da invenção implementada por computador, em conformidade com a Resolução INPI/PR nº 158, de 28 de novembro de 2016, compreendendo a permissão de patente concedida ou pedido de patente depositado no INPI.

Na possibilidade desse ato, o contrato deverá conter o número do pedido da patente, respeitando os dispostos nos artigos 61, 62 e 63, da Lei nº 9.279 de 1996.

Segunda: Licença de uso de programas de computador (*software*), em conformidade com a Lei de Direitos Autorais (Lei nº 9.610/98 e pela Lei de Proteção da Propriedade Intelectual de Programa de Computador, Lei nº 9.609/98).

O contrato nesse ato deverá ser escrito de acordo com a determinação do Art. 50 da Lei nº 9.610/98, a saber: “A cessão total ou parcial dos direitos de autor, que se fará sempre por escrito, presume-se onerosa”.

Em ambos os casos, a licença só será concedida a requerente com legítimo interesse e que tenha capacidade técnica e econômica para realizar a exploração eficiente do objeto da patente e/ou pedido de patente.

Do mesmo modo para explorar a licença de uso de *software* respeitando a proteção aos direitos relativos aos programas de computador, que é assegurado pelo prazo de 50 anos contados a partir de 1º de janeiro do ano subsequente ao da sua publicação, ou na ausência desta, da sua criação, em conformidade com os Artigos 1º e 2º; § 2º da Lei 9.609/98.

Para a admissibilidade do contrato deverão ser observadas as condições previstas no Artigo 1º do Capítulo I do Anexo da Resolução INPI/PR nº 199/2017.

O pedido de averbação poderá ser apresentado por qualquer uma das partes em formulário próprio do INPI com os documentos previstos na Instrução Normativa INPI/PR nº 070/2017 e poderão ser protocolados na sede do INPI ou em suas Regionais.

Os documentos necessários para proceder com o registro contratual serão:

- Formulário de pedido de averbação ou registro;
- Comprovante de recolhimento da retribuição devida, com a respectiva Guia de Recolhimento da União (GRU);
- Procuração, observado o disposto nos artigos 216 e 217 da Lei 9.279/96;

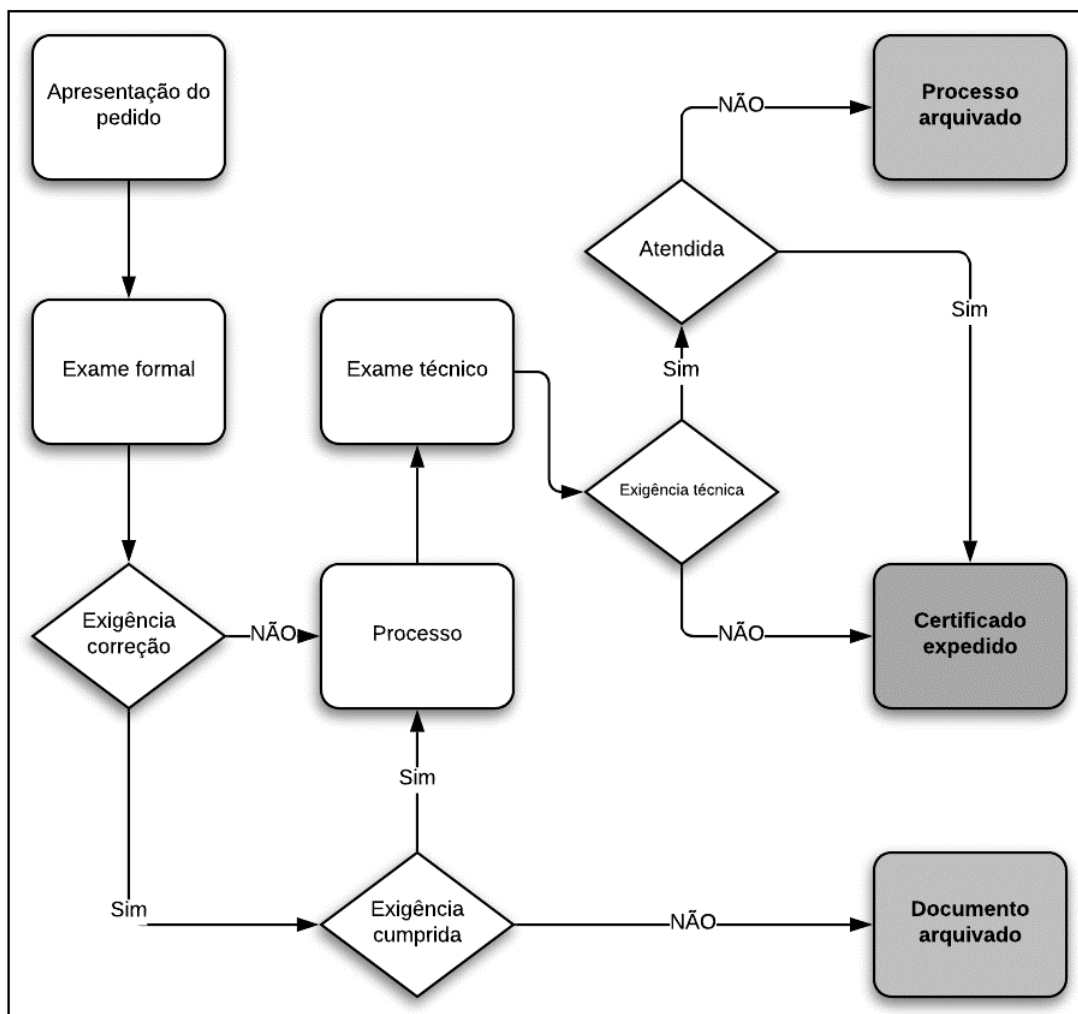
- Contrato, fatura ou instrumento representativo do ato;
- Formulários Ficha Cadastro de Pessoa Jurídica ou Física contratantes;
- Estatuto, contrato social ou ato constitutivo de Pessoa Jurídica e última alteração contratual da empresa cessionária, licenciada, domiciliada no Brasil;
- Outros documentos, a critério da parte interessada, pertinentes ao negócio jurídico.

