UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
BACHARELADO EM ARQUIVOLOGIA

JOHN ANDERSON FERNANDES DOS SANTOS

SEGURANÇA DA INFORMAÇÃO E PRESERVAÇÃO EM DOCUMENTOS ARQUIVÍSITICOS DIGITAIS: AS CADEIAS DE REGISTRO ATRAVÉS DO BLOCKCHAIN.

JOÃO PESSOA
2024

JOHN ANDERSON FERNANDES DOS SANTOS

SEGURANÇA DA INFORMAÇÃO E PRESERVAÇÃO EM DOCUMENTOS ARQUIVÍSITICOS DIGITAIS: AS CADEIAS DE REGISTRO ATRAVÉS DO BLOCKCHAIN.

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharela em Arquivologia pela Universidade Federal da Paraíba.

Orientador: Prof. Dr. Luiz Eduardo Ferreira da Silva.

JOÃO PESSOA
2024

Catalogação na publicação
Seção de Catalogação e Classificação

S237s Santos, John Anderson Fernandes dos.
Segurança da informação e preservação em documentos arquivísticos digitais: as cadeias de registro através do blockhain / John Anderson Fernandes dos Santos. - João Pessoa, 2024.
37 f. : il.

Orientação: Luiz Eduardo Ferreira da Silva.
TCC (Graduação) - UFPB/CCSA.

1. Segurança da informação. 2. Plataforma blockchain. 3. Preservação digital. 4. Documentos arquivisticos digitais. 5. Arquivologia. I. Silva, Luiz Eduardo Ferreira da. II. Título.

UFPB/CCSA CDU 930.25

Elaborado por ANA CLAUDIA LOPES DE ALMEIDA - CRB-15/108

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DA PARAÍBA

FOLHA Nº 6 / 2024 - CCSA - CARQ (11.01.13.08)

Nº do Protocolo: 23074.042686/2024-90

João Pessoa-PB, 27 de Maio de 2024

FOLHA DE APROVAÇÃO DE TRABALHO DE CONCLUSÃO DE CURSO

JOHN ANDERSON FERNANDES DOS SANTOS

AS CADEIAS DE REGISTRO ATRAVÉS DO BLOCKCHAIN NA ARQUIVOLOGIA:

SEGURANÇA DA INFORMAÇÃO, PRESERVAÇÃO DIGITAL EM DOCUMENTOS DE ARQUIVOS

Monografia apresentada ao Curso de graduação em Arquivologia da Universidade Federal da Paraíba, em cumprimento às exigências para a obtenção do grau de bacharel em Arquivologia.

Data de aprovação: 13 de maio de 2024

Resultado: APROVADO

BANCA EXAMINADORA:

Assinam eletronicamente esse documento os membros da banca examinadora, a saber: Prof. Dr. Luiz Eduardo Ferreira da Silva (orientador) e Profa. Dra. Claudialyne da Silva Araújo (membro). A banca teve como membro externo a Profa. Ma. Gerlane Farias Alves (UEPB).

(Assinado digitalmente em 27/05/2024 15:40)
CLAUDIALYNE DA SILVA ARAUJO
PROFESSOR DO MAGISTERIO SUPERIOR
Matrícula: 1726643

(Assinado digitalmente em 27/05/2024 16:09)
LUIZ EDUARDO FERREIRA DA SILVA
PROFESSOR DO MAGISTERIO SUPERIOR
Matrícula: 1031494

Para verificar a autenticidade deste documento entre em **https://sipac.ufpb.br/documentos/** informando seu número: **6**, ano: **2024**, documento(espécie): **FOLHA**, data de emissão: **27/05/2024** e o código de verificação: **a8f3ec721b**

JOHN ANDERSON FERNANDES DOS SANTOS

SEGURANÇA DA INFORMAÇÃO E PRESERVAÇÃO EM DOCUMENTOS ARQUIVÍSITICOS DIGITAIS: AS CADEIAS DE REGISTRO ATRAVÉS DO BLOCKCHAIN.

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharela em Arquivologia pela Universidade Federal da Paraíba.

Aprovada em __/__/_____.

