UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Marília

ALEXANDRE FERNAL

# ***BLOCKCHAIN E* OS IMPACTOS NA ARQUIVOLOGIA:** UM MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Marília
2022

Alexandre Fernal

# ***BLOCKCHAIN* E OS IMPACTOS NA ARQUIVOLOGIA:** UM MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Tese apresentada ao Programa de Pós-Graduação em Ciência da informação como parte das exigências para a obtenção do título de Doutor em Ciência da Informação pela Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP), Câmpus de Marília.

Área de Concentração: Informação, Tecnologia e Conhecimento

Orientador (a): Profª. Drª. Telma Campanha de Carvalho Madio

Marília
2022

F362b

Fernal, Alexandre
BLOCKCHAIN E OS IMPACTOS NA ARQUIVOLOGIA: UM MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS / Alexandre Fernal. -- Marília, 2022
119 p. : il.

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília
Orientadora: Telma Campanha de Carvalho Madio

1. Arquivologia. 2. Ciência da Informação. 3. Autenticidade. 4. Autenticação. 5. Documentos Arquivísticos. I. Título.

**Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).**

**Essa ficha não pode ser modificada.**

Alexandre Fernal

# ***BLOCKCHAIN*** **E OS IMPACTOS NA ARQUIVOLOGIA**: UM MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Tese apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade Estadual Paulista “Júlio de Mesquita Filho” (Unesp), como requisito parcial para a obtenção do título de Doutor em Ciência da Informação

Área de concentração: Informação, Tecnologia e Conhecimento.
Linha de pesquisa: Produção e Organização da Informação.

Banca Examinadora

Profª. Drª. Telma Campnha de Carvalho Madio
Universidade Estadual Paulista (UNESP) – Câmpus Marília
Orientadora

Prof. Dr. Daniel Flores
Universidade Federal Fluminense (UFF)

Prof. Dr. José Carlos Abbud Grácio
Universidade Estadual Paulista (UNESP) – Câmpus Marília

Prof. Dr. Edberto Ferneda
Universidade Estadual Paulista (UNESP) – Câmpus Marília

Prof. Dr. Moises Rockembach
Universidade Federal do Rio Grande do Sul (UFRGS)

Marília, 05 de setembro de 2022.

*Aos meus pais José Ascânio Fernal*
*e Nobuko Kaminagakura Fernal*
*À minha irmã Rita de Cássia Fernal*

## AGRADECIMENTOS

À minha família e aos parentes, em especial aos meus avós paternos Vinício Fernal (*in memorian*), Olga Zeringota Fernal *(in memorian)* e aos meus avós maternos Satoru Kaminagakura (*in memorian*) e Tokiko Kaminagakura (*in memorian*).

À Universidade Estadual Paulista “Júlio de Mesquita Filho” Faculdade de Filosofia e Ciências (FFC) - Câmpus de Marília (UNESP), instituição que propiciou a realização das profundas reflexões teóricas arquivísticas.

À Universidade Estadual de Londrina (UEL), instituição que propiciou a realização das profundas reflexões teóricas e as práticas arquivísticas por meio da docência, na qual o meu nome se inscreve, com muita dedicação e perseverança, ainda que simbolicamente, em algumas de suas paredes, pelos corredores e algumas salas, com o meu próprio sangue.

Aos meus ex-alunos do curso de graduação em Arquivologia, na Universidade Estadual de Londrina (UEL), os quais me incutiram o gosto por ensinar e investigar em especial aos ex orientandos de TCC.

Aos amigos e colegas do PPGCI - UNESP, pela convivência, pelas parcerias nas produções intelectuais.

Agradeço aos membros da banca examinadora, professores: Dr. Daniel Flores, Dr. José Carlos Abbud Grácio, Dr. Edberto Ferneda, Dr. Moises Rockembach pelos valiosos comentários e sugestões no projeto de pesquisa.

Um agradecimento especial ao Benjamin Luiz Franklin e Eliandro dos Santos Costa, pela paciência e parceria, sem a qual teria sido impossível chegar ao final desta jornada arquivística, porque amizade e lealdade são valores que desconhecem fronteiras.

Finalmente, a orientadora professora Drª. Telma Camapanha de Carvalho Madio, agradeço pelos ensinamentos, incentivos, treinamentos, disponibilidade, boa vontade,

as orientações indispensáveis. Sobretudo, pelo imprescindível processo de aprendizagem. Sinto-me honrado por ter sido seu discípulo.

“[...] *blockchain* é a maior invenção da história da computação”

“*Blockchain* representa a segunda era da *internet*”

Don Tapscott (2018, p. 1)

## RESUMO

Na contemporaneidade, com o advento das tecnologias da informação e comunicação, acelerou-se o processo de ruptura no contexto da gênese dos documentos arquivísticos nos ambientes informacionais tradicionais para os ambientes informacionais digitais. Nesse cenário, os documentos arquivísticos digitais encontram-se, em sua grande maioria, em sistemas descentralizados. Nessa direção, surge em 2008, a tecnologia *blockchain,* que poderá ser utilizada para autenticação distribuída automatizada, em vista de que a tecnologia consiste em um grande banco de dados distribuído, que arquiva todas as movimentações realizadas de forma irreversível, posto que dispõe de um *ledger* – livro razão, o qual configura-se como um *distributed ledger technologies* – tecnologia de registros distribuídos. Sendo assim, questiona-se, portanto: de que modo a tecnologia *blockchain* poderá corroborar nas aplicações descentralizadas na autenticação dos documentos arquivísticos digitais no contexto da Arquivologia e como a tecnologia *blockchain* pode melhorar a interação no âmbito da confiança social institucional? Assim, objetiva-se analisar os impactos da tecnologia *blockchain* no contexto dos documentos arquivísticos digitais em sistemas descentralizados. Para tanto, realizou-se uma pesquisa bibliográfica de natureza pura, de cunho teórico, documental, exploratória, descritiva e qualitativa, acerca da literatura científica nacional e internacional publicada em livros, artigos, teses e dissertações. Como resultado demonstrou-se as relações de aplicação da tecnologia *blockchain* na autenticação distribuída*,* no contexto arquivístico por meio de três modelos distintos, quais sejam: modelo do Reino Unido, o *Archangel*, o modelo Canadense DIDC e modelo da administração pública do Governo de Dubai. Nessas conjunturas foi proposto modelo lógico para aplicação da tecnologia *blockchain* para autenticação distribuída automatizada ao longo do ciclo de vida dos documentos arquivísticos digitais.



**Palavras–chave:** *Blockchain*; Confiança; Autenticação; Arquivologia; Documentos Arquivísticos Digitais.

## ABSTRACT

In contemporary times, with the advent of information and communication technologies, the process of rupture in the context of the genesis of archival documents from traditional informational environments to digital informational environments was accelerated. In this scenario, digital archival documents are, for the most part, in decentralized systems. In this direction, appears in 2008, the blockchain technology, which can be used for automated distributed authentication, given that the technology consists of a large, distributed database, which archives all the movements carried out in an irreversible way, since it has a ledger which configures itself as a distributed ledger technology. Therefore, the question is: how can blockchain technology support decentralized applications in the authentication of digital archival documents in the context of Archival Science and how can blockchain technology improve interaction within the scope of institutional social trust? Thus, the objective is to analyze the impacts of blockchain technology in the context of digital archival documents in decentralized systems. Therefore, bibliographical research of a pure nature, of a theoretical, documentary, exploratory, descriptive, and qualitative nature, was carried out on the national and international scientific literature published in books, articles, theses and dissertations. As a result, it was demonstrated the application relationships of blockchain technology in distributed authentication, in the archival context through three different models, namely: the United Kingdom model, the Archangel, the Canadian DIDC model and the public administration model of the Government of Dubai. In these contexts, a logical model was proposed for the application of blockchain technology for automated distributed authentication throughout the life cycle of digital records.



**Keywords:** Blockchain; Trust; Authentication; Archival science; Digital Archival Documents.

## LISTA DE FIGURAS

Figura 1 – Metodologia de pesquisa.....21
Figura 2 – Anatomia do bloco..... 36
Figura 3 – Condição para inserção de novo bloco..... 38
Figura 4 – Modelo Birch, Brown, Parula..... 40
Figura 5 – Modelo Suiches..... 42
Figura 6 – Repositório digital *ArXiv* ..... 45
Figura 7 – Coleta de metadados..... 47
Figura 8 – Repositório digital MIT.....49
Figura 9 – Repositório digital do Instituto Antônio Carlos Jobim ..... 50
Figura 10 – Modelo simplicado OAIS ..... 53
Figura 11 – Modelo OAIS detalhado..... 54
Figura 12 – Componentes do ECM.....65
Figura 13 – Componentes da autenticidade.....68
Figura 14 – Modelo PREMIS.....72
Figura 15 – Os quinze elementos do padrão de metadados *Dublin Core*..... 74
Figura 16 – EAD e os principais elementos descritivos.....76
Figura 17 – Arquitetura METS..... 77
Figura 18 – Camada de confiança de interação da tecnologia *blockchain*..... 80
Figura 19 – Modelo *Archangel*..... 82
Figura 20 – Modelo Canadense para aplicação da tecnologia *blockchain*..... 84
Figura 21 – Diagrama de funcionamento dos *sidechains*.....85
Figura 22 – Modelo de utilização da tecnologia *blockchain* em Dubai.....87
Figura 23 – Autenticação descentralizada de DAD.....89
Figura 24 – Aplicação detalhada na autenticação distribuída de DAD.....90
Figura 25 – Diagrama de blocos do funcionamento da aplicação *blockchain* no âmbito da Arquivologia.....92
Figura 26 – Tipos de *blockchain*.....93

## LISTA DE QUADROS

Quadro 1: Principais mecanismos do consenso aplicados tecnologia *blockchain*.....39

Quadro 2: Procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e analógicos.....95-96

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ABNT | Associação Brasileira de Normas Técnicas |
| AC | Antes de Cristo |
| ADI | *Archiving of Digital Information* |
| AIIM | *Association for Information and Image Management* |
| AIP | *Archival Information Package* – Pacote de Submissão de Arquivos |
| ALCTS | *Association of Library Collection and Technical Services* |
| AMD | *Administrative Metadata* |
| ASI | *Agenzia Spaziale Italiana* |
| BPM | *Business Process Management* |
| CCSDS | *Consultive Committee for Space Data System* |
| CER | *Commite on Eletronic Records* |
| CIA | Conselho Internacional de Arquivos |
| CM | *Content Management* |
| CMIS | *Content Management Interoperability Services* |
| CNES | *Centre National d'Etudes Spatiales* |
| CNSA | *China National Space Adminstration* |
| CONARQ | Conselho Nacional de Arquivos |
| CPARLG | *Commission on Preservation and Access e Research Library Group* |
| CSA | *Canadian Space Agency* |
| CT | *Collaboration Tools* |
| CTDE | Câmara Técnica de Documentos Eletrônico |
| DBTA | Dicionário Brasileiro de Terminologia Arquivística |
| DC | Depois de Cristo |
| DCMI | *Dublin Core Metadata Initiative* |
| DICI | Diálogo Científico |
| DLR | *Deutsches Zentrum Für Luft und Raumfahrt* |
| DMD | *Descriptive Metadata* |
| DMS | *Document Management System* |
| EAD | *Encoded Archival Description* |
| e-ARQ | BRASIL Modelo de Requisitos para Sistemas Informatizados para Gestão Arquivística de Documentos |
| ECM | *Enterprise Content Management* – Gestão de Conteúdos Empresariais |
| ESA | *European Space Agency* |
| E-mail | *Eletronic Mail* |
| EUA | Estados Unidos da América |
| FILESEC | *File Section* |
| HP | *Hewllet Packard* |
| HTML | *Hypertext Markup Language* |
| IBBD | Instituto Brasileiro de Bibliografia e Documentação |
| IBICT | Instituto Brasileiro de Informação em Ciência e Tecnologia |
| ICA | *International Council Archives* |
| ICT | *Information and Communication Technologies* |

| | |
|---|---|
| INPE | Instituto Nacional de Pesquisas Espaciais |
| INTERCOM | Sociedade Brasileira de Estudos Interdisciplinares da Comunicação |
| ISAAR(CPF) | *International Standard Archival Authority Record For Corporate Bodies, Persons and Families* |
| ISAD (G) | *General International Standard Archival Description* |
| ISO | *International Organization for Standartization* |
| ISQ | *Information Standard Quartely* |
| JAXA | *Japan Aerospace Exploration Agency* |
| MCT | Ministério da Ciência e Tecnologia |
| METS | HDR Padrão de Codificação e Transmissão de Metadados *Header* |
| METS | Padrão de Codificação e Transmissão de Metadados |
| MIT | *Massachusetts Institute of Technology* |
| NASA | *National Aeronautics and Space Administration* |
| NISO | *National Information Standards Organization* |
| NOBRADE | Norma Brasileira de Descrição Arquivística |
| OA | *Open Access* |
| OAI | *Open Archives Initiative* |
| OAI-PMH | *Open Archives Initiative – Protocol for Metadata Harvesting* |
| OAIS | *Open Archives Information System* |
| OASIS | *Organization for the Advanced of Structured Information Standards* |
| OAWG | *Open Access Working Group* |
| OCLC | *Online Computer Library Center* |
| ODT | *Open Document Text* |
| OP | *Open Source* |
| OWL | *Ontology Web Language* |
| PDF | *Portable Document Format* |
| PMEST | Personalidade Matéria Energia Espaço Tempo |
| PORTCOM | Rede de Informação em Comunicação dos Países de Língua Portuguesa |
| PPGCI | Programa de Pós Graduação em Ciência da Informação |
| PREMIS | *Preservation Metada Implementation Strategy* |
| R | Reservado |
| RFSA | *Russian Federal Space Agency* |
| RLG | *Research Library Group* |
| RM | *Records Management* |
| S | Secreto |
| SAA | *Society of American Archivist* |
| SAAI | Sistema Aberto de Arquivamento de Informação |
| SIGAD | Sistema Informatizado de Gestão Arquivística de Documentos |
| SINAR | Sistema Nacional de Arquivos |
| SIP | *Submission Information Package* – Pacote de Submissão de Informação |
| STRUCTMD | *Structural Metadata* |
| TF | *Task Force* |
| TIC | Tecnologias de Informação e Comunicação |
| TTD | Tabela de Temporalidade de Documentos |
| U | Ultra secreto |
| UEL | Universidade Estadual de Londrina |

| | |
|---|---|
| UKSA | *United Kingdom Space Agency* |
| USA | *United States of America* |
| USLC | *United States of Library Congress* |
| USP | Universidade de São Paulo |
| WCM | *Web Content Management* |
| WF | *Workflow* |
| XML | *EXtensible Markup Language* |

**SUMÁRIO**


**1 INTRODUÇÃO** 15
1.1 PROBLEMA 16
1.2 JUSTIFICTIVA 17
1.3 OBJETIVOS 19
1.3.1 OBJETIVO GERAL 19
1.3.2 OBJETIVOS ESPECÍFICOS 19
1.4 METODOLOGIA 19

**2 MODERNIDADE LÍQUIDA/PÓS-MODERNIDADE** 25

**3 *BLOCKCHAIN*** 31

**4 REPOSITÓRIOS DIGITAIS** 44
4.1 INICIATIVAS E ESTRATÉGIAS DE IMPLEMENTAÇÃO DOS REPOSITÓRIOS DIGITAIS 48
4.2 MODELO OPEN ARCHIVES INFORMATION SYSTEM (OAIS) 52
4.3 GESTÃO DE DOCUMENTOS – RECORDS MANGEMENT (RM) 57
4.4 GESTÃO DE CONTEÚDOS EMPRESARIAIS – ENTERPRISE CONTENT MANAGEMENT (ECM) 64

**5 AUTENTICIDADE** 68

**6 IMPACTOS DA TECNOLOGIA *BLOCKCHAIN* NO CONTEXTO DA ARQUIVOLOGIA:** MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS 80
6.1 MODELOS LÓGICOS PARA UTILIZAÇÃO DA TECNOLOGIA BLOCKCHAIN NO CONTEXTO DA ARQUIVOLOGIA 82

**7 CONSIDERAÇÕES FINAIS** 102

**REFERÊNCIAS** 104

# 1 INTRODUÇÃO

Na pós-modernidade, com o advento das tecnologias da informação e comunicação (TIC), emergem tecnologias como, por exemplo, o *blockchain,* que possui como cerne a distribuição de registros em sistemas de consenso descentralizados, os quais operam sem uma autoridade central como na arquitetura centralizada cliente/servidor. Essa tecnologia apresenta-se como uma ruptura paradigmática no que diz respeito a questões relacionadas à autenticação em contextos descentralizados.

A tecnologia *blockchain* possui como característica fundamental a imutabilidade dos dados gravados em seus blocos, posto que uma vez registrado os dados em um bloco, esses não podem ser modificados. Essas cadeias de blocos funcionam como um *ledger* – livro razão aberto e distribuído ponto a ponto, o qual armazena as operações realizadas de ativos de forma permanente e auditável ao longo do tempo.

Nesse sentido, o *blockchain* utiliza-se de protocolos de validação consensual como o *proof of work* (PoW) – prova de trabalho e *proof of stake* (PoS)– prova de validação, os quais poderão corroborar com a preservação digital de longa duração, em vista de que, com o uso da árvore de *merkle,* podem ser analisadas todas cadeias de blocos até o bloco zero, isto é, o bloco gênesis e consequentemente, auditar todas as alterações ocorridas nos documentos arquivísticos digitais (DAD) ao longo do tempo ocasionadas pelas estratégias de preservação digital.

Ademais, com o uso da tecnologia *blockchain* observa-se a possibilidade de relacionar sua utilização como um importante apoio para autenticação distribuída dos DAD em uma cadeia de custódia arquivística descentralizada.

Dessa forma, a tecnologia *blockchain* é um tipo de *distributeb ledger technologie* (DLT), que dispõe de uma base de dados, a qual poderá verificar a proveniência e autenticação distribuída automatizada dos DAD, na qual é armazenado cronologicamente os dados transacionados, preservando permanentemente os dados por meio de uma distribuição ponto a ponto e com algoritmos de consensos para verificar autenticação sem a necessidade de terceiros confiáveis (COLLOMOSSE *et al.*, 2018).

No Brasil, não se dispõe de um modelo específico para aplicação da tecnologia *blockchain* na arquivística. Durante a pesquisa observou-se que, existem algumas iniciativas ainda incipientes para uso do *blockchain* além do setor financeiro,

em específico para criptomoedas.

No cenário internacional foram detectados três modelos distintos, institucionalizados em uso, a saber: o modelo do Reino Unido, denominado de *Archangel*, modelo Canadense DIDC e modelo de Dubai para administração pública. O modelo do Reino Unido o *Archangel* um dos três supracitados, é o que mais dispõe de requisitos necessários para aplicação na arquivística. Logo, nessa perspectiva foi proposto um modelo de aplicação da tecnologia *blockchain,* no âmbito da Arquivologia ao longo do ciclo de vida dos documentos arquivísticos digitais.

## 1.1 PROBLEMA

Na contemporaneidade com os impactos das TIC, alterou-se profundamente as formas de produção da informação orgânica e por conseguinte, sua materialidade e seu registro em um determinado suporte.

Nesse sentido, os DAD, apresentam um conjunto de características as quais problematizam as questões relacionadas de como produzir uma trilha de auditoria imutável ao longo do seu ciclo de vida nos ambientes informacionais digitais descentralizados.

Nessa direção, Cook (2012, p. 08), expõe que:

> O pós-moderno interrompe e se rebela contra o moderno. As noções de verdade universal ou conhecimento objetivo baseadas nos princípios do racionalismo científico do Iluminismo, ou no emprego do método científico ou crítica textual clássica, são descartados como quimeras. Usando análise lógica implacável, os pós-modernistas revelam a falta de lógica de textos supostamente racionais. O contexto por trás do texto, as relações de poder que moldam o patrimônio documental, e de fato, a estrutura dos documentos [...]. Os fatos nos textos não podem ser separados de sua interpretação, seja a intepretação em andamento, ou interpretação passada, nem o autor separado do assunto ou público, ou o autor separado da criação, e nem autoria separada do contexto. Nada é neutro. Nada é imparcial. Nada é objetivo. Tudo é moldado, apresentado, representado, reapresentado (COOK, 2012, p. 08).

Dessa forma, na pós-modernidade, a administração pública controlada pelo Estado, tem seu funcionamento de forma majoritária em um contexto de arquitetura hierárquica no modelo cliente servidor para autenticação de DAD em aplicações distribuídas. Assim, emana uma divergência significativa imposta nas vicissitudes da pós-modernidade na degradação da confiança em sistemas centralizados para

autenticação automatizada e distribuída do DAD, posto que esses sistemas não atendem de forma satisfatória aos contextos distribuídos (COLLOMOSSE *et al.* 2018).

Ademais, pode-se verificar que, essa degradação na confiança social institucional sob a égide do Estado ocorre, uma vez que, em muitos contextos centralizados, foram detectadas deficiências, em especial na formação de uma triha de auditoria descentralizada e imutável acerca dos registros dos DAD (COLLOMOSSE *et al.* 2018).

Observa-se que os DAD são de formas significativas diferentes dos documentos tradicionais analógiocos. Os DAD são voláteis, sujeitos a perdas, alterações intencionais ou não intencionais e corrupção.

Nesse sentido, acessibilidade dos DAD está sujeita a obsolescência e incompatibilidade de *hardware* e *software*. Nessa direção, ainda que o produtor se baseie em um DAD, isto é, nato digital no curso dos negócios é necessário manter uma cadeia de custódia digital arquivística, que contemple o modelo descentralizado, em vista de que os DAD atualmente na contemporaneidade encontram-se em sua grande maioria em sistemas distribuídos.

Assim, com base na problemática dos DAD, impostas pelas conjunturas da contemporaneidade nos ambientes informacionais digitais descentralizados, o problema de pesquisa aponta o seguinte questionamento: De que modo a tecnologia *blockchain* poderá colaborar nas aplicações descentralizadas na autenticação dos DAD no contexto da Arquivologia e como a tecnologia *blockchain* pode melhorar a interação no âmbito da confiança social institucional?

## 1.2 JUSTIFICATIVA

Essa pesquisa pretende colaborar de forma significativa com o domínio da Ciência da Informação, em especial com a Arquivologia, no que diz respeito a autenticação documental, em contextos descentralizados nos ambientes informacionais digitais e demonstrar a viabilidade de formação de uma trilha de auditoria ininterrupta e imutável ao longo do ciclo de vida do DAD.

Dessa forma, para Collomosse *et al.* (2018), a integridade do documento de arquivo é fundamental para a confiança dos usuários nos arquivos. Essa confiança atualmente é construída sob o contexto da reputação institucional, isto é, credibilidade

em uma autoridade central, quais sejam: o Estado, Universidade, instituições arquivísticas.

Nessa direção, no Brasil o Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal, vinculada à Casa Civil da Presidência da República, que objetiva assegurar a infraestrutura de chaves públicas Brasileira (ICP-Brasil), a qual é a autoridade suprema da cadeia de certificação (AC Raiz), institucionalizou, por meio da Instrução Normativa Nº 19, de 10 novembro 2021, a oficialização na utilização da tecnologia *blockchain* nos carimbos de tempo em documentos oficiais do governo (BRASIL, 2021). Na Instrução Normativa supracitada, o requisito nº 27 diz que:

> Quanto ao arquivamento perene das árvores de encadeamento do tempo, o servidor de carimbo de tempo (SCT) de implementar mecanismo de envio para bases de registro distribuídos (*blockchain*) segundo o *framework hyperledger*, de blocos com resumos criptográficos das árvores. (BRASIL, 2021, p. 15).

Sendo assim, propor novas possibilidades de abordagens arquivísticas por intermédio de tecnologias descentralizadas, torna-se altamente viável como, por exemplo, a utilização da tecnologia *blockchain*, que configura-se como tipo de *Distributed Ledger Technology* (DLT), cujo âmago de sua característica consiste na descentralização , uma vez que por intermédio da criptografia poderá realizar autenticações descentralizadas e automatizadas, bem como verificar a proveniência dos DAD (COLLOMOSSE *et al.* 2018).

Logo, para Silva (2000):

> [...] o tempo urge e o alerta lançado pelos colegas canadianos na década de oitenta para a necessidade de uma Arquivística integral, a nosso ver mesmo assim insuficiente, significou que não é mais possível enfrentar os desafios da Sociedade da Informação com a mente fechada no paradigma historicista, tecnicista e custodial herdado da Era das Luzes. A viragem de paradigma está aí. Já nos "entrou em casa" e temos de estar lúcidos e atentos para que não nos leve de arrasto, precipitando-nos no abismo da mais espessa e ignara incerteza (SILVA 2000, p. 31).

A justificativa dessa pesquisa surge como uma alternativa factível para autenticação de DAD, em contextos descentralizados em que poderá apoiar a cadeia de custódia digital arquivística, bem como colaborar na melhora da interação no âmbito da confinaça social institucional.

## 1.3 OBJETIVOS

### 1.3.1 OBJETIVO GERAL

Analisar os impactos da tecnologia *blockchain* no contexto da Arquivologia.

### 1.3.2 OBJETIVOS ESPECÍFICOS

- Apresentar a tecnologia *blockchain* e suas estruturas fundamentais;
- Indicar os principais modelos de uso da tecnologia *blockchain* no contexto arquivísitco;
- Apontar as relações de aplicação da tecnologia *blockchain* na autenticação distribuída;
- Propor modelo de autenticação descentralizada com aplicação da tecnologia *blockchain* ao longo do ciclo de vida dos documentos arquivísticos digitais.

## 1.4 METODOLOGIA

A pesquisa científica configura-se como um método de investigação, que propõe como objetivo, a solução de problemáticas por meio da produção de novos conhecimentos (BARROS; LEHFELD, 2002; GIL, 2002). Para Marconi e Lakatos, o método científico (2003, p. 83) “[...] é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista.”

Ainda, de acordo com Marconi e Lakatos (2008, p.157), a pesquisa científica “considerada um procedimento formal com método de pensamento reflexivo que requer tratamento científico e se constitui no caminho para se conhecer a realidade ou para descobrir verdades parciais”.

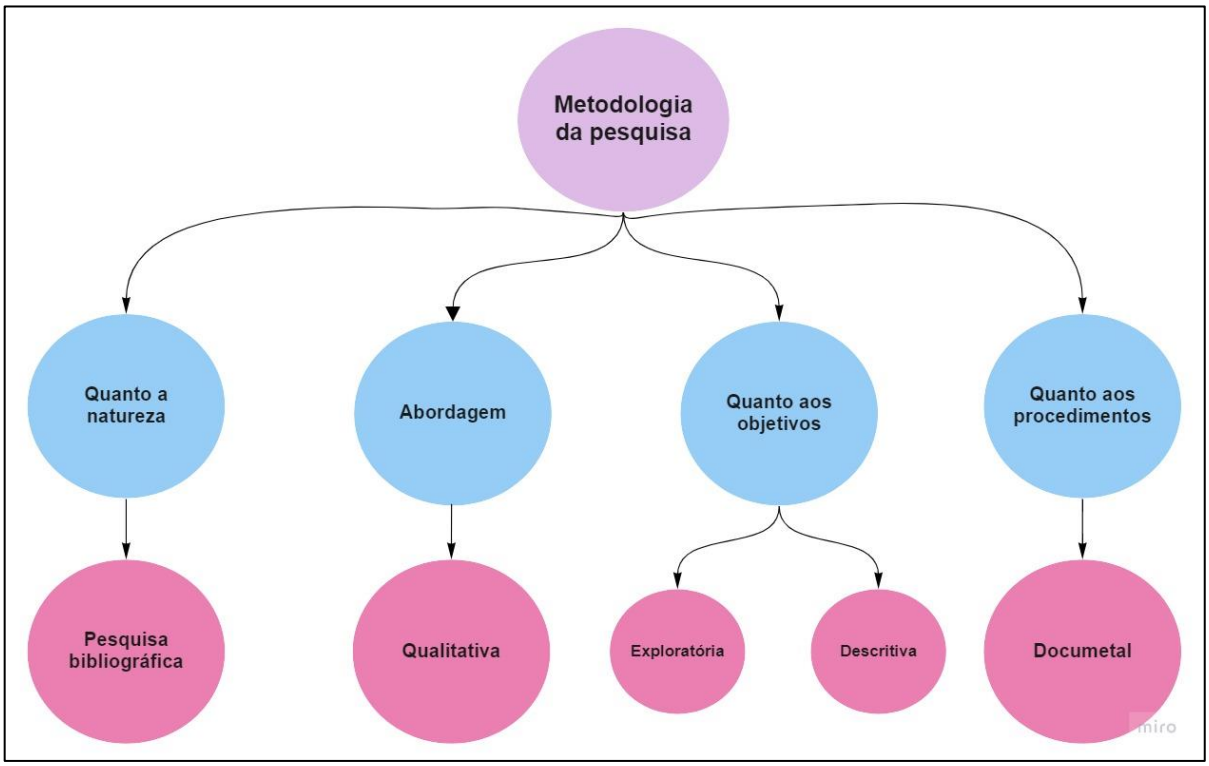
Caracteriza-se o presente estudo como de natureza pura, a qual “[...] procura desenvolver os conhecimentos científicos sem a preocupação direta com suas aplicações e consequências práticas. Seu desenvolvimento tende a ser formalizado, com vistas na construção de teorias e leis” (GIL, 2008, p.26), como teórica, "dedicada a reconstruir teorias, conceitos, ideias, ideologias, polêmicas, tendo em vista, em

termos imediatos, aprimorar fundamentos teóricos" (DEMO, 2000, p.20), bibliográfica e documental, “desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos.” (GIL, 2002, p.44), de cunho exploratório, que “[...] busca levantar informações sobre determinado objeto, delimitando assim um campo de trabalho, mapeando as condições de manifestações desse objeto”. (SEVERINO, 2016, p. 132). Ainda quanto aos objetivos é descritiva, em vista de que “As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno” (GIL, 2008, p.42), A respeito da abordagem delimita-se a pesquisa como qualitativa, que:

> Não tem qualquer utilidade na mensuração de fenômenos em grandes grupos, sendo basicamente úteis para quem busca entender o contexto onde algum fenômeno ocorre. Em vez da medição, seu objetivo é conseguir um entendimento mais profundo e, se necessário, subjetivo do objeto de estudo, sem preocupar-se com medidas numéricas e análises estatísticas. (LANDIM, *et al*. 2006, p. 55).

Nesse sentido, Marconi e Lakatos (2008, p.3) afirmam que “Toda pesquisa deve basear-se em uma teoria, que serve como ponto de partida para a investigação bem sucedida de um problema.” A presente pesquisa surgiu baseando-se nesses pressupostos com o intuito de ampliar o conhecimento acerca da temática da autenticação documental no contexto da Arquivologia nos ambientes informacionais digitais descentralizados. A figura 01, apresenta a metodologia de pesquisa adotada.

**Figura 01:** Metodologia de pesquisa.




Fonte: elaborado pelo autor 2022.

A figura 01, apresentou a síntese das escolhas metodológicas para realização da pesquisa. Esse estudo, conforme Gil (2008), enquadra-se como puro. Sendo assim, as abordagens bibliográficas buscam aclarar um problema com base em referências teóricas publicadas em artigos científicos, livros, dissertações e teses.

De acordo com Martins e Lintz (2000, p. 30):

> A pesquisa bibliográfica trata de uma abordagem metodológica mais frequente dos estudos exploratórios de pesquisa. A própria pesquisa procura explicar e discutir o tema proposto pelo trabalho exposto com base nas referências teóricas publicadas e relevantes.

A abordagem é qualitativa, posto que qualquer pesquisa que produza resultados não alcançados, por meio de procedimentos estatísticos, considera-se qualitativa (MAGALHÃES, 2007). Quanto aos objetivos, é exploratória, visto que este tipo de pesquisa tem por enfoque familiarizar-se com o fenômeno ou obter uma nova percepção e descobrir novas ideias. Na abordagem exploratória, desenvolvem-se descrições precisas das situações e aponta as relações efetivas entre seus componentes. Essa requer um planejamento muito flexível para que, possibilite

examinar os mais diversos aspectos de um problema (CERVO; BERVIAN; SILVA, 2007). Para Sampieri (1991, p. 59) os estudos exploratórios:

> Servem para aumentar o grau de familiaridade com fenômenos relativamente desconhecidos, obter informações sobre a possibilidade de levar adiante uma investigação mais completa sobre um contexto particular da vida real e estabelecer prioridades para investigações posteriores, entre outras utilizações.

Além disso, o estudo enquadra-se como pesquisa documental, que visa abordar os aspectos jurídicos administrativos, relacionados a autenticidade, autenticação dos documentos com base nos dispositivos jurídicos, a saber: Leis, Decretos, Resoluções, Portarias, Instruções Normativas, Diretrizes com o objetivo de identificar os pilares que compõem esses dispositivos jurídicos na contemporaneidade nos ambientes informacionais digitais no âmbito arquivístico.

Segundo Gil (2002), a investigação documental é aquela realizada com base nos próprios documentos “que não receberam qualquer tratamento analítico” ou “[...] que de alguma forma já foram analisados”.

O desenvolvimento da pesquisa documental faz-se em meio a documentos textuais, audiovisuais, iconográficos, sonoros e quaisquer documentos relacionados ao objeto de investigação. Podem ser coletados na forma pura, isto é, que não sofreram intervenções analíticas, e/ou em circunstâncias denominadas como fonte secundária, ou seja, documentos provenientes de outra fonte de informação. (GIL, 2008).

Tomando-se por base das premissas a respeito das escolhas metodológicas, seguem os procedimentos metodológicos: bibliográfico na literatura nacional e internacional em livros, periódicos, dissertações e teses, nos idiomas português e inglês, em relação aos seguintes temas tratados na pesquisa: *Blockchain*, Pós-modernidade, Modernidade Líquida, Certificação Digital, Criptografia, Hash, Assinatura Digital, Arquivologia: Princípios Arquivísticos, Autenticidade Documental, Repositórios Digitais, Metadados, Preservação Digtial, Gestão de Documentos, Autenticação e Confiança. O levantamento bibliográfico acerca dos assuntos investigados foram realizados, sem delimitações temporais, nas seguintes fontes de dados: no acervo bibliográfico da Universidade Estadual Paulista “Júlio de Mesquita filho” (UNESP), no sistemas de bibliotecas da Universidade Estadual de Londrina (UEL); nas bases de dados utilizou-se a Base de Dados Referências de artigos em

Periódicos em Ciência da Informação (BRAPCI), na base de dados em arquivística (BDA), Bibliotecas digitais de teses e dissertações dos programas de pós-graduação em Ciência da Informação nacionais e internacionais, Biblioteca digital Brasileira de teses e dissertações (BDTD), repositórios digitais institucionais em Ciência da Informação, Arquivística e Computação.