Os prazos para o processo de averbação, desde o requerimento até a decisão, estarão em conformidade com Resolução INPI/PR nº 199/2017: trinta (30) dias a partir da data de publicação do requerimento na Revista da Propriedade Industrial (RPI).

Quando houver alguma exigência a cumprir, o prazo será de até sessenta (60) dias a contar da data de publicação na RPI, em observância ao disposto no Art. 224, da Lei 9.279/96, sob pena de arquivamento.

Após a conclusão da averbação, as decisões do contrato serão publicadas da Revista da Propriedade Industrial (RPI) disponível no *site* do INPI.

A **Figura 45**, a seguir, demonstra o fluxo do processo para a averbação:

Figura 45 - Fluxo do processo para averbação do contrato

Fonte: Autoria Própria (2019).

Conforme observado na **Figura 45**, caso haja alguma exigência para correção após o exame formal, o processo só iniciará após a exigência cumprida, sendo o documento arquivado caso não aconteça. O mesmo ocorrerá após a etapa do exame técnico, caso haja exigência técnica a ser cumprida, o certificado só será emitido após a exigência ser atendida, do contrário o processo será arquivado.

Em conformidade com o INPI (2019), os principais efeitos observados após averbação do contrato de transferência da tecnologia desse projeto serão: Permitir dedução fiscal dos *royalties* para a empresa receptora da tecnologia e produzir efeitos perante terceiros.

Em conformidade com os Artigos 62, 121, e 140 da LPI (Lei nº 9.279/96), para que se produzam os efeitos em relação a terceiros e para que haja a dedução fiscal dos *royalties*, valores pagos por exploração da patente, e/ou a remuneração que envolva a transferência da tecnologia, somente serão admitidos após a averbação dos contratos no INPI.

6 CONCLUSÕES

Esse trabalho iniciou-se a partir da observação da grande facilidade da falsificação de atestados médicos-odontológicos a partir da utilização de meios informatizados, possibilitando fraudes em várias instâncias pelo uso do documento falso.

A pesquisa constatou evidências de significativos prejuízos socioeconômicos de empresas das esferas pública e privada ao receberem atestados médicos-odontológicos falsos como justificativa de ausência ao trabalho, além da obtenção de benefícios indevidos junto a outras entidades com o auxílio do documento falsificado.

Tais constatações revelaram a importância de estudar o tema, pois entender como garantir o registro e a autenticidade de atestados médicos-odontológicos de forma unificada se tornou a questão-problema a ser respondida.

Portanto, essa pesquisa teve por objetivo propor um modelo de registro unificado para verificação de autenticidade de atestados médicos-odontológicos em rede *blockchain*, propondo-se a elencar as possibilidades de proteção intelectual da solução proposta e os meios para transferi-la ao mercado produtivo.

Para alcançar esse objetivo de forma específica, primeiramente, foram modelados processos de negócio envolvendo as operações de registro e validação de autenticidade do documento. O propósito é criar um fluxo orientador tanto no âmbito da implementação da operação em *softwares* clientes, quanto do desenvolvimento futuro de uma plataforma que implemente o modelo, também no que se refere à usabilidade de quem operará o sistema.

Em seguida, elaborou-se a arquitetura tecnológica prevendo a sua modelagem, as regras de negócio e os casos de uso que serviram de diretrizes de desenvolvimento de um sistema como protótipo para validar o modelo proposto nessa pesquisa.

Essa etapa se tornou altamente relevante, pois uma vez que a emissão (seja de forma manual ou impressa) de um atestado ocorre em papel, a fragilidade da comprovação de que o documento não foi falsificado por um terceiro se torna difícil.

Portanto, a arquitetura desenvolvida com base em tecnologia *blockchain* possibilita a existência de um mecanismo facilitador para que médicos e cirurgiões-dentistas emitam atestados através de um meio digital-tecnológico, distribuído e seguro de modo a ter, em um só repositório nacional, cada atestado emitido no país registrado eletronicamente.

Esse modelo de registro tecnológico único garante a rastreabilidade e a validação de todos os atestados emitidos, pois somente àqueles que participam da rede de registro terão autonomia para a emissão digital do documento e a sua consulta por meios tecnológicos,

eliminando os terceiros falsificadores desse processo de emissão.