BANCA EXAMINADORA

_____
Prof. Luiz Eduardo Ferreira da Silva (Orientador)
Universidade Federal da Paraíba (UFPB)

_____
Profa. Dra. Claudialyne da Silva Araújo
Universidade Federal da Paraíba (UFPB)

_____
Prof. Ma. Gerlane Farias Alves
Universidade Federal da Paraíba (UFPB)

AGRADECIMENTOS

À coordenação do curso de Arquivologia da Universidade Federal da Paraíba, pelo belíssimo trabalho e apoio aos discentes.

Ao professor Luiz Eduardo, pelas leituras sugeridas ao longo dessa orientação e pela dedicação demonstrada.

Aos meus pais e minha irmã, pela compreensão da minha ausência nas reuniões familiares durante este período de estudos.

Aos meus colegas de classe, pelos momentos de amizade compartilhados ao longo do curso.

A todos vocês, minha sincera gratidão!

RESUMO

Este estudo visa entender o papel das tecnologias de informação na Arquivologia, focando na segurança da informação e na tecnologia blockchain para garantir a autenticidade, integridade e durabilidade dos documentos digitais. Sendo assim, objetivamente busca identificar como as Cadeias de Registro através do blockchain podem oferecer soluções para a segurança da informação e a preservação digital. A metodologia adotada é qualitativa, envolvendo uma revisão sistemática da literatura científica. Através desta análise, serão obtidos insights sobre as vantagens e desafios da implementação das Cadeias de Registro através do blockchain na Arquivologia. Por fim, esse estudo traz uma possibilidade de pensar a tecnologia blockchain, segurança da informação e a preservação digital em documentos arquivísticos.

Palavras-Chave: Segurança da Informação; Plataforma Blockchain; Preservação Digital; Documentos Arquivístivos Digitais; Arquivologia.

ABSTRACT

This study aims to understand the role of information technologies in Archival Science, focusing on information security and blockchain technology to ensure the authenticity, integrity, and durability of digital documents. Therefore, it objectively seeks to identify how blockchain-based Registry Chains can offer solutions for information security and digital preservation. The methodology adopted is qualitative, involving a systematic review of scientific literature. Through this analysis, insights will be gained into the advantages and challenges of implementing blockchain-based Registry Chains in Archival Science. Ultimately, this study presents a possibility of considering blockchain technology, information security, and digital preservation in archival documents.

KEYWORDS: Information Security; Platform Blockchain; Digital Preservation; Archival Documents Digital; Archival Science.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

DAD Documentos Arquivísticos Digitais
POW Proof of Work – Prova de Trabalho
POS Proof of Stake – Prova de Participação

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, observou-se um crescimento notável no uso de documentos digitais no Brasil. Essa tendência reflete o crescente de interesse tanto de instituições públicas, quanto privadas em aproveitar os benefícios da tecnologia para otimizar processos e reduzir atrasos associados às demandas documentais. No entanto, mesmo com os avanços proporcionados pelos documentos digitais arquivísticos, um desafio persistente que surge é a garantia da segurança das informações, a preservação digital e um repositório com uma metodologia arquivística confiável.

Nesse víeis, a guarda e preservação de documentos arquivísticos digitais encaminhou-se por sistema centralizado, entidade central (que tem controle de registros), na qual muitas das vezes sujeitos a problemas de transparência, autenticidade e manipulações. Porém, uma mudança significativa tem ocorrido à medida que a tecnologia avança, impulsionando a adoção de sistema descentralizado, ou seja, o blockchain, dando mais confiabilidade aos documentos digitais.