A seleção dos textos e coleta de dados foram relizadas por meio de palavras chave supracitadas nas bases de dados. Relizou-se a seleção dos materiais pertinentes para pesquisa e foram realizadas as leituras dos textos e por conseguinte o fichamento dos textos com conteúdo pertinente para o desenvolvimento da tese.

Nessa direção, a seção 1 compreende a introdução e escopo da tese. A seção expõe o problema de pesquisa, justificativa, objetivo geral, objetivos específicos e metodologia.

Na seção 2, é apresentado de forma sintética, a contemporaneidade, tomando-se por base, o contexto do mundo líquido proposto por Zygmunt Bauman. Logo, por intermédio do entendimento do conceito de modernidade líquida, a qual proporcionará os subsídios imprescindíveis, que demonstrará os impactos das tecnologias de comunicação e informação e por conseguinte, o surgimento de tecnologias descentralizadas nos ambientes informacionais digitais, tais como: *blockchain*, as quais podem configurar-se em possibilidades de novas abordagens na arquivologia.

Na seção 3, apresenta-se em um primeiro momento, um introito acerca, dos conceitos básicos a respeito da criptografia e função *hash,* os quais são pré-requisitos altamente desejados e necessários para a compreensão da certificação digital e da tecnologia *blockchain*. A seção aborda as estruturas fundamentais da tecnologia *blockchain*.

Na seção 4, apresenta-se um estudo relacionado aos repositórios digitais com relção as iniciativas e estratégias de implementação, modelo conceitual *Open Archives Information System* (OAIS), gestão de documentos – *records management* (RM) e gestão de conteúdos empresariais - *Enterprise Content Management* (ECM).

A seção 5, aborda os conceitos acerca dos metadados e da autenticidade documental, bem como seus componente, tais como: integridade e autenticidade.

Na seção 6, de discussão e resultados da tese é apresentado os impacos da tecnologia *blockchain* no contexto arquivístico, por meio das camadas de confiança da interação da tecnologia *blockchain* e apresenta-se os principais modelos lógicos

para autilização da tecnologia *blockchain* na Arquivologia, a saber: modelo do Reino Unido, o *Archangel*, modelo Canadense o DIDC e modelo da admisntração pública do Governo de Dubai. Por fim, demonstra-se a proposta de um possível modelo para aplicação na autenticação descentralizada automatizada dos DAD ao longo de seu ciclo de vida.

## 2 MODERNIDADE LÍQUIDA/PÓS-MODERNIDADE

Essa seção tem como enfoque apresentar, de forma sintética, a contemporaneidade, tomando-se por base o contexto do mundo líquido proposto por Bauman. Logo, por intermédio do entendimento do conceito de modernidade líquida, a qual proporcionará os subsídios imprescindíveis, que demonstrará os impactos das tecnologias de comunicação e informação e por conseguinte o surgimento de tecnologias descentralizadas nos ambientes informacionais digitais, tais como: *blockchain*, as quais podem configurar-se em possibilidades de novas abordagens na arquivologia.

A modernidade líquida é um conceito proposto pelo sociólogo polonês Zygmunt Bauman, de origem judaica, o qual iniciou suas pesquisas na Universidade de Varsóvia. No entanto, emigrou da Polônia e reconstruiu sua carreira como pesquisador no Canadá, Estados Unidos da América (EUA) e Austrália. Por fim, estabeleceu-se na Universidade de *Leeds*, na Inglaterra, Grã Bretanha (BAUMAN, 2001).

De acordo com Bauman (2001) a utilização dos conceitos pós-moderno ou pós-modernidade poderá produzir imprecisões conceituais. Dessa forma, o autor renuncia a adoção desses conceitos, uma vez que o discurso a respeito da temática torna-se dúbio. Sendo assim, Bauman (2004, p.321) pontua:

> Uma das razões pelas quais passei a falar em modernidade líquida e não em pós-modernidade é que fiquei cansado de tentar esclarecer uma confusão semântica que não distingue sociologia pós-moderna de sociologia da pós-modernidade, pós-modernismo de pós-modernidade. No meu vocabulário, pós-modernidade significa uma sociedade (ou, se prefere, um tipo de condição humana), enquanto pós-modernismo refere-se a uma visão de mundo que pode surgir, mas não necessariamente, da condição pós-moderna.

Para Bauman (2004), há uma continuidade da modernidade na pós-modernidade com pontos diferentes. Assim, não se trata de uma ruptura de época, de moderna para pós-moderna, mas de uma transformação no âmago estrutural de forma contínua. Nessa direção, Bauman (2004), frequentemente era denominado de pós modernista. Dessa forma, o termo modernidade líquida foi cunhado pelo autor, o qual o emprega, em suas obras intelectuais, em substituição aos termos pós-moderno e pós-modernidade.

O repúdio ao conceito de pós-modernidade se caracteriza pelo fato problemático da produção de sentido, posto que, modernidade é entendida como um período histórico que começou na Europa, no século XVII, com profundas transformações sócio estruturais e intelectuais. Atingiu, seu ápice primeiramente, como projeto cultural, com base no iluminismo e, posteriormente, como forma de vida socialmente consumada, com o desenvolvimento da sociedade industrial (BAUMAN, 1999).

O mundo líquido é utilizado para explicar o sentido de um ambiente fluido, leve, rodeado de precariedade e incertezas, no qual suas principais características são: continuidade e descontinuidade da modernidade, que são permeadas de instabilidade, inconstância, flexibilidade, vulnerabilidade e leveza (BAUMAN, 2001). Nesse sentido, os líquidos:

> [...] diferentemente dos sólidos, não mantém sua forma com facilidade. Enquanto os sólidos têm dimensões especiais claras, mas neutralizam o impacto, portanto, diminuem a significação do tempo (resistem efetivamente a seu fluxo ou tornam irrelevante), os fluidos não se atêm muito a qualquer forma e estão constantemente prontos e propensos a mudá-la. (BAUMAN, 2001, p.08).

O derretimento dos sólidos trata de desconstruir para construir. Se, na modernidade, os princípios e os pressupostos teóricos atendiam as necessidades, essas certezas não se aplicam ao contexto da modernidade líquida, na qual tudo flui com rapidez. As mudanças são rápidas e, consequentemente, nada é fixo.

De acordo com Bauman (2001, p. 21), “[...] fixar-se muito fortemente, sobrecarregando os laços com compromissos mutuamente vinculantes, pode ser positivamente prejudicial, dadas as novas oportunidades que surgem em outros lugares”.

O momento atual é extremamente favorável para análise da modernidade, cuja a fidedignidade e validade das conquistas e os desastres modernos podem ser discutidos, desconsiderados e revalidados. Todavia, a fluidez está presente neste cenário, a qual se caracteriza por evitar que os padrões se perpetuem em rotinas e tradições.

Para Bauman (2001), não existe um momento de ruptura entre modernidade e modernidade líquida. Observa-se um processo intenso, de liquefação dos consolidados constructos modernos. A interdisciplinaridade torna-se imprescindível

neste mundo líquido para compreensão desta conjuntura híbrida, na qual as disciplinas dialogam para construir as abordagens inovadoras.

A vida moderna é desenraizadora, isto é, derrete os sólidos. No entanto, isso era realizado para ser novamente reenraizado e atualmente as tecnologias (*Know-Hows*) permanecem em fluxo, voláteis, desreguladas, flexíveis (BAUMAN, 2004).
Na concepção de Bauman (2005 p. 57), os fluidos

> "São assim chamados porque não conseguem manter uma forma por muito tempo e, ao menos que sejam derramados num recipiente apertado, continuam mudando de forma sob a influência até mesmo das menores forças".

Nessa direção, é imprescindível que a informação seja explicitada em uma materialidade, posto que na sua ausência, as abordagens sociais, culturais e éticas perdem seu sentido (FROHMANN, 2008).

Nos ambientes informacionais digitais, a materialidade da informação orgânica, bem como o seu registro em um DAD é contrastiva, em vista de que a dimensão física e a intelectual são interdependentes, uma vez que ao longo do tempo o suporte, no qual foi registrada a informação, sofrerá separação do conteúdo. Nesta conjuntura, o DAD poderá ter comprometida sua fixidez e o conteúdo tornar-se instável, como resultado dos atributos do mundo líquido, no qual está presente o intenso processo de liquefação dos sólidos constructos teóricos da arquivística clássica.

Nos ambientes informacionais digitais, a informação é materializada por meios institucionais e tecnológicos. Verifica-se a existência de vastas pesquisas a respeito dos efeitos da oralidade, as tabuletas de argila, o papiro, o papel, a imprensa, o telégrafo, o rádio, o filme, a televisão acerca das estruturas de informação (FROHMANN, 2008).

Os objetos digitais são, fundamentalmente, distintos de variadas formas de todos esses. São casos paradigmáticos de um novo tipo de documentação, com base na sua imersão tecnológica, sua levíssima fisicalidade eletrônica, quase sem peso, a qual outorga-lhe grande velocidade, força e energia. A documentação digital desafia o cenário tradicional (FROHMANN, 2008).

Dessa forma, o objeto digital é independente e não solidário ao suporte, no qual eram registradas as informações nos documentos tradicionais em papel. A sua

fisicalidade leve não preserva a inalterabilidade da relação com o suporte, conteúdo e estrutura. Surgem múltiplas relações, que contradizem a milenar unidade de informação com sua materialidade e o suporte (SILVA, 2011).

Observa-se que, o conceito de materialidade, favorece a compreensão do caráter social e público da informação no mundo líquido. Todavia, na sociedade contemporânea, em alguns aspectos, seguem intocados por mudanças como, por exemplo, a criação, distribuição, acesso às informações e autenticidade (HEDSTROM, 2001).

Os objetos digitais têm sua fisicalidade extremamente leve, a qual exerce força e poder por intermédio de sua materialidade. A materialização da informação em ambientes informacionais digitais, por meio de sua imersão nas TIC, culmina em características públicas, sociais, políticas e culturais (FROHMANN,2008).

Ademais, a fisicalidade da informação orgânica está relacionada ao meio pelo qual se concretiza o registro. Tomando-se por base suas propriedades físicas, todo objeto pode suportar informação, em uma escala elementar ou referencial do registro, isto é, uma letra, um número, uma palavra, um conceito, *bits*, dados, metadados. O suporte, no qual foi registrada a informação, poderá comportar especificidades, a saber: áudio, imagens, multimídias, *hiperlinks*, interconexão de sistemas ou redes. (RABELLO, 2019).

Nessa direção, de acordo com Dicionário Brasileiro de Terminologia Arquivística (DBTA), o conceito de documento é definido como uma, “Unidade de registro de informações, qualquer que seja o suporte ou formato” (BRASIL 2005, p.73). Já para a Câmara Técnica de documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ) do Arquivo Nacional (AN), o documento arquivístico é o “Documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência” (BRASIL, 2020a, p. 24).

Sendo que, os documentos arquivísticos podem ser analógicos ou digitais. A CTDE, manifesta a distinção entre o conceito de documentos eletrônicos e documentos digitais: os eletrônicos se referem à “Informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico”, já os digitais à “Informação registrada, codificada em dígitos binários, acessíveis e interpretável por meio de sistema computacional” (BRASIL, 2009, p.13).

Nota-se, então, uma distinção conceitual entre os documentos eletrônicos e documentos digitais, sendo aqueles analógicos ou digitais, enquanto estes como eletrônicos, entretanto, por uma sequência de *bitstream.* Por fim, o conceito de objeto digital é um:

> Conjunto de uma ou mais cadeias de *bits* que registram o conteúdo do objeto e de seus metadados associados. A anatomia do objeto digital é percebida em três níveis: 1. nível físico – refere-se ao objeto digital enquanto fenômeno físico que registra as codificações lógicas dos bits nos suportes. Por exemplo, no suporte magnético o objeto físico é a seqüência do estado de polaridades (negativa e positiva); nos suportes ópticos é a seqüência de estados de translucidez (transparência e opacidade); 2. nível lógico – refere-se ao objeto digital enquanto conjunto de sequências de bits, que constitui a base dos objetos conceituais; 3. nível conceitual – refere-se ao objeto digital que se apresenta de maneira compreensível para o usuário, por exemplo, o documento visualizado na tela do computador (BRASIL, 2009, p.18).

Verifica-se que, as informações orgânicas materializadas e registradas em um suporte analógico, com exceção dos analógicos eletrônicos, dispõem de um conteúdo informacional estável e com menor grau de fluidez. Por sua vez, o suporte digital, cujo conteúdo instável é muito mais fluido, posto que seu registro ao nível de camada lógica pode ser representado com valores lógicos de 0 e 1, ou seja, dígitos binários (RABELLO, 2019).

Desse modo, o documento corresponde à materialidade da informação, em vista de que a concepção da materialidade é imprescindível para a compreensão do caráter social da informação (FROHMANN, 2008).

A concepção de documento de arquivo, autêntico, o qual poderá conduzir à verdade, é o mote central da Diplomática, em conjunto com os preceitos positivistas, os saberes da Diplomática Clássica, que orientaram outras metodologias no século XXI, tais como: os saberes jurídicos, historiográficos e arquivísticos. Portanto, nessa concepção, a presunção de permanência da semântica originária do documento, desde as evidências físicas, materializada em um registro institucionalizado, representado, intermediado e concebido como meio de prova é fundamental para os DAD (RABELLO, 2019).

Dessa forma, novas tecnologias como, por exemplo, o *blockchain* poderá ser utilizado no contexto da Arquivologia para fins de autenticação descentralizada, com

base na contemporaneidade e seus quesitos fundamentais, tais como: fluidez, momentaneidade, desapego e rapidez.

## 3 *BLOCKCHAIN*

Essa seção, apresenta em um primeiro momento um introito acerca dos conceitos básicos a respeito da criptografia e função *hash,* os quais são pré-requisitos altamente desejados e necessários para a compreensão da certificação digital e da tecnologia *blockchain*.

O certificado digital para o Instituto Nacional de Tecnologia da Informação (ITI) (BRASIL, 2021), é um registro eletrônico digital assinado, o qual é gerado por intermédio de um procedimento da certificação digital, que comprova as relações entre chaves criptográficas.

Para Menke (2005, p. 42) “A ferramenta tecnológica da assinatura digital tem por finalidade jurídica comprovar a autoria e validar a manifestação da vontade, associando um indivíduo a uma declaração de vontade veiculada eletronicamente”.

Logo, a assinatura digital é:

> O resultado de uma operação matemática, utilizando algoritmos de criptografia assimétrica. Além de viável tecnicamente e de confiabilidade garantida, pode ser obtida através da utilização de certificado digital de assinatura, que confirma identidade do titular e autentica sua assinatura eletrônica (MARCACINI, 2002, p.32).

A criptografia divide-se em dois tipos básicos, tais como: assimétrica e simétrica. A primeira consiste-se em duas chaves, uma pública e uma privada, na qual os dados criptografados com o uso de uma chave, só podem ser decifrados com outra chave. A segunda, a simétrica, utiliza-se de uma única chave para cifrar e decifrar os dados (KOBAYASHI, 2007). Sendo que, o certificado digital no Brasil, deve ser emitido por uma Autoridade Certificadora (AC), a qual é a entidade responsável por emitir e garantir a validade do certificado.

O certificado digital da Infraestrutura de Chaves Públicas – Brasil (ICP Brasil), além de personificar o cidadão na rede mundial de computadores, garante, por força da Lei nº 14.063 de 23 de setembro de 2020, validade jurídica aos atos praticados com seu uso (BRASIL, 2020b). A ICP-Brasil trabalha com uma hierarquia, na qual a Autoridade Certificadora Raiz (AC Raiz) é o ITI, autarquia federal vinculada a Casa Civil da Presidência da República. O ITI é responsável por gerar as chaves da AC e regulamentação de atividades de cada uma. Para uma assinatura, em suporte papel, geralmente é usado algum tipo de marca física para identificação de autenticação da

assinatura digital utilizados na confirmação de identidade na *web*, em *e-mail*, em redes privadas e em documentos digitais com verificação da integridade de suas informações (RESENDE, 2009). A série S reúne certificados com sigilo, os quais são utilizados na codificação de documentos de base de dados, de mensagens e de outras informações eletrônicas sigilosas. Todas as séries são diferenciadas por seu uso, nível de segurança e de validade (RESENDE, 2009).

Segundo Barboza (2018), no Brasil, os tipos de certificados mais usados são os tipos A1 e A3. O certificado digital A1 é o de menor segurança, o qual é gerado e armazenado no próprio computador. Os dados são protegidos por uma senha de acesso. Somente é possível acessar e mover com a chave privada associada. Caso a chave privada seja perdida, um novo certificado deverá ser adquirido e todas as etapas deverão ser refeitas pelo usuário. O certificado do tipo A3 grava-se em dispositivos eletrônicos próprios, como *token* ou *smart card*. Portanto, a chave privada pode ser transportada de maneira segura realizando transações eletrônicas, com garantia e integridade das informações. A partir do momento que for necessário, quando algo assinado fosse enviado a AC, com um tipo de certificado diferente, se tornaria um problema administrar todos os formatos diferentes. Para resolver esse problema, foi criado e aprovado pela *International telecomunication Union* (ITU), um padrão para certificado. O padrão chamado é X-509 e seu uso está bem difundido (TANENBAUM, 2003).

Assim como na criptografia assimétrica, a assinatura digital é uma sequência de números resultantes de uma operação matemática conhecida como função *hashing*. Essa função analisa todo o documento ou arquivo, com a base no algoritmo matemático, que gera um tamanho específico em *bytes*, que representa o documento, conhecido como resumo. A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, posto que os algoritmos de criptografia assimétrica são muito lentos (MONTEIRO; MIGNONI 2007). A submissão de resumos criptográficos ao processo de decifragem com a chave privada reduz o tempo de operação para gerar uma assinatura, por serem os resumos, em geral, muito menores que o documentos.

A autenticação dos algoritmos de criptografia de chave pública opera em conjunto com uma função resumo, também conhecida como assinatura digital utilizados na confirmação de identidade na *web*, em *e-mail*, em redes privadas e em

documentos digitais com verificação da integridade de suas informações (RESENDE, 2009).

A Medida Provisória n° 2.200-2, de 24 de agosto de 2001, foi o marco inicial, que possibilitou garantir a validade jurídica dos documentos digitais e a utilização de certificados digitais para atribuir autenticação aos documentos. Esse fato tornou o certificado digital um instrumento válido juridicamente em todo território nacional (BRASIL, 2001). Os criptos sistemas provêm técnicas para embaralhar ou cifrar mensagens de forma que, aparentemente, tornam ilegíveis, e, que posteriormente, possam obter novamente a mensagem original por meio do texto embaralhado. Quaisquer criptos sistemas devem garantir que as mensagens que trafegam em um canal de comunicação tenham privacidade e que a mensagem seja autentica sem alteração (MARTINI, 2001). Os criptos sistemas pode ser dividido em dois tipos distintos, segundo o método que realizam: criptografia simétrica e assimétrica. Segundo Train (2007) a criptografia simétrica é o tipo mais simples de criptografia, pois o emissor e o receptor fazem o uso de uma única chave para codificar e decodificar uma determinada informação. Portanto, a chave que o emissor usa para codificar a informação é a usada pelo receptor para decodificá-la. Na sequencia, é apresentada as conjunturas do surgimento da tecnologia *blockchain* e seus conceitos fundamentais.

O prelúdio da tecnologia *blockchain* foi no início da década de 1970, com o surgimento das bases de dados. Esse período, em questão ficou conhecido como *big iron,* no qual as grandes corporações do setor tecnológico como, por exemplo, *International Bussines Machine* (IBM) armazenavam seus dados em grandes bancos de dados (CESAR, 2019). Nessa direção, nos anos 1990, o criptógrafo norte americano, David Chaum foi pioneiro na criação da primeira moeda *on-line* na Holanda, o *DigiCash*, que consistia em uma extensão de um algoritmo criptográfico conhecido como Rivest, Shamir, Adleman (RSA), que inicialmente despertou o interesse de várias instituições financeiras em seu uso. Porém, o acumulo de erros administrativos ao longo do ciclo de vida do *DigiCash*, culminou no seu desuso e por conseguinte no seu desaparecimento em 1998. (NARAYANAN *et al.* 2016).

Já a segunda geração de dinheiro digital na *Internet* se apropriaram das experiências do *DigiCash*. Dessa forma, os sistemas para pagamentos monetários tendo como base a *internet*, destacou-se o *paypal*, que oferecia aos usuários possibilidade de utilizar dinheiro nas plataformas de navegadores *web*. O *paypal* foi

capaz de realizar, pela primeira vez, a transferência de recurso financeiros *on line* por meio de uma rede *peer to peer* – ponto a ponto (P2P) (PERSET, 2010).

Finalmente o evento, que transformou o contexto das criptomoedas foi a crise das hipotecas conhecida como *subprime* em 2008 nos Estados Unidos da América (EUA), a qual quase neutralizou o sistema financeiro dos EUA, que provocou também problemas significativos para grande maioria das instituições financeiras. Sendo assim, esse evento catastrófico, com um viés financeiro, despertou o alerta para as principais economias globais, que culminou na conjuntura necessária para o surgimento da tecnologia conhecida como *blockchain* (BARKATULLAH, HANKE 2015).

Logo surge, em 2008 o b*lockchain*, com a publicação do artigo *Bitcoin*: *a peer-to-peer eletronic cash system*. O autor ou seus autores utilizaram o pseudônimo conhecido por Satoshi Nakamoto para apresentar a tecnologia cunhando-se assim o conceito de *blockchain* e *bitcoin*, a pesquisa supracitada apresenta os princípios fundamentais, bem como o funcionamento do *blockchain* com sua aplicação em criptomoedas (NAKAMOTO, 2008).

Nesse sentido, para Dannen (2017) a tecnologia *blockchain* tem como base a convergência de três tecnologias principais distintas, pré-existentes e consagradas, a saber: redes *peer to peer* - ponto a ponto (P2P), criptografia assimétrica e *hash* criptográfico. Para Nakamoto (2008), o *blockchain* tem como fundamento cinco princípios distintos, tais como: função matemática de mão única, isto é, *hash*, carimbo de registro do tempo de criação ou modificação do arquivo – *true time stamp*, assinatura digital, rede descentralizada – *peer to peer* – ponto a ponto (P2P) e algoritmo de produção de novos blocos para cadeia de blocos pré-existentes.

Nota-se que, o conceito de *Blockchain* é distinto do conceito de *bitcoin*, essas tecnologias frequentemente são associadas como sinônimos. A criptomoeda *bitcoin* configura-se, como uma das várias aplicações de possíveis usos do *blockchain*, sendo o *bitcoin* o primeiro uso da tecnologia (TAPSCOTT, TAPSCOTT, 2017).

Percebe-se, a diferença entre *blockchain* e *bitcoin*, sendo aquele um *distributed ledger technology* (DLT), plataforma na qual é construída o *bitcoin*. Nessa direção, como o objeto de estudo dessa pesquisa tem em seu escopo a tecnologia *blockchain* e suas possibilidades de aplicação além do *bitcoin*, as características detalhadas da criptomoeda não serão abordadas. O *blockchain,* enquanto uma tecnologia, pode ser compreendida em três tipos principais, quais sejam: *blockchain*

1.0, *blockchain* 2.0, *blockchain* 3.0. A primeira categoria refere-se as criptomoedas e atividades no contexto de pagamentos digitais. Já o segundo tipo refere-se ao setor financeiro com associação da *internet of things* (IoT) – *internet* das coisas, as tecnologias de *smart contracts* – contratos inteligentes com aplicações para ativos econômicos e financeiros. Por fim, a terceira diz respeito a outros domínios como, por exemplo, governo, saúde, cultura e arte (SWAN, 2015).

A tecnologia *blockchain* consiste em um banco de dados distribuídos na rede mundial de computadores, no qual todos os registros e saídas de dados são gravados cronologicamente em uma cadeia de blocos. Alguns participantes, isto é, os mineradores dessas redes ofertam esforços computacionais para gravação de novos blocos, e ao realizar essas operações, esses efetuam cálculos de *hash* para solucionar os problemas criptográficos apresentados obtendo, por conseguinte, uma parte do valor transacionado nas operações, que são entendidas como mineração (NAKAMOTO, 2008).

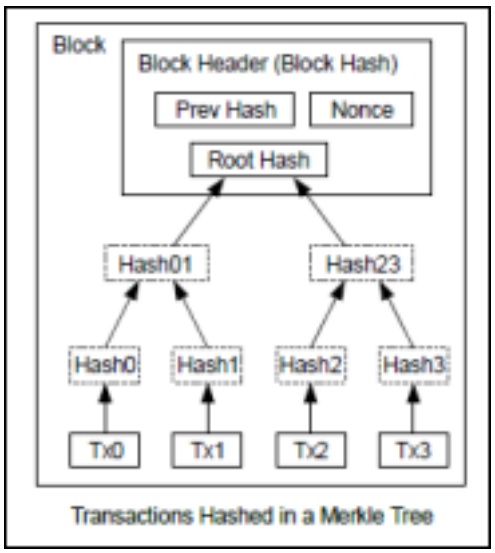
O *blockchain* é composto por uma cadeia de registros imutáveis públicos e distribuídos, cujas cadeias de registro são encadeadas uma as outras por intermédio de chaves públicas, de entrada e saídas. São consideradas imutáveis, em vista de que quando um registro é inserido, esse não pode ser alterado. As cadeias são públicas, visto que o acesso poderá ser realizado por meio da *internet.* E por fim, as cadeias de registro estão armazenadas e replicadas em várias máquinas conectadas na rede mundial de computadores, isto é, o sistema não é armazenado em um único servidor central (NARAYANAN; BONNEAU; FELTEN; MILLER; GOLDFEDER; OKURPSKI; 2016).

Dessa forma, o *blockchain* é um grande banco de dados distribuído, que arquiva todas as movimentações financeiras das transações de forma irreversível. Dispõe de um sistema de inventário com gravação, rastreamento, monitoramento e transferência de ativos. A primeira aplicação funcional do *blockchain* foi a *cripto* moeda denominada *bitcoin* (SWAN, 2015). Assim, o blockchain é um *ledger* - livro razão distribuído e imutável, que forma um banco de dados distribuído por intermédio de uma rede *peer to peer* (P2P), na qual são registradas operações com ativos e transações, que podem ser: tangíveis e intangíveis. O primeiro pode ser, por exemplo, os registros de imóveis como propriedades. Já o segundo são marcas e diretos autorais. Os sistemas atuais de *ledger* centralizados tradicionais podem apresentar certas deficiências, tais como: custo operacional elevado, pouca

transparência e dificuldade na execução de auditabilidade, que podem culminar em fraude e resultados equivocados. Dessa forma, o *blockchain* se configura em um sistema *ledger* descentralizado e apresenta certas vantagens ao modelo centralizado como as redes baseadas em cliente servidor, em vista de que podem reduzir os custos operacionais, bem como prover transparência nos processos de auditoria, evitando-se as atividades fraudulentas.

Sendo assim, o *blockchain* é uma arquitetura de blocos de dados distribuídos conectados por meio de criptografia. Esses blocos são encadeados de forma linear e por conseguinte dispõem de uma cronologia, a qual é conectada com próximo bloco, forma-se então uma cadeia de blocos, isto é, o *blockchain*. Logo, com o advento da tecnologia *blockchain* viabilizou-se inicialmente os registros distribuídos por meio de criptografias para uso em moedas digitais. Nesse sentido, Nakamoto, em 2008, concebeu a tecnologia *blockchain,* a qual é composta pela convergência de vários componentes tecnológicos, que será apresentada na figura 02.

**Figura 02**: Anatomia do bloco.




Fonte: Nakamoto, 2008.

A figura 02 apresentou anatomia de um bloco, que fará parte da cadeia de blocos. O bloco é composto de várias camadas, a saber: *Block (Current_ block_header_version), Block Header - Block hash, Reference Prev Block - prev hash (Hash_Prev_Block), nonce (nNonce), Root node - Root hash (Hash_Merkle_Root).* O *block* é a versão do bloco, ou seja, o número de cada bloco. Já o *Header* é o resumo criptográfico do bloco. O terceiro o *Reference Prev Block* é o *hash* do bloco anterior.

O *Nonce* é o sequencial numérico atribuído para o bloco de forma aleatória. E por fim, *Root Hash,* que armazena a raiz dos resumos criptográficos, a qual é utilizada para prover integridade aos blocos (NAKAMOTO, 2008).

Nessa direção, o *blockchain* surge como uma proposta que dispõe de um mecanismo de consenso baseado no modelo de *proof of work,* que foi inicialmente sinalizada por Cynthia Dwork e Moni Naor em 1992, no artigo intitulado *Pricing via processing or combatting junk mail*, o qual não utilizou o termo *proof of work* (PoW). Todavia, já apresentava que o usuário deveria provar que realizou alguma tarefa para viabilizar a utilização de um determinado serviço, com o objetivo final de inviabilizar o uso de serviços desprovido de serventia (DWORK; NAOR, 1992). O termo PoW foi cunhado, posteriormente, em 1999, por Markus Jakobsson e Ari Juels, formalizado por intermédio do trabalho *Proffs of Works and a bread pudding protocols* (JUELS; JAKOBSSON, 1999).

O consenso distribuído em uma rede *peer to peer* (P2P), do tipo distribuída é o processo realizado por meio de algoritmos pelos quais os nós participantes da rede ponto a ponto estão de acordo acerca de um conjunto de dados, que representa um valor único (BASHIR, 2017). Dessa forma, o procedimento de consenso é formado por uma sequência lógica de ações, ou seja, um algoritmo de consenso que permite a validação dos valores propostos pela maioria dos nós (BASHIR, 2017).

Sendo assim, a tecnologia *blockchain* atualmente utiliza-se dos principais métodos de validação consensual, tais como: *proof of work* e *proof of stake*. O primeiro consiste, em um mecanismo de consenso, no qual cada nó participante da rede busca uma possível solução para o enigma criptográfico com objetivo de adicionar um novo bloco à cadeia de blocos existentes. Para criação de blocos novos pressupõe a participação dos mineradores, os quais empenham-se em conseguir uma solução ao desafio critptográfico. Para algumas aplicações com a tecnologia *blockchain,* o procedimento de consenso consiste em propor um valor pré-determinado denominado de *nonce*, que está contido no cabeçalho do bloco *Head,* e, por conseguinte, quando o valor do *hash* seja inferior ao parâmetro dificuldade *threshold* estabelecido, ocorre a inserção de um novo bloco. A figura 03, demonstra por meio de um algoritmo a condição para inserção de novos blocos nas cadeias de blocos pré existentes.

**Figura 03:** Condição para inserção de novo bloco

| Se *HASH* < menor que < *NONCE* |
| --- |
| Adicionar novo bloco |

Fonte: Baseado em Nakamoto (2008).

A figura 03, apresentou como os mineradores realizam a inserção de novos blocos, que ocorre quando se obtém uma solução criptográfica. Tomando-se por base um *threshold* global (dificuldade) e o maior índice de bloco conhecido pelo minerador, este seleciona um *nonce* (número aleatório) e aplica um algoritmo com uma função aleatória para o *hash*, nos campos do *header* – cabeçalho.

Assim, enquanto o resultado do *hash* não for menor que o *threshold*, o *nonce* é substituído por outro *hash*. Logo, quando o *hash* for menor que o *nonce*, um novo bloco será adicionado, em vista de que a condição pré-estabelecida com o algoritmo proposto será contemplada.

Nesse sentido, pode-se constatar que, com base no PoS, derivou-se o *Delegated Proof of Stake* (DPoS), no qual consiste em um mecanismo que definem determinada quantidade de participantes e selecionam seus representantes para gerar e validar blocos (ZHENG; XIE; DAI; CHEN; WANG, 2017).

Verificou-se que, o mecanismo de consenso *proof of stake* (PoS) – prova de participação consiste na seleção do nó participante de forma aleatória, que poderá inserir um bloco novo à cadeia de blocos pré-existente. Esse algoritmo de validação consensual foi proposto por Nick Szabo (2011), o grande diferencial do PoS em relação ao PoW, versa na validação e aprovação de novos blocos, de forma distinta da mineração de *hashes* propostas pelos PoW.

Por fim, nota-se a existência do *Proof of Activity* (PoA), o qual é um mecanismo de consenso híbrido, em vista de que utiliza características do algoritmo PoW e PoS, usufruindo dos benefícios de ambos. Esse algoritmo de validação consensual determina, que o bloco minerado seja assinado por vários minerados para ser validado. Assim, caso algum dos nós participantes concentrar mais de 50% da rede, esse não estará habilitado a inserir novos blocos (ZHENG; XIE; DAI; CHEN; WANG, 2017). O PoA determina, como ponto central, quais os usuários ativos, são contemplados das atividades ofertadas na rede (BENTOV, LEE, MIZIRAHI, ROSENFELD, 2014).

O quadro 01, apresenta os principais mecanismos de validação consensual.

Quadro 01: Principais mecanismos de consenso aplicados na tecnologia *blockchain*

| Mecanismos de Consenso | *Proof of Work* (PoW) | *Proof of Steak* (PoS) | *Delegated proof of steak* (DPoS) | *Proof of Activity* (PoA) |
|---|---|---|---|---|
| Tipos de Mecanismos | Puro | Puro | Puro | Híbrido |
| Idealizadores /Percursores | Cynthia Dwork e Moni Naor Satoshi Nakamoto | Nick Szabo | Daniel Larimer | Iddo Bentov, Charles Lee, Alex Mizrahi e Meni Rosenfeld |
| | Verificação se algum minerador Chegou a uma solução. | Sorteio baseado na quantidade de ativos | Processo de Seleção de testemunhas de criação dos blocos e delegados | Verificação do cabeçalho do bloco vazio Verificação dos usuários ganhadores do Sorteio |
| Formas de Consenso | | | | Verificação se é uma extensão Legítima |
| Tolerância a Falhas | 50% do poder De Mineração | 50% da posse da quantidade de moedas | 50% da Quantidade de representantes Maliciosos | 50% dos usuários maliciosos *Online* |
| Estabilidade e Robustez | Sim | Sim | Sim | Sim |
| Poder computacional e consumo elétrico | Alto | Baixo | Baixo | Médio |
| Características que dificultam Fraude | Computação Intensiva | Valorização Dos ativos pela demanda | Embaralhamento Dos representantes Vigilância | Tragédia dos comuns (se você age mal, prejudica todos, inclusive a si próprio) |
| Criação de blocos | Mineradores | O usuário escolhido no sorteio | Os representantes Escolhidos por votos | A ultima testemunha Aleatória |
| Vantagens | Adoção e aceitação mais Difundidas Segurança pela dificuldade de Fraude | Baixo uso de recursos de *software e hardware* | Mais rápido que POW e POS Tem mais Participação dos usuários. | Tenta ser o mais justo possível na repartição das taxas e na escolha dos usuários |
| Desvantagens | Consumo Energético Ineficiente | Problema de concentração de riqueza | Muito dependente Da Participação dos votantes | Consumo energético ineficiente |

Fonte: elaborado com base em: ALIAGA; LUCENA; LEAL; HENRIQUES, (2018)

A tecnologia *blockchain* divide-se em três categorias: *blockchain* público, *blockchain* privado ou permissivo e híbrido (ARRUDA, 2017).