Para validar a arquitetura elaborada, o passo seguinte foi desenvolver e apresentar um sistema protótipo com base nas regras de negócio e casos de uso apresentados nos resultados da pesquisa. A finalidade foi validar o modelo teórico de registros de atestados de forma prática, e proporcionar aprendizados no que se refere ao desenvolvimento de redes distribuídas *blockchain*, e implementação da estrutura tecnológica necessária a uma plataforma futura que porventura venha ser desenvolvida pelo mercado produtivo.

Os aprendizados gerados pela experiência da construção do protótipo possibilitaram o surgimento de uma arquitetura capaz de atender, não somente o registro de atestados médicos-odontológicos, mas qualquer tipo de demanda em que documentos médicos com informações de pacientes sejam registrados em rede *blockchain*, de forma a gerar uma base nacional que possibilitem dados estatísticos.

Finalmente, a pesquisa elencou as possibilidades de proteção intelectual e transferência de tecnologia, avaliando o processo de averbação contratual junto ao Instituto Nacional de Propriedade Industrial (INPI), visando transferir os produtos criados nesse trabalho ao mercado produtivo.

As avaliações realizadas nessa etapa mostraram a possibilidade da reivindicação de uma patente de invenção implementada por um programa de computador amparada pela Resolução INPI/PR 158/2016, que dispõe sobre a possibilidade da proteção do efeito técnico de um modelo implementado em um sistema, caso este atenda aos requisitos de patenteabilidade, sendo essa ainda uma possibilidade iminente após o findo dessa pesquisa.

No entanto, ao finalizar essa etapa constatou-se que, para os resultados apresentados pela pesquisa, a proteção por Registro de Programa de Computador seria a opção que melhor atenderia a proteção do produto gerado nesse estudo, sendo essa a opção adotada. O registro foi obtido junto ao INPI, mediante atendimento dos requisitos prévios exigidos para a sua obtenção.

Quanto às limitações desse estudo, diante da metodologia proposta, percebe-se que o trabalho poderia ter sido realizado com um estudo mais amplo de viabilidade econômico-financeira, analisando melhor os aspectos associados ao retorno de investimento, simulações de riscos e análise de cenários que pudessem proporcionar uma melhor visualização por parte de investidores.

Porém, diante do tempo metodológico, a pesquisa reteve-se a realizar apenas pequenas projeções de custos envolvidos nos aspectos mais essenciais da viabilidade técnica limitando-se a apenas demonstrar os custos envolvidos relacionados ao uso de servidor de rede e equipe

mínima de projeto.

Também não foram abordados nesse trabalho questões relacionadas aos impactos da implementação e implantação dessa solução na vida dos pacientes, bem como o levantamento dos impactos causados no dia a dia dos médicos e cirurgiões-dentistas. Esses dados poderão ser coletados através de entrevistas e experimentação do protótipo junto a esses profissionais de saúde.

Para trabalhos futuros recomenda-se um estudo de viabilidade econômico-financeira e jurídica, que venha dimensionar outros aspectos relacionados a questões legislativas, tributárias e regulamentais, assim como variáveis contábeis e econômicas para investimento.

Embora a arquitetura elaborada e confirmada por um protótipo de *software* demonstrou satisfatória robustez para a geração de uma base de dados com registro de documentos médicos e dados de paciente em geral, recomenda-se estudos futuros para que essa base de dados, uma vez institucionalizada nacionalmente, venha, a partir do registro de atestados médicos-odontológicos, proporcionar inteligência para gestão de áreas da saúde.

A base de dados poderá fornecer dados segmentados por região, por CID, informar a série histórica de afastamento do trabalho para empresas e outras entidades interessadas, ou quando um indivíduo vier a solicitar benefícios junto a um órgão como o INSS (Instituto Nacional do Seguro Social), por exemplo.

As sugestões e recomendações acima demonstram, ainda, oportunidades de pesquisa dentro do tema estudado, e são altamente relevantes para que o presente estudo alcance uma maior completude.

Soluções envolvendo tecnologias disruptivas tendem a gerar inovações aplicadas a resolver problemas reais no mundo real, e esse trabalho procurou comprovar isso através da proposição de uma inovação simples, conveniente e acessível ao setor produtivo.

O modelo proposto oferece um novo meio para o processo de emissão de atestados médicos-odontológicos em esfera nacional, de forma a contribuir com a minimização de prejuízos socioeconômicos, e preservar a autonomia e a autoridade dos profissionais de saúde supracitados, excluindo desse meio àqueles que aproveitam da fragilidade do documento em papel para falsificá-lo.

Em sua conclusão, efetivamente o trabalho conseguiu demonstrar e validar que um modelo de registro de atestados institucionalizado em um repositório único, com regras de validação implementadas por uma tecnologia como a *blockchain*, poderá garantir a sua autenticidade e rastreabilidade contribuindo, assim, no combate à sua falsificação.