A tecnologia blockchain é uma estrutura de dados que registra transações em uma rede de computadores, com blocos vinculados por criptografia. Cada bloco contém informações sobre a transação, como remetente, destinatário e quantidade de ativos. A descentralização do blockchain elimina a necessidade de uma autoridade central, com a verificação realizada por todos os participantes da rede. Isso assegura segurança e transparência, pois todas as transações são visíveis para todos. Uma vez adicionado, um bloco não pode ser alterado ou excluído, garantindo a imutabilidade daquele registro e dando veracidade à autenticidade dos documentos digitais. Essas características tornam o blockchain ideal para aplicações que exigem alta segurança e transparência, como criptomoedas e contratos inteligentes

Com efeito, a plataforma blockchain tem suas raízes no ano de 2008, quando um indivíduo ou grupo de pessoas sob o pseudônimo "Satoshi Nakamoto" publicou um white paper intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System". Esse documento apresentava o conceito fundamental da blockchain como um componente central do Bitcoin, uma criptomoeda descentralizada. A blockchain, como proposta, oferecia um método de registro distribuído e transparente para transações financeiras, eliminando a necessidade de intermediários confiáveis (Nakamoto, 2008).

A tecnologia blockchain permitia que todas as transações fossem registradas em um livro-razão público, compartilhado entre todos os participantes da rede. Cada bloco de

transações era vinculado ao anterior através de criptografia, formando uma cadeia de blocos (blockchain) imutável e transparente. Esse processo de validação e consenso descentralizado se tornou a base para a confiabilidade e segurança das transações. Á medida que o Bitcoin ganhava atenção e adoção, os pesquisadores e inovadores perceberam que a blockchain tinha potencial para além das criptomoedas. Conforme a compreensão da tecnologia blockchain cresceu, muitas outras criptomoedas e projetos começaram a explorar diferentes casos de uso para a tecnologia. Surgiram blockchains com diferentes mecanismos de consenso, como Proof of Work (PoW), Proof of Stake (POS), buscando melhorar a escalabilidade e a eficiência.

A plataforma blockchain tem a capacidade de fornecer uma solução eficaz para os desafios enfrentados no campo arquivístico, nos documentos arquivísticos digitais. Ela oferece mecanismos de verificação de proveniência e autenticação distribuída, garantindo a integridade e a autenticidade dos documentos arquivísticos digitais (DAD). A verificação de proveniência, ou seja, a capacidade de rastrear a origem de um documento desde sua criação, é fundamental na Arquivologia para estabelecer a segurança da informação trazendo a autenticidade e confiabilidade de registros. A blockchain facilita esse processo ao registrar cada transação em blocos sequenciais, criando um histórico imutável.

Logo, o **objetivo geral** desta pesquisa é compreender a segurança da informação e tecnologia do blockchain possam garantir autenticidade, integridade e durabilidade dos documentos digitais. A abordagem convencional muitas vezes não é suficiente para lidar com esses desafios. Portanto, **especificamente** busca: **a)** identificar como as Cadeias de Registro através do blockchain podem oferecer soluções para a segurança da informação e a preservação digital que incluem a compreensão dos aspectos teóricos da segurança da informação**, b)** examinar a identificação de fatores fundamentais para a preservação digital e a avaliação da aplicação do protocolo do blockchain (consenso) no campo dos arquivos digitais**, c)** apontar como as ferramentas de tecnologias de informação arquivística pode contribuir para a guarda confiável dos documentos digitais. Com isso partimos da seguinte pergunta: **De que forma os protocolos da a plataforma do blockchain pode contribuir para a autenticidade, integridade dos registros dos documentos digitais arquivísticos?**

Logo, **a justificativa** da condução deste estudo para o pesquisador ocorre devido à grande demanda de informações e construção de sistemas, que muitas vezes, não atendem a demanda da linguagem arquivística. Dito isso, houve aumento de documentos arquivísticos digitais, uma vez que trazer esse debate para a Arquivologia enquanto possibilidade um novo olhar para as necessidades de registro. Ademais, o blockchain

emerge como uma tecnologia promissora, oferecendo uma abordagem inovadora para enfrentar esses desafios.

Portanto, a pesquisa adotada é de natureza qualitativa, do tipo exploratória, e envolve uma revisão bibliográfica. As fontes utilizadas foram o Google Acadêmico e a Scielo Por meio dessa análise, serão obtidos insights sobre as vantagens e os desafios da implementação das Cadeias de Registro através do blockchain na Arquivologia. Contudo, ao sintetizar essas informações, este estudo contribuirá para o avanço do conhecimento sobre como a tecnologia blockchain pode ajudar na segurança da informação e a preservação digital em documentos arquivísticos, promovendo uma abordagem mais robusta e confiável para lidar com os desafios do mundo digital.