O *blockchain* público, dispõe de acesso público por qualquer usuário da *internet* em uma arquitetura descentralizada. A inserção de novos blocos é realizada por meio dos algoritmos de consenso. Logo, a vantagem consiste-se na descentralização em oposição ao modelo de sistemas com arquitetura cliente/servidor. Sendo assim, não é possível o controle central do Estado (ARRUDA, 2017; ALIAGA, HENRIQUES, 2017; ALVES *et al.* 2018)

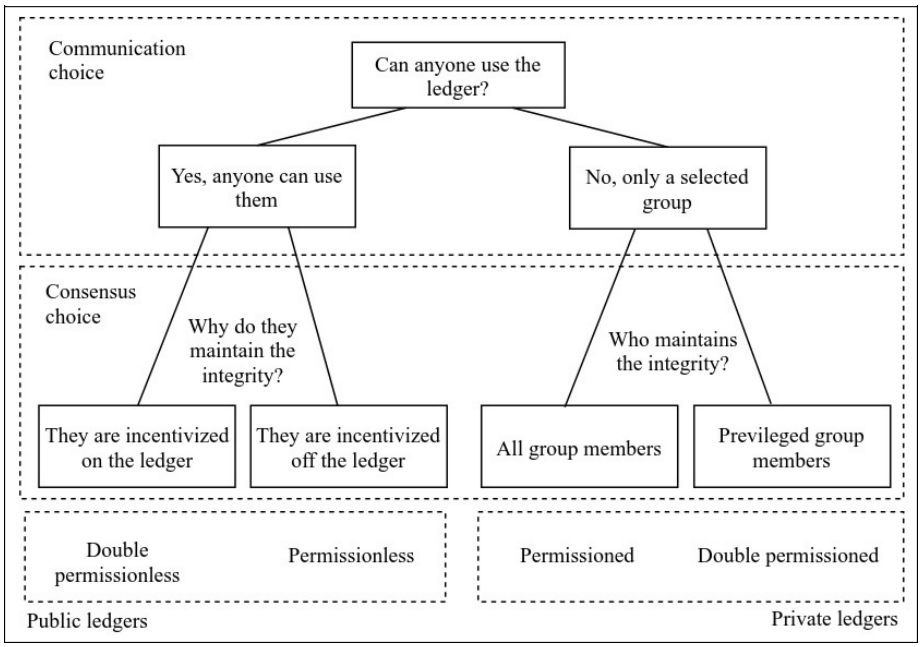
No tocante, do *blockchain* privado ou permissivo, esses são administrados e controlados por grupos de personalidades privadas pré-definidas. O acesso é realizado por intermédio de protocolos de segurança, que bloqueiam a conexão em domínio público, a qual gera maior rapidez nos processos. As operações são realizadas em ambiente interno e controlado, que viabiliza a correção de possíveis erros e são altamente recomendadas, quando existe o armazenamento de informações confidenciais e sensíveis. Essas características principais são os diferenciais do *blockchain* privado em relação ao público (ARRUDA, 2017; ALIAGA, HENRIQUES, 2017; ALVES *et al.* 2018).

Já o *blockchain*, da categoria híbrida consiste em uma rede ou grupo de personalidades privadas, que somam esforços para viabilizar as potencialidades do sistema. Os nós da rede possuem autoridade para definir suas parcerias e o nós existentes na cadeia como, por exemplo, o *Hyperledger*.

Nota-se a existências de várias iniciativas e estratégias para determinar a real necessidade de implementação da tecnologia *blockchain.* Todavia, será apresentado os dois principais modelos lógicos para análise de viabilidade de uso da tecnologia *blockchain*, a saber: modelo Birch, Brown, Parula (2016) e o modelo Suichies (2015).

A figura 04, apresenta modeo lógico para análise de viabilidade para aplicação da tecnologia *blockchain.*

**Figura 04**: Modelo Birch, Brown, Parula.




Fonte: Birch, Brown, Parula (2016).

O modelo conceitual para decisão acerca do uso da tecnologia *blockchain*, proposto por Birch, Brown, Parula (2016), consiste a *priori,* em focar no uso de uma DLT, uma vez determinada a necessidade de seu uso, essa poderá ser do tipo *blockchain.* O modelo está dividido em três partes distintas, quais sejam: *communication choice*, *consensus choice* e *types of ledgers – public and private*.

A primeira parte inicia-se por meio de uma pergunta: *can anyone use the ledger*? – Qualquer um pode usar o livro razão?, no caso para referida pergunta, existem duas possibilidades: *yes, anyone can use them* – sim, qualquer pode usar, ou no, *only a selected group* – não somente um grupo selecionado.

Na segunda parte, o *consensus choice,* está dividido em duas partes, com as respectivas perguntas: *why do they maintain the integrity*? – por que eles mantêm a integridade?, *why maintain the integrity*? por que manter a integridade. Na primeira pergunta duas respostas são possíveis: *they are incentivized on the ledger*? – eles são incentivados no livro razão, *they are incentivized off the legder*? - eles são incentivados fora do livro razão. Na segunda pergunta também são possíveis duas respostas: *all groups members* – todos os membros do grupo, *previleged group members,* membros privilegiados dos grupos.

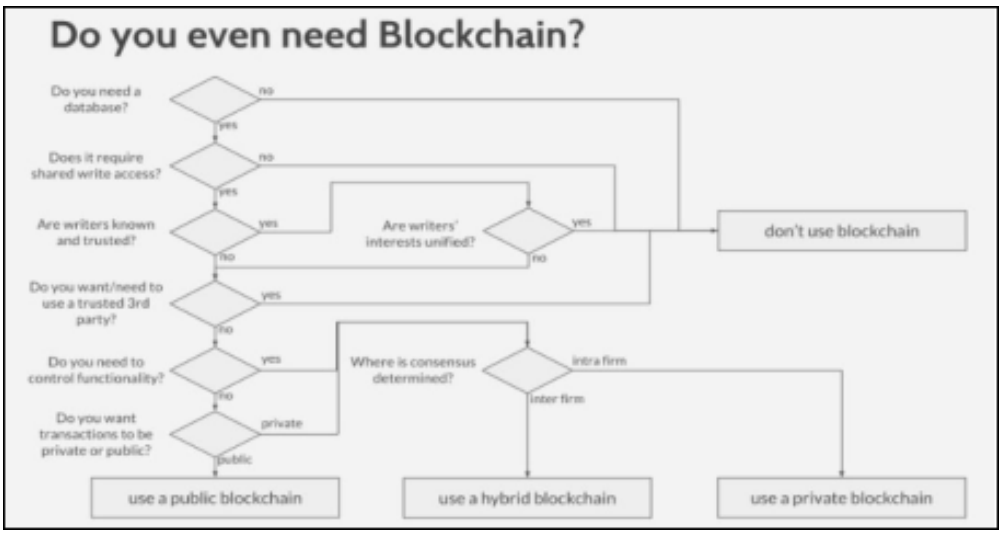
Por fim, a terceira parte os *types of ledgers*: *public and private* os tipos de livro razão: público e privado. Para os *publics ledgers* – livros razão públicos,

existem duas possibilidades: *double permissionless* - e *permissionless*, os quais são selecionados de acordo com as respostas obtidas na segunda parte, o *consensus choice*. Já no caso dos *private ledgers* é possível também duas possibilidades: *permissioned*, *double permissioned*, os quais são derterminados pelas respectivas respostas na segunda parte do *consensus choice*.

Percebe-se que, o modelo conceitual proposto por Birch, Brown e Parula determina inicialmente a viabilidade de uso de uma DLT, que poderá posteriormente culminar na implementação da tecnologia *blockchain*.

A figura 05, a seguir, exemplifica modelo lógico acerca da real necessidade e viabilidade de aplicação da tecnologia *blockchain*.

**Figura 05:** modelo Suichies.




Fonte: Suichies, (2015).

A figura 05, apresentou o modelo conceitual para aplicação da tecnologia *blockchain* proposto por Suiches (2015), que se inicia com a seguinte pergunta: *do you need a data base*? – você precisa de um banco de dados. Caso a reposta seja não, então não utilize a tecnologia *blockchain*. No caso de um resposta positiva, passa-se para o próximo nível, com a seguinte pergunta: *does it required shared write access* – é necessário acesso para gravação compartilhada?. Caso a reposta seja negativa, não utilize a tecnologia *blockchain.* Nesse sentido, se resposta for sim, então inicia-se o próximo nível, com a pergunta: *are writers known and trusted*? - os produtores são conhecidos e confiáveis?. No caso de uma resposta positiva, desloca-se para uma questão secundária: *are writers interests unified*? – os interesses dos

produtores são unificados?, se o resposta for um sim, então não utilize a tecnologia *blockchain.* Para uma resposta negativa retorna-se para próxima questão: *do you want/need to use a trusted 3rd party*? – você quer/precisa de um terceira parte confiável?. Se sim, então não utilize a tecnologia *blockchain.* Para uma resposta negativa inicia-se outra nível com a seguinte pergunta: *do you need control functionality?* – você precisa de uma funcionalidade de controle?, para uma resposta positiva, então inicia-se uma questão secundária: *where is consensus determined*? – onde o consenso e determinado. Se for *intra firm* – dentro da empresa, *use a private blockchain* – use *blockchain* privado. Se for *inter firm* - entre empresas, use a *hybrid blockchain*. Caso a resposta seja não, inicia-se a próxima questão: *do you want transactions to be private or public*? Você quer que as transações sejam privadas ou públicas?, caso seja público, *use a public blockchain*? – *use blockchain público*. Por outro lado, se resposta for *private* – privado, retorne a questão *where is consensus determined*? – onde o consenso é determinado, para então determinar se o uso será um *blockchain* híbrido ou privado.

# 4 REPOSITÓRIOS DIGITAIS

O processo de comunicação científica, nos últimos três séculos, utilizou-se dos periódicos científicos como o seu principal canal de comunicação, que surgiu em vista da necessidade de acesso e disseminação dos resultados das pesquisas. Todavia, no final do século XX, a comunicação científica entra em colapso devido à crise dos periódicos científicos, os quais tiveram seus custos elevados, extrapolando significativamente os orçamentos destinados à sua aquisição (WEITZEL, 2006).

Esse aumento significativo, portanto, culmina na queda das assinaturas dos periódicos científicos. A descentralização e o crescimento vertiginoso informacional também influenciaram de forma expressiva no processo de comunicação científica (WEITZEL, 2006).

Assim, percebe-se que as revistas científicas detinham o monopólio na publicação dos resultados científicos. Entretanto, com o advento das TIC e dos meios institucionais, surgiram novas possibilidades nesse contexto, que propiciaram a eclosão de estratégias e movimentos específicos no processo de comunicação científica, tais como: Movimento de Acesso Livre (*Open Access*) e Iniciativa de Arquivos Abertos (*Open Archives Initiative*).

Segundo Alves (2008), o movimento de acesso livre (*Open Access*) surgiu em 2002, em Budapeste, Hungria, por meio do *Open Access Working Group* (OAWG) – Grupo de Trabalho do movimento de Acesso Livre, e definiu as estratégias básicas para o acesso da informação científica. Logo após o movimento de acesso livre, emerge a Iniciativa de Arquivos Abertos (*Open Archives Initiative* – OAI), que institui um padrão de interoperabilidade entre os repositórios digitais, configurando-se como uma opção para o processo de comunicação científica.

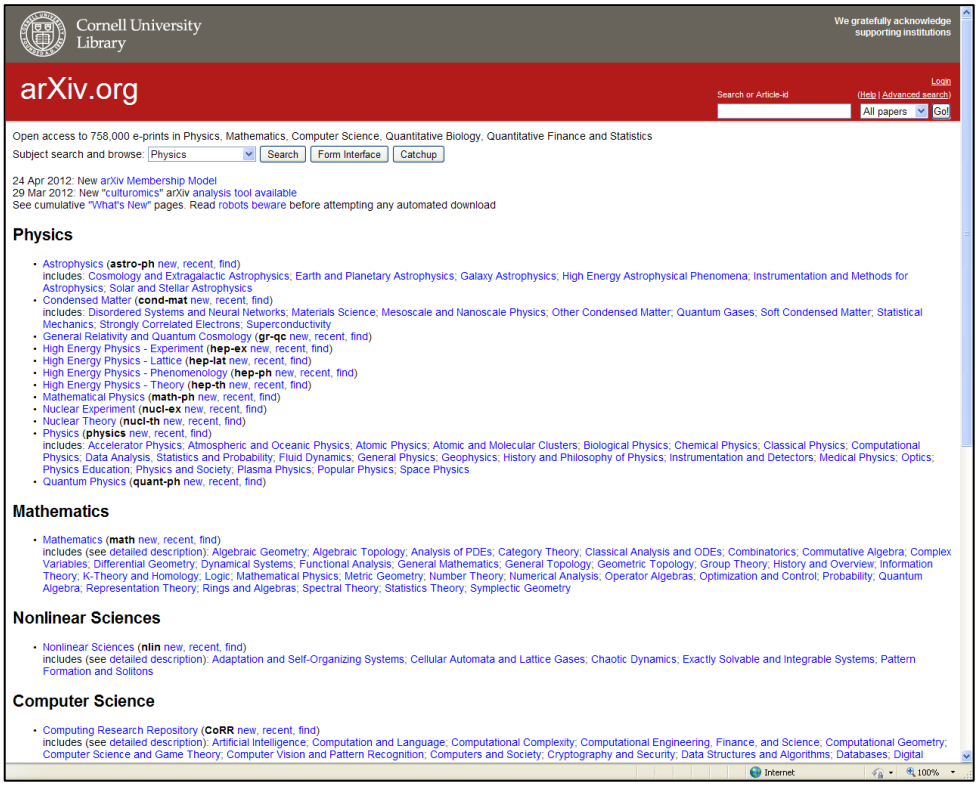
O movimento *Open Access* propõe duas estratégias básicas para o acesso à informação científica denominadas como: via dourada (*golden way*) e via verde (*green way*). A primeira aconselha que os periódicos científicos sejam publicados de acordo com o conceito de livre acesso a seus conteúdos que é assegurado pelos editores científicos. Em relação à segunda, o auto-arquivamento é realizado pelo próprio autor do artigo científico já publicado ou aceito para publicação, sob autorização do editor para que o torne acessível em um repositório de acesso livre. Constata-se que estes

dois procedimentos, via dourada e via verde, são de fundamental importância para o movimento dos arquivos abertos (MARCONDES; SAYÃO, 2009).

O primeiro repositório digital surgiu no início da década de 1990 no Laboratório Nacional de Física Nuclear de Los Alamos, Novo México, nos Estados Unidos da América (EUA), o qual criou e implementou o repositório digital pioneiro denominado *ArXiv* nas áreas da Ciência da Computação, Física, Matemática e Ciências não Lineares. O repositório *ArXiv* foi desenvolvido, experimentalmente, como uma alternativa ao modelo adotado no processo de comunicação científica o qual foi propiciado pela crise das revistas científicas (ALVES, 2008).

A Figura 06, apresenta a página inicial do repositório digital *ArXiv*.

**Figura 06:** Repositório digital ArXiv.




Fonte: http://www.arxiv.org/. Acesso em: 10 jun. 2022.

Os repositórios digitais distribuem-se em dois tipos principais, tais como: os repositórios temáticos e os repositórios institucionais. De acordo com Café *et al*. (2003, p. 2) um repositório temático:

> [...] se constitui em um conjunto de trabalhos de pesquisa de uma determinada área do conhecimento, disponibilizados na internet.

> Esses repositórios utilizam tecnologias abertas e seguem a filosofia da iniciativa dos arquivos abertos, promovendo a maior acessibilidade à produção dos pesquisadores e à discussão entre seus pares.

Percebe-se que os repositórios temáticos são constituídos de arquivos digitais sobre um assunto de determinada área do conhecimento, disponíveis em acesso aberto o que favorece maior visibilidade da produção científica. Segundo Café *et al.* (2003) o repositório institucional é o agrupamento de vários repositórios temáticos alojados em uma instituição. Em uma universidade, por exemplo, cada departamento de estudo trata de uma área específica do conhecimento, ou seja, o seu repositório temático será específico no assunto deste departamento. A junção de todos os repositórios das diversas repartições de pesquisa comporá o repositório institucional. Sanchez e Melero (2006, p. 3, tradução nossa) discursam sobre o surgimento e o conceito dos repositórios institucionais:

> Os repositórios institucionais surgem como uma resposta das instituições, principalmente as acadêmicas contra as políticas inflacionistas das revistas cientificas tradicionais que sempre tendema elevar constantemente os preços e as necessidades das instituições de conservar, preservar e disponibilizar para sua comunidade acadêmica e pesquisadores seu patrimônio intelectual.

Os repositórios institucionais propiciam, por intermédio do movimento do acesso livre, uma alternativa ao monopólio dos grandes editores científicos em vista de que possibilitam o acesso livre ao seu conteúdo científico produzido no âmbito acadêmico. O acesso à literatura científica é essencial para cientistas e pesquisadores no desenvolvimento de suas pesquisas. Desse modo, Lynch (2003, p. 2, tradução nossa) afirma que o repositório institucional de uma universidade é “Um conjunto de serviços que a universidade oferece para os membros de sua comunidade, visando o gerenciamento e disseminação dos materiais digitais criados pela instituição e pelos seus membros.”

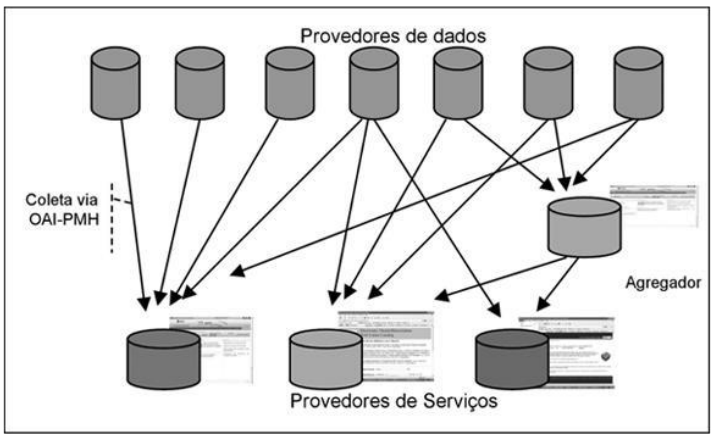
Sendo assim, Crow (2002) considera que os repositórios institucionais de acesso aberto são coleções digitais que armazenam, preservam, disseminam e permitem o acesso à produção intelectual de uma comunidade universitária. Os repositórios institucionais funcionam como indicadores de qualidade institucional da própria universidade ao demonstrar a relevância da produção científica de sua comunidade universitária.

As pesquisas acadêmicas científicas, de modo geral, são financiadas pelo governo com a utilização de verbas públicas. Os pesquisadores, para obterem acesso à literatura científica, a qual foi gerada nas instituições públicas, necessitarão arcar com o custo da assinatura de uma revista científica, a fim de acessar sua própria produção, o que produz uma redundância de custos para as instituições.

Dessa forma, em particular, as instituições públicas devem prover o acesso livre aos resultados dessas pesquisas (KURAMOTO, 2006). Constata-se que um repositório institucional de acesso aberto tem como características básicas: acesso público transparente, ampla tipologia documental, conteúdo heterogêneo, multidisciplinaridade e preservação digital. Os repositórios institucionais fornecem acessibilidade às informações, aos arquivos digitais dos gêneros textuais, sonoros e iconográficos, possibilitam armazenamento, organização, disseminação da informação e preservam a integridade do arquivo digital.

Os repositórios institucionais de acesso livre utilizam o protocolo *Open Archives Initiative – Protocol for Metadata Harvesting* (*OAI-PHM*). Este protocolo compartilha metadados idênticos, o qual possibilita a interoperabilidade entre os repositórios por meio da coleta de metadados dos provedores de dados (WEITZEL,2006). A Figura 07, apresenta o processo de coleta de metadados.

Figura 07: Coleta de metadados.




Fonte: Kuramoto (2006).

Os cilindros menores, na parte superior da figura citada, representam os provedores de dados, enquanto os cilindros maiores na parte inferior simbolizam os provedores de serviço. O protocolo OAI-PMH é um protocolo de comunicação, o qual possibilita a coleta de metadados (*harvesting*) de um determinado provedor de dados.

Ao realizar a coleta de metadados, o provedor de serviço o faz por meio do mecanismo de colheita (*Harvester*) e do serviço agregador. O mecanismo de colheita, ao acessar um provedor de dados, estabelece a conexão com o *software* desse provedor em específico, que atende a demanda do *harvester* por intermédio do acesso aos metadados requisitados (KURAMOTO, 2006).

Os repositórios digitais, portanto, são constituídos por documentos eletrônicos, arquivos digitais e objetos digitais e DAD, os quais permitem, assim, o acesso livre (*Open Access*) às informações por meio da *internet*, que possibilita a consulta remota e simultânea.

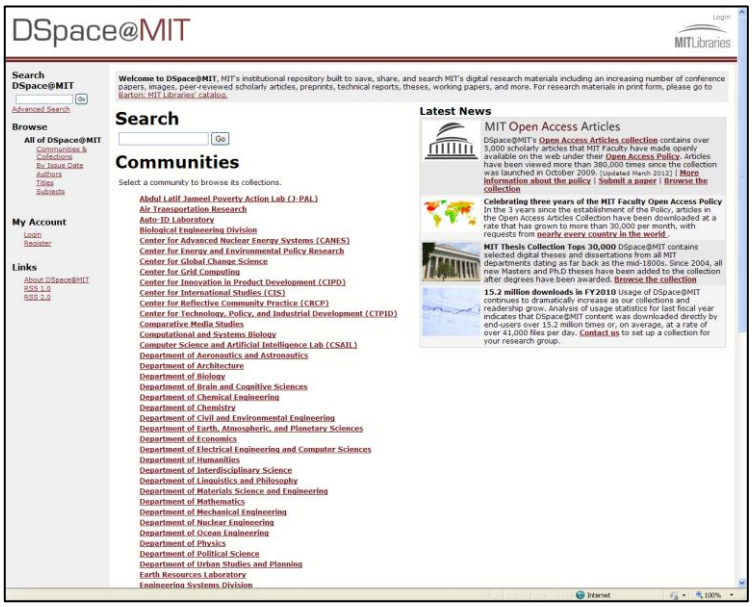
## 4.1 INICIATIVAS E ESTRATÉGIAS DE IMPLEMENTAÇÃO DOS REPOSITÓRIOS DIGITIAS

Para implementar os repositórios digitais, existem várias ferramentas e *softwares* disponíveis, tais como: *Eprints*, *Fedora*, *DSpace, Archivematica, Alfresco*. O *DSpace*, foi a escolha institucional do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), para a distribuição no Brasil. Já o *Alfresco*, dispõe de características nativas imprescindíveis na gestão de conteúdos empresariais – *Enterprise Content Management* (ECM). Por fim, o *Archivematica* que possui características para os arquivos permanentes para fins de preservação, bem como é altamente viável para tornar-se em um forte candidato para configurar-se como um repositório digital arquivístico digital confiável (RDC-Arq).

Desenvolvido pelo *Massachusetts Institute of Technology* (*MIT*) e pela *Hewlett Packard* (*HP*) o *Dspace* configura-se como um *software* livre (*Open Source*) para a construção de repositórios digitais. Apresenta uma estrutura baseada em um modelo organizacional a fim de representar as várias unidades administrativas existentes nas instituições.

A Figura 08, demonstra o repositório digital do *MIT* desenvolvido com a ferramenta *DSpace*.

**Figura 08:** Repositório digital *MIT*.




Fonte: http://dsapce.mit.edu. Acesso em: 28 jun.2022.

De acordo com Santarem Segundo *et al.* (2010) o *framework Manakin* é uma ferramenta para o desenvolvimento e customização de interfaces de repositórios digitais, criado em *San Antonio*, *Texas*, nos EUA pela *Texas A&M University* que em conjunto com o *software DSpace* facilita a customização das diversas formas de apresentação das informações. O *framework Manakin* integra-se perfeitamente ao *software DSpace.* O *Manakin* possui diversas funcionalidades com ênfase para alteração da exibição das informações armazenadas e para auxiliar a customização da interface de representação de comunidades, acervos e itens de um repositório digital. Essa customização da interface é executada por meio da configuração de temas tornando-se de extrema relevância no desenvolvimento da apresentação visual das informações.

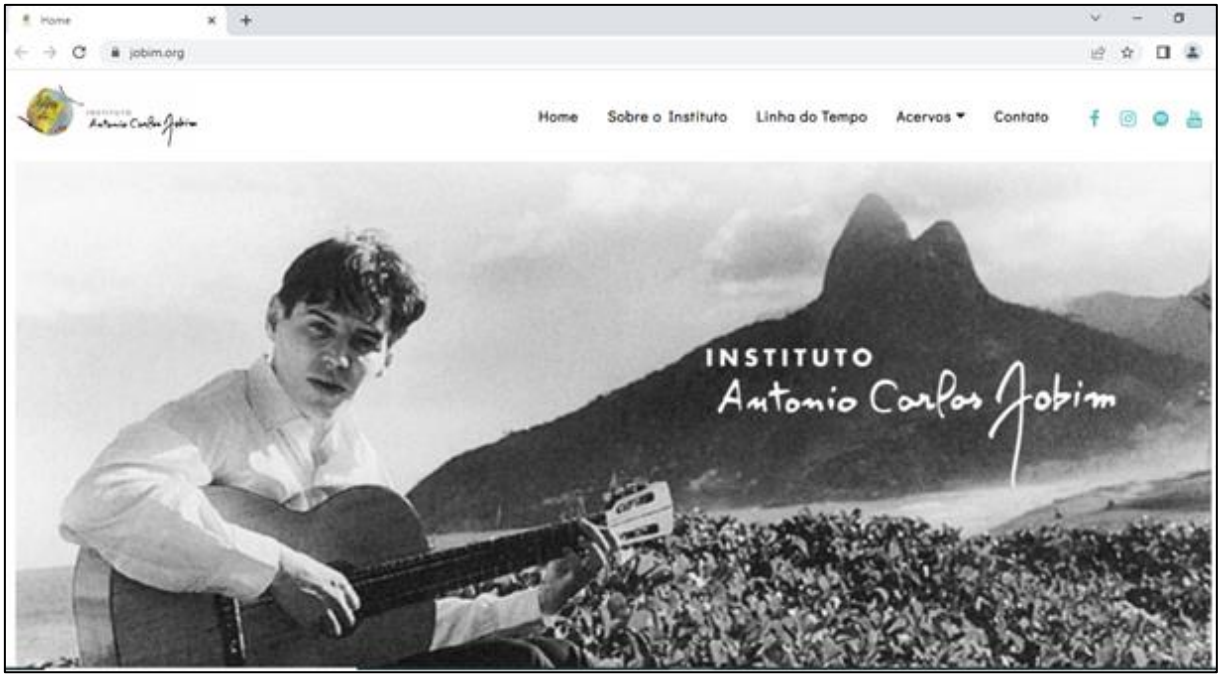
O *framework Manakin* tem como uma de suas qualidades essenciais a função de prover a subdivisão do repositório digital em várias categorias de serviços e classes de apresentação, adequando-se de forma conveniente às hierarquias organizacionais e às necessidades informacionais de cada instituição bem como de seus usuários.

Nesse sentido, a utilização do *framework Manakin* corrobora para a customização dos repositórios digitais propiciando um incremento na usabilidade de modo a tornar-se mais eficiente a navegação e recuperação da informação.

A Figura 09 apresenta o repositório digital do Instituto Antônio Carlos Jobim, o qual foi desenvolvido com o *software DSpace* e customizado com o *framework*

*Manakin*.

**Figura 09:** Repositório digital do Instituto Antônio Carlos Jobim.




Fonte: http://www.jobim.org. Acesso em: 28 jul. 2022.

No Brasil, o objetivo do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) é apoiar ações para divulgar a utilização de *softwares* como o *DSpace*. Segundo Kuramoto (2007) o IBICT é um órgão do governo federal, subordinado ao Ministério da Ciência e Tecnologia (MCT). A sua função legal é fomentar o registro e a disseminação da informação em ciência e tecnologia. O supracitado Instituto (IBICT, 2014, p. 1) tem como missão “Promover a competência, o desenvolvimento de recursos e a infraestrutura de informação em Ciência e Tecnologia para a produção, socialização e integração do conhecimento científico-tecnológico.” A instituição surgiu como base no Instituto Brasileiro de Bibliografia e Documentação (IBBD) que, no final da década de 1970, passou a ser denominado de Instituto Brasileiro de Informação em Ciência e Tecnologia, o qual administra e aperfeiçoa os fluxos estratégicos de informação em ciência e tecnologia no Brasil e apoia o acesso livre à informação científica por meio de uma política nacional.

O manifesto Brasileiro de apoio ao acesso livre à informação científica declara que:

> Uma versão completa da obra e todos os materiais suplementares incluindo uma cópia da licença, como acima definida, é depositada e, portanto, publicada em um formato eletrônico normalizado e apropriado em pelo menos um repositório que utilize normas técnicas adequadas (como as definições estabelecidas pelo modelo *Open Archives*) e que seja mantido por uma instituição acadêmica, sociedade científica, organismo governamental, ou outra organização estabelecida que pretenda promover o acesso livre, a distribuição irrestrita, a interoperabilidade e o arquivamento a longo prazo. (IBICT, 2014, p. 1).

Verifica-se que o papel do IBICT frente às questões relacionadas ao acesso livre à produção científica é de extrema relevância para a comunidade científica em vista de que propicia a quebra de paradigma do acesso à informação científica.

Percebe-se que os repositórios digitais atendem os requisitos da declaração do manifesto Brasileiro de apoio ao acesso livre à informação (IBICT, 2014). O IBICT desenvolveu versões em português dos *softwares DSpace* e *Eprints*, os quais foram traduzidos em parceria com a equipe da Rede de Informação em Comunicação dos Países de Língua Portuguesa (PORTCOM) da Sociedade Brasileira de Estudos Interdisciplinares da Comunicação (INTERCOM) e do Núcleo de Pesquisa *Design* de Sistemas Virtuais Centrado no Usuário da Universidade de São Paulo (USP).

O *software Eprints* sofreu alteração em sua denominação para Diálogo Científico (DICI). O *DSpace* não sofreu quaisquer alterações em seu nome (IBICT, 2014). Constata-se que o IBICT incentiva o registro, a disseminação e a visibilidade da literatura científica por meio da utilização dos repositórios digitais ao disponibilizar versões em língua portuguesa. A ferramenta com maior utilização e incentivo para a construção dos repositórios digitais, atualmente no contexto da informação científica, é o *software DSpace*.

O repositório digital *Alfresco* possui seu enfoque na gestão de conteúdo – *Enterprise Content Management* (ECM), o qual surge em 2005, idealizado por John Powel e Jonh Newton. Desenvolvido em linguagem *JAVA* pela *Alfresco*, como uma alternativa de código aberto no contexto dos repositórios digitais para gestão de conteúdos. Disponível em duas versões: a primeira *Enterprise Edition* e a segunda versão *Community Edition*, ambas de código fonte aberto (CARUANA *et al.* 2010).

Dessa forma, o repositório digital *Alfresco* configura-se como uma das principais alternativas de código aberto no gerenciamento de conteúdos e na preservação digital (SHARIFF *et al.* 2013). O *Alfresco* gerencia qualquer tipo de conteúdo, isto é, qualquer objeto digital ou arquivos não estruturados, semi-

estruturados e estruturados. Esse tipo de repositório digital destaca-se em relação a outros repositórios digitais, uma vez que já dispõe de várias funcionalidades incorporadas, a saber: gerenciamento de metadados, controle de versão, gerenciamento do ciclo de vida documental, gestão documental, fluxo de trabalho (*workflow)*, associação com outros conteúdos, marcação (*tagging*), comentários, gerenciamento de conteúdo *web,* colaboração de conteúdos, integração de *e-mails* e permite apresentar e publicar informações por meio da *Internet* (CARUANA, *et al.* 2010).

Nesse sentido, o repositório digital *Alfresco* contempla o modelo OAIS e sua capacidade de gerenciamento de conteúdo está em conformidade com o padrão *Content Management Interoperability Services* (CMIS), que é homologada atualmente pela *Organization for the Advanced of Structured Information Standards* (OASIS).

O repositório digital *Alfresco* dispõe de várias capacidades e características nativas desta plataforma aberta para organização e representação da informação e do conhecimento, dentre as quais destacam-se: gestão de documentos, gerenciamento de conteúdo *web*, gestão de imagem, suporte multiplataforma, servidores em *cluster* e federados, colaboração na *web* 2.0, *Content Management Interoperability Services* (CMIS) (BHAUMIK, 2011).

O repositório digital Alfresco é composto de vários serviços característicos da plataforma, quais sejam: banco de dados *PostgreS*, aplicação de servidor *web Tomcat* e Apache *Solr*.