REFERÊNCIAS

- ANDROULAKI, E. *et al.* Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. EuroSys 18. **Proceedings of the Thirteenth EuroSys Conferenc.** Article N°. 30. Porto, Portugal, 2018.
- ARRUDA, G. O. A tecnologia a serviço da democracia: O processo eleitoral na era da informação. **Revista da Advocacia Pública Federal.** V.1, n.1. Brasília-DF, 2017.
- ASSAFIM, J. M. L. **A transferência de tecnologia no Brasil:** aspectos contratuais e concorrenciais da propriedade industrial. Rio de Janeiro: Lumen Juris, 2013.
- AZARIA, A. *et al.* MedRec: Using Blockchain for Medical Data Access and Permission Management. **2nd International Conference on Open and Big Data.** IEEE Computer Society, 2016.
- BAGNATO, V. S.; ORTEGA, L. M.; MARCOLAN, D. **Guia Prático II: Transferência de Tecnologia Parcerias entre Universidade e Empresa.** São Paulo: Agência USP de Inovação, 2014. Disponível em: http://www.inovacao.usp.br/wp-content/uploads/sites/300/2017/10/cartilha_TT_bom.pdf. Acesso em: 26 jul. 2019.
- BARAZETTI, G., MORANDINI, R. I., BONAMIGO, E. L. Atestado médico falso: punibilidade questionada. **Anais de Medicina,** 2014. Recuperado de <https://portalperiodicos.unoesc.edu.br/anaisdemedicina/article/view/4647>
- BARBOSA, D. B. **Contratos em Propriedade Intelectual.** Disponível em: http://www.denisbarbosa.addr.com/arquivos/apostilas/ufrj/contratos_propriedade_intelectual.pdf. Acesso em: 25 mar. 2019.
- BARTON, J. H. Transferência de Tecnologia: novos rumos. **Pontes.** V. 3 n. 3. Junho, 2007.
- BOOCH, G; RUMBAUGH, J; JACOBSON, I. **UML Guia do Usuário.** 2. ed. São Paulo: Elsevier, 2006.
- BRAGA, I. F. A; ERTLER, L. Z.; PEREIRA, R. B. M. Entendimento dos julgados do Tribunal de Justiça do Estado de São Paulo sobre a emissão de atestado médico falso: uma análise jurisprudencial. **Revista Brasileira de Medicina do Trabalho.** Rio de Janeiro. 2018.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto-Lei 2.848.** Artigo 302 e 304, de 24 de dezembro de 1940. Código Penal. Disponível em: <https://bit.ly/1QOCMUS>. Acesso em: 01 de ago. 2018.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 605, de 5 de janeiro de 1949.** Repouso semanal remunerado e o pagamento de salário nos dias feriados civis e religiosos. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L0605.htm. Acesso em: 05 nov. 2019.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 5.081, de 24 de agosto de 1966.** Regula o Exercício da Odontologia. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L5081.htm. Acesso em: 05 nov. 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 5.648, de 11 de dezembro de 1970**. Cria o Instituto Nacional da Propriedade Industrial e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5648.htm. Acesso em: 12 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 8.955 de 15 de dezembro de 1994**. Dispõe sobre o contrato de franquia empresarial (*franchising*) e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8955.htm. Acesso em: 11 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 9.279 de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 11 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 9.609, 19, de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 11 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 9.610, Artigo 7º, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9610.htm. Acesso em: 12 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 12 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 10.973, de 2 de dezembro de 2004**. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 12 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto 5.563, de 11 de outubro de 2005**. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Decreto/D5563.htm. Acesso em: 01 de ago. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 05 nov. 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 13.243, de 11 de janeiro de 2016**. Dispõe sobre estímulos ao desenvolvimento científico, à

pesquisa, à capacitação científica e tecnológica e à inovação e altera a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 6.815, de 19 de agosto de 1980, a Lei nº 8.666, de 21 de junho de 1993, a Lei nº 12.462, de 4 de agosto de 2011, a Lei nº 8.745, de 9 de dezembro de 1993, a Lei nº 8.958, de 20 de dezembro de 1994, a Lei nº 8.010, de 29 de março de 1990, a Lei nº 8.032, de 12 de abril de 1990, e a Lei nº 12.772, de 28 de dezembro de 2012, nos termos da Emenda Constitucional nº 85, de 26 de fevereiro de 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13243.htm. Acesso em: 12 dez. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto 9.283, de 7 de fevereiro de 2018**. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 13.243, de 11 de janeiro de 2016, o art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666, de 21 de junho de 1993, o art. 1º da Lei nº 8.010, de 29 de março de 1990, e o art. 2º, caput, inciso I, alínea "g", da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm#art83. Acesso em: 01 de ago. 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 28 jul. 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 13.787 de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 05 nov. 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei 13.874, de 20 de setembro de 2019**. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nos 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015, de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm. Acesso em: 05 nov. 2019.

BROWN, *et al.* **Corda: An Introduction**, 2016. Disponível em: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf. Acesso em: 17 mai. 2010.

CACHIN, C. Architecture of the Hyperledger Blockchain Fabric. **IBM Research – Zurich CH-8803**. Ruschlikon, Switzerland, 2016.