2 DOCUMENTO ARQUIVÍSTICO E DOCUMENTO ARQUIVÍSTICO DIGITAL

O objetivo da Arquivologia é gerenciar eficazmente a informação que são "produzidas por uma entidade pública ou privada ou por uma família ou pessoa no transcurso das funções que justificam sua existência como tal, guardando esses documentos relações organizas entre si" (Bellotto, 2006, p.37). Bellotto (2006) fala da produção de documentos por entidades públicas ou privadas, famílias ou pessoas, que justificam sua existência como tal. Esses documentos possuem relações organizadas entre si e são guardados com o intuito de preservar a memória e a história da entidade ou pessoa que os produziu.

Conforme definido pelo e-ARQ Brasil (2011), um documento é considerado arquivístico quando é produzido e/ou recebido por uma pessoa, seja física ou jurídica, e possui a característica de organicidade. Bellotto (2006) e o e-ARQ Brasil (2011) compartilham a definição de documentos arquivísticos, destacando que eles podem ser produzidos por diversas entidades ou indivíduos, desde que estejam relacionados às atividades que justificam sua existência. Ambos enfatizam a importância das relações organizacionais entre esses documentos, ressaltando sua relevância na preservação da memória e história da entidade ou pessoa que os gerou.

De acordo com a definição apresentada no Glossário de Documentos Arquivísticos Digitais (CDTE/CONARQ, 2014, p. 18), um documento arquivístico é "produzido (elaborado ou recebido) no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência". Esta definição enfatiza que os documentos arquivísticos são criados com a finalidade de registrar uma ação específica e, como resultado, possuem um valor probatório significativo.

Schellenberg considera como documento arquivístico:

> Todos os livros, papéis, mapas, fotografias ou outras espécies documentárias, independentemente de sua apresentação física ou características, expedidos ou recebidos por qualquer entidade pública ou privada no exercício de seus encargos legais ou em função das suas atividades e preservados ou depositados para preservação por aquela entidade ou por seus legítimos sucessores como prova de suas funções, sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informativo dos dados neles contidos. (Schellenberg, 2006, p.41)

O autor expõe a ideia de que os documentos arquivísticos, independentemente de sua apresentação física, constituem um conjunto diversificado de materiais, como livros e

fotografias, que são produzidos por entidades públicas ou privadas. Estes documentos são meticulosamente conservados com o propósito de documentar e disponibilizar provas referentes às ações, políticas e decisões efetuadas por tais entidades, sendo esse imperativo justificado pelo valor informativo inerente a eles. (Schellenberg, 2006, p.41)

Quando abordamos a temática dos documentos de arquivo, observamos as definições e características inerentes àqueles que abrigam informações registradas em diversos tipos de suportes, Bellotto (2006, p.36) afirma que:

> A forma/ função pela qual o documento é criado é o que determina o seu uso e seu destino de armazenamento futuro. É a razão de sua origem e seu emprego, e não o suporte ao qual está constituído, que vai determinar sua condição de documento de arquivo, de biblioteca, de centro de documentação ou museu.

Tanto os documentos arquivísticos físicos quanto os digitais distinguem-se do documento em si devido às características que possuem, sob a perspectiva diplomática, são:

> Forma fixa, conteúdo estável, relação organiza, contexto identificável, ação e o envolvimento de cinco pessoas, autor, redator, destinatário, originador e produtor. Há que ressaltar que entre essas cinco pessoas, pelo menos as três primeiras têm de estar presentes num documento arquivístico. (Rondinelli, 2013, p.235).

No que diz respeito aos documentos arquivísticos, é imperativo observar as características de unidade, organicidade, confiabilidade (fidedignidade), autenticidade e acessibilidade, que se constituem como requisitos fundamentais. Essas exigências são aplicáveis tanto a documentos arquivísticos físicos quanto digitais, conforme estabelecido pelas diretrizes do e-ARQ Brasil em (2005).