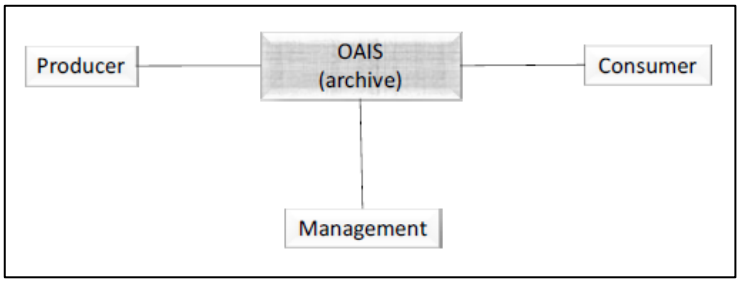
## 4.2 MODELO *OPEN ARCHIVES INFORMATION SYSTEM* (OAIS)

O modelo conceitual *Open Archives Information System* (OAIS), foi desenvolvido pelo *Consultative Committee for Space Data Systems* – Comitê Consultivo para Sistemas Espaciais de Dados (CCSDS), o qual foi fundado em 1992 pelas principais agências espaciais mundiais, a saber: *Agenzia Spaziale Italiana* (ASI)**,** *Canadian Space Agency* (CSA), *Centre National d'Etudes Spatiales* (CNES), *China National Space Administration* (CNSA), *Deutsches Zentrum für Luftund Raumfahrt* (DLR), *European Space Agency* (ESA), Instituto Nacional de Pesquisas Espaciais (INPE), *Japan Aerospace Exploration Agency* (JAXA), *National Aeronautics and Space Administration* (NASA), *Russian Federal Space Agency* (RFSA) e United Kingdom Space Agency (UKSA)**,** com base na solicitação da *International*

*Organization for Standardization* - Organização Internacional de Padronização (ISO)20. O CCSDS coordenou a elaboração do OAIS para preservação digital de longo prazo (DAY, 1999).

Dessa forma, o OAIS consolidou-se em 2003 como uma normatização da ISO 14721:2012, tornando-se a norma mais relevante, que descreve as aplicações no âmbito dos repositórios digitais (USA, 2012). No Brasil, a norma internacional supracitada foi traduzida, adaptada e publicada pela Associação Brasileira de Normas Técnicas (ABNT), sob a norma NBR 15472:2021, Sistema Aberto de Arquivamento de Informação (SAAI) (BRASIL, 2014b). A figura 10, a seguir, apresenta o modelo simplificado OAIS.

**Figura 10**: Modelo simplificado OAIS.

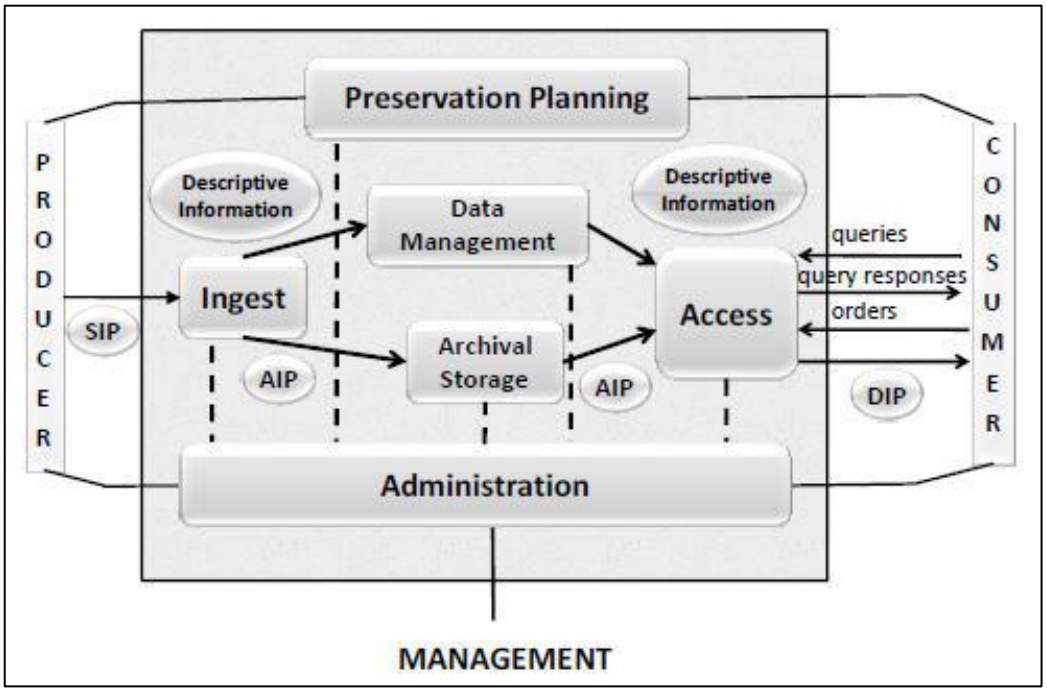



Fonte: USA (2012).

O modelo de referência funcional do OAIS simplificado é composto basicamente pelo produtor, consumidor, administrador e as operações concernentes no contexto OAIS do objeto digital. O *producer* (produtor) fornece as informações relevantes a serem preservadas. O *consumer* (consumidor) é composto pelos sujeitos informacionais ou sistemas, que interagem com o serviço OAIS para o acesso das informações preservadas. O *management* (administrador) é a entidade responsável pelas políticas no contexto do repositório digital (THOMAZ; SOARES, 2004).

A figura 11 apresenta o modelo OAIS detalhado, com os componentes funcionais, os pacotes de informação, e as entidades externas.

**Figura 11**: Modelo OAIS detalhado.




Fonte: USA (2012).

O modelo OAIS dispõe de um esquema de seis funções principais detalhadas, que devem estar em consonância com os repositórios digitais, tais como: *ingest, archival storage, data management, adminstration, preservation planing, Access.* O *ingest* (recepção) é responsável pela ingestão do *Submission Information Package* – Pacote de Submissão de Informação (SIP) dos produtores e preparação dos conteúdos de armazenamento e gerenciamento. Após admissão do SIP, é gerado o *Archival Information Package* - Pacote de Informação para Arquivamento (AIP), que contém a formatação dos dados, padrões das extensões dos arquivos definidos pelas políticas, gera-se a informação descritiva associada necessária para recuperação dos objetos e que transfere o AIP para o *data management* – gerenciamento de dados ou para *archival storage* – armazenamento (USA, 2012).

O *data management* mantém e acessa a informação descritiva e os dados administrativos dos objetos digitais. Logo, sua função é administrar a base de dados do arquivo, promover atualizações da base e permitir consulta aos dados para gerar relatórios (LAVOIE, 2000).

O *archival storage* provê a armazenagem, manutenção e recuperação do AIP. Contempla o recebimento de novos AIP, gerencia a hierarquia da área de

armazenamento, executa rotinas de verificação de erros, oferece capacidade de recuperação de falhas e desastres (USA, 2012).

O *preservation planning* é responsável pela aplicação das políticas de preservação digital. No quesito obsolescência tecnológica, o ambiente do OAIS é frequentemente avaliado e monitorado com o objetivo de garantir o acesso a longo prazo das informações armazenadas. Avalia, constantemente, o conteúdo dos objetos digitais para recomendar a utilização das estratégias de preservação digital a serem adotadas (USA, 2012).

O *administration* gerencia a rotina operacional do repositório, isto é, coordena as seis funções do OAIS. Na administração do sistema, incluem-se solicitar e negociar acordos de submissões com os produtores, realizar auditorias da submissões, gerenciar a configuração de *hardware* e *software* do sistema e responsabilizar-se pela aplicação das políticas (USA, 2012). O *access*, atende as demandas informacionais dos sujeitos, que podem ser uma solicitação específica de um determinado arquivo ou uma *querie* – consulta a ser realizada para o índice do repositório. Essas solicitações são atendidas por meio da geração do *dissemination information package* – pacote de disseminação da informação (USA, 2012).

Observa-se que, o desenvolvimento do modelo de referência OAIS, surgiu por meio da cooperação de várias agências espaciais, na qual a Brasileira INPE é integrante, que culminou no surgimento da CCSDS.

A Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ), do Arquivo Nacional estabelece, por intermédio da resolução nº 39, de 29 de abril de 2014, as diretrizes para implementação de repositórios digitais confiáveis e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR) (BRASIL, 2014b). De acordo com a resolução nº 39 do CONARQ, os requisitos para um repositório digital confiável, são: infraestrutura organizacional, gerenciamento do documento digital, tecnologia, infraestrutura técnica e segurança (BRASIL, 2014b).

A infraestrutura organizacional compreende o âmbito no qual o repositório digital é implementado e deve contemplar determinados requisitos, a saber: governança e viabilidade organizacional, estrutura organizacional e de pessoal, transparência de procedimentos, arcabouço político, sustentabilidade financeira, contratos licenças e passivos (BRASIL, 2014b).

O gerenciamento do documento digital diz respeito ao uso do modelo conceitual OAIS. Os repositórios digitais devem estar alinhados como o referido modelo. As seis categorias preconizadas para gerenciar os arquivos digitais são contempladas por intermédio do modelo de referência OAIS. São elas: admissão, captura de documentos digitais e criação do pacote de arquivamento, planejamento de preservação, armazenamento e preservação – manutenção do AIP, gerenciamento de informação, gerenciamento de acesso (BRASIL, 2014b).

Por fim, a tecnologia, infraestrutura e segurança apontam as melhores práticas para a gestão de dados e segurança, tais como: infraestrutura de sistema, tecnologias apropriadas e os quesitos de segurança. Nessa direção, ainda de acordo com a resolução nº 39, são apresentados alguns padrões e normas de referência, que devem ser aplicados nos repositórios digitais confiáveis.

Verifica-se que, os repositórios digitais devem estar em consonância com o modelo conceitual OAIS 14:721:2003, para fins de preservação digital de longa duração e acesso. Sendo assim, as soluções tecnológicas para implementação, devem estar alinhadas com o referido modelo conceitual.

Logo, a utilização do repositório digital *Alfresco*, propiciará um incremento significativo nos fazeres arquivísticos no que diz respeito aos ambientes informacionais digitais, nas operações concernentes à gestão de conteúdos empresarias, a qual configura-se como um nova possibilidade de atuação do Arquivista e no âmbito da gestão de documentos, única e exclusivamente nos documentos correntes e intermediários, em vista de que o *Alfresco* e demais repositórios digitais supracitados, com exceção do *Archivematica*, de acordo com a resolução nº 43, do Conselho Nacional de Arquivos não são considerados um repositório digital arquivístico confiável, quando utilizado para os documentos de guarda permanente, isto é, para preservação digital duradoura. Nesse sentido, os documentos permanentes devem ser migrados para um repositório arquivístico digital confiável para fins de preservação digital de longa duração conforme a Resolução nº 43, de 04 de setembro de 2015, na qual pode-se utilizar o Archivematica (BRASIL, 2015).

A certificação e auditoria dos repositórios digitais confiáveis são facilitados, posto que os repositórios supracitados dispõem do código fonte aberto. O metadados de preservação *Preservation Metadata*: *Implementation Strategy* (PREMIS) devem ser utilizados nesse contexto. Esses metadados são perfeitamente aplicáveis aos

repositórios digitais. Quanto à Norma Geral de Descrição Arquivística (ISAD (G)) e a Norma Brasileira de Descrição Arquivística (NOBRADE) são contempladas por meio da descrição arquivística codificada (EAD), que serão discutidas nas próximas seções. A respeito do modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD) (e-ARQ BRASIL, 2020), as especificações técnicas e funcionais são possíveis de ser utilizadas no contexto dos repositórios digitais, por meio de customização do código fonte. O Padrão de Codificação e Transmissão de Metadados (METS) necessita ser aplicado no contexto dos repositórios digitais confiáveis.

Assim, percebe-se a relevância da utilização dos repositórios digitais bem como ambientes informacionais de arquivo e, por conseguinte, um ambiente de atuação do Arquivista, que responde uma demanda da contemporaneidade por intermédio da utilização destas plataformas abertas para organização e representação da informação orgânica no âmbito da Arquivologia.

A subseção 4.3, a seguir, apresentará a gestão documental.

## 4.3 GESTÃO DE DOCUMENTOS – *Records Management* (RM)

Esta subseção aborda a revisão dos conceitos, etapas e os componentes da gestão documental – *Records Management* (RM) de acordo com as principais instituições e pesquisadores acerca das temáticas. A gestão de documentos surge a partir da Segunda Guerra Mundial, em decorrência do aumento vertiginoso da produção documental, que compeliu a necessidade de gerir este grande acúmulo de massas documentais (MORENO, 2008).

Os Estados Unidos da América (EUA), entre outros países anglo-saxônicos, desenvolveram, no final de 1940, o conceito de gestão de documentos denominado de *records management*, cujo foco inicial era administrativo e econômico, posto que se objetivava a otimização do funcionamento administrativo, limitar a produção documental e estabelecer o prazo de guarda dos documentos (INDOLFO, 2007).

Dessa forma, a gestão documental origina-se com base na inviabilidade do tratamento dos documentos de acordo com as abordagens tradicionais aplicadas frente às massas documentais produzidas e acumuladas pelas administrações, que aumentavam em progressão geométrica. Logo, emergiram soluções práticas por meio de reformas apresentadas pelas comissões governamentais dos EUA e do Canadá,

no final da década de 1940. Após o término da Segunda Guerra Mundial, institui-se a racionalidade administrativa, que intervém no ciclo de vida dos documentos como a produção, utilização, conservação e destinação documental (FONSECA, 1998).

A gestão de documentos Norte Americana foi sancionada por meio da legislação que define gestão documental como:

> [...] o planejamento, controle, direção, organização, treinamento, promoção e outras atividades gerenciais relacionadas à criação, manutenção, uso, e eliminação de documentos, com a finalidade de obter registro adequado e apropriado das ações e transações do Governo Federal e efetiva e econômica gestão das operações das agências. (UNITED STATES OF AMERICA, 1968, p. 1, tradução nossa).

No Brasil, a legislação específica que trata da gestão documental regulamenta-se pela Lei Federal 8.159 de 8 de janeiro de 1991, que dispõe acerca da política nacional de arquivos públicos e privados e dá outras providências. O artigo 3º apresenta o conceito de gestão documental como:

> "[...] conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para a guarda permanente". (BRASIL, 1991, p. 1).

Nesse sentido, Calderon *et al.* (2004, p. 101) afirmam que:

> O termo gestão está relacionado à administração, ao ato de gerenciar. Isso significa que é preciso ir além do ato de registro da informação em um suporte, é preciso também que se tenha um planejamento de tal forma, que, mesmo com uma quantidade exacerbada de documentos gerados diante das ferramentas tecnológicas disponíveis nos dias atuais, seja possível localizar e utilizar a informação no tempo exato e necessário para uma tomadade decisão.

A teoria das três idades determina o ciclo vital dos documentos, que compreende três fases dos arquivos. São elas: arquivo corrente, arquivo intermediário e arquivo permanente. A primeira refere-se aos documentos de uso funcional e frequentemente consultados. A segunda está relacionada aos documentos com menor utilização no cotidiano administrativo, ou seja, que já cumpriram seu prazo jurídico administrativo, no entanto há possibilidade de uso desta documentação. Já a

terceira é denominada de arquivos históricos, que deverão ser preservados permanentemente, cujo valor documental torna-se secundário (BELLOTTO, 2006).

Para o norte americano Schellenberg (2006) os documentos possuem dois valores: o valor primário e o secundário. Aquele se refere ao objetivo com que foi criado o documento, e que se considera o seu uso para fins administrativos, jurídico legal e fiscal, enquanto este será de interesse para outros fins, como a capacidade do documento de prover prova ou servir como fonte de informação para pesquisa nas diversas áreas da Ciência.

De acordo com os canadenses Rousseau e Couture (1998) existem três correntes do pensamento arquivístico acerca da gestão documental. A primeira é exclusivamente administrativa denominada de *records management*, em que seu foco é o valor primário do documento. A segunda, a arquivística tradicional, cuja diretriz são os arquivos permanentes de valor secundário e, por fim, uma abordagem nova denominada de arquivística integrada, que considera, concomitantemente, o valor primário e secundário dos documentos. A gestão documental envolve diversas atividades, tais como: produção de documentos, utilização dos documentos, tramitação, organização e arquivamento, reprodução, classificação e avaliação (BERNARDES; DELATORRE, 2008).

A classificação surgiu, nos primórdios da humanidade sendo concebida como uma arte. Entretanto, assumiu o *status* de procedimento científico recentemente. Dessa forma, a classificação quando entendida como arte era utilizada de várias formas e modos. O seu aprimoramento desenvolvia-se de acordo com as evoluções dos conhecimentos com base nos trabalhos de grandes filósofos, quais sejam: Indic Vedas, Bíblia, enciclopédia do egípcio Amenope (1250 A.C), Caius Plinius Secundus (23-79 D.C), enciclopédia da Idade Média de Isidro de Sevilla, Vicent de Beauvais, Bartholomaeus Anglicus, Brunetto Latini, as encilopédias da Renascença de Georg Valla, Rafael Maffei, Johann Heinrich Alsted, Wolfgang Ratke, Diderot, d'Alembert (1751-1780). Essas obras foram organizadas de forma sistemática como consequência de ideias pré-concebidas (DAHLBERG, 1972).

O pensamento lógico surge na Grécia com Aristóteles em sua obra intitulada *Órganon*, que aborda os estudos do filósofo acerca da lógica formal por meio dos seguintes tratados: Categorias, Primeiros Analíticos, Segundos Analíticos, Tópicos e Refutações Sofísticas. A lógica formal divide-se em: conceito, juízo e raciocínio (ARISTÓTELES, 2005).

Assim, Porfírio, por intermédio dos estudos de Aristóteles, propõe uma representação gráfica da abordagem lógica, a qual provém da ideia de árvore concebida na sua obra denominada de *Isagoge,* que apresenta uma disposição lógica e ontológica dos elementos (MONTEIRO; GIRALDES, 2008).

O esquema da Árvore de Porfírio culmina em um conjunto hierárquico, do geral para o específico, isto é, multinível. Nota-se que o conhecimento, inicialmente, não era sistematizado em uma abordagem esquemática como atual. A partir de 1491, o humanista e poeta italiano Angelo Poliziano, apresenta o seu *Panepistemon*, o qual demonstra, esquematicamente, as relações entre áreas do conhecimento. Dessa forma, após Poliziano, em 1605, Francis Bacon publicou um plano de classificação das Ciências intitulado *De dignitate et augmentis scientiarum.* Com a publicação do Novo *Órganon,* o qual foi reformulado do *Órganon* de Aristóteles, três grandes categorias foram propostas por Francis Bacon, a saber: memória, razão e imaginação (DAHLBERG, 1972).

No início do século XX, emerge-se uma nova teoria da classificação proposta por Ranganathan [1], que consiste em três pontos fundamentais, os quais contribuíram de forma notória para a moderna teoria da classificação. A primeira contribuição são os três níveis para elaboração de um sistema de classificação, quais sejam: plano da ideia, plano verbal e plano notacional. A segunda contribuição é a abordagem analítico-sintética para a identificação dos assuntos, que é realizado por intermédio das cinco categorias representadas por Personalidade, Matéria, Energia, Espaço e Tempo (PMEST). A terceira são seus 18 princípios para o arranjo de elementos não repetíveis das facetas (DAHLBERG, 1972).

A classificação é imprescindível para que se administre os arquivos em todo seu ciclo de vida com eficiência, uma vez que todas as atividades inerentes à gestão documental dependerão da classificação. Os arquivos classificados de forma apropriada cumprirão perfeitamente as necessidades das atividades correntes que deverão ser agrupadas de acordo com as necessidades informacionais dos sujeitos.

Os documentos são classificados para que representem a organização e as funções que criaram tais documentos (SCHELLENBERG, 2006). Assim, são três os métodos de classificação de documentos: funcional, organizacional e por assuntos. A classificação funcional dispõe os documentos de forma hierárquica e organizados por

[1] RANGANATHAN, S. R. Prolegomena to Library Classification. **Bombay:** Asia Publishing House, 1967.

meio das funções, subfunções e atividades. Já a classificação organizacional é composta, por sua vez, pelo grupo, subgrupo e atividade. Por fim, o método de classificação por assunto aplica-se a situações específicas e extraordinárias aos documentos produzidos com base em determinado campo do conhecimento, isto é, os documentos de pesquisa (SCHELLENBERG, 2006).

A avaliação documental é um método interdisciplinar que identifica os valores primários e secundários dos documentos e averigua seu ciclo de vida, com o objetivo de determinar o prazo de guarda ou eliminação, que propiciará a racionalização, eficiência administrativa e a preservação documental. Os métodos de avaliação devem ser realizados em conjuntos documentais. Os procedimentos de avaliação requerem a composição de comissões de avaliação, que são formadas por profissionais habilitados e capacitados em diferentes áreas do conhecimento, a qual será de suma relevância para se atribuir valores aos documentos (BERNARDES, 1998).

A tabela de temporalidade é um instrumento de gestão documental que avalia e determina o prazo de guarda dos documentos com base na legislação vigente, que dispõe a respeito do período de arquivamento dos documentos nos arquivos corrente e intermediário e sua destinação final, descarte ou guarda permanente nos arquivos históricos (BERNARDES, 1998).

O Conselho Internacional de Arquivos (CIA) estabelece as diretrizes gerais para descrição arquivística, por meio da norma geral internacional de descrição arquivística (ISAD(G)), que deverá ser usada, simultaneamente, com as normas de descrição de cada país ou subsidiar a sua elaboração. Objetiva-se, com a descrição arquivística, compreender e identificar o âmbito e o conteúdo informacional dos documentos arquivísticos, o qual proverá o acesso aos arquivos (CONSELHO INTERNACIONAL DE ARQUIVOS, 2001).

De acordo com o CIA, a descrição arquivística conhecida no cenário internacional por *archival description*, é:

> A elaboração de uma acurada representação de uma unidade de descrição e de suas partes componentes, caso existam, por meio da extração, análise, organização e registro de informação que sirva para identificar, gerir, localizar e explicar documentos de arquivo e o contexto e o sistema de arquivo que os produziu. (CONSELHO INTERNACIONAL DE ARQUIVOS, 2001, p. 14).

Os documentos de arquivo possuem componentes informacionais característicos que são registrados durante as etapas da gestão documental para propiciar seu gerenciamento e, consequentemente, sua preservação, os quais devem ser acessíveis para atender a demanda informacional dos usuários. A descrição arquivística poderá ser realizada em qualquer fase do ciclo de vida documental. Os sistemas de informação para automação de arquivos poderão integrar ou selecionar, de acordo com as demandas características informacionais dos documentos para efetuar atualizações ou possíveis alterações (CONSELHO INTERNACIONAL DE ARQUIVOS, 2001).

A Norma Brasileira de Descrição Arquivística (NOBRADE) (BRASIL, 2006b) estabelece os padrões de descrição arquivística em congruência com as normas internacionais vigentes como a ISAD(G) e a norma internacional de registro de autoridade arquivística para entidades coletivas, pessoas e famílias (ISAAR (CPF)) que são utilizadas prioritariamente em documentos permanentes. Entretanto, poderá ser utilizada em arquivos correntes e intermediários, tendo por objetivo o acesso e intercâmbio de informações no contexto nacional e internacional (BRASIL, 2006b).

A NOBRADE propicia a estruturação da informação por meio de uma descrição geral, cuja interferência se reduz consideravelmente na apresentação final das formas de descrição. Esta norma foi desenvolvida tanto para sistemas automatizados quanto manuais. Todavia, a sua utilização para processos de automação de arquivos é notória. O princípio arquivístico da proveniência constitui a base do desenvolvimento da NOBRADE e a descrição multinível que emprega os axiomas da ISAD(G), a saber: descrição do geral para o particular, informação relevante para o nível de descrição, relações entre descrições e evitar a redundância da informação (BRASIL, 2006b).

Aplica-se esta normatização descritiva a quaisquer documentos dos mais variados suportes e gêneros. O princípio de descrição multinível configura-se como uma consequência do princípio arquivístico de respeito aos fundos que deverá ser considerdo na elaboração de uma estruturação geral para sistemas de descrição arquivística manuais ou automáticos (BRASIL, 2006b).

Nesse sentido, os repositórios digitais enquadram-se como uma ferramenta estratégica na gestão documental, uma vez que todas as etapas concernentes a gestão de documentos são contempladas e podem ser integradas com a preservação digital duradoura por meio da plataforma unificada dos repositórios digitais.

A Câmara Técnica de Documentos Eletrônicos (CTDE) do Conselho Nacional de Arquivos (CONARQ) estabeleceu por meio do modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD) (e-ARQ BRASIL, 2020), as especificações dos quesitos necessários, que devem ser contemplados pelas instituições produtoras e/ou recebedoras de documentos, pelo sistema de gestão arquivística, cujo objetivo é garantir sua confiabilidade e autenticidade, bem como a sua acessibilidade ao longo do tempo (BRASIL, 2020). Nessa direção, ainda de acordo com a CTDE, por meio da resolução nº 37, de 19 de dezembro de 2012, é formalizada as diretrizes para a presunção de autenticidade de documentos arquivísticos digitais. A autenticidade dos documentos arquivísticos digitais envolve três aspectos imprescindíveis: legal, diplomático e histórico (BRASIL, 2012d).

O aspecto legal diz respeito a legislação territorial vigente de circulação do documento. Entretanto, quando o documento circular além do território Brasileiro deverá ser analisado o entorno, no qual o documento está em tramite para determinar as legislações específicas pertinentes acerca das respectivas jurisdições.

A diplomática tem como “ [...] objetivo o estudo da estrutura formal e da confiabilidade e autenticidade dos documentos”. (BRASIL, 2012d, p. 3). No quesito diplomático, são analisados o contexto da gênese documental, bem como a assinatura pelo produtor competente para tal. Por fim, o elemento histórico envolve os documentos autênticos, que atestam eventos que de fato aconteceram.

De acordo com o CONARQ (BRASIL, 2020, p.10) o SIGAD é um: Conjunto de procedimentos e operações técnicas, características do sistema de gestão arquivística de documentos, processados por computador. Pode compreender um *software* particular, um determinado número de *softwares* integrados, adquiridos ou desenvolvidos por encomenda, ou uma combinação destes. O sucesso do SIGAD dependerá, fundamentalmente, da implantação prévia de um programa de gestão arquivística de documentos.

Assim, o e-ARQ Brasil estabelece os requisitos mínimos para um SIGAD, para quaisquer plataformas tecnológicas, quais sejam: captura, avaliação, pesquisa, localização, apresentação, segurança, armazenamento e preservação.

## 4.4 GESTÃO DE CONTEÚDOS EMPRESARIAIS - *ENTERPRISE CONTENT MANAGEMENT* (ECM)

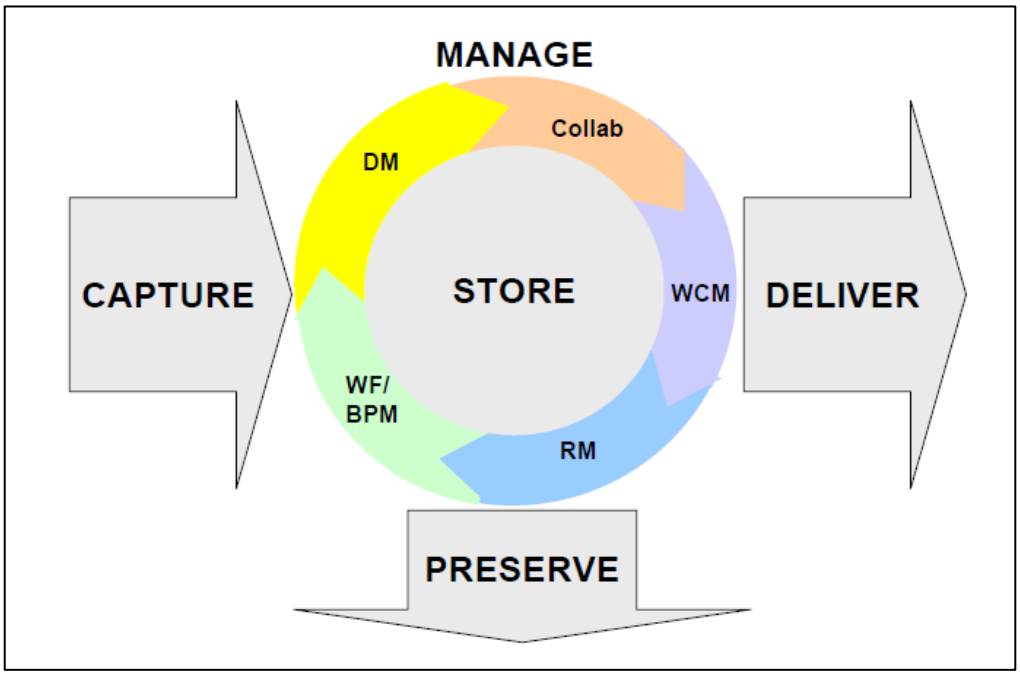
A gestão de conteúdo – *Content Management* (CM) é um conceito recente, o qual surge com base nos sistemas de gerenciamento das informações corporativas, que possibilita sua organização, representação e acesso (HELFIN; HENDLER, 2000). A interoperabilidade entre os diferentes serviços de gestão de conteúdos são realizadas por meio da interface do *Content Management Interoperability Services* (CMIS), que é composta por duas partes. A primeira consiste em um conjunto de serviços para o repositório como a navegação e criação de conteúdos. A segunda é uma linguagem de consulta no contexto do repositório para realizar a busca de conteúdos (BERGLJUNG, 2014).

A *Association for Information and Image Management* (AIIM) é uma organização sem fins lucrativos, que foi fundada em 1943, cujo objetivo principal constitui-se em auxiliar os utilizadores de ferramentas ECM na compreensão dos desafios associados à gestão de conteúdos e nos processos de negócios. Esta é uma organização reconhecida como líder mundial acerca da temática, em vista de que cunhou o conceito de gestão de conteúdos empresariais (ECM) e contribui para os avanços das pesquisas relacionadas ao contexto do ECM (AIIM, 2015).

De acordo com AIIM (2015, tradução nossa p. 01), a gestão de conteúdos empresariais (ECM) consiste nas “Estratégias, métodos e ferramentas utilizadas para capturar, gerenciar, armazenar, preservar e distribuir conteúdo e documentos relacionados aos processos organizacionais”. Para Jenkins (2004), o ECM é um sistema que captura, armazena, recupera os conteúdos digitais no âmbito organizacional. Esses conteúdos digitais podem ser imagens, textos, relatórios, vídeo, áudio, dados transacionais, catálogos e códigos fontes.

Nessa direção, para a viabilização das estratégias e métodos concernentes ao ECM são imprescindíveis cinco componentes, a saber: captura, gestão, preservação, armazenamento e difusão, os quais serão apresentados na figua 12.

**Figura 12:** Componentes do ECM.




Fonte: Kampfmeyer , 2006.

Na figura 12, observa-se todos os componentes referentes ao ECM e as etapas da gestão de conteúdos. A captura (*Capture*) compreende um conjunto de funcionalidades de processamento de recolhimento documental e de conteúdos, independentemente do contexto da gênese (PROVOOST, 2006). Verifica-se que, o processo de captura de documentos e conteúdos, contempla os documentos produzidos nos ambientes informacionais analógicos, isto é, clássicos que deverão ser digitalizados e os documentos cuja gênese é o ambiente informacional digital, moderno líquido, o qual produz arquivos natos digitais. A gestão (*Manage*) diz respeito ao conjunto de etapas, tecnologias e aplicações utilizadas para gerir conteúdos. Essa arquitetura de gestão contempla vários componentes tecnológicos, tais como: *Collaboration* (CT), *Web Content Mangement* (WCM), *Records Management* (RM), *Workflow* (WF), *Business Process Management* (BPM), *Document Management System* (DMS) (PETERMAN, 2009).

O (*Store*) refere-se ao armazenamento dos conteúdos, no repositório digital. A armazenagem não configura-se como preservação digital, os conceitos de armazenamento e preservação são distintos (PROVOOST, 2006).

A preservação (*Preserve*) consiste na preservação digital, a qual deverá ser realizada no contexto do RDC-Arq. Por fim, o *Deliver* (Difusão), que contempla a

difusão dos conteúdos em diversas extensões e perspectivas, para as mais diversas necessidades dos sujeitos informacionais (VIEIRA, 2012).

De acordo com Machado (2008) as informações podem ser estruturadas, semiestruturadas e não estruturadas. O enfoque do ECM é a informação não estruturada. Nesse domínio, a informação estruturada e conteúdo estruturado são aqueles que se encontram disponíveis e organizados em tabelas, cuja recuperação torna-se mais rápida. Já a informação não estruturada e o conteúdo não estruturado são difíceis de recuperar, e, muitas vezes, em determinadas conjunturas, torna-se inviável sua recuperação, uma vez que esses não estão organizados em tabelas (RAMALHO, 2010).

A informação estruturada contempla regras formais extremamente rígidas no contexto de sua gênese e ao longo do ciclo de vida. A estruturação dessas informações é realizada por intermédio de metodologias específicas, de acordo com as possíveis conjunturas informacionais como, por exemplo, os bancos de dados, no qual será possível estabelecer as relações entre as tabelas de dados (MACHADO, 2008).

Nessa direção, a estruturação da informação não permite que essa seja ambígua, em vista de que a produção de sentidos diferenciados é extirpada desse âmbito (BRODER *et al.* 2006). Por outro lado, a informação não estruturada é aquela resultante do senso comum com base na subjetividade do produtor, na qual inviabiliza-se a extração objetiva dos elementos descritivos e estruturais em uma abordagem semiautomática ou automatizada. Os conteúdos disponíveis em *web sites,* em sua grande maioria, dispõem de informações não estruturadas (MACHADO, 2008).

A informação semiestruturada enquadra-se no contexto das informações codificadas em linguagens de marcações, a saber: HTML e XML. O *eletronic mail (email)* – correio eletrônico e páginas em HTML, por exemplo, são consideradas informações semiestruturadas. As linguagens de marcação especificam as marcas permitidas, as exigidas, estabelece a distinção entre o texto e as marcas, bem como seu significado (ALMEIDA, 2002).

Assim, torna-se extremamente pertinente a utilização de uma abordagem e metodologia para o âmbito dos dados não estruturados, uma vez que os dados não estruturados estão presentes no cotidiano das instituições públicas, privadas e das pessoas físicas. Neste cenário de dados não estruturados, outro agravante que surge é a impossibilidade de estruturar todos esses dados.

Para Provoost (2006), os conceitos de *Content Management System* (CMS), *Document Management System* (DMS) são frequentemente confundidos como sinônimos e, muitas vezes, entendidos como ECM. Entretanto, nota-se uma sutil distinção entre os conceitos. Essa diferenciação entre os conceitos é imprescindível para evitar a imprecisão conceitual.

Dessa forma, CMS é apenas o sistema de gestão de conteúdo, isto é, conjunto de ferramentas utilizadas para gerir conteúdos informacionais. Já o DMS é o sistema de gerenciamento de documentos. Logo, o ECM é composto por um conjunto de estratégias, métodos e ferramentas na gestão de conteúdos empresarias, na qual está previsto CMS e o DMS.