CAIXA ECONÔMICA FEDERAL. **Perguntas frequentes sobre FGTS**. Disponível em:

<http://www.caixa.gov.br/beneficios-trabalhador/fgts/perguntas-frequentes/Paginas/default.aspx>. Acesso em: 08 nov. 2019.

CASARIN, H; CASARIN, S. J. **Pesquisa científica**: da teoria à prática. Curitiba: InterSaberes, 2012. *E-Book*.

CERCA de 30 mil atestados médicos falsos são apresentados por mês no ES. **G1 Portal de Notícias**. Espírito Santo. Disponível em: <https://glo.bo/2vO9rcH>. Acesso em: 11 ago. 2017.

CERCA de 30 mil atestados médicos falsos são apresentados por mês no Espírito Santo. **Jornal Diário do Noroeste**. Disponível em: <http://linharesemidia.com.br/jornais/diariodonoroeste/1747.pdf>. Acesso em: 25 jul. 2018.

CHRISTIDIS, K; DEVETSIOKIOTIS, M. Blockchains and Smart Contracts for the IoT. **IEEE Access**, 2016. Disponível em: <https://doi.org/10.1109/ACCESS.2016.2566339>. Acesso em: 13 fev. 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM nº 1.658/2002 de 20 de dezembro de 2002**. Normatiza a emissão de atestados médicos e dá outras providências. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/166esoluções/BR/2002/1658>. Acesso em: 01 mai. 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM nº. 1.851/2008, de 18 de agosto de 2008**. Altera o Art. 3º da Resolução CFM nº 1.658, de 13 de fevereiro de 2002, que normatiza a emissão de atestados médicos e dá outras providências. Disponível em: http://www.portalmedico.org.br/166esoluções/CFM/2008/1851_2008.pdf. Acesso em: 01 mai. 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CRM/AC nº. 06/2009, de 22 de setembro de 2009**. Complementação da Resolução CFM nº 1.658/2002, que regulamenta a emissão de Atestado Médico. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/AC/2009/6_2009.pdf. Acesso em: 01 mai. 2019.

CONSELHO REGIONAL DE MEDICINA DO ACRE (CFM-AC). **Resolução CRM/AC nº. 06/2009**. Complementação da Resolução CFM nº 1.658/2002, que regulamenta a emissão de Atestado Médico. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/AC/2009/6_2009.pdf. Acesso em: 05 nov. 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM nº 2.217, de 27 de setembro de 2018**. Código de Ética Médica. Disponível em: <https://portal.cfm.org.br/images/PDF/cem2019.pdf>. Acesso em: 05 nov. 2019.

CORDEIRO, L. Pedidos ilegais de auxílio-doença em Londrina causaram prejuízo de R\$ 1,1 milhão, diz PF. **G1 Norte e Noroeste RPC**. Londrina-PR, 2019. Disponível em: <https://g1.globo.com/pr/norte-noroeste/noticia/2019/04/02/pedidos-ilegais-de-auxilio-doenca-em-londrina-causaram-prejuizo-de-r-11-milhao-diz-pf.ghml>. Acesso em: 01 mai. 2019.

COSTA, C. O. M. **Transferência de Tecnologia Universidade-Indústria no Brasil e a**

Atuação de Núcleos de Inovação Tecnológica. 2013. 51f. Dissertação (Mestrado em Engenharia de Produção) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2013.

CROSBY, M.; PATTANAYAK, P.; VERMA, S.; KALYANARAMAN, V. BlockChain Technology, Beyond Bitcoin. **Sutardja Center for Entrepreneurship & Technology Technical Report.** October 16, 2015.

DESCUBRA como a sua prescrição pode entregar muito mais para o seu paciente. **MEMED.** Disponível em: <https://memed.com.br/>. Acesso em: 25 jul. 2018.

FERREIRA, F. L. **Blockchain e Ethereum: Aplicações e Vulnerabilidades.** Monografia. 2017. 37 f. (Bacharelado em Ciência da Computação) – Instituto de Matemática e Estatística. Universidade de São Paulo, São Paulo-SP, 2017.

FINCK, M. Blockchains and Data Protection in the European Union. **Max Planck Institute for Innovation & Competition Research Paper**, nº. 18-01, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322. Acesso em: 07 nov. 2019.

GATES, M. Ethereum: Complete guide to understanding Ethereum Blockchain, Smart Contracts, ICOs, and Decentralized Apps. 1. ed. **Wise Fox Publishing**, 2017.

GOPICHAND, A. N. V. K; SAILAJA, M; KAVITHA, B; SIVAPARVATHI, V. A. Detailed Study and Advancement of Blockchain. **International Journal For Innovative Engineering and Management Research.** Vol. 07, Issue 12, Nov. 2018. Pages: 275–288.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social.** 6. ed. São Paulo: Atlas, 2008.

GIL, A. C. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2010.

GREVE *et al.* S. Blockchain e a Revolução do Consenso sob Demanda. *In:* VERDI, F.; UEYAMA, J.; ROSSETO, S. (org.). **Livro de Minicursos do SBRC 2018.** 1. ed. Porto Alegre: Sociedade Brasileira de Computação, v. 1, p. 1-52, 2018.

GUEDES, G. T. A. **UML 2: Uma abordagem prática.** 2. ed. São Paulo: Novatec Editora, 2011.

HUCKLE *et al.* Internet of Things, Blockchain and Shared Economy Applications. **Procedia Computer Science.** v.98. 461-466, 2016.

IBM WATSON. **Inteligência Artificial para Negócios.** Disponível em: <https://www.ibm.com/watson/br-pt/>. Acesso em: 19 jan. 2019.

VIDAL-QUADRAS TRIAS DE BES, M. **Transferencia de tecnología: contratos de cesión y licencia de patentes y know-how.** Las Claves del Derecho. Barcelona, 2015.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA (INMETRO). **Sistema Internacional de Unidades – SI.** 1ª. Edição Brasileira do BIPM. Rio de Janeiro, 2012. Disponível em: http://www.inmetro.gov.br/inovacao/publicacoes/si_versao_final.pdf. Acesso em: 10 nov. 2019.

INSTITUTO NACIONAL DE PROPRIEDADE INDUSTRIAL (INPI). **Contratos de transferência de tecnologia - Mais informações.** Disponível em: <http://www.inpi.gov.br/menu-servicos/transferencia/transferencia-de-tecnologia-mais-informacoes>. Acesso em: 10 mar. 2019.

INSTITUTO NACIONAL DE PROPRIEDADE INDUSTRIAL (INPI). **Legislação - Transferência de Tecnologia.** Disponível em: <http://www.inpi.gov.br/menu-servicos/transferencia/legislacao-transferencia-de-tecnologia>. Acesso em: 10 mar. 2019.

JUSBRASIL. **Base de dados para consultas jurídicas.** 2018. Disponível em: <https://bit.ly/2K6xkk4>. Acesso em 25 jul. 2018.

KIAPINE, G. Contrato de transferência de tecnologia “know-how”. **Jusbrasil**, 2019. Disponível em: <https://gabkiapine.jusbrasil.com.br/artigos/199081088/contrato-de-transferencia-de-tecnologia>. Acesso em: 10 mar. 2019.

LIMA, J. P. S. **Validação de Dados Através de Hashes Criptográficos: Uma Avaliação na Perícia Forense Computacional Brasileira.** Dissertação (Mestrado). 2015. 115 f. (Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2015.

LIN, I.-C; LIAO, T.-C. A Survey of Blockchain Security Issues and Challenges. **International Journal of Network Security**, Vol.19, nº.5, PP.653-659, Sept. 2017. Disponível em: https://www.researchgate.net/publication/329683614_A_survey_of_blockchain_security_issues_and_challenges. Acesso em: 06 nov. 2019.

LINUX FOUNDATION. Hyperledger blockchain technologies for business: Introduction to Hyperledger. Business Blockchain Design Philosophy and Consensus. **Hyperledger.Org**. Disponível em: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf. Acesso em: 10 mai. 2019.

LOTUFO, R. A.; TOLEDO, P. T. M.; SANTOS, M. E. R. (orgs). **Transferência de Tecnologia: estratégias para estruturação e gestão de Núcleos de Inovação Tecnológica.** Campinas: SP, Komedi, 2009. Disponível em: http://www.inova.unicamp.br/sites/default/files/documents/Livro%20Transferencia%20de%20tecnologia_0.pdf. Acesso em: 19 mai. 2019.

LUCENA, A. U.; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum. *In: IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP*, 9, 29-30 de setembro, Campinas, São Paulo, 2016. Disponível em: <https://diegoazziufabc.files.wordpress.com/2017/08/estudo-de-arquiteturas-dos-blockchains.pdf>. Acesso em: 05 nov. 2018.

LUZ, A. A. **Mecanismos de transferência de tecnologia no Processo de formação de spin-offs.** 2012. 149 f. Dissertação (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação em Engenharia de Produção. Universidade Tecnológica Federal do Paraná, Ponta Grossa, 2012.

MARCONI, M. A.; LAKATOS, E. M. **Técnicas de pesquisa: planejamento e execução de**

pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados. 5. ed. São Paulo: Atlas, 2002.

MARCONI, M. A.; LAKATOS, E. M. Fundamentos de Metodologia Científica. 7. ed. São Paulo: Atlas, 2010.