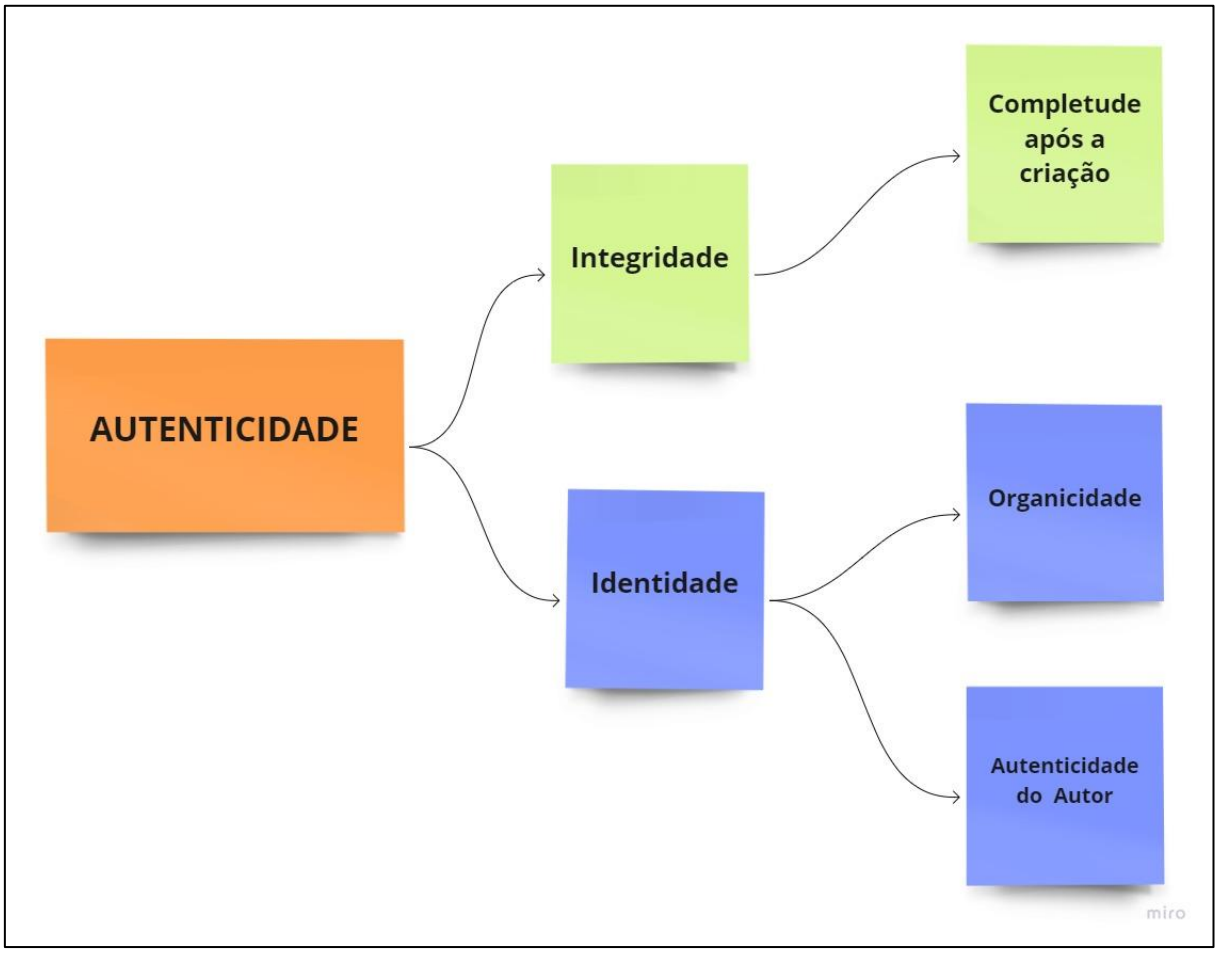
O ECM é composto por uma visão e um *framework,* que integra uma ampla gama tecnológica de formatos e conteúdos no contexto organizacional. O ECM representa parte da solução, o qual combina um conjunto de tecnologias, a saber: gestão documental, gestão de registros, gestão de conteúdo *web*, acesso e recuperação da informação. Todavia, essas tecnologias não são suficientemente agregadoras de valores no contexto organizacional. O ECM deve propiciar as melhores práticas e vincular-se com os processos de negócios (SHEGDA;GILBERT, 2009).

## 5 AUTENTICIDADE

No contexto da Arquivologia para as questões relacionadas aos requisitos de presunção da autenticidade para documentos arquivísticos digitais, a câmara técnica de documentos eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ), do Arquivo Nacional (AN) aponta, que a autenticidade dos documentos arquivísticos digitais é, constantemente, comprometida devido a obsolescência tecnológica. Dessa forma, a presunção da autenticidade deve ter como base a utilização de tecnologias e métodos administrativos, que possam garantir a identidade e integridade documental (BRASIL, 2012).

A figura 13, apresenta os componentes da autenticidade, a saber: identidade e integridade.

**Figura 13:** Componentes da autenticidade




Fonte: elaborado com base em Lemieux *et al.,* 2019.

A figura 13, apresentou a síntese dos componentes da autenticidade sob a perspectiva do projeto INTERPARES 2.

De acordo com o CONARQ (BRASIL, 2020a, p.12), a autenticidade é a “Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade”.

A identidade é o conjunto de atributos de um documento de arquivo, o qual se manifesta como único diferenciando-se de outros documentos. Já a integridade é a qualidade de transmitir a mensagem, que propiciou seu contexto da gênese para cumprir com seus objetivos (BRASIL, 2012).

A CTDE, do CONARQ (BRASIL, 2012, p. 5), manifesta a distinção entre autenticidade e autenticação. Autenticidade se refere à “[...] qualidade do documento ser verdadeiro, isto é, ser exatamente aquele que foi produzido.”, enquanto autenticação “[...] é a declaração da autenticidade feita em um dado momento por uma pessoa autorizada para tal.”

Nessa direção, para o *International Research on Permanent Authentic Records in Eletronic Systems 2* (InterPARES 2) (2010), a autenticidade refere-se aos elementos de identidade dos documentos de arquivo. Para assegurar, que a autenticidade possa ser presumida e mantida ao longo do tempo, deve-se definir e conservar a identidade dos documentos e proteger sua integridade, em vista de que autenticidade poderá ser comprometida quando os documentos são transmitidos ao longo do tempo.

A identidade é o conjunto dos atributos de um documento arquivístico, que o caracterizam como único e o diferenciam de outros documentos, são atributos: data, autor, destinatário, assunto, identificador numérico. A integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem, que sucedeu-se no ato de sua gênese, sem alterações em sua forma e conteúdo. Em suma, a Identidade e integridade são evidenciadas sob a ótica do seu contexto jurídico, administrativo e da proveniência (BRASIL, 2012).

O princípio da proveniência de acordo com Bellotto (2002a, p. 23), é o “Princípio segundo o qual os arquivos originários de uma instituição ou de uma pessoa devem manter sua individualidade, não sendo misturados aos de origem diversas.”

De acordo com o Dicionário Brasileiro de Terminologia Arquivística (DBTA) (BRASIL, 2005, p. 127), a proveniência é o “Princípio básico da arquivologia segundo

o qual o arquivo produzido por uma entidade coletiva, pessoa ou família não deve ser misturado aos de outras entidades produtoras. Também chamado princípio do respeito aos fundos.” Segundo Rousseau e Couture (1998, p. 79), o princípio da proveniência:

> É a base teórica, a lei que rege todas as intervenções arquivísticas. O respeito deste princípio, na organização e no tratamento dos arquivos qualquer que seja a sua origem, idade, natureza ou suporte, garante a constituição e a plena existência da unidade de base arquivística, a saber o fundo de arquivo. O princípio da proveniência e o seu resultado, o fundo de arquivo, impõem-se à arquivística, uma vez que esta tem por objetivo gerir o conjunto das informações geradas por um organismo ou por uma pessoa no âmbito das atividades ligadas à missão, ao mandato e ao funcionamento do dito organismo ou ao funcionamento e à vida da referida pessoa.

Para Rousseau e Couture (1998, p. 41) o fazer arquivístico está “Intimamente ligada à existência dos arquivos. Porém, a estruturação destes hábitos de trabalho em torno de um mesmo objeto e o aparecimento de princípios aos arquivos constitui um fenômeno contemporâneo.” Ainda de acordo Rousseau e Couture (1998, p. 92) “O fundo de arquivo que tem a sua origem teórica na aplicação do princípio da proveniência é uma pedra de toque da prática arquivística.”

O DAD é considerado autêntico quando preserva inalterada sua identidade, que possuía no momento de sua gênese, na qual sua integridade poderá ser presumida ao longo do tempo (DURANTI, 2009).

A identidade do DAD é manifestada por intermédio de metadados, quais sejam: nome dos reponsáveis por sua produção, data, hora, transmissão, ação do objetivo do documento, organicidade, extensão do arquivo (DURANTI, 2009).

Para Bellotto (2002b, p. 23), o princípio da organicidade é a “Qualidade segundo a qual os arquivos refletem a estrutura, funções e atividades da entidade produtora/acumuladora em suas relações internas e externas.” O Manual de Arranjo e Descrição de Arquivos, da Associação dos Arquivistas Holandeses (1973), a respeito da organicidade diz que “O arquivo é um todo orgânico, um organismo vivo, que cresce, se forma e sofre transformações segundo regras fixas. Se se modificam as funções das entidades modificam-se, concomitantemente a natureza do arquivo”. (MULLER; FEITH; FRUIN, [1898] 1973, p. 13).

Sendo assim, a CTDE (BRASIL, 2009, p. 18) define a organicidade como um “Atributo de um acervo documental decorrente da existência de relação orgânica entre

seus documentos. Essencial para que um determinado conjunto de documentos seja considerado um arquivo.”

O documento arquivístico se caracteriza pela relação orgânica, ou seja, pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa por meio do registro ou do plano de classificação ou do arquivamento, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas. Assim, os procedimentos de gestão arquivística devem registrar e manter as relações entre os documentos e a sequência das atividades realizadas, por meio da aplicação de um plano de classificação (BRASIL, 2020).

Nessa direção, os metadados de acordo com o *COMMITTE ON ELETRONIC RECORDS* (CER) do *INTERNATIONAL COUNCIL ON ARCHIVES* (ICA) (1997), são dados sobre dados. Esse conceito é de grande relevância para os DAD, uma vez que os metadados fornecerão os dados necessários a respeito do contexto e estruturação do objeto digital tornando-o compreensível e utilizável. Dessa forma, os DAD são dependentes dos metadados que descrevem o recurso, evidenciam o contexto da gênese documental e os dados estruturais dos objetos digitais.

O conceito proposto pelo CER (ICA, 1997), acerca dos metadados, inicialmente constitui-se de forma simplista. Entretanto, demonstra-se a imprescindibilidade da associação dos metadados com os DAD. De acordo com o Glossário da Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ) (BRASIL, 2010, p. 17), os metadados são “Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo.”

Para a *information Standards Quaterly* (ISQ) da *National Information Standards Organization* (NISO) todas as funções concernentes à preservação digital, depende da disponibilidade dos metadados, que descrevem seu conteúdo e permitem o acesso a longo prazo. Dessa forma, existem três tipos de metadados: descritivo, estrutural e administrativo (NISO, 2004).

Os metadados estruturais indicam como os DAD são compostos e agrupados, por exemplo, como são ordenadas as páginas para formar um determinado arquivo (NISO, 2004). De acordo com Ferreira (2011), os metadados estruturais ou

metadados técnicos referem-se as informações específicas, que devem assegurar que os DAD funcionem de forma adequada e incluem também informações acerca do *hardware* e *software*.

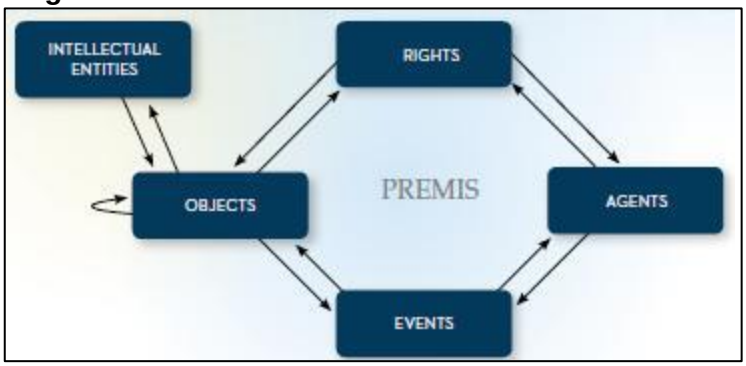
Os metadados do tipo administrativo fornecem as informações para auxiliar o processo de gestão de um determinado recurso. São subdivididos em metadados para gestão de direitos e de preservação. O primeiro trata dos direitos de propriedade intelectual. O segundo provê as informações necessárias para o armazenamento e a preservação digital (NISO, 2004). Nessa direção, os metadados administrativos, também são entendidos como metadados de preservação, tem como objetivos a gestão, tomada de decisão, armazenamento e auxilio na aplicação das estratégias (FERREIRA, 2011).

Por fim, os metadados administrativos fornecem as informações necessárias para determinar a proveniência dos arquivos digitais (NISO, 2010). O padrão de metadado utilizado para preservação digital é o *Preservation Metadata: Implementation Strategies* (PREMIS), o qual consiste em um dicionário de dados e codificação XML *Schema*, que são utilizados para codificar as informações necessárias para apoiar o processo de preservação digital. Os elementos de dados são compostos por cinco categorias: entidades intelectuais, objetos, eventos, agente e os direitos (USA, 2015).

O PREMIS, surgiu em 2003 por meio da iniciativa da *Online Computer Library Center* (OCLC) e do *Research Library Group* (RLG), que foi fundado pela *New York Public Library* e por três universidades: *Columbia*, *Harvard* e *Yale* (USA, 2015).

A figura 14 apresenta o modelo do *Preservation Metadata Implementation Strategies* (PREMIS).

**Figura 14:** Modelo PREMIS.




Fonte: NISO, 2010.

A entidade intelectual pode ser descrita como o ambiente tecnológico (*software* e *hardware*), que suporta um objeto digital, o qual captura e preserva, por exemplo, no âmbito de um repositório digital (USA, 2015). Os DAD são unidades discretas de informação que serão preservadas (USA,2015). Os eventos são as ações que envolvem os DAD e os agentes associados no processo de depósito dos objetos (USA, 2015). Os agentes podem ser pessoas físicas, pessoas jurídicas e *softwares*, que estejam associados com os eventos e com os direitos anexados no contexto do objeto (USA, 2015).

Os *Rights* dizem respeito aos direitos e permissões referentes a um objeto ou agente (USA, 2015). Observa-se que o padrão de metadados PREMIS, fornece os subsídios necessários para preservação digital duradoura no contexto dos (RDCARQ), uma vez que o referido dicionário de dados foi elaborado em consonância com o modelo conceitual OAIS – ISO 14721. Assim, o metadado de preservação fornecerá a conjuntura imprescindível para acessar o DAD.

O metadado do tipo descritivo é um recurso com o propósito de identificação, que inclui elementos, tais como: título, resumo, autor e palavras-chave. Os metadados são fundamentais para garantir que os recursos permaneçam acessíveis no futuro (NISO, 2004). Os repositórios digitais utilizam como padrão de metadados o *Dublin Core Metadata Initiative* (DCMI). O *Dublin core* (DC) é composto por um conjunto de quinze elementos que descrevem os recursos digitais, que permite a interoperabilidade dos dados e a recuperação da informação entre os repositórios digitais por meio do protocolo OAIPMH (DCMI, 2015).

No contexto da Arquivologia, o DC não é o padrão estabelecido para os DAD de cunho orgânico. O esquema padrão de metadados para representar uma estrutura de descrição de documento arquivístico é o *encoded archival description* (EAD), o qual é codificado em XML (SOCIETY OF AMERICAN ARCHIVIST, 2015).

A Figura 15, apresenta os quinze elementos do padrão de metadados do tipo descritivo: o *Dublin Core*.

**Figura 15:** Os quinze elementos do padrão de metadados *Dublin Core*.

| Elementos | Descrição |
|---|---|
| Título | Nome dado ao recurso |
| Criador | Entidade originalmente responsável pela criação do conteúdo do recurso |
| Assunto | Tema do conteúdo do recurso. Pode ser expresso em palavras-chaves e/ou Categoria. Recomenda-se o uso de vocabulários controlados |
| Descrição | Relato do conteúdo do recurso. Exemplos: texto livre, sumário e resumo |
| Publicador | Entidade responsável por tornar o recurso disponível |
| Colaborador | Entidade responsável pela contribuição intelectual ao conteúdo do recurso |
| Data | Data associada a um evento ou ciclo de vida do recurso |
| Tipo | Natureza ou gênero do conteúdo do recurso. Exemplos: texto, imagem, som, dados, software |
| Formato | Manifestação física ou digital do recurso. Exemplos: html, pdf, ppt, gif, xls |
| Identificador | Referência não-ambígüa (localizador) para o recurso dentro de dado contexto |
| Fonte | Referência a um recurso do qual o presente é derivado |
| Idioma | Língua do conteúdo intelectual do recurso |
| Relação | Referência para um recurso relacionado |
| Cobertura | Extensão ou escopo do conteúdo do recurso; pode ser temporal e espacial |
| Direitos autorais | Informação sobre os direitos assegurados dentro e sobre o recurso |

Fonte: http://www.sbu.unicamp.br/seer/ojs/index.php/sbu_rci/article/viewFile/358/237. Acesso em: 02 jul. 2022.

A figura 15, apresentou o padrão de metadados DC composto por quinze elementos qualificadores que descrevem um determinado recurso. O elemento título corresponde ao nome do recurso. Todavia, no caso dos DAD, o referido elemento pode ser compreendido como um tipo documental.

Segundo o Dicionário Brasileiro de Terminologia Arquivística (DBTA) (BRASIL, 2005, p. 85), espécie documental “É a configuração que assume um documento de acordo com a disposição e a natureza das informações nele contidas”. Ainda de acordo com o DBTA (BRASIL, 2005, p. 163) tipo documental “É a configuração que assume uma espécie documental de acordo com a atividade que a gerou”. O elemento criador é a entidade que produziu o arquivo digital. Este qualificador diz respeito ao contexto da gênese documental e, consequentemente, ao princípio da proveniência, de respeito aos fundos.

O assunto é o conteúdo informacional do recurso, que pode ser representado por meio de palavras-chave ou categorias, ou seja, a substância do ato é o texto e suas subseções. A descrição é a síntese do recurso. O publicador é responsável pelo acesso e disseminação do recurso. O colaborador é aquele que contribuiu intelectualmente a respeito do conteúdo informacional. A data associa-se a um determinado evento, que pode ser tópica ou cronológica. Já o ciclo de vida refere-se a fase corrente, intermediária ou permanente.

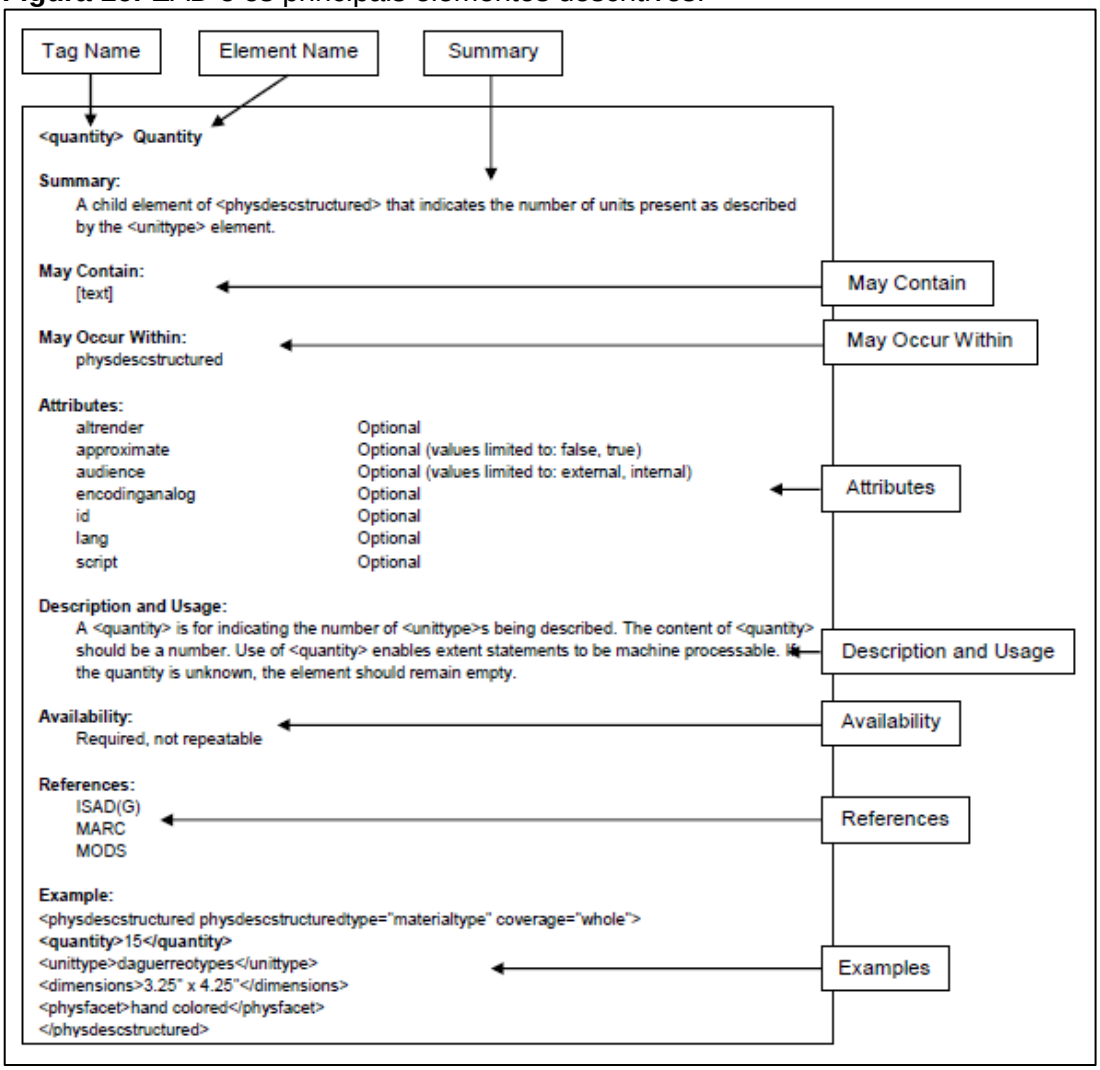
O tipo é o gênero documental no qual enquadra-se o recurso. São gêneros documentais: textual, iconográfico, áudio, vídeo, audiovisual. O formato é a extensão do arquivo como, por exemplo, *portable document format* (PDF), *open document text* (ODT). O identificador pode ser um sequência lógica numérica, utilizada para recuperar a informação posteriormente. A fonte é um apontamento específico para as diversas versões de um determinado recurso do qual o atual é derivado. O idioma é a língua no qual recurso foi produzido.

A relação recomenda as melhores práticas para identificar referências para um determinado recurso relacionado. A cobertura é a jurisdição na qual o recurso é relevante, a qual pode ser temporal ou espacial. O primeiro é o nome do local do âmbito da gênese documental ou coordenadas geográficas como latitude e longitude. O segundo diz respeito ao nome estabelecido para o período ou escopo do período.

O *Encoded Archival Description* (EAD) – descrição arquivística codificada surgiu em 1998 por iniciativa da *Society of American Archivists* (SAA), que é um padrão hierárquico internacional de metadado para transmissão de descrições arquivísticas. O EAD é codificado em XML, que utilizou como base para sua formalização, a norma ISAD(G) (USA, 2015).

A figura 16, apresenta o Encoded Archival Description (EAD), e seus principais elementos descritivos.

**Figura 16:** EAD e os principais elementos descritivos.




Fonte: Society of American Archivist (2015).

A figura 16, apresentou os principais elementos de descrição do EAD. O EAD *header* é composto pela *tag name*, *element name*, *summary*, *may contain*, *may occur within*, *attributes*. O *element tag name* diz respeito ao nome da marca que será utilizada para o documento, por exemplo, <CERT_NASC> (Society of American Archivist, 2015). O *element name* é a versão expandida da marca, que pode ser um *element tag* composto, uma frase, por exemplo, <Certidao_Nascimento> (Society of American Archivist, 2015).

O *Summary* é a síntese do conteúdo, que define o elemento para uma consulta rápida. O *May contain* identifica a composição do texto e subseções (USA, 2015). O *May Occur Within* fornece a identificação de todos os elementos de instâncias superiores, no qual o elemento descrito pode surgir. Demonstra informações adicionais acerca de um determinado elemento (USA, 2015).

O *Attributes* é a identificação de todos os atributos associados a cada elemento, que estão codificados em XML (USA, 2015). O *description and usage* descreve de forma detalhada o conteúdo informacional do objeto digital (USA, 2015).

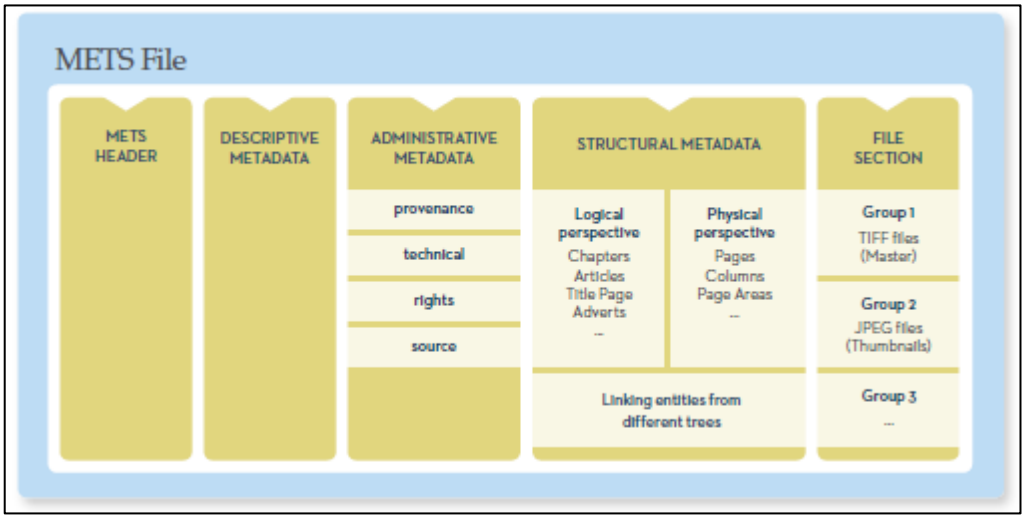
O *availability* indica o contexto de hierarquia, se o elemento descritivo é obrigatório, opcional, repetível ou não (USA, 2015). O *references* é responsável por reconhecer elementos em outros padrões de descrição, por exemplo, ISAD (G), NOBRADE, EAD e DC (USA, 2015). O *examples* são exemplos de elementos descritivos marcados utilizados para indicar como os atributos e elementos podem ser utilizados em conjunto (USA, 2015).

O *Metadata Encoding and Transmission Standard* (METS) – padrão para codificação e transmissão de metadados surgiu, em 2001, por iniciativa da *Digital Library Federation* nos EUA. Atualmente, o padrão de codificação supracitado é mantido pela *United States Library of congress* (USLC) – Biblioteca do Congresso Norte Americano (NISO, 2010).

O METS é um modelo para codificar metadados estruturais, administrativos e descritivos por intermédio de uma codificação em XML, cujo objetivo é a gestão dos DAD e prover sua interoperabilidade (NISO, 2010).

A figura 17, apresenta a arquitetura do *metadata encoding and transmission standard* (METS).

**Figura 17:** Arquitetura METS.




Fonte: NISO, 2010.

A arquitetura METS é composta por vários componentes, tais como: *METS header*, *descriptive metadata*, *administrative metadata*, *structural metadata* e *file sections*.

O METS *Header* (METSHDR) – METS cabeçalho contém a descrição do recurso, que compreende toda arquitetura de metadados como, por exemplo, criador, editor, entidade (NISO, 2004). O *descriptive metadata* (DMD) – metadados descritivos referem-se aos metadados, que descrevem elementos externos, internos, apontam e localizam os padrões para o METS, tais como: EAD, DC, PREMIS (NISO, 2004).

O *administrative metadata* (AMD) – metadados adminstrativos proveem as informações acerca da armazenagem, dos direitos da propriedade intelectual, âmbito da gênese do objeto e determina a proveniência dos arquivos (NISO, 2010). O *structural metadata* (STRUCTMD) metadados estruturais registra a estrutura hierárquica dos objetos, as ligações de estrutura do conteúdo dos arquivos com os metadados pertinentes a cada qualificador, registra as entidades com as diferentes estruturas hierárquicas e permite registrar hiperligações entre os nós hierárquicos por intemédio de um mapa estrutural (NISO,2010).

O *file section* (FILESEC) – seção de arquivos lista todos os arquivos de acordo com seus respectivos conteúdos e versões disponívies (NISO, 2010). Verifica-se que, o padrão METS associa-se a um conjunto de metadados dos tipos administrativos, estruturais e descritivos, os quais podem ser internos ou externos aos arquivos digitais. Fornece compatibilidade com os padrões de metadados arquivísticos como, por exemplo, o EAD. Permite sua aplicação na estratégia de preservação digital, encapsulamento no âmbito dos RDC-Arq e a interoperabilidade das informações. Propicia estabelecer a proveniência dos arquivos, bem como mapear toda cadeia de custódia dos documentos orgânicos desde o contexto de sua gênese ao longo do seu ciclo de vida.

Dessa forma, a utilização de vários padrões de metadados são essenciais e altamente desejados no contexto da Arquivologia, uma vez que são necessários para a recuperação da informação, para gestão de documentos, gestão de conteúdos e para preservação de longa duração.

Para a CTDE (BRASIL, 2012), os métodos de autenticação com o uso tecnologias não são seguras ao longo do tempo, isto é, a utilização de tecnologias a longo prazo tem a sua validade comprometida ou quando são migrados os arquivos, posto que as assinaturas digitais não podem ser transferidas para as novas cadeias

de *bits*. Dessa forma, as migrações sucessivas nos documentos arquivísticos digitais ao longo do tempo não viabilizam que a assinatura digital seja preservada na nova cadeia de *bits,* comprometendo sua autenticação.

Oberva-se que, para garantir a autenticidade implica-se na adoção de um conjunto de ações coordenadas e de gestão de documentos, em vista de que a autenticidade está ligada ao modo, forma e o estado de transmissão do documento, bem como as questões relacionadas com sua preservação e custódia” (BRASIL, 2012).

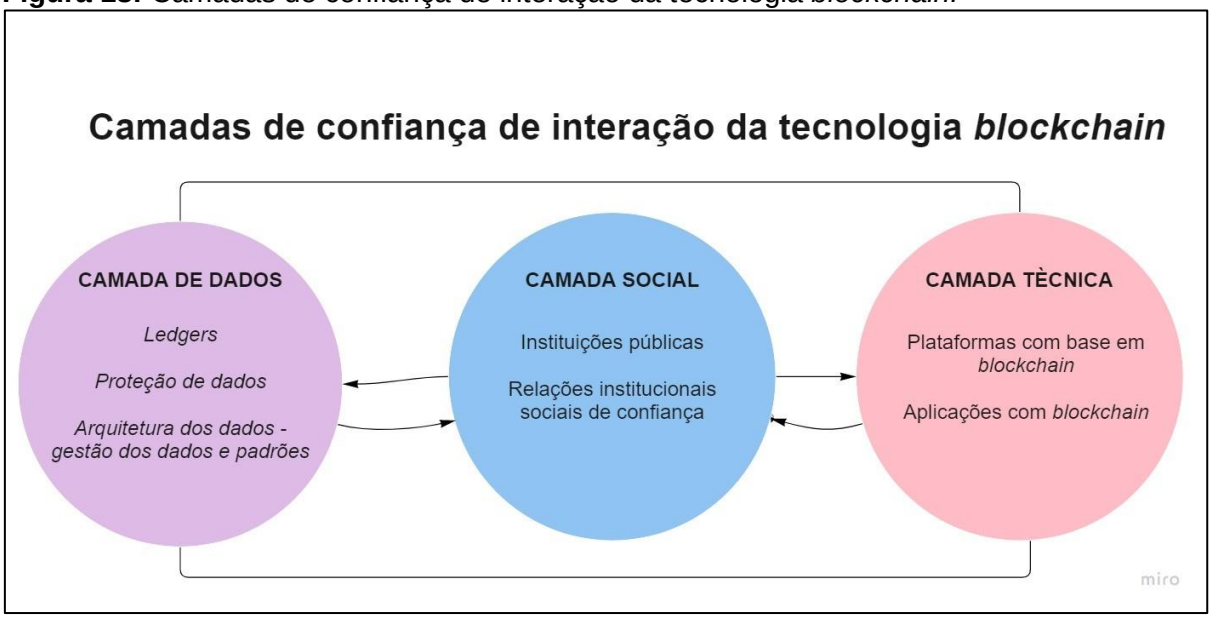
## 6 IMPACTOS DA TECNOLOGIA *BLOCKCHAIN* NO CONTEXTO DA ARQUIVOLOGIA: MODELO LÓGICO PARA AUTENTICAÇÃO DISTRIBUÍDA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Na comtemporaneidade, surge a tecnologia *blockchain*, como uma tecnologia alternativa de confiança. A confiança é o vínculo da sociedade, na qual as sociedades contemporâneas dificilmente perduram sem os seus fundamentos. De acordo com Duranti e Rogers (2016), o conceito de confiança é polissêmico com muitas definições. Nas corporações, a confiança envolve as partes interessadas em alguma operação comercial tomando-se por base um alinhamento de sistemas de valores em relação a benefícios específicos. Na jurisprudência, a confinaça é geralmente descrita como uma relação de vulnerabilidade e dependência, na qual participamos voluntariamente. Em suma, a confiança significa confiar principalmente nas instituições, que compõem o Estado. Todavia, determinados grupos da sociedade civil desconfiam cada vez mais das autoridades centralizadas sob o controle do Estado.

Nessse sentido, Collomosse *et al.* (2018) apontam, que a confiança nas instituições públicas diminuiu, incluindo-se as arquivísitcas, esses lugares tradicionalmente entendidos como confiáveis para preservar e manter a integridade e autenticidade dos DAD ao longo do tempo. A degradação da confiança ocorre, em vista de que, em muitos contextos de sistemas centralizados, provaram-se suas fragilidades, bem como não atendem a sistemas alternativos distribuídos de forma satisfatória.

A figura 18, apresenta as camadas de confiança social e sua interação com a tecnologia *blockchain.*

**Figura 18:** Camadas de confiança de interação da tecnologia *blockchain.*




Fonte: Elaborado com base em Lemieux *et al.,* 2019

A figura 18, apresentou as camadas de confiança social, bem como sua interação com a tecnologia *blockchain*. A camada social é representada pelas instituições públicas, as quais operam, em sua grande maioria, no modelo de arquitetura centralizada. Essa camada compreende as relações institucionais sociais de confiança.

A camada de dados estabelece o uso de *ledgers*, que no caso em específico, é a tecnologia *blockchain*, com intuito de realizar a proteção e gestão dos dados, por meio de uma arquitetura descentralizada, com uma validação consensual ponto a ponto.

Por fim, a camada técnica, que compreende as plataformas com base na tecnologia *blockchain*, para viabilizar as aplicações distribuídas e o estabelecimento de padrões de confiança. Dessa forma, a camada social, que promove as relações institucionais sociais de confiança pode utilizar-se do *blockchain* para ações de auditoria, culminando na transparência social, viablilizadas com o uso do *blockchain* por intermédio das camadas de dados e técnica. Verifica-se, assim, que ao usufruir de uma camada de consenso distribuído, tais como: *proof of work, proof of stake,* na qual opera a tecnologia *blockchain,* poderá ocasionar uma ruptura no modelo de confiança estabelecidos outrora em modelos centralizados.

Dessarte, a tecnologia *blockchain* modifica o poder de uma autoridade central para o consenso distribuído, isto é, quanto mais participantes, mais resiliente é uma rede ponto a ponto. Além disso, a quantidade elevada de entidades, que fazem uso e contribuem com as informações armazenadas, propiciam uma maior valoração de rede P2P. No contexto da Administração Pública, se faz necessário a cooperação e colaboração dos diversos entes para culminar-se o sucesso em um projeto descentralizado. Assim, deve- se estruturar a governança, com o objetivo de identificar as principais funções e responsabilidades relacionados com o uso da tecnologia *blockchain* e garantir que haja incentivos na participação das partes interessadas (BRASIL, 2020c).

Observa-se que, os projetos de implementação do *blockchain* são, por natureza, colaborativos, em vista de que significa alteração de um modelo, que normalmente uma única organização é responsável por administrar os dados, para um modelo, no qual as decisões do projeto são tomadas por um consórcio de entidades. Dessa forma, criar uma estrutura de governança para organizações colaborativas é fundamental para o sucesso nos projetos de tecnologias descentralizadas como, por exemplo, do blockchain. Dessa forma, o consórcio de entidades deve estabelecer as responsabilidades entre os diferentes níveis de

participantes na rede P2P, tais como: comitê de governança, usuários, nós colaboradores, operadores técnicos. As redes mais complexas podem ter necessidade de definir classes de participantes, que poderão votar em relação a um assunto específico da rede como no caso do mecanismo, o qual poderá ser interno *on chain* ou externo *off chain* à rede *blockchain* (BRASIL, 2020c).

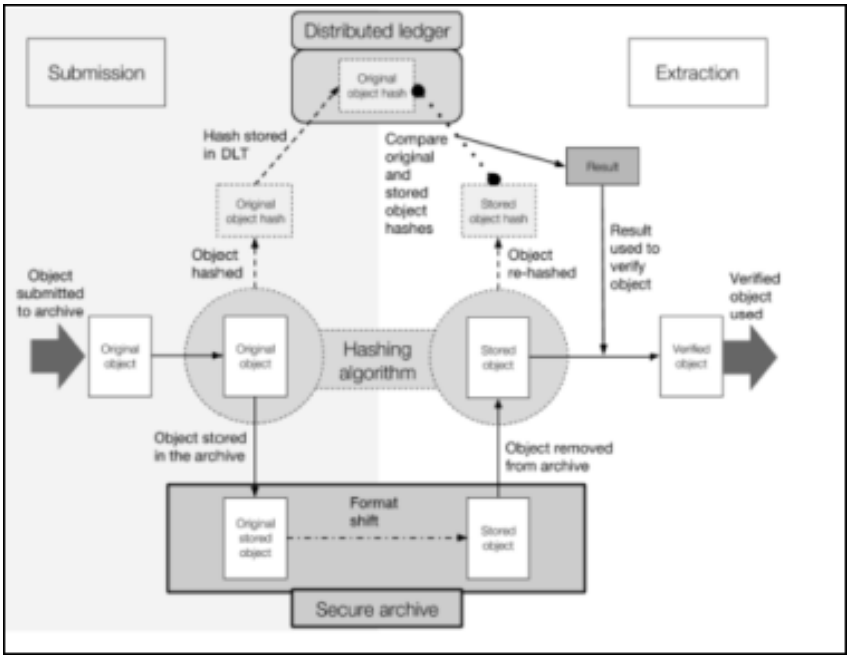
## 6.1 MODELOS LÓGICOS PARA UTILIZAÇÃO DA TECNOLOGIA *BLOCKCHAIN* NO CONTEXTO DA ARQUIVOLOGIA

No Reino Unido, a iniciativa para uso da tecnologia *blockchain*, foi realizada no âmbito da autenticação distribuída de arquivos permanentes, por meio do modelo denominado *Archangel*.

O arquivo nacional do Reino Unido utiliza-se da tecnologia *blockchain,* para autenticações distribuídas de DAD. O modelo Archangel para autenticação distribuída faz uso da tecnologia *blockchain* para gerar entradas imutáveis para os DAD nos arquivos Nacionais do Reino Unido*.* O projeto *Archangel* é constituído pelos Arquivos Nacionais do Reino Unido, Universidade de Surrey e Instituto de Dados Abertos do Reino Unido, os quais são financiados pelo Conselho de Pesquisas em Engenharia e Ciências Físicas (EPSRC), no qual o principal objetivo do *Archangel* é produzir uma trilha de auditoria distribuída para os DAD (*COLOMOSSE et al. 2018).*

A figura 19, a seguir, apresenta o modelo *Archangel* para autenticação de DAD permanentes no âmbito arquivístico.

**Figura 19:** Modelo *Archangel.*




Fonte*: Colomosse et al*. (2018).

A figura 19, demonstrou a concepção da arquitetura da plataforma *Archangel,* um repositório digital descentralizado, cujos documentos são processados para extração de provas de conteúdos, os quais são armazenados de forma imutável em um *blockchain.*

Nessa direção, a autenticação do documento, bem como a proveniência, podem ser verificadas a qualquer momento por intermédio da reextração de *hashes* e comparando com os *previous hash* do *blockchain.*

O modelo *Archangel* é composto por duas partes distintas: *submission* – submissão e *extraction* – extração. Na parte da submissão, o objeto digital, compreendido como *original object* – objeto original, é aplicado *hashing algoritm*, obtendo-se, assim, a função *hash*, isto é, resumo criptográfico do DAD. Esse resumo é um metadado primitivo, do tipo *string*. Após a aplicação, a função *hash* é realizada a ingestão, ou seja, o arquivamento no *secure archive* – arquivo seguro. O *hash* obtido do objeto digital original é armazenado na DLT, do tipo *blockchain*. Logo, com o *root hash* inicia-se a formação do *blockchain*, com a criação do bloco zero, também compreendido como bloco gênesis.

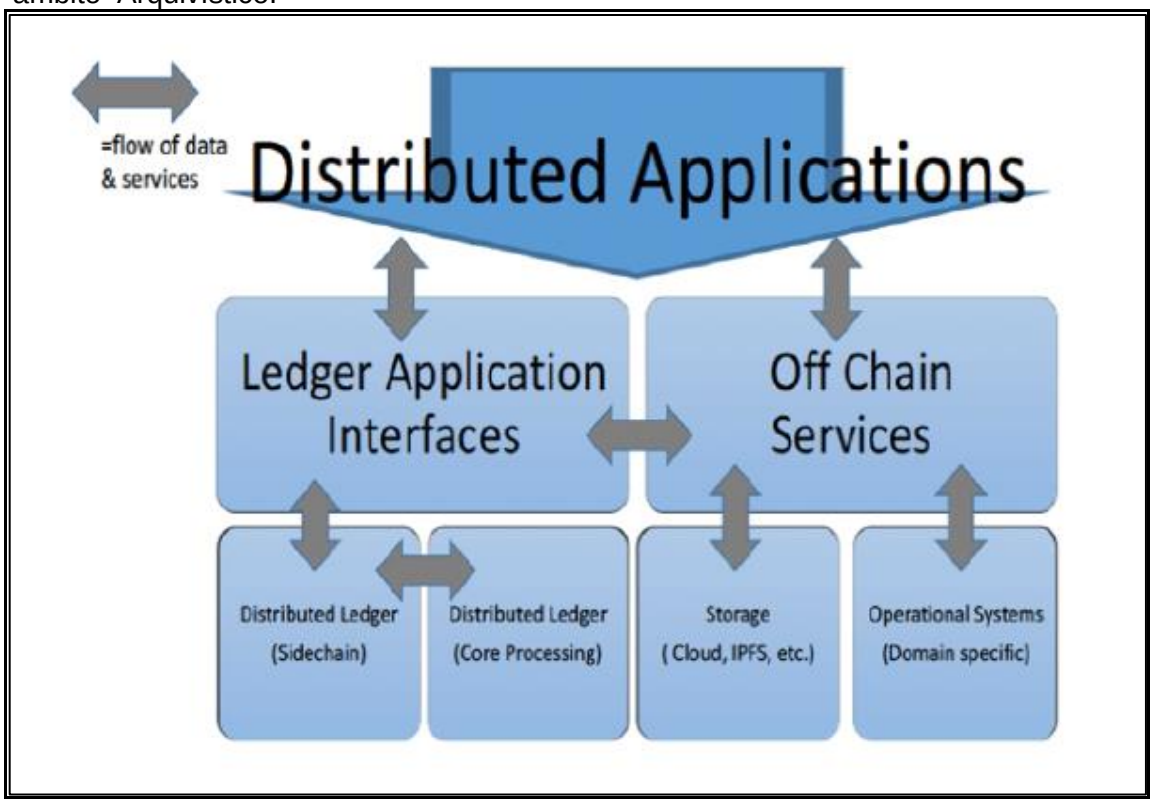
Na segunda parte do modelo *extraction* – extração, consiste na comparação de *hashes* existentes no *blockchain* com objetivo de verificar a autenticação e proveniência dos DAD. O objeto digital original armazenado ao longo do tempo sofrerá os efeitos da obsolescência da tecnologia, principalmente na sua camada lógica, em vista de que será necessário aplicar estratégias de preservação digital, que altera a extensão dos DAD. Nessa direção, é aplicado a função *hash* nesse novo objeto digital.

O novo *hash* é validado por meio dos mecanismos de consensos, e após sua comparação com *previous hash* obtém-se um resultado válido e por conseguinte um novo bloco é adicionado, garantindo-se, assim, autenticação e a possibilidade de verificação da proveniência do objeto digital.

Nessa direção, no Canadá, o uso da tecnologia *blockchain* aplicada aos arquivos, foi apresentada em 2018 no *Digital Identity Design Challenge* (DIDC), promovido pelo *Digital ID & Authentication Council of Canada* (DIACC), para sua aprovação, e, posteriormente, sua institucionalização para uso.

O modelo Canadense para utilização da tecnologia *blockchain* é apresentado por meio da figura 20.

**Figura 20:** modelo canadense para aplicação da tecnologia *blockchain* no âmbito Arquivístico.




Fonte: Lemieux *et al*., 2019.

A figura 20, apresentou o modelo de aplicação do *blockchain* no contexto de aplicações distribuídas para autenticação de DAD em ambientes informacionais descentralizados.

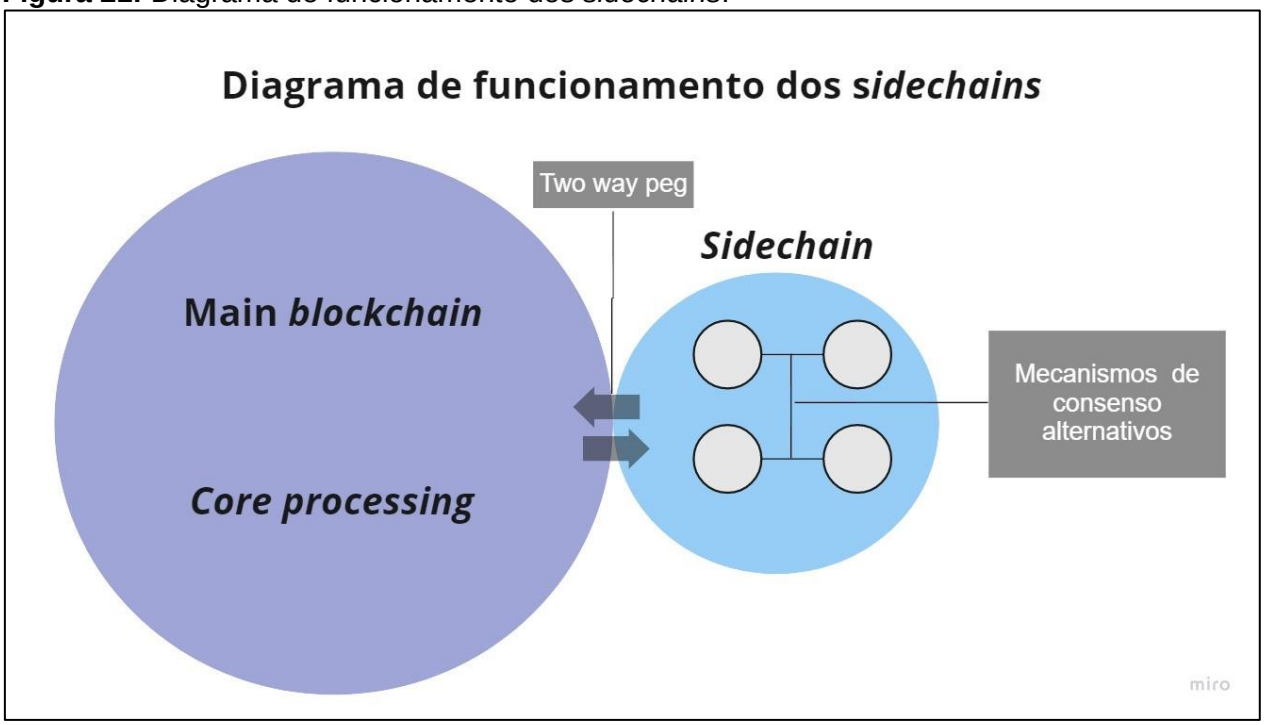
O modelo Canadense para aplicações da tecnologia *blockchain* compreende uma abordagem, que faz uso de serviços distribuídos. O referido modelo abrange o fluxo de dados e serviços, que estão em um contexto de aplicação distribuída. Nessa direção, de aplicações e serviços distribuídos, ocorrem os *off chain services* – os serviços fora da cadeia de fluxos, em vista de que não operam no modelo cliente servidor. Esses podem fazer uso do *ledger application interfaces* – interfaces de aplicação com uso de *ledger*. O *off chain services* é composto dos *storages* como, por exemplo, serviços *cloud* de armazenamento e sistemas operacionais que funcionam de forma distinta da arquitetura cliente servidor, os quais podem utilizar-se das *ledger application interfaces* – interfaces de aplicação com *ledger.* O *ledger application interfaces* é viabilizado por meio do *distributed ledger*, com uso de DLT (LEMIEUX *et al*., 2019).

No caso das DLT, essas, no modelo supracitado, podem ser de dois tipos, a saber: *distributed ledger sidechain* – cadeia lateral e *distributed ledger core processing* – processamento principal.

O primeiro, os *sidecahains*, que são *blockchain* especializados, isto é, autorizado e privado que trabalham com o processamento de transações do *blockchain* principal. Esses são utilizados para melhorar a eficiência do processamento das operações e permitir a flexibilização para customizar os mecanismos de consenso, recursos de contratos inteligentes e dados. O segundo, o *distributed ledger core processing*, é o *blockchain* principal na qual as transações são agrupadas em blocos criptografados, cujo *hash* é inserido no cabeçalho de um bloco proposto, minerado e propagado para a rede distribuída – P2P (LEMIEUX *et al*., 2019).

A figura 21, apresenta o diagrama detalhado de funcionamento dos *sidechain com o main blockchain.*

**Figura 21:** Diagrama de funcionamento dos *sidechains*.




Fonte: Elaborado com base em Lemieux *et al*., 2019.

O diagrama de funcionamento dos *sidechains* é composto pelo *min blockchain* e os *sidechains* e interligado pelo protocolo *two way peg* (2WP). O *core processing* é o processamento principal das cadeias de blocos, o qual cria, valida e adiciona os blocos sequenciais imutáveis e que faz uso dos princiapis mecanismos de validação

consensual. Os *sidechains* contemplam os mecanismos de validação consensuais alternativos, os quais tem por objetivo resolver problemas de saturação no *main core*, por intermédio de uma nova cadeia de blocos, que pode ser conectada, e, por conseguinte, interagir com uma cadeia de blocos existentes (LEMIEUX *et al*., 2019).

Nota-se que os *sidechains* tem grande relevância, posto que permitem dinamizar as operações do main *blockchain*. Além disso, o *sidechains* aumentam o nível de segurança das operações com os *hashes*, em vista de que agregam novas funcionalidades ao *blockchain* existente, sem a necessidade de alterar o *main core*. A conexão entre o *main core* e os *sidechains* é realizada por meio do 2WP, que é um protocolo de transferência com uma conexão de duas vias (LEMIEUX *et al*., 2019).

Nos Emirados Árabes Unidos (EAU), a tecnologia *blockchain* é utilizada pelo governo de Dubai, nos mais diversos setores da governança pública. Nessa direção, com a concepção do atual governante Mohammed Bin Rashid Al Maktoum, é altamente desejável e necessário que Dubai se prepare e, molde-se para o futuro. Logo, fundou-se a *Dubai Future Foundation* (DFF), cujo objetivo é a adoção de tecnologias inovadoras, bem como sua utilização em nível global. Assim, foi institucionalizado o *Global Blockchain Council* (GBC) para analisar as possíveis aplicações da tecnologia *blockchain* no contexto administrativo governamental de Dubai (UNITED ARAB EMIRATES, 2022).

Verifica-se que, o Governo de Dubai percebeu o potencial do uso da tecnologia *blockchain* e idealizou o Dubai *blockchain Strategy*, o qual tem por objetivo tornar o Governo de Dubai o primeiro no cenário mundial a realizar todas as operações governamentais por meio da utilização do *blockchain*, com a seguinte arquitetura, a saber: eficiência do governo, criação de indústrias e liderança internacional (UNITED ARAB EMIRATES, 2022).

Ademais, o primeiro ministro de Dubai, Mohammed Bin Rashid Al Maktoum, está implementando essa tríade para que o território de Dubai seja um padrão global de inovação no uso da tecnologia *blockchain,* em concomitância ao projeto *Dubai blockchain Strategy*, surge o *World Blockchain Forum*, que foi elaborado para discutir e debatar tecnologias relacionadas aos usos do *blockchain*, tais como: operações financeiras com uso de criptmoedas, transações digitais de ativos, *internet* das coisas (IoT) (UNITED ARAB EMIRATES, 2022).

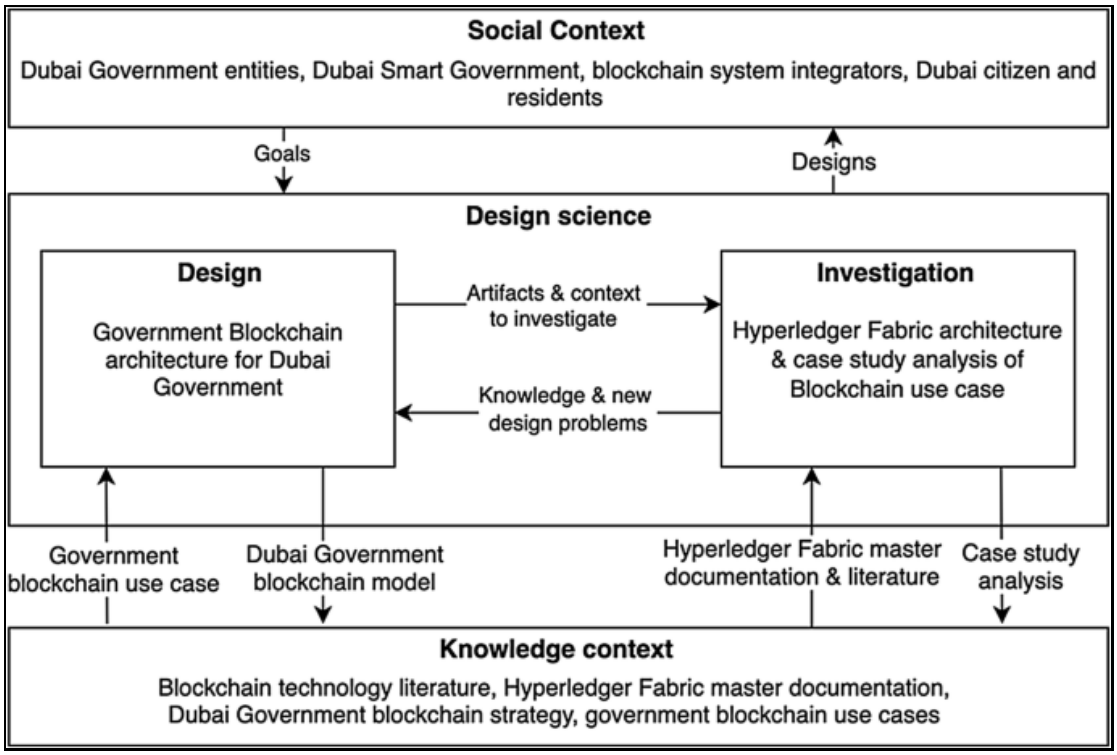
Os EAU adotaram a tecnologia *blockchain* no âmbito governamental e regulamentaram seu uso com o objetivo de melhorar a qualidade de vida em Dubai.

O lançamento, e, por conseguinte, a institucionalização da tecnologia *blockchain* em 2016, teve seu primeiro uso em plataformas de pagamentos para aumentar a eficiência da produtividade. Na ocasião, o *blockchain* foi considerado uma tecnologia inovadora com a concepção de um aplicativo multifacetado, que inclui as criptomoedas (UNITED ARAB EMIRATES, 2022).

Assim, o governo de Dubai deseja ampliar o produto interno bruto (PIB), com a expansão no uso do *blockchain* e metaverso*.* Para tal, se faz necessário acelerar o desenvolvimento de padrões globais na construção de plataformas seguras e criar modelos na administração pública, em setores vitais de Dubai, tais como: turismo, educação, varejo, trabalho remoto, saúde e setor jurídico (UNITED ARAB EMIRATES, 2022).

A figura 22, apresenta o modelo para utilização da tecnologia *blockchain* proposto pelo Governo de Mohammed Bin Rashid Al Maktoum para o contexto administrativo governamental de Dubai (UNITED ARAB EMIRATES, 2022).

**Figura 22:** Modelo de utilização da Tecnologia *Blockchain* em Dubai.




Fonte: UNITED ARAB EMIRATES, 2022.

A figura 22, apresentou o uso do modelo de utilização da tecnologia *blockchain*, em Dubai, que se consiste em duas partes distintas, quais sejam: *social*

*context – contexto social* e *knowledge context* – contexto conhecimento.

No contexto social está compreendido que a tecnologia *blockchain* será utilizada pelas seguintes abordagens, *Dubai goverment enteties, Dubai smart goverment, blockchain system integrators, Dubai citizen and residents*. O *Dubai goverment enteties* é o uso da tecnologia *blockchain* nas atividades administrativas dos diversos órgão que compõem o governo. O *Dubai smart govement* contempla a utilização dos *smart contracts* nas funções administrativas governamentais. O *blockchain system integrators* é a integração da administração pública com os setores governamentais, bem como às corporações de natureza privada. Por fim, o *Dubai Citizen and residents* muda a forma de interagir com a cidade, em vista da implementação da concepção das *smarts cities* que, por exemplo, pode criar um espaço governamental em consonância com âmbito privado sem uso de documentos analógicos.

Observa-se, assim que no contexto governamental de Dubai, a tecnologia *blockchain* poderá ser utilizada na cadeia de suprimentos, nas transações no cenário corporativo podendo utilizar-se das DLT, para registrar os históricos das operações financeiras de contratos, ativos e fluxos da cadeia de suprimetos, em um registro em tempo real, imutável e distribuído. Dessa froma, os ponteciais consumidores podem verificar as notificações realizadas por uma corporação acerca do processo de produção e logística de um determinado ativo.

Nota-se que a utilização da tecnologia *blockchain* poderá corroborar com a segurança da informação, no que diz respeito ao armazenamento de arquivos, em vista de que protege as bases de dados de possíveis ataques cibernéticos. O sistema dsitribuído em uma rede P2P dispensa a necessidade de uma arquitetura cliente servidor, tornando-se mais flexível. Já para o uso governamental, poderão ser utilizados os contratos inteligentes, com o intuito de desburocratização das operações e maior agilidade nos processos, posto que, os contratos inteligentes, podem ser executados por intermédio de uma rede *blockchain*.

Por outro lado, o contexto do conhecimento engloba algumas iniciativas, quais sejam: *blockchain technology literature*, *hyperledger fabric master documentation, Dubai goverment blockchain strategy*, *goverment blockchain use case*.

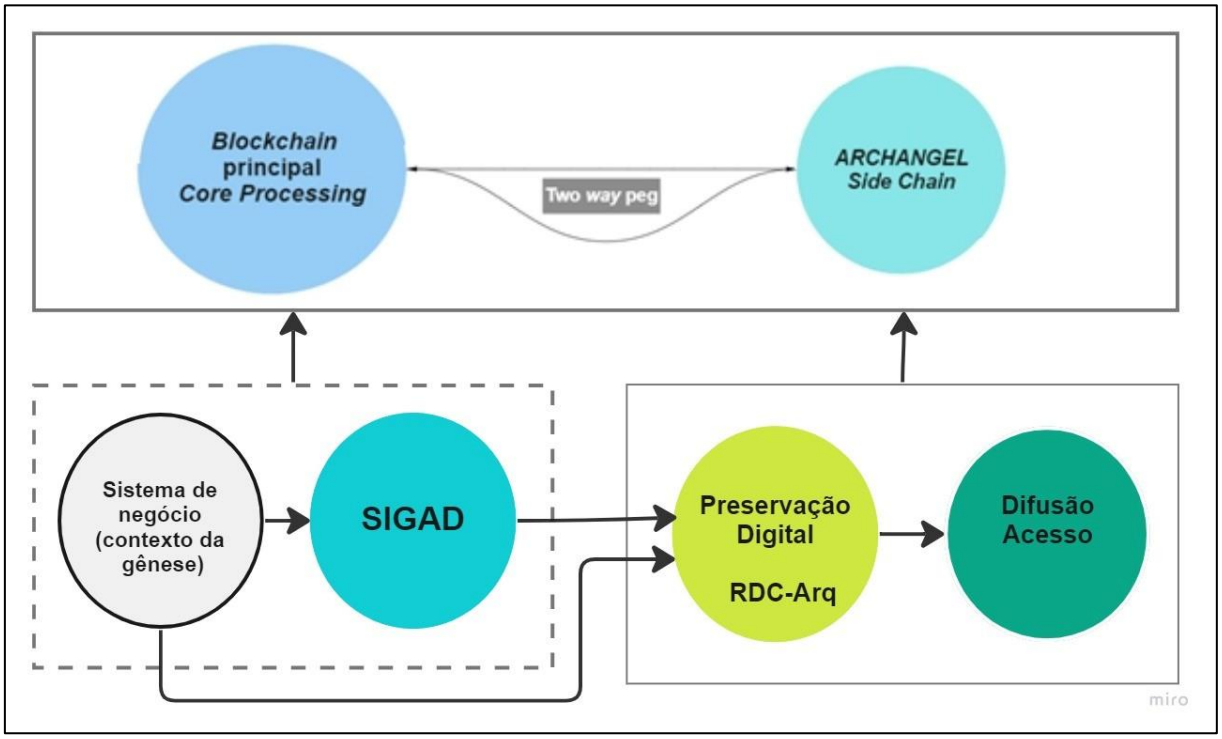
Para viabilizar o desenvolvimento e aplicação da tecnologia *blockchain* no contexto governamental de Dubai, o modelo proposto que contempla o *social context* e *knoeledge contexto,* estão alinhados aos programas DFF e WBF.

Com base nos modelos de aplicação da tecnologia *blockchain*, investigados em âmbito mundial, verificou-se o uso de três modelos lógicos para fins arquivístico da tecnologia *blockchain*, modelo do Reino Unido o *Archangel*, modelo do Canadá DIDC e modelo do governo de Dubai.

Nessa direção, propõe-se um possível modelo lógico para autenticação distribuída, tomando-se por base os modelos supracitados para aplicação da tecnologia *blockchain* no âmbito da arquivologia desde o contexto da gênese do DAD, até sua destinação final.

A figura 23, apresenta o modelo de aplicação da tecnologia *blockchain* na autenticação descentralizada para DAD, ao longo do seu ciclo de vida.

**Figura 23:** Autenticação descentralizada de DAD.



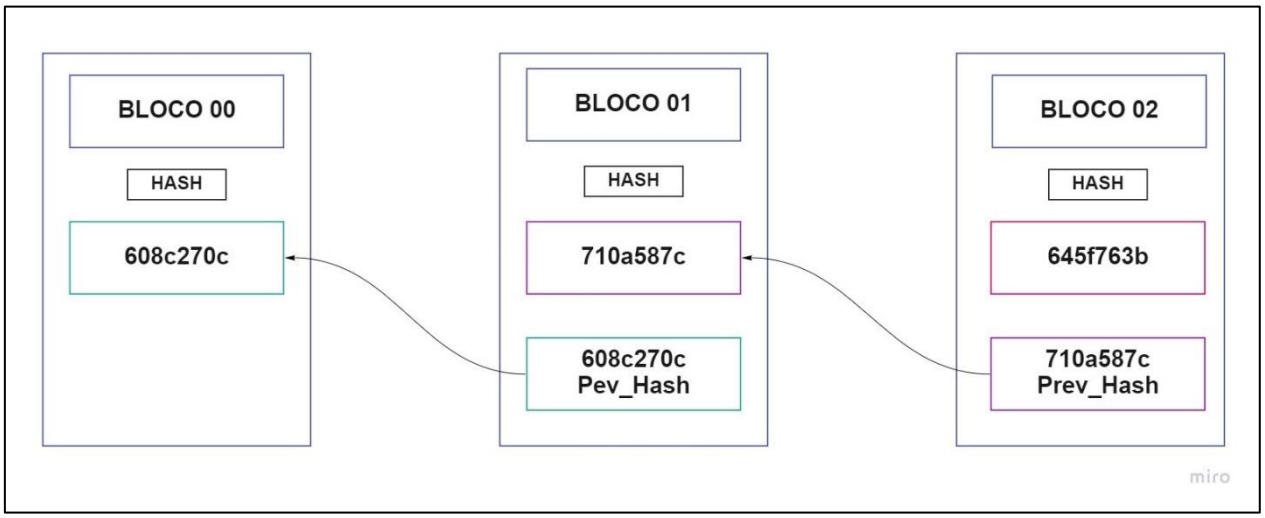

Fonte: Elaborado pelo autor.

A figura 23, apresentou modelo para aplicação da tecnologia *blockchain,* no âmbito da Arquivologia, desde o contexto da gênese até sua destinação final. O modelo proposto para autenticação inicia-se no contexo de gênese, isto é, quando é produzido um DAD no contexto dos sistemas de negócios, o qual gera um resumo criptográfico para o DAD por meio de uma função *hash.* Esse resumo, consiste-se em um metadado do tipo *string,* o qual inicia o bloco gênesis, o *root hash.* O bloco 00

fica armazenado no *core processing*. Após o DAD ser produzido nos ambientes de negócios, se faz necessário realizar a gestão documental no sistema informatizado de gestão arquivística de documentos (SIGAD), o qual segue o requisitos do e-ARQ Brasil. Posteriomente, é realizado o recolhimento do DAD para ambiente de preservação RDC-Arq e acesso/difusão por meio do ATOM. Logo, gera-se *root hash* na gênese documental, e, ao longo do ciclo de vida do DAD, são gerados outros *hashes*, principalmente no momento do recolhimento do DAD do SIGAD para o ambiente de preservação, cujos *hashes* constituem blocos, que serão validados e adicionados na cadeia de blocos de forma permanente com o objetivo final de criar uma trilha de auditoria ininterrupta e auditável.

A Figura 24, demonstra a aplicação detalhada da tecnologia *blockchain* na autenticação distribuída dos DAD em seu ciclo de vida, o qual compreende o *main blockchain – core processing* e o *sidechain*, na qual pode ser utilizada arquitetura Archangel.

**Figura 24:** Aplicação detalhada na autenticação distribuída de DAD.




Fonte: Elaborado pelo autor.

A figura 24, apresentou aplicação da tecnologia *blockchain* na autenticação distribuída dos DAD, cujo objetivo é produzir uma trilha de auditoria ininterrupta e imutável ao longo do ciclo de vida dos DAD, que poderá ser utilizada também para verificação da proveniência.