MILLER, D.; Blockchain and the Internet of Things in the Industrial Sector. **IT Professional**. v.20. May./Jun. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8378971>. Acesso em: 25 mai. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Instrução Normativa nº 031/2013, de 04 de dezembro de 2013**. Estabelecer normas gerais de procedimentos para explicitar e cumprir dispositivos da Lei de Propriedade Industrial - Lei nº 9279, de 14 de maio de 1996, no que se refere às especificações formais dos pedidos de patente. Disponível em: http://www.inpi.gov.br/menu-servicos/patente/in_31_in_17_2013_administrativo_versao_03_12_2013_0.pdf Acesso em: 09 jan. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Resolução nº 170/2016, de 15 de julho de 2016**. Disciplina o Peticionamento Eletrônico do Sistema e-CONTRATOS. Disponível em: <http://www.inpi.gov.br/menu-servicos/arquivos-dicig/Resoluo1702016PeticionamentoEletrnicodoSistemaeCONTRATOS.pdf>. Acesso em: 11 jan. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Resolução nº 158/2016, de 28 de novembro de 2016**. Institui as Diretrizes de Exame de Pedidos de Patentes Envolvendo Invenções Implementadas por Programas de Computador. Disponível em: http://www.inpi.gov.br/menu-servicos/arquivos-dirpa/158_2016_patentesprogramacomputador.pdf. Acesso em: 09 jan. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Instrução Normativa INPI/PR nº 070/2017, de 11 de abril de 2017**. Dispõe sobre o procedimento administrativo de averbação de licenças e cessões de direitos de propriedade industrial e de registro de contratos de transferência de tecnologia e de franquia. Disponível em: <http://www.inpi.gov.br/sobre/legislacao-1/IN702017.pdf>. Acesso em: 11 jan. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Resolução INPI/PR nº 199/2017, de 07 de julho de 2017**. Dispõe sobre as diretrizes de exame para averbação ou registro de contratos de licença de direito de propriedade industrial e de registro de topografia, circuito integrado, transferência de tecnologia e franquia. Disponível em: <http://www.inpi.gov.br/menu-servicos/arquivos-dicig/Resoluo1992017DiretrizesCGTEC.pdf>. Acesso em: 11 jan. 2019.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. INPI. **Instrução Normativa nº 099/2019, de 08 de fevereiro de 2019**. Disciplina o processo de registro de programas de computador. Disponível em: <http://www.inpi.gov.br/sobre/legislacao-1/IN992019.pdf>. Acesso em: 12 jan. 2019.

MOUGAYAR, W. **Blockchain para negócios**: promessa, prática e aplicação da nova tecnologia na Internet. Rio de Janeiro: Altabooks, 2018.

MOUGAYAR, W. **The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology**. 1. ed. New Jersey, 2016.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 05 nov. 2018.

NOWIŃSKI, W.; KOZMA, M. How Can Blockchain Technology Disrupt the Existing Business Models. **Entrepreneurial Business and Economics Review**, V. 5. N.3, 2017. 173-188. Disponível em: <http://doi.org/10.15678/EBER.2017.050309>. Acesso em: 08 nov. 2018.

O'CONNOR, C. **What blockchain means for the Internet of Things**. In: IBM (ed.) Internet of Things Blog. 2016. Disponível em: <https://www.ibm.com/blogs/internet-of-things/watson-iot-blockchain/>. Acesso em: 9 jan. 2019.

PARK, J. H.; PARK, J. H.. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. **Symmetry**. V.9. 2017.

PARODI, L. **Falsificação de Documentos em Processos Eletrônicos**. Rio de Janeiro: Brasport, 2018.

PINTO, M. M. A. **Proposta de framework de uma cadeia de suprimentos verde a partir da transferência de tecnologia**. 2016. 134 f. Dissertação (Mestrado em Engenharia de Produção) - Universidade Tecnológica Federal do Paraná, Ponta Grossa, 2016.

PIRES, H. F. Bitcoin: a moeda do ciberespaço. **Geosp – Espaço e Tempo (Online)**, V. 21, n. 2, p. 407-424, agosto, 2017. Disponível em: <http://www.revistas.usp.br/geosp/article/view/134538>. Acesso em: 17 mai. 2019.

PRADO, M. C. A. **Contrato internacional de transferência de tecnologia: patente e know-how**. Porto Alegre: Livraria do Advogado, 1997.

PRESCRIÇÃO digital uma revolução em andamento na relação médico paciente. **CryptoID portal de conteúdo de certificação digital**. 2016. Disponível em: <https://bit.ly/2Bipip1>. Acesso em: 25 jul. 2018.

PRIETO-CASTRILLO, F.; KUSHCH, S.; CORCHADO, J. M. Distributed Sequential Consensus in Networks: Analysis of Partially Connected Blockchains with Uncertainty. **Hindawi Journals Complexity**. v. 2017. Disponível em: <https://doi.org/10.1155/2017/4832740>. Acesso em: 28 set. 2018.

PRODANOV, C.; FREITAS, E. C. de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho**. 2. ed. Novo Hamburgo: Feevale, 2013. *E-Book*.

PROJECT MANAGEMENT INSTITUTE (PMI). **Guia PMBOK: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos**. 6. ed. Pennsylvania: PMI, 2017.

R3. **Delivering blockchain technology to transform the way the world does business**. Disponível em: https://www.r3.com/wp-content/uploads/2018/09/US_18_R3_FS_v7.pdf. Acesso em: 08 mai. 2019.

RAMSAY, S. **The General Data Protection Regulation vs. The Blockchain - A legal study**

on the compatibility between blockchain technology and the GDPR. Thesis in Law and Informatics, Stockholm University. 2018. Disponível em: <https://pdfs.semanticscholar.org/c231/c390f1bb345a2f6ebceee792264f227f9d32.pdf>. Acesso em 08 nov. 2019.

REBELO, M. P. Os desafios do RGPD perante as novas tecnologias blockchain. **Revista Bioética y Derecho**, 2019; V46: 117-131. 2019. Disponível em: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200008. Acesso em: 08 nov. 2019.