O bloco 00 é o bloco gênesis, bloco inicial que contém o *Root hash* referente ao DAD nos sistemas de negócio, no caso a função *hash*, isto é, o resumo critptográfico do documento arquivístico digital, representado por meio de um

metadado, qual seja: 608c270c. O bloco 01, seguinte do *blokchain,* dispõe do *Prev hash* (608c720c) – *hash* referente ao bloco gênesis, o bloco 01 é encadeado ao bloco 00 – gênesis, em vista de que os *hashes* foram validados por meio dos algoritmos de validação consensual, a saber: *proof of work* e *proof of stake*. Já o bloco 02, tem acesso ao *Prev Hash* (710a587e) do bloco 01. No caso, o bloco 02 aponta para o bloco anterior, ou seja, para o bloco 01, após a validação consensual, iniciando-se a formação do *blockchain.*

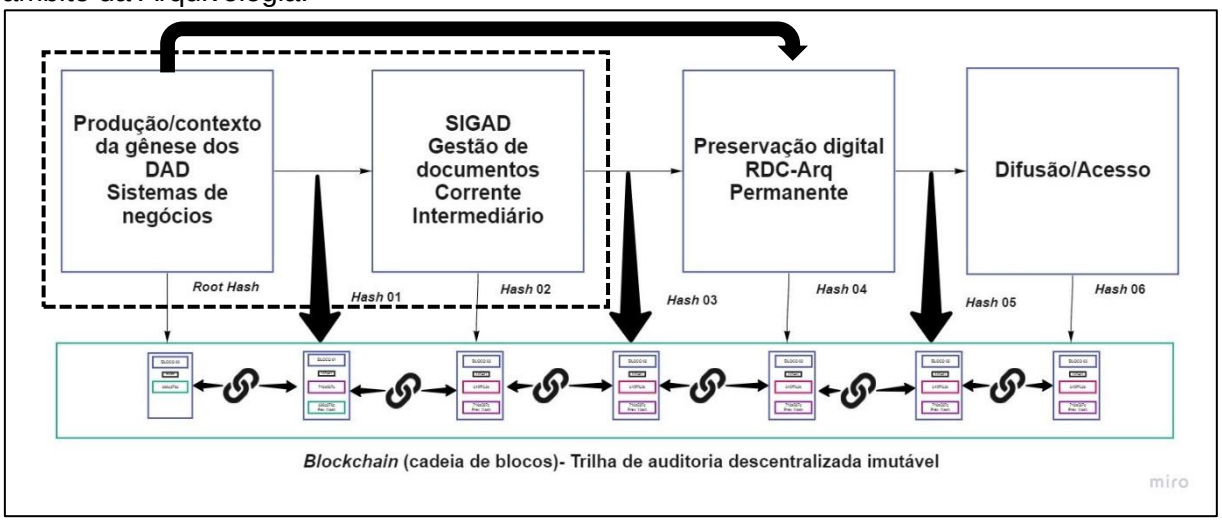
Nesse sentido, demonstra-se, por intermédio da figura 24, as questões relacionadas à autenticação distribuída de documentos arquivísticos digitais, a qual poderá utilizar-se dos *sidechain* e da arquitetura do projeto *Archangel* para auxiliar na construção das cadeias de blocos, bem como produzir as trilhas de auditorias para fins de verificação da proveniência.

O resumo inicial – *Root Hash*, é obtido por intermédio de um algoritmo de função *hash,* o qual foi aplicado no documento arquivístico digital. Com base no metadado em questão, isto é, 608c270c referente ao bloco 00 – gênesis, é possível garantir autenticação, em vista de que, ao comparar o documento arquivístico digital com o resumo *hash,* esse será válido. Todavia, quando o documento arquivístico digital sofrer quaisquer modificações como, por exemplo, migração da sua extensão em decorrência da obsolescência tecnológica de um arquivo de texto (TXT), com o *hash* inicial de 608c270c, convertido para *portable document format* (PDF), esse sofrerá alteração em seu resumo, posto que ocorreram modificações na camada lógica do objeto digital. O documento arquivístico digital receberá um novo resumo, tal como: 710a587, cujo objeto digital com extensão em pdf, posteriormente, sofrerá uma nova migração da extensão pdf para pdf/a, alterando-se, novamente, sua camada lógica, e, consequentemente, seu resumo, o qual será modificado para 745f763b.

Nessa direção, o *blockchain* consiste-se em uma cadeia de blocos estruturados em uma sequência linear, validados por meio de algoritmo de consenso, que resolve o desafio criptográfico proposto no qual um novo bloco é adicionado à cadeia de blocos pré-existentes, possuindo, cada bloco, um *hash* exclusivo e o *hash* do bloco anterior.

A figura 25, apresenta a síntese de aplicação da tecnologia *blockchain* no contexto da Arquivologia, por intermédio de um diagrama de blocos.

**Figura 25:** Diagrama de blocos do funcionamento da aplicação da tecnologia *blockchain* no âmbito da Arquivologia.




Fonte: Elaborado pelo autor.

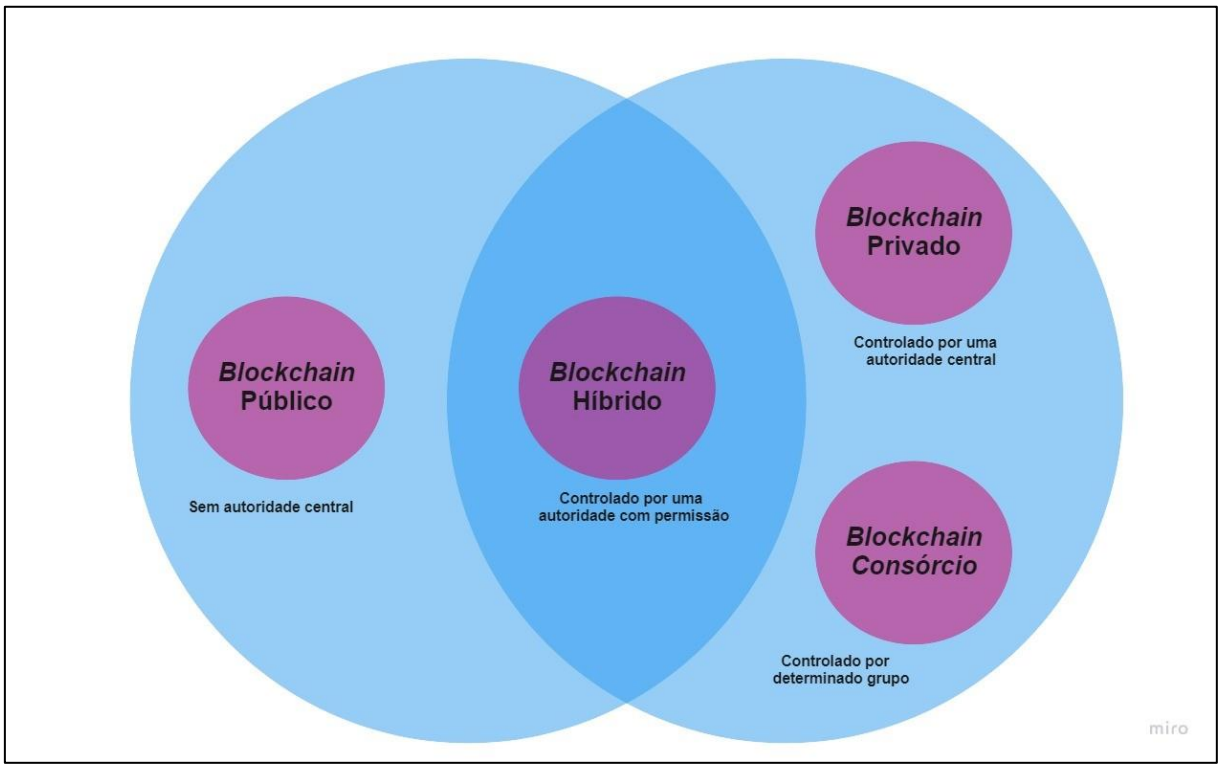
A figura 25, apresentou diagrama de aplicação da tecnologia *blockchain* para autenticação descentralizada de DAD, desde a sua produção até a preservação/acesso de longa duração. Ademais, nota-se a eficiência do *blockchain* na autenticação descentralizada nos ambientes informacionais digitias, em vista de que, o processo de gerar os resumos criptográficos, podem ser realizados de forma automatizada e descentralizada nas migrações a serem realizadas: no SIGAD, no RDC-Arq e plataformas de difusão e acesso. Por fim, em todos os eventos ao longo do ciclo de vida dos DAD, podem ser gerados *hashes*, que serão validados e adicionados à cadeia de blocos, construindo-se uma trilha de auditoria descentralizada e imutável.

Nesse cenário, a tecnologia *blockchain* fornece a solução para problemática da autenticação em ambientes descentralizados, bem como auxílio às questões relacionadas à preservação digital de longa duração, uma vez que poderá garantir que as migrações realizadas no documento arquivístico digital sejam modificações autorizadas com uso de algoritmos de validação consensual que propiciam um registro cronológico inalterável, na qual as trilhas de auditorias são realizadas com os registros dos metadados criptografados com o uso do algoritmo árvore de *merkle,* que realiza auditoria desde o último *hash* do bloco até o bloco gênesis.

Logo, o tipo de *blockchain* indicado para o modelo proposto de aplicação, deve ser o *blockchain* híbrido.

A figura 26, apresenta os tipos de *blockchain* existentes.

**Figura 26:** Tipos de *blockchain.*




Fonte: Elaborado pelo autor.

A figura 26, apresentou os tipos de *blockchain* existentes. O *blockchain* recomendado para o âmbito arquivístico deve ser o híbrido, posto que reúne características do público e privado. No *blockchain* híbrido o controle da rede *blockchain* é exercido por uma autoridade com permissão, a qual pode ser uma rede ou grupo de pessoas, que colaboram seus esforços para potencializar o sistema. Os nós são independentes e podem definir suas parcerias, bem como quais *Hyperledger* farão parte da cadeia de blocos em que permite o controle de acesso e envio aos dados sensíveis. Já o *blockchain* público, dispõe de acesso público por qualquer usuário da *internet*. Sendo assim, não é possível restringir o acesso e envio de operações com ativos. No tocante do *blockchain,* privado ou consórcio, são administrados e controlados por grupos privados pré-definidos ou por uma autoridade central. Dessa forma, perdem a sua essência da abordagem descentralizada, inviabilizando-se, assim, seu uso no contexto arquivístico.

O *blockchain* do tipo híbrido faz uso do mecansimo de validação consensual de blocos denominados de *Proof of Activity* (PoA) – prova de atividade, que é composto pelo *Proof of Work* – prova de trabalho (PoW), *Proof of Stake* – prova de participação (PoS).

Sendo assim, os sistemas de negócios são um sistema informatizado, cuja principal função é apoiar a realização de atividades específicas na organização, que produzem e mantêm dados, informações e documentos a respeito das funções desenvolvidas. Esses sistemas mantêm o registro das atividades na forma de tabelas de banco de dados, podendo, em certos casos, dispor de informação materializada e registrada, isto é, o documento nas mais diversas extensões, como, por exemplo: pdf, txt, jpg, dwg (BRASIL, 2020).

O e-ARQ Brasil foi elaborado com base em documentos similares já publicados no ano de 2000, por diferentes instituições Européias e Norte Americanas. Inicialmente, foi utilizado o modelo de requisitos para a gestão de arquivos eletrônicos, (MoReq), publicado em 2001 pelo DLM Forum e Comissão Européia (DLM FORUM; COMISSAO EUROPEIA, 2010). Nesse sentido, utilizou-se também o *Departament of Defense* 5015.2 *Design criteria standard for electronic records management software applications* (DOD 5015.2-STD) (UNITED STATES OF AMERICA, 2002), *Requirements for electronic records management systems: Functional requirements* (UNITED KINGDOM, 2002) e publicações do InterPARES Project 1 e as normas ISO 15.489/2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002).

Assim, o e-ARQ Brasil:

> “É uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade. Além disso, o e-ARQ Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais. O e-ARQ Brasil estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado (BRASIL, 2020, p. 15).

Observa-se, assim, que os objetivos principais do e-Arq Brasil são orientar a implementação da gestão arquivística de documentos analógicos e digitais e prover os requisitos técnicos e funcionais, bem como padrões de metadados, os quais orientam a seleção ou desenvolvimento dos sistemas informatizados de gestão arquivística (BRASIL, 2020).

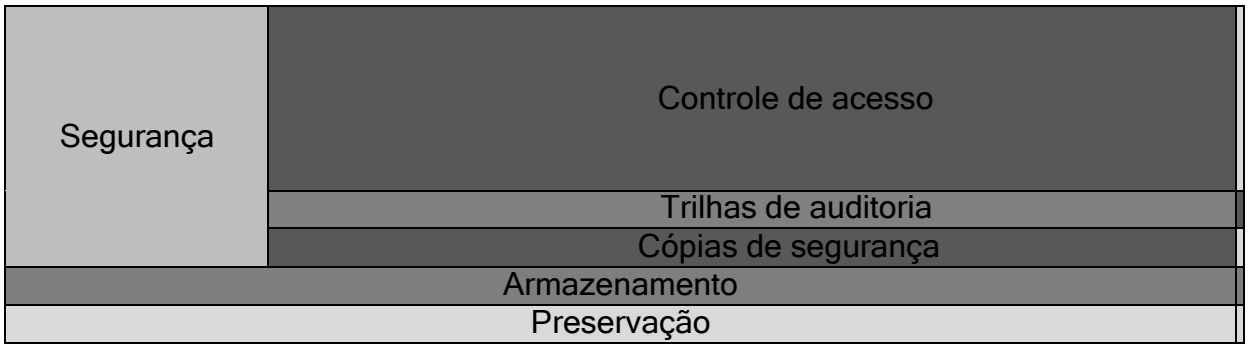
Logo, o SIGAD é um:

> É um sistema informatizado que apoia a gestão arquivística de documentos. O sucesso do SIGAD dependerá, fundamentalmente, da implementação prévia de um programa de gestão arquivística de documentos. O SIGAD deve ser capaz de gerenciar, simultaneamente, os documentos digitais e os não digitais. No caso dos documentos não digitais, o sistema registra apenas as referências sobre os documentos e, para os documentos digitais, a captura, o armazenamento e o acesso são feitos por meio do SIGAD. Deve-se também considerar os documentos híbridos, compostos por partes digitais e não digitais, gerenciando cada uma dessas partes adequadamente (BRASIL, 2020, p.26).

Assim, o quadro 2 apresenta os procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e analógicos.

**Quadro 2**: Procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e analógicos.

<table>
<tr><td colspan="3">Sistema Informatizado de Gestão<br>Arquivística de Documentos (SIGAD)</td></tr>
<tr><td rowspan="4">Captura</td><td colspan="2">Registro</td></tr>
<tr><td colspan="2">Classificação</td></tr>
<tr><td colspan="2">Indexação</td></tr>
<tr><td colspan="2">Atribuição de restrição de<br>Acesso</td></tr>
<tr><td rowspan="4">Avaliação</td><td colspan="2">Arquivamento</td></tr>
<tr><td colspan="2">Prazo de guarda</td></tr>
<tr><td rowspan="3">Destinação</td><td>Eliminação</td></tr>
<tr><td>Transferência</td></tr>
<tr><td>Recolhimento</td></tr>
<tr><td>Pesquisa</td><td colspan="2" rowspan="3">Recuperação da Informação</td></tr>
<tr><td>Localização</td></tr>
<tr><td>Apresentação</td></tr>
</table>




Fonte: Elaborado pelo autor.

O quadro 2, expõe o procedimento e operações técnicas dos SIGAD. Nessa direção, a captura é a incorporação do documento no SIGAD, por intermédio das seguintes etapas: registro, classificação, indexação, atribuição de restrição de acesso e arquivamento (BRASIL, 2011).

O registro é a atribuição de um identificador numérico, que poderá ser sequencial, que é realizada na etapa de ingestão dos objetos digitais. Posteriormente, será aplicado os metadados do tipo descritivo.

A classificação consiste-se na aplicação de um instrumento, o plano de classificação de documentos (PCD), cuja aplicação poderá ser manual ou automatizada, com o objetivo de evidenciar a relação orgânica dos objetos digitais.

A indexação é a designação de termos para descrever o recurso. Esta etapa é realizada na descrição documental. Nota-se que, a qualidade da descrição, realizada por meio de metadados, impactará de forma direta e proporcional na consistência do índice, que por sua vez influencia a recuperação das informações.

A restrição de acesso poderá ser implementada com a utilização do gerenciamento de categorias. Os documentos podem ser considerados ostensivos ou sigilosos. O primeiro não tem restrição de acesso. O segundo contempla vários graus de sigilo. De acordo com o Decreto Nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e que dispõe sobre o núcleo de segurança e credenciamento, seu artigo 52 indica os graus de sigilos. São eles: ultrasecreto (U), secreto (S), reservado (R) (BRASIL, 2012a).

A avaliação documental é a análise dos documentos com enfoque nos prazos de guarda e sua destinação, que podem ser a eliminação, transferência ou recolhimento. Esses procedimentos são contemplados na gestão documental –

*records management,* com a aplicação de instrumentos específicos como, por exemplo, a tabela de temporalidade de documentos (TTD).

A segurança é composta pelo controle de acesso, trilhas de auditoria e cópias de segurança. As rotinas de *backup* podem se realizadas manualmente ou automaticamente. Todavia, as cópias de segurança não são consideradas estratégias de preservação digital. O objetivo concentra-se na restauração do sistema em situações de desastre. Assim, as replicações de *bit* a *bit* e os sistemas de redundância são necessários, porém, não suficientes para preservação duradoura.

No âmbito da preservação digital, de acordo com Hedstrom, (1998, p.01 tradução nossa) é o:

> Planejamento, alocação de recursos e aplicação de métodos de preservação e tecnologias necessárias para que a informação digital de valor contínuo permaneça acessível e utilizável por longo prazo. Intencionalmente utilizei o termo contínuo em vez de permanente para evitar o absolutismo e o idealismo que o referido termo implica (O'Toole). A concepção de preservação digital engloba os documentos cuja gênese é o ambiente informacional digital quanto aos documentos convertidos de suportes tradicionais para formatos digitais.

Nesse sentido, a Câmara Técnica de Documentos Eletrônicos (CTDE) (BRASIL, 2010, p.19) compreende a preservação digital como um "Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário".

Para Ferreira (2006) a preservação digital:

> Consiste na capacidade de garantir que a informação digital permaneça acessível e com qualidade de autenticidades suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da suacriação.

Nesse sentido, Conway (1996 p.4 tradução nossa) define a preservação digital como a "Aquisição, organização e distribuição de recursos para evitar uma maior deterioração ou renovar a usabilidade de grupos selecionados de materiais". O *COMMITTEE ON ELECTRONIC RECORDS* (CER) do *INTERNATIONAL COUNCIL ON ARCHIVES* (ICA, 1997), considera que a preservação digital tem alguns quesitos fundamentais, tais como: os

arquivos devem permanecer fisicamente intactos, identificados e legíveis. É considerado legível todo registro digital armazenado que permita sua recuperação para o processamento por meio de equipamentos eletrônicos digitais cuja camada conceitual deverá estar intacta.

Sendo assim, Lee *et al.* (2002) dizem que a preservação digital implica na retenção do objeto digital e seu significado. É, por conseguinte, necessário que as estratégias de preservação digital sejam capazes de compreender e reproduzir a forma ou função original do arquivo, sua autenticidade e acessibilidade. A preservação digital torna-se complexa, uma vez que os objetos digitais são dependentes dos ambientes tecnológicos.

A preservação digital é uma combinação coordenada de políticas, estratégias e ações que devem garantir a reprodução de conteúdo autenticado por um longo período. As políticas de preservação digital são fundamentais nas instituições para preservar o conteúdo digital para o acesso futuro. Essas especificam os formatos de preservação digital dos arquivos, o nível de preservação que deverá ser aplicado, garante a conformidade com as normas e legislação vigentes e estabelecem as melhores práticas para uma gestão responsável dos ambientes informacionais digitais (ASSOCIATION OF LIBRARY COLECTION AND TECHNICAL SERVICES, 2007).

A preservação digital, de acordo com o arquivo nacional da Nova Zelândia (New Zealand, 2011, p.15), é o “Termo coletivo para ações que proverá o acesso ao conteúdo digital no futuro. O método de preservação é definido por uma filosofia ea compreensão prática do conteúdo digital.”

Na concepção do arquivo nacional da Nova Zelândia, o foco da preservação digital está voltado para o conteúdo do objeto digital, que se desvincula do suporte no qual a informação foi registrada.

Dessa forma, a preservação digital engloba ações que abordam a criação, integridade e manutenção dos conteúdos digitais (ASSOCIATION OF LIBRARY COLECTION AND TECHNICAL SERVICES, 2007).

Para Kirchhoff (2008), a preservação digital consiste na gestão das políticas e nas atividades necessárias para garantir a usabilidade, autenticidade e acessibilidade dos conteúdos digitais de forma duradoura.

A preservação digital eficaz requer gerenciamento do ciclo de vida de informação digital, com base no ponto de criação por meio do armazenamento, migração e o acesso em uma base contínua (HEDSTROM, 1998).

No contexto da preservação digital existem várias estratégias, tais como: migração, encapsulamento, emulação e refrescamento. A migração, para Waters e Garret (1996), é a transferência periódica dos objetos digitais de uma determinada geração específica de *hardware* e *software* para outra subsequente. O objetivo da migração é manter íntegro os objetos digitais. A estratégia de migração consiste-se em:

> Copiar a informação digital de um suporte que está obsoleto ou fisicamente deteriorado para um suporte mais novo; e/ou converterde um formato ultrapassado para outro mais atual; e/ou transferir documentos de uma plataforma de *hardware/software* em processo de descontinuidade para outra. (THOMAZ, 2004, p. 4).

De acordo com a *Task Force on the Archiving of Digital Information,* da *Commission on Preservation and Access* e *Research Library Croup* :

> Existe uma variedade de estratégias de migração para a transformação de informação digital contida em sistemas obsoletos para sistemas de *hardware* e *software* atuais, para que essa informação continue acessível e usável. Nenhuma estratégia única pode ser aplicada a todos os formatos de informação digital e nenhum dos métodos de preservação atuais é totalmente satisfatório.As estratégias de migração e seus custos variam dependendo dos contextos de aplicação, dos formatos, dos graus de preservação que as estratégias atendem e das suas possibilidades de recuperação. (TASK FORCE, 1996, p. 27, tradução nossa).

A migração é o processo de conversão de um objeto digital obsoleto para outro atualizado. Os arquivistas geralmente utilizam a estratégia de migração para garantir a acessibilidade do conteúdo digital, que converte um objeto digital obsoleto em um formato atual, bem como todo o *hardware* e *software* necessários para o processamento desse. Entretanto, alguns atributos dos recursos podem ser perdidos no processo de migração. Após migrado, o objeto poderá não corresponder ao objeto anterior ao da migração. As perdas que poderão ocorrer no objeto vão depender do tipo de migração escolhida, a nova extensão do objeto, o

grau de intervenção humana e os trabalhos descritivos pós-migração (AUSTRALIA, 2012).

A estratégia de preservação digital, denominada migração, consiste-se na atualização do *hardware* e *software* obsoletos. O planejamento da migração deve considerar a utilização de formatos abertos de armazenamentos padronizados, bem como os metadados, índices, trilhas de auditoria e garantia de integridade dos objetos digitais (GÓMEZ DELGADO, 2009).

A emulação é a estratégia de preservação digital baseada na capacidade de continuamente se desenvolver *softwares* emuladores, os quais funcionam de forma idêntica com os programas utilizados no contexto da gênese dos objetos digitais. A preservação do fluxo de *bits* original permanece intacta, a qual poderá garantir autenticidade documental, uma vez que nenhuma alteração foi realizada no objeto digital original. Porém, a emulação torna-se inviável para grandes quantidades de documentos e para os mais variados formatos em que se encontram os objetos digitais (SWEDEN, 2005).

A emulação mantém o objeto digital intacto, em sua perspectiva original, sem alterar a sequência lógica dos b i t s . Essa estratégia preserva o conteúdo digital em seu estado original, bem como os aspectos tangíveis do seu nível conceitual, quais sejam: cor, *layout*, funcionalidade (AUSTRALIA, 2012).

O conceito essencial da emulação é o acesso confiável ou a execução do *software* e os dados originais em uma plataforma nova, atualizada, que emula a plataforma obsoleta (GRANGER, 2000).

De acordo com Rothenberg (1999), a emulação é a única forma de executar um determinado *software* original em um futuro distante. É uma estratégia amplamente utilizada, na qual um sistema de computador atual reproduz o comportamento de outro sistema obsoleto.

Assim, demonstrou-se, por meio de um modelo lógico de aplicação da tecnologia *blockchain,* um possível uso no contexto da Arquivologia para autenticação descentralizada automatizada, propiciando-se, nesse sentido, uma interação sólida no âmbito da confiança social institucional visto que a tecnologia *blockchain* se inicia com a produção dos DAD, isto é, desde o momento da gênese dos DAD até sua destinação final, a saber: eliminação ou preservação/acesso de longa duração. Portanto, pode-se verificar que o *blockchain* aplica-se nesse âmbito

supracitado, bem como em todas as etapas do ciclo de vida dos DAD e na autenticação em ambientes informacionais descentralizados. Ademais, a tecnologia *blockchain* pode gerar, em cada fase do ciclo de vida dos DAD, um resumo criptográfico *hash*, com o objetivo de prover uma trilha de auditoria imutável do ciclo de vida dos DAD, o qual viabiliza uma verificação da proveniência.

# 7 CONSIDERAÇÕES FINAIS

Na pós-modernidade, a Arquivologia poderá utilizar-se da tecnologia *blockchain* para apoiar a autenticação distribuída dos DAD, corroborando-se, assim, com a cadeia de custódia digital arquivística.

Demonstrou-se as relações, e, por conseguinte, as aplicações da tecnologia *blockchain* no contexto da autenticação distribuída para fins arquivísticos, em vista de que o protocolo do *blockchain* criptografa, envia e valida transações, que propiciam um registro cronológico inalterável de todas as operações realizadas. Nessa direção, as vantagens de aplicação na autenticação dos documentos arquivísticos digitais realizadas com o *blockchain* reside na validação de forma descentralizada, por um procedimento de validação consensual, quais sejam: *proof of work* - prova de trabalho, *proof of stake* - prova de participação.

Essas formas de validações consensuais são realizadas por meio de algoritmos que analisam os metadados dos registros criptografados, os quais verificam os *hashes* de toda cadeia de blocos até o bloco zero, ou seja, bloco gênese do documento. Sendo assim, torna-se exequível a preservação dos *hashes* das cadeias de registro ao longo do tempo, a qual poderá garantir a autenticação dos DAD ao longo do seu ciclo de vida. A auditoria é realizada por meio do *ledger,* dos registros em conjunto com algoritmo denominado árvore de *merkle,* que poderá verificar se o documento sofreu alterações, corrompimento e adulterações não autorizadas.

Verificou-se que, no Brasil, não existe um modelo específico para aplicação da tecnologia *blockchain* na arquivística. Porém, existem algumas iniciativas incipientes para uso do *blockchain* além do setor financeiro, em específico para criptomoedas. No cenário internacional foram detectados três modelos distintos, institucionalizados em uso, a saber: o modelo do Reino Unido, denominado de *Archangel,* modelo Canadense DIDC e modelo de Dubai para administração pública.

O modelo do Reino Unido, o *Archangel* dos três supracitados, é o que mais dispõe de requisitos necessários para aplicação na arquivística. Porém, sua aplicação restrinje-se apenas para os arquivos permanentes. Já o modelo Canadense contempla as aplicações dsitribuídas dos fluxos de dados e serviços. Por fim, o modelo de Dubai, o qual é utilizado de forma mais abrangente na governança e admisntração pública, que poderá contemplar os DAD.

Nessa perspectiva foi proposto um modelo de aplicação da tecnologia *blockchain*, no âmbito da Arquivologia ao longo do clico de vida dos documentos arquivísticos digitais. O modelo para autenticação descentralizada automatizada contempla o contexto da gênese do DAD, até sua destinação final.

Observa-se, assim, que os novos desafios dos sistemas distribuídos, que surgem nos ambientes informacionis digitais com uso das TIC, e dos aparatos institucionais, em especial a tecnologia *blockchain,* fazem um convite para discutir e debater seus impactos na Arquivologia, principalmente na autenticação automatizada e distribuída dos DAD.

# REFERÊNCIAS

ALMEIDA, M. B. Uma introdução ao XML, sua utilização na Internet e alguns conceitos complementares. **Ciência da Informação**, Brasília, v. 31, n. 2, p. 5-13, maio/ago. 2002. Disponível em: http://www.scielo.br/pdf/ci/v31n2/12903.pdf. Acesso em: 22 jun. 2022.

ALIAGA, Y. E. M.; LEAL, V. C.; LUCENA, A. U.; HENRIQUES, M. A. A. Avaliação de mecanismos de consenso para blockchains em busca de nova estratégia mais eficiente e segura. *In*: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18. 2018, Natal. **Anais ...** Porto Alegre: Sociedade Brasileira de Computação, 2018. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/4267. Acesso em: 03 nov. 2021.

ALIAGA, Y. E. M.; HENRIQUES, M. A. A. Uma comparação de mecanismos de consenso em blockchains. In: X ENCONTRO DE ALUNOS E DOCENTES DO DCA/FEEC /UNICAMP (EADCA), 2017, Campinas. **Anais...** Campinas: EADCA, 2017. Disponível em:https://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcax/trabalhos/artigo_20_Mecanismos_Consenso_Blockchains_Yoshitomi_Maehara_Prof_Marco_Aurelio.pdf. Acesso 03 nov. 2021.

ALVES, P. H.; LAIGNER, R.; NASSER, R.; ROBICHEZ, G.; LOPES, H.; KALINNOWSKI, M. Desmistificando Blockchain: Conceitos e Aplicações In: MACIEL, C.; VITERBO, J. **Computação e Sociedade**. Sociedade Brasileira de Computação, 2018. Disponível em: https://www.researchgate.net/publication/327060805.Desmistificando_Blockchain_Conceitos_e_Aplicacoes. Acesso em: 03 nov. 2021.

ALVES, V. B. A. Open archives: via verde ou via dourada?. **Ponto de Acesso**, Salvador, v.2 n.2, p.127-137, ago/set. 2008. Disponível em: http://www.portalseer.ufba.br/index.php/revistaici/article/view/1780/2172. Acesso em: 02 abr. 2022.

ARISTÓTELES. **Órganon**. 1. ed. Bauru: EDIPRO,2005.

ASSOCIATION FOR INFORMATION AND IMAGE MANAGEMENT (AIIM). 2015. Disponível em: http://www.aiim.org/. Acesso em: 20 dez. 2014.

ASSOCIATION FOR LIBRARY COLLECTIONS AND TECHNICAL SERVICES (ALCTS). **Definition of digital preservation**. 2007. Disponível em: http://www.ala.org/alcts/resources/preserv/defdigpres0408. Acesso em: 30 jun. 2022.

ARRUDA, G. O. A tecnologia a serviço da democracia: o processo eleitoral na era da informação. **Revista da Advocacia Pública Federal,** p. 139-149, 2017. article/view/2229/pdf. Acesso em: 06 nov. 2021.

AUSTRALIA, NATIONAL ARCHIVES OF AUSTRALIA (NAA). **An approach to the preservation of digital records**. 2012. Disponível em: http://www.naa.gov.au/Images/An-approach-Green-Paper_tcm16-47161.pdf. Acesso em 30 jun. 2022.

BARBOZA, E. S. **Autenticação multifatorial em hardware para o processo de assinatura digital da Nf-e**. Orientador: Manoel Eusébio de Lima. 2018. 154p. Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2018. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/32403/1/DISSERTA%c3%87%c3%83O%20Eudes%20da%20Silva%20Barboza.pdf. Acesso em: 04 out. 2021.

BARKATULLAH, J.; HANKE, T. Goldstrike 1: Cointerra's first-generation cryptocurrency mining processor for bitcoin. 2015. **IEEE micro 35**, n. 02. 68-76. Disponível em: https://www.computer.org/csdl/magazine/mi/2015 /02/mmi2015020068/13rRUwj7cs2. Acesso em: 03 set. 2021.

BARROS, A. J. P.; LEHFELD, N. A. S. **Projeto de pesquisa*:*** propostas metodológicas. Petrópolis: Vozes, 2002.

BASHIR, I. **Mastering Blockchain**. 1. ed. Packt Publishing Ltd. 2017.

BAUMAN, Z. **Identidade**: entrevista a Benedetto Vecchi. 1 ed. Rio de Janeiro: Jorge Zahar, 2005.

BAUMAN, Z. **Modernidade líquida**. 1. ed. Rio de Janeiro: Jorge Zahar, 2001.

BAUMAN. Z. Entrevista com Zigmunt Bauman. **Revista Tempo Social**, São Paulo, v. 16, n. 1, p. 321-325, jun. 2004. Disponível em: http://www.scielo.br/pdf/ts/v16n1/v16n1a15.pdf. Acesso em: 03 nov. 2021.

BAUMAN, Z. **Globalização**: as consequências humanas. 1 ed. Rio de Janeiro: Jorge Zahar, 1999.

BELLOTO, H. L. **Arquivos permanentes tratamento documental**. 4. ed. Rio de Janeiro: FGV, 2006.

BELLOTO, H. L. **Como fazer análise diplomática e análise tipológica de documento de arquivo**. São Paulo: Arquivo do Estado de São Paulo e Imprensa Oficial do Estado de São Paulo, 2002a. Disponível em: https://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf8.pdf. Acesso em: 12 nov. 2021.

BELLOTTO, H. L. **Arquivística**: objeto, princípios e rumos. São Paulo: Associação dos Arquivistas de São Paulo, 2002b.

BENTOV, I.; LEE, C.; MIZIRAHI, A.; ROSENFELD, M. Proof of activity: Extending bitcoin’s proof of work via proof of stake. 2014. **ACM SIGMETRICS Performance Evaluation Review**. 2014. V. 42, n. 03, p. 1-19, dez. 2014. Disponível em: https://eprint.iacr.org/2014/452.pdf. Acesso em: 05 nov. 2021.

BERGLJUNG, M. **Alfresco Content Management Interoperability System (CMIS)**. 1 ed. Birmingham: Packt Publishing Ltd. 2014.

BERNARDES, I. P. **Como avaliar documentos de arquivo**. São Paulo: Arquivo do Estado de São Paulo e Imprensa oficial do Estado de São Paulo, 1998. Disponível em: https://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf1.pdf. Acesso em: 20 jul. 2022.

BERNARDES, I. P.; DELATORRE, H. **Gestão documental aplicada**. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em:http://www.arquivoestado.sp.gov.br/saesp/GESTAO_DOCUMENTAL_APLICADA_Ieda.pdf. Acesso em: 01 jun. 2022.

BHAUMIK, S. **Alfresco 3 cookbook**. 1 ed. Birmingham: Packt Publishing Ltd. 2011.

BIRCH, D.; BROWN, R. G.; PARULAVA, S. Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis. **Journal of Payments Strategy & Systems**. 2016. V. 10, n. 211. Disponível em: https://www.finyear.com/Blockchain-A-legacy-of-transparency_a36758.html. Acesso 03 jan. 2022. 62

BRASIL. Ministério da Justiça. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **e-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos (SIGAD). 2011. Disponível em: http:// http://www.documentoseletronicos.arquivonacional.gov.br/media/e-arq-brasil-2011-corrigido.pdf. Acesso em: 10 maio 2022.