REDAÇÃO multimídia ESHOJE. Atestado médico online será ampliado para todo o Espírito Santo. **ESHOJE**. Espírito Santo. 9 de setembro de 2014. Disponível em: <https://bit.ly/2L5mhI8>. Acesso em: 25 jul. 2018.

SALIMITARI, M; CHATTERJEE, M. A Survey on Consensus Protocols in Blockchain for IoT Networks. Department of Computer Science. University of Central Florida-Orlando. **arXiv.org**, 2019. Disponível em: <https://arxiv.org/pdf/1809.05613.pdf>. Acesso em: 27 mai. 2019.

SILVA *et al.* Processo de averbação de contratos de transferência de tecnologia no Brasil. **Revista GEINTEC**. Vol. 5/n. 1/ p.1652-166. São Cristóvão/SE, 2015.

SILVA, V. A. F.; BOVÉRIO, M. A. Blockchain: uma tecnologia além da criptomoeda virtual. **Revista Interface Tecnológica**, v. 15, n. 1, p. 109-121, 2018. Disponível em: <https://doi.org/10.31510/infa.v15i1.326>.

SOFTWARE ENGINEERING INSTITUTE. **What is your definition of software architecture**. Carnegie Mellon University, 2017.

SOMMERVILLE, I. **Engenharia de Software**. 9. ed. São Paulo: Pearson do Brasil, 2011.

SOUZA, M. M. C. A. Gestão de Núcleos de Inovação Tecnológica. *In*: CONGRESSO INTERNACIONAL IGLU, II, 2011, Florianópolis, SC. **Anais [...]** Florianópolis, 2011. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/26132/5.26.pdf?sequence=1>. Acesso em: 26 jul. 2019.

SWAN, M. **Blockchain**: Blueprint for a new economy. USA: O'Reilly Media, 2015.

SWANSON, T. Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. **Report, available online**, Apr. 2015. Disponível: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>. Acesso em: 14 mai. 2019.

SUKHWANI *et al.* Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). **ResearchGates**. Conference Parper. 2017

SUN *et al.* Blockchain-based sharing services: What blockchain technology can contribute to smart cities. **Financial Innovation**. 2016.

SZABO, N. **Smart Contracts**. 1994. Disponível em:

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinter school2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em: 11/10/2019.

TASCA, P; THANABALASINGHAM, T.; TESSONE, C. J.; *Ontology of Blockchain Technologies. Principles of Identification and Classification*. **arXiv.org**, 2017. Disponível em: <https://128.84.21.199/abs/1708.04872v1>. Acesso em: 12 dez. 2018.

TARTUCE, F. **Direito Civil V. 3:** teoria geral dos contratos e contratos em espécie. 9. ed. rev., atual. e ampl.. São Paulo: Método, 2014.

TRAUTMAN, L. J. Is Disruptive Blockchain Technology the Future of Financial Services. **The Consumer Finance Law Quarterly Report**. v.232, 2016.

TRELEAVEN, P.; BROWN, R. G.; YANG, D. Blockchain Technology in Finance. **IEEE Computer Society**, 2017. Disponível em: <https://doi.org/10.1109/MC.2017.3571047>. Acesso em: 14 mai. 2019.

VAILATI, P. V.; TRZECIAK, D. S.; CORAL, E. (orgs). **Estruturação e gestão de núcleos de inovação tecnológica: Modelo PRONIT**. Blumenau: Nova Letra, 2012. 338p.

VALENTA, M; SANDNER, P. Comparison of Ethereum, Hyperledger Fabric and Corda. **FSBC Working Paper**. Frankfurt School Blockchain Center, 2017. Disponível em: http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf. Acesso em: 05 mai. 2019.

VENOSA, S. S. **Direito civil:** teoria geral das obrigações e teoria geral dos contratos. 13. ed. v. 2. São Paulo: Atlas, 2013.

WALSH *et al.* New kid on the block: a strategic archetypes approach to understanding the Blockchain. **Thirty Seventh International Conference on Information Systems**. Dublin, 2016. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1032&context=icis2016>. Acesso em: 14 mai. 2019.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **Índice Global de Inovação, 2019**. Disponível em: https://www.wipo.int/export/sites/www/pressroom/pt/documents/pr_2019_834.pdf. Acesso em 10/12/2019.

YERMACK, D. Corporate Governance and Blockchains. **Review of Finance**. V 21, 2017. Disponível em: <http://dx.doi.org/10.2139/ssrn.2700475>. Acesso em: 12 dez. 2018.

ZHAO, J. L; FAN, S; YAN, J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. **Financial Innovation**, 2016. Disponível em: <http://dx.doi.org/10.1186/s40854-016-0049-2> . Acesso em: 10 de jul. 2019.

ZHENG *et al.* An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. **IEEE 6th International Congress on Big Data**. 2017. DOI: <https://doi.org/10.1109/BigDataCongress.2017.85>. Acesso em: 10 de out. 2019.

ZHENG *et al.* **Blockchain challenges and opportunities: a survey.** International Journal of Web and Grid Services. Vol. 14. No.4. 2018. DOI: 10.1504/IJWGS.2018.095647. Acesso em: 02 ago. 2019.