BRASIL. Casa Civil. Presidência da República. Instituto Nacional de Tecnologia da Informação (ITI). **Glossário**. 2021a. Disponível em: https://www.gov.br/iti/ptbr/centrais-de-conteudo/glossario. Acesso em: 03 nov. 2021.

BRASIL. Casa Civil. Presidência da República. Instituto Nacional de Tecnologia da Informação (ITI). **Instrução normativa ITI nº19, de 10 novembro de 2021**. 2021b. Disponível em: https://www.in.gov.br/web/dou/-/instrucao-normativa-iti-n-19-de-10-de-novembro-de-2021-359443482. Acesso em: 03 fev. 2021.

BRASIL. Casa Civil. Presidência da República. Subchefia para assuntos jurídicos. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 23 nov. 2021.

BRASIL. **Lei Federal 8.159**, de 08 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Presidência da república. Casa civil. Subchefia para assuntos jurídicos, Brasília, Distrito Federal, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em: 01 jun. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Glossário**. 2009. Disponível em:https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/2009_glossario_v5.pdf . Acesso em: 07 nov. 2021.

BRASIL. Ministério da Justiça. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Glossário**. 2010. Disponível em: http://www.documentoseletronicos.arquivonacional.gov.br /media/publicacoes/glossario/2010glossario_v5.1.pdf. Acesso em: 07 jul. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Arquivo Nacional (AN). Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Glossário de Documentos Arquivísticos Digitais**. 2020a. Disponível em: http://antigo.conarq.gov.br/images/ctde/ Glossário/glosctde_2020_08_07.pdf. Acesso em: 09 dez. 2021.

BRASIL. Ministério da Justiça e Segurança Pública. Arquivo Nacional (AN). Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Resolução nº 37, de 19 de Dezembro de 2012 – Diretrizes para presunção da autenticidade de documentos arquivísticos digitais**. 2012d. Disponível em: http://conarq.gov.br/images/publicacoes_textos/ conarq_presuncao_autenticidade_com pleta.pdf. Acesso em: 09 dez. 2021.

BRASIL. Ministério da Justiça. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Resolução nº39**, de 29 de abril de 2014. 2014b. Disponível em: http:// http://www.conarq.arquivonacional.gov.br/media/publicacoes/resol_conarq_39_repositorios.pdf. Acesso em: 15 jul. 2022.

BRASIL. Ministério da Justiça. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Resolução nº 43**, de 04 de setembro de 2015. Disponível em: https://www.gov.br/conarq/pt-br/centraisde-conteudo/publicacoes/conarq_diretrizes_rdc_arq_resolucao_43.pdf. Acesso em: 15 jun. 2022.

BRASIL. Ministério da Justiça. Arquivo Nacional. Conselho Nacional de Arquivos (CONARQ). **Norma Brasileira de Descrição Arquivística (NOBRADE)**. 2006b. disponível em: http://www.conarq.arquivonacional.gov.br/ Media/publicacoes/nobrade.pdf. Acessoem: 01 fev. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Arquivo Nacional (AN). **Dicionário Brasileiro de terminologia arquivística (DBTA)**. 2005. Disponível em: http://www.arquivonacional.gov.br/images/pdf/Dicion_Term_Arquiv.pdf. Acesso em: 21 nov. 2021.

BRASIL. **Lei Federal 12.682**, de 09 de julho de 2012. Dispõe sobre a elaboração e o arquivamento de documentos em meios magnéticos. Presidência da república. Casa civil. Subchefia para assuntos jurídicos, Brasília, Distrito Federal, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm. Acesso em: 10 jul. 2022.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para assuntos jurídicos. **Lei nº 14.063 de 23 setembro de 2020 - Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos.** (2020b) Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 15 dez. 2021.

BRASIL. República Federativa do Brasil. Tribunal de Contas da União (TCU). **Levantamento da tecnologia blockchain**. 2020c. Disponível em: https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/Blockchain_sumario_executivo.pdf. Acesso em: 20 jul. 2022.

BRODER, A. Z.; CARMEL, D.; HERSCOVICI, M.; SOFFER, A.; ZIEN, J. United States of America. United States Patent. **System, method and computer program product for performing unstructured information management and automatic text analysis, including a search operator functioning as a weighted and (WAND)**. 2006. Disponível em: http://www.google.com.ar/patents/US7146361. Acesso em: 20 jun 2022.

BUYYA, R.; YEO, C. S; VENUGOPAL, S.; BROBERG, J.; BRANDIC, I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems. Amsterdam: **Elsevier**, v. 25, n. 6, p. 599-616, Jun/2009. Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.144.8397&rep=rep1&type=pdf. Acesso em: 10 dez. 2021.

CAFÉ, L; MELO, B. A; BARBOZA, E. M. F; NUNES, E. M. A; MÁRDERO ARELLANO, M. A. Repositórios institucionais: nova estratégia para publicação científica na Rede. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO (INTERCOM), 26. 2003, Belo Horizonte. **Anais...** Belo Horizonte: INTERCOM, 2003. Disponível em: http://dspace.ibict.br/dmdocuments/ENDOCOM_CAFE.pdf. Acesso em: 20 jun 2022.

CALDERON, W. R.; CORNELSEN, J. M.; PAVEZI, N.; LOPES, M. A. O processo de gestão documental e da informação arqui-vística no ambiente universitário. **Ciência da Informação**. Brasília, v. 33, n. 3, p. 97-104, set/dez. 2004. Disponível em: http://revista.ibict.br/ciinf/index.php/ciinf/article/view/612/546. Acesso em: 01 jun. 2022.

CARUANA, D.; NEWTON, J.; FARMAN, M.; UZQUIANO, M. G.; ROAST, K. **Professional Alfresco**: pratical solutions for enterprise content management. 1 ed. Indianapolis: Wiley Publishing, 2010.

CERVO, A. L; BERVIAN, P. A; SILVA, R. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CESAR, D. M. F. **Blockchain aplicado à aviação**: uma revisão integrativa da literatura. Dissertação (Mestrado em Aeronáutica) – Escola de Aeronáutica - Instituto Superior de Educação e Ciências, Lisboa. 2019. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/35461/1/Denis%20Cesar%20Final.pdf. Acesso em: 04 set. 2021.

CHICARINO, V. R.; JESUS, E. F.; ALBUQUERQUE, C. V. N.; ROCHA, A. A. A. **Uso de blockchain para privacidade e segurança em internet das coisas**. Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, 2017. Disponível em: https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf. Acesso em: 22 dez. 2021.

COLLOMOSSE, J.; BUI, T.; BROWN, A.; SHERIDAN, J.; GREEN, A.; BELL, M.; FAWCETT, J.; HIGGINS, J.; THEREAUX, O. ARCHANGEL: Trusted Archives of Digital Public Documents. 2018. **ACM DocEng'18**. Disponível em: https://arxiv.org/pdf/1804.08342.pdf. Acesso em: 25 fev. 2022.

CONSELHO INTERNACIONAL DE ARQUIVOS (CIA). **Norma geral internacional de descrição arquivísitica (ISAD(G))**. 2001. Disponível em: http://www.conarq.arquivonacional.gov.br/Media/publicacoes/isad_g_2001.pdf. Acesso em: 01 jul. 2022.

COMISSÂO EUROPEIA (CE). MoReq2010. Dsiponível em: https://ec.europa.eu/info/index_pt. Acesso em: 20 jun. 2022.

CONWAY, P. **Preservation in the digital world.** Council on Library and Information Resources (CLIR). 1996. Disponível em: http://www.clir.org/pubs/reports/reports/conway2/index.html. Acesso em 05 jun. 2022.

COOK, T. A ciência arquivística e o pós modernismo: novas formulações para um conceito antigo. **InCID: Revista de Ciência da Informação e Documentação**., Ribeirão Preto, v. 3, n. 2, p. 3-27, jul./dez. 2012. Disponível em: https://www.revistas.usp.br/incid/article/view/48651. Acesso em: 03 jan. 2022.

CROW, R. The case for institutional repositories: a sparc position paper. **Scholarly Publishing & Academic Resources Coalition**. Washington, DC. 2002. Disponível em: http://www.arl.org/sparc/bm~doc/ir_final_release_102.pdf. Acesso em: 10 jun. 2022.

DAHLBERG, I. Teoria da classificação, ontem e hoje. In: Conferência Brasileira de classificação Bibliográfica, 1972, Rio de Janeiro. **Anais...** Brasília: IBICT/ABDF, 1979. v.1, p. 352-370. Disponível em: http://www.conexaorio.com/biti/dahlbergteoria/dahlberg_teoria.htm>. Acesso em: 19 jun. 2022.

DANNEN, C. **Introducing Ethereum and Solidity**. Foundations of Cryptocurrency and blockchain Programming for Beggniners. Apress. 2017.

DAY, M. Metadata for digital preservation: an update. **ARIADNE**, Bath, p. 1-11, dez. 1999. Disponível em: http://www.ariadne.ac.uk/issue22/metadata. Acesso em: 04 jul. 2022.

DEMO, P. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2000.

DLM FORUM FOUNDATION. **MoReq**: Model Requirements for the Management of Electronic Records. Luxembourg: European Communities, 2002. Disponivel em: https://moreq.info/. Acesso em: 24 jun. 2022.

DUBLIN CORE METADATA INITIATIVE (DCMI). 2015. Disponível em: http://dublincore.org/. Acesso em: 20 jul. 2022.

DURANTI, L. From digital diplomatics to digital records forensics. **Archivaria**, n. 68, p. 39–66, 2009. Disponível em: https://archivaria.ca/index.php/archivaria /article/view/13229/14548. Acesso em: 22 maio 2022.

DURANTI, L. **Merging Concepts of Forensic Disciplines for the Control of Digital**. 2012. Disponível em: http://www.interpares.org/display_file.cfm? doc=ip3_canada_dissemination_jar_duranti_asb-1-2_2012.pdf. Acesso em: 15 dez. 2021.

DURANTI, L. Structural and formal analysis: the contribution of diplomatics to archival appraisal in the digital environment. In: **The Future of Archives and Recordkeeping**: A Reader. London: Facet, 2010. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_dissemination_bc_duranti_hill-ed_2010.pdf. Acesso em: 23 jan. 2022.

DURANTI, L. MACNEIL, M. The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project. **Archivaria**. 1996. Disponível em: https://archivaria.ca/index.php/archivaria/ article/view/12153/13158. Acesso em: 15 dez. 2021.

DURANTI, L.; ROGERS. C. Trust in Records and Data Online. *I***ntegrity in Government through Records Management** *: Essays in Honour of Anne Thurston*, 2 ed. 2016. Disponível em: http://www.recordsinthecloud.org/ritc/research. Acesso em: 02 jun. 2022.

DURANTI, L.; THIBODEAU, K. The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES. **Archival Science**, n. 6, v.1 p. 13-68, 2006. Disponível em: https://www.researchgate.net/publication/225115957_The_Concept_of_Record_in_Interactive_Experiential_and_Dynamic_Environments_the_View_of_InterPARES. Acesso em: 15 dez. 2021.

DURANTI. L. The Long-Term Preservation of Accurate and Authentic Digital Data: The InterPARES Project. **Data Science Journal**, n. 4, p. 106-118, out. 2005.

DWORK, C.; NAOR, M. Pricing via processing or combatting junk mail. **CRYPTO** .1992. Advances in Cryptology - CRYPTO' 92, v. 740, p. 139–147, 1992.

FERREIRA, C. A. S. **Preservação da informação digital**: uma perspectiva orientada para as bibliotecas. 2011. Dissertação (Mestrado em Informação, Comunicação e Novas Media) – Universidade de Coimbra. Coimbra, 2011. Disponível em: https://estudogeral.sib.uc.pt/handle/10316/15001 . Acesso em: 15 jul. 2022.

FERREIRA, M. **Introdução à preservação digital:** conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/ 1822/5820/1/livro.pdf. Acesso em: 15 jun. 2022.

FONSECA, M. O. Informação, arquivos e instituições arquivísticas. **Arquivo e administração**, Rio de Janeiro, v.1, n.1, p. 33-44, jan/jun. 1998. Disponível em: http://www.brapci.ufpr.br/download.php?dd0=11750. Acesso em: 01 jul. 2022.

FROHMANN, B. O caráter social, material e público da informação. In: FUJITA, M.S.L.; MARTELETO, R.M.; LARA, M.L.G. **A dimensão epistemológica da Ciência da Informação e suas interfaces técnicas, políticas e institucionais nos processos de produção, acesso e disseminação da informação**. São Paulo: Cultura Acadêmica, 2008.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002. p. 176.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

GÓMEZ DELGADO, A. La conservación a largo plazo de documentos electrónicos: normativa ISO y esfuerzos nacionales e internacioanles, **Arch-e revista Andaluza de archivos,** Andaluzia, n.01, p. 1-25, maio. 2009. Disponível em: http://www.juntadeandalucia.es/culturaydeporte/archivos_html/sites/default/contenidos/general/revista/numeros/Numero_1/galeria/01-02_Alejandro_Delgado_Gxmez.pdf. Acesso em: 30 jun. 2022.

GRANGER, S. Emulation as a digital preservation strategy. **D-Lib Magazine**, v.06, n. 10, p. 1-11, out. 2000. Disponível em: http://www.dlib.org/dlib/october00/granger/ 10granger.html. Acesso em: 30 jun. 2022.

HEDSTROM, M. Digital preservation: a time bomb for digital libraries. 1998. **Kluwer Academic Publisher**, Netherlands, p. 189-202. Disponível em: http://deepblue.lib.umich.edu/bitstream/handle/2027.42/42573/?sequence=1. Acesso em: 30 jun. 2022.

HEDSTROM, M. Digital preservation: problems and prospects. **Digital Library Network (DLnet)**. n. 20, p. 1-12, 200.1 Disponível em: http://www.dl.slis.tsukuba.ac.jp/DLjournal/No_20/1-hedstrom/1-hedstrom.html. Acesso: 28 nov. 2021.

HELFIN, J.; HENDLER, J. Semantic Interoperability on the web. **Anais…** Extreme Markup Languages 2000, 2000. p. 111-120. Disponível em: http://www.cse.lehigh.edu/~heflin/pubs/extreme2000.pdf. Acesso em: 03 jun. 2022.

INDOLFO, A. C. Gestão de documentos: uma renovação epistemológica no universo da arquivologia. **Arquivística.net**, Rio de Janeiro, v. 3, n. 2, p. 28-60, jul/dez. 2007. Disponível em: http://www.arquivistica.net/ojs/viewarticle.php?id=155&l ayout=abstract. Acesso em: 30 jun. 2022.

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA (IBICT), 2014. Disponível em: http://dspace.ibict.br/. Acesso em: 02 Jul. 2022.

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). Commite on Electronic Records (CER). **Guide for managing electronic records from an archival perspective**. 1997. Disponível em: http://www.ica.org/10824/studies-and-case-studies/ica-studyn8-guide-for-managing-electronic-records-from-an-archival-perspective.html. Acesso em 05 jul. 2022.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). **InterPARES Project**. Disponível em: http://www.interpares.org/. Acesso em: 24 jul 2022

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS 2 (InterPARES 2). **Diretrizes do produtor**: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. 2010. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/diretrizes_produtor_digital.pdf. Acesso: 29 abr. 2022.

JENKINS, T. **Enterprise Content Management**: what you need to know. 1 ed. Waterloo: Open Text Corporation, 2004.

JUELS. A.; JAKOBSSON. Proofs of works and bread pudding protocols. Springer **Science Bussines Media Dordrecht**, Boston, MA. v.23, 258–272, 1999. Disponível em: https://link.springer.com/content/pdf/10.1007%2F978-0-387-35568-9_18.pdf. Acesso em: 05 jan. 2021.

KAMPFFMEYER, U. Enterprise Content Management. **Anais...** Köln: Digital Management Solutions EXPO (DMS), 2006. p. 1-82. Disponível em: http://www.projectconsult.net/files/ECM_Enterprise_Content_Management_ Kampffmeyer_2006.pdf. Acesso em: 05 jun. 2022.

KIRCHHOFF, A. J. Digital preservation: challenges and implementation. **Learned Publishing**, Portico, v.21, n.04, p. 285-294, out. 2008. Disponível em: http://www.portico.org/digital-preservation/wp-ontent/uploads/2010/01/ALPSPFINAL-Kirchhoff.pdf. Acesso em: 30 jun. 2022.

KOBAYASHI, L. O. M. **Abordagem criptográfica para integridade e autenticidade em imagens médicas**. Orientador: Sergio Shiguemi Furuie. 2007. 136 p. Tese (Doutorado Engenharia de telecomunicações e controle). Escola politécnica, Universidade de São Paulo, São Paulo, 2007. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-14012008-122458/publico/Kobayashi_Tese_Revisado.pdf. Acesso em: 04 dez. 2021.

KURAMOTO, H. Informação científica: proposta de um novo modelo para o Brasil. **Ciência da Informação**, Brasília, v.35, n.2, p.91-102, maio/ago. 2006. Disponível em: http://revista.ibict.br/cienciadainformacao/index.php/ciinf/article/view/831/677. Acesso em: 21 jun. 2022.

KURAMOTO, H. **Iniciativas do IBICT para implementação tecnológicas para gestão e acesso à informação**. 2007. Disponível em: http://cdij.pgr.mpf.gov.br/noticias/palestra_cbbd/T3_A1.pdf. Acesso em: 10 jun. 2022.

LANDIM, F. L. P.; LIRA, R. C. M.; LOURINHO, L. A.; SANTOS, Z. M. S. A. Uma reflexão sobre as abordagens em pesquisa com ênfase na integração qualitativo-quantitativa. **RBPS**. Fortaleza. 2006, v.19 n 1. p. 53-58. Disponível em: https://periodicos.unifor.br/RBPS/article/view/961/2123. Acesso em: 15 dez. 2021.

LAVOIE, B. Meeting challenges of digital preservation: the OAIS reference model. **Online Computer Library Center Research (OCLCR)**. Dublin, n.243:26-30, p.1-4, jan/fev. 2000. Disponível em: http://www.oclc.org/research/publications/library/2000/lavoie-oais.html>. Acesso em: 06 jun. 2022.

LEE, K.H.; SLATERRY, O.; LU, R.; TANG, X.; MCCRARY, V. The state of the art and practice in digital preservation. **Journal of research of the National Institute of Standards and Technology**, Gaithesburg, v. 107, n.1, p. 93-106, jan/fev. 2002. Dsiponível em: http://nvlpubs.nist.gov/nistpubs/jres/107/1/j71lee.pdf. Acesso em: 10 jul. 2022.

LEMIEUX, V. L.; HOFMAN, D.; BATISTA, D.; JOO, A. **Blockchain Technology and Recordkeeping**. Project Underwritten by: ARMA Canada Region. 2019. Disponível em: http://armaedfoundation.org/research-program_menu/research-reports/. Acesso em: 12 jul. 2022.

LOPES, A. D. M. **VoIP em Redes Peer-to-peer**. 2014. 110 f. Dissertação (Mestrado em engenharia de comunicações) – Universidade do Minho, Braga. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/35186/1/Disserta%C3%A7%C3%A3o_Ant%C3%B3nio%20D.%20da%20M.%20Lopes_2014.pdf. Acesso em: nov. 2019.

LYNCH, C. A. **Institutional repositories**: essential infrastructure for scholarship in the digital age. Association of Research Libraries, Washington, DC. n.226, p. 1-7, fev. 2003. Disponível em: http://www.arl.org/resources/pubs/br/br226/br226ir.shtml>. Acesso em: 11 jun. 2022.

MACHADO, J. M. C. R. **Recuperação de informações em ambientes semiestruturados**. 2008. Dissertação (Mestrado em Engenharia Informática e de Computadores) Universidade Técnica de Lisboa – Instituto Superior Técnico, Lisboa, 2008. Disponível em: http://dited.bn.pt/31611/2598/3144.pdf. Acesso em: 20 maio de 2022.

MACNEIL, H. “Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records.” **Archivaria**. p. 52-78. Jan. 2000. Disponível em: https://archivaria.ca/index.php/archivaria/article/view/12765/13955. Acesso em: 14 dez. 2021.

MACNEIL, H.; GILLILAND-SWETLAND, A. **Authenticity Task Force Report**. In: DURANTI, L. The Long-Term Preservation of Authentic Electronic Records: Finding of the InterPARES Project. San Miniato (Italy): Archilab, 2005. Disponível em: http://www.interpares.org/book/interpares_book_d_part1.pdf. Acesso em 13 dez. 2021.

MAGALHÂES, L. E. R. **O trabalho científico**: da pesquisa à monografia. Curitiba: FESP, 2007.

MARCACINI, A. T. R. **O documento eletrônico como meio de prova**. 2002 Disponível em: http://augustomarcacini. cjb. net/textos/docelet2. html. Acesso em: 10 dez. 2021.

MARCONDES, C. H; SAYÃO, L. Repositórios institucionais e livre acesso. In: SAYÃO, L. (Org). *et al*. **Implantação e gestão de repositórios institucionais**: políticas, memória, livre acesso e preservação. 1.ed. Salvador: EDUFBA, 2009. Disponível em: http://repositorio.ufba.br/ri/bitstream/ufba/473/3/implantacao_repositorio_web.pdf. Acesso em: 04 maio 2022.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas. 2003. 312 p.

MARCONI, M. A.; LAKATOS, E. M. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 7. ed. São Paulo: Atlas. 2008. 296 p.

MARTINI, R. **Criptografia e cidadania digital**. Rio de Janeiro: Editora Ciência Moderna Ltda. 2001.

MARTINS, G. A.; LINTZ, A. **Guia para a Elaboração de Monografias e Trabalhos de Conclusão de Curso.** São Paulo: Atlas, 2000.

MENKE, F. Assinatura eletrônica no Direito Brasileiro. **Revista dos Tribunais**: São Paulo, 2005.

MONTEIRO, E. S.; MIGNONI, E. M. **Certificação Digital**: Conceitos e Práticas, Rio de Janeiro: Brasport, 2007.

MONTEIRO, S. D.; GIRALDES, M. J. C. Aspectos lógicos - filosóficos da

organização do conhecimento na esfera da ciência da informação. **Inf. & Soc: Est.**, João Pessoa, v.18, n.3, p. 13-27, set/dez. 2008. Disponível em: http://www.ies.ufpb.br/ojs/index.php/ies/article/view/1775/2269. Acesso em: 19 jun. 2022.

MORENO, N. A. Gestão documental ou gestão de documentos: trajetória histórica. In: BARTALO, L.; MORENO. N. A. (Orgs). **Gestão em arquivologia abordagens múltiplas**. Londrina: EDUEL, 2008.

NATIONAL INFORMATION STANDARDS ORGANIZATION (NISO). Information Standards Quarterly (ISQ). **Special Issue:** digital preservation. 2010. Disponível em:http://www.niso.org/apps/group_public/download.php/4299/isqv22no2.pdf. Acesso em: 30 jun. 2022.

NATIONAL INFORMATION STANDARDS ORGANIZATION (NISO). **Understanding metadata**. 2004. Disponível em: http://www.niso.org/publications/press/UnderstandingMetadata.pdf. Acesso em: 30 jun. 2022.

MULLER, S.; FEITH, J.; FRUIN, R. **Manual de arranjo e descrição de arquivos**. Trad. Manoel Adolpho Wanderley. 2. ed. Rio de Janeiro: Arquivo Nacional, (1898) 1973.

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 01 nov. 2019.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. **Bitcoin and Cryptocurrency Technologies**. 2016. Princeton University Press. **Network (DLnet)**. n. 20, p. 1-12, 2001. Disponível em: https://www.uio.no/studier/emner/matnat/ifi/IN5420/v18/timeplan/resources/bitcoin-and-cryptocurrency-techniques.pdf. Acesso em: 01 nov. 2019

NEW ZEALAND. Archives New Zealand. Te Rua Mahara o te Kāwanatanga. **Digital preservation strategy**. 2011. Disponível em: http://archives.govt.nz/advice/government-digital-archive-programme/digitalpreservation-strategy/digital-preservation-strat. Acesso em: 05 jun. 2022.

NUNES, N. S. **Public Key Infrastructure** (PKI), 2007. Disponível em: http://www.gta.ufrj.br/grad/07_2/delio/index.html. Acesso em 20 nov. 2021.

PAES, Marilena Leite. **Arquivo teoria e prática**. 3.ed. Rio de Janeiro: Editora FGV, 2004. 228 p.

PERSET, K. **The economic and social role of Internet intermediaries**. 2010. Disponível em: https://www.oecd.org/sti/ieconomy/44949023.pdf. Acesso em: 05 jun. 2021.

PETERMAN, N. **Threat modeling of Enterprise Content Management Systems**. 2009. Dissertação (Ciência da Informação) – Universidade de Vrije, Amsterdam, Holanda, 2009. Disponível em: http://www.iids.org/aigaion/indexempty.php?page=

actionattachment&action=open&pub_id=296&location=ThesisNickPeterman_1543490_V1.pdf-234384ae81a690392cbcb212b03788e1.pdf>. Acesso em: 15 jun. 2022.

PROVOOST, L. **A SOA-Enabled Enterprise Content Management System.** 2006. Tese (Ciência da Computação) – Universidade de Utrecht, Holanda, 2006. Disponível em: http://foswiki.cs.uu.nl/foswiki/pub/Students/LeeProvoost/thesis_public.pdf>. Acesso em: 05 jun. 2022.

RABELLO, R. Informação materializada e institucionalizada como documento: caminhos e articulações conceituais. **Brazilian Journal of Information Studies: Research Trends**. 2019. P. 5-25. v.13, n.02. Disponível em: https://doi.org/10.36311/1981-1640.2019.v13n2.02.p5. Acesso em: 05 jan. 2022.

RAMALHO, F. R. **Análise conceptual do domínio Enterprise Content Management**. 2010. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Engenharia da Universidade do Porto, Porto, 2010. Disponível em: http://repositorio-aberto.up.pt/bitstream/10216/60474/1/000144996.pdf. Acesso em 05 jun. 2022.

RESENDE. A. D. **Certificação Digital.** 2009. Disponível em: http://www.unigran.br/revistas/juridica/ed_anteriores/22/artigos/artigo09.pdf. Acesso em: 05 dez. 2021.

ROTHENBERG, J. **Avoiding technological quicksand**: finding a viable technical foundation for digital preservation. 1999. Disponível em: http://www.clir.org/pubs/reports/rothenberg/pub77.pdf. Acesso em: 30 jun. 2022.

ROUSSEAU, J. Y.; COUTURE, C. **Os Fundamentos da disciplina arquivística**. 1.ed. Lisboa. Dom Quixote. 1998.

SAMPIERI, R. H. **Metodologia de la Investigación**. México: McGraw-Hill, 1991.

SANCHEZ, G. B. S.; MELERO, M. R. **La denominación y El contenido de los repositórios institucionales en acceso abierto**: base teórica para la ruta verde. 2006. Disponível em: http://digital.csic.es/bitstream/10261/1487/1/OA2rm.pdf. Acesso em: 12 jun. 2022.

SANTAREM SEGUNDO, J. E; CAMARGO, L. S. A; SHINTAKU, M; VIDOTI, S. A. B.G. Integração do framework manakin com a plataforma DSpace para múltiplas apresentações visuais de informações nos repositórios digitais. **Revista digital de Biblioteconomia e Ciência da Informação**, Campinas, v.07, n.02, p. 10-26, jan/jun. 2010.

SCHELLENBERG, T. R. **Arquivos modernos**: princípios e técnicas. 6. ed. Rio de Janeiro: FGV, 2006. 388 p.

SEVERINO, Antônio Joaquim**. Metodologia do Trabalho Científico**. 24ed. São Paulo: Cortez Editora, 2016.

SHARIFF, M.; SHAH, S.; AVATANI, R, R.; PRAJAPATI, J.; PAL, V.; CHOUDHARY, V.; BHANDARI, A.; MAJMUDAR, P. **Alfresco 4 Enterprise Content Management Implementation**. 3 ed. Birmingham: Packt Publishing Ltd. 2013

SHEGDA, K, M.; GILBERT, M. R. Key Issues for Enterprise Content Management in 2009. **Gartner**, Stamford, p. 2-7, mar. 2009. Disponível em: https://www.gartner.com/doc/917113/key-issues-enterprise-content-management. Acesso em: 05 jul. 2022.

SILVA, A. M. Gestão da informação arquivística e suas repercussões na produção do conhecimento científico. In: SEMINÁRIO INTERNACIONAL DE ARQUIVOS DE TRADIÇÃO IBÉRICA, 2000, Rio de Janeiro. **ANAIS...** Rio de Janeiro: Arquivo Nacional, 2000. Disponível em: http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?sid=74. Acesso em: 25 nov. 2021.

SILVA, A. M. O impacto do uso generalizado das TIC (Tecnologias de Informação e Comunicação) no conceito de ensaio analítico-crítico (II). **Prisma.COM**. Porto, n.18, p.1-25, 2011. Disponível em: http://revistas.ua.pt/index.php/prismacom/article/view/2229/pdf. Acesso em: 06 dez. 2021.

SOCIETY OF AMERICAN ARCHIVIST (SAA). **Encoded archival description (EAD)tag library version EAD3**. 2015. Disponível em: http://www2.archivists.org/sites/all/files/TagLibrary-VersionEAD3.pdf. Acesso em: 20 jul. 2022.

STANDARDS AUSTRALIA INTERNATIONAL. **Australian standard AS ISO 15489:2017 - Records management. Part 1**: general [and] Part 2: guidelines. Sidney, 2002. Disponível em: https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/it-021/as--iso--15489-dot-1-colon-2017. Acesso em: 24 jul 2022.

SUICHES, B. **Why blockchain must die in 2016**. 2015. Disponível em: https://www.linkedin.com/pulse/why-blockchain-must-die-2016-bart-suichies. Acesso em: 18 jan. 2022.

SWAN, M. **Blockchain**: blueprint for a new economy. Boston: O'Reilly Media, 2015.

SZABO, N. **Bitcoin, what took ye so long?** 2011. Disponível em: http://unenumerated.blogspot.com.br/2011/05/bitcoin-what-took-ye-so-long.html. Acesso em: 20 dez. 2020.

SWEDEN. National Archives of Sweden (NAS). **Digital preservation in archives: Overview of current research and practices**. 2005. Disponível em: http://www.ltu.se/cms_fs/1.83844!/file/Digital%20Preservation%20in%20Archives.pdf. Acesso em: 30 jun. 2022.

TANENBAUM, A. S. **Computer network.** 4 ed. Campus. Amsterdam – Holanda, 2003.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution**. New York: Penguin Random House LLC, 2017.

TASK FORCE ON THE ARCHIVING OF DIGITAL INFORMATION. **Preserving digital information**: report of the task force on archiving of digital information. Washington: Commission on Preservation and Access, 1996. Disponível em: http://www.clir.org/pubs/reports/pub63watersgarrett.pdf/. Acesso em: 07 jun. 2022.

THOMAZ, K. P. A preservação digital e o modelo de referência: open archival information system. **DataGramaZero**, Revista de Ciência da Informação, v. 5, n. 1, fev, 2004. Disponível em: http://www.dgz.org.br/fev04/Art_01.htm. Acesso em: 15 jun. 2022.

THOMAZ, K. P.; SOARES, A. J. A Preservação digital e o modelo de referência Open Archival Information System (OAIS). **DataGramaZero**, v. 5, n. 1, fev. 2004. Disponível em: http://www.dgz.org.br/fev04/Art_01.htm. Acesso em: 07 jun. 2022.

TRAIN, S. **Como os Certificados Digitais estão Facilitando a Vida das Pessoas**. Identidade Digital. 2 ed. Revista e ampliada – São Paulo, 2007.

UNITED ARAB EMIRATES (UAE). Dubai Government. **Dubai Future Fondation** (DFF). Disponível em: https://www.dubaifuture.ae/. Acesso em: 20 maio 2022.

UNITED STATES OF AMERICA (USA). Department of Defense (DoD). **Design criteria standard for electronic records management software applications**: DOD 5015.2-STD. Washington, 2002. Disponível em: http://jitc.fhu.disa.mil/projects/rma/downloads/p50152s2.pdf. Acesso em: 24 jun. 2022.

UNITED STATES OF AMERICA (USA). Law 44 United States code (USC) records management by the archivist of United States and by the administrator of general services. **Chapter 29 Public printing and documents**. 1968. Disponível em: http://www.law.cornell.edu/uscode/text/44/2901. Acesso em: 01 jul. 2022.

UNITED STATES OF AMERICA (USA). National Aeronautics and Space Administration (NASA) Headquarters. Consultative Committee for Space Data Systems (CCSDS). Recommendation for Space Data System Practices. **Reference model for an Open Archival Information System (OAIS)**. 2012. Disponível em: http://public.ccsds.org/publications/archive/650x0m2.pdf. Acesso em: 05 jul. 2022.

UNITED STATES OF AMERICA (USA). Library of Congress. Preservation Metadata (PREMIS) Maintenance Activity. **PREMIS data dictionary for preservation metadata**. 2015. Disponível em:http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf. Acesso em: 05 jul. 2022.

UNITED KINGDOM. **e-Government Metadata Standard** (e-GMS) v. 3.0, 2004. Disponivel em: https://cdn.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf . Acesso em: 24 jun. 2022.

VIEIRA, D. F. A. **Definição de uma Estratégia para a Gestão de Conteúdos: o Caso de Estudo da Área de Consultoria da Unidade de Engenharia de Sistemas de Produção do INESC TEC**. 2012. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Engenharia da Universidade do Porto, Porto, 2012. Disponível em: http://repositorioaberto.up.pt/bitstream/10216/68431/1/000154601.pdf. Acesso em: 10 jun. 2022.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE International Congress on Big Data (BigData Congress), 2017, Honolulu HI. **Anais…** Honolulu HI: IEEE BigData congress, 2017. Disponível em: https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends. Acesso em: 04 nov. 2021

WATERS, D.; GARRET, J. Task force on archiving of digital information. **Preserving digital Information**. 1996. Disponível em: http://www.clir.org/pubs/reports/pub63watersgarrett.pdf. Acesso em: 30 jun. 2022.

WEITZEL, S. R. O papel dos repositórios institucionais e temáticos na estrutura da produção cientifica. **Em Questão**. Porto Alegre, v.12, n.1, p.51-71, jan/jun. 2006. Disponível em: http://seer.ufrgs.br/index.php/EmQuestao/article/view/19/7. Acesso em: 30 maio 2022.