Além disso, as informações relacionadas ao documento digital, abrangendo sua origem e seu papel na instituição, serão discutidas em seguida, destacando-se a relevância dos metadados como elementos cruciais para a preservação da fidedignidade e autenticidade dos documentos digitais.

2.1 AS CARACTERÍSTICAS DOS DOCUMENTOS ARQUIVÍSTICOS

Para que os documentos digitais alcancem o status de arquivísticos digitais, é imperativo que eles compartilhem as mesmas características legais inerentes a documentos

convencionais.

Segundo MacNeil (2000, apud Rondinelli, 2005, P.66) a autenticidade é “a capacidade de se provar que um documento arquivístico é o que diz ser”.

e-ARQ Brasil (2006, p.22) fala:

> Um documento arquivístico autêntico é aquele que é o que diz ser, independente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao momento da produção, a autenticidade está ligada a transmissão do documento e à sua preservação e custódia.

Entende-se que a **autenticidade** dos documentos está intrinsecamente ligada aos processos de sua produção, tramitação e à sua armazenagem segura. A existência de marcações registradas sugere a autenticidade de um documento, com especial relevância no contexto digital. É fundamental que tais documentos sejam estritamente controlados desde o momento de sua concepção até sua destinação final, garantindo, desse modo, a preservação, a integridade, bem como a tramitação e o acesso adequados aos registros ao longo do tempo.

No que diz respeito a **fidedignidade** de um documento, está relacionada ao processo de sua criação, ou seja, sua produção. De acordo com MacNeil (2000, citado por Rondinelli, 2005, p. 64), o autor argumenta, sob uma perspectiva diplomática, que a autenticidade de um documento arquivístico repousa em sua capacidade de confirmar e dar suporte aos eventos que ele registra.

Quando se discute a questão da fidedignidade de documentos, torna-se imperativo compreender que a documentação desempenha um papel fundamental na comprovação dos fatos que ela atesta. A autenticidade de um documento se refere à sua capacidade de ser o que alega ser, enquanto a fidedignidade diz respeito à confiabilidade na qual se pode acreditar no conteúdo atestado por esse documento.

Conforme a NBR ISSO/IEC 17799:2001, a **integridade** “salvaguarda da exatidão e completeza da informação e dos métodos de processamento”. Documentos arquivísticos íntegros são aqueles que preservam sua integridade ao longo de seu fluxo de tramitação, permanecendo livres de quaisquer modificações não autorizadas. Nesse sentido, é fundamental que os documentos, independentemente de sua forma física ou digital, cheguem ao destinatário sem sofrer quaisquer alterações não autorizadas durante o processo de produção e envio. (CONARQ, 2012, p.2).

No contexto digital, a integridade e a confiabilidade dos documentos arquivísticos

dependem da presença de metadados nos sistemas de gestão arquivística eletrônica. É por meio desses metadados que se torna possível garantir as características de autenticidade e fidedignidade dos documentos digitais. Em resumo, os metadados desempenham um papel fundamental ao atribuir autenticidade e preservar a integridade dos documentos arquivísticos em meio digital. (D-Lib Magazine, 1999).

A preservação adequada do documento arquivístico é essencial para conferir-lhe a característica fundamental da confidencialidade. Conforme definido pela norma NBR ISSO/IEC 17799 (2001, p.2), a **confidencialidade** pode ser descrita como a "garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso". O controle do acesso aos documentos, conforme enfatizado pelo EARQ-Brasil (2006, p.31):

> A atribuição de restrições deve ser feita no momento da captura, com base no esquema de classificação de segurança e sigilo elaborado pelo órgão ou entidade que envolve os seguintes passos:
>
> - Identificar a ação ou atividade que o documento registra;
> - Identificar a unidade administrativa à qual o documento pertence;
> - Verificar a precaução de segurança e o grau de sigilo;
> - Atribuir o grau de sigilo e as restrições de acesso ao documento;
> - Registrar o grau de sigilo e as restrições de acesso no sistema de gestão arquivística de documentos;

A confidencialidade na gestão de documentos depende da atenção dos arquivistas aos sistemas de informação. É crucial que esses sistemas registrem metadados detalhados sobre o controle de acesso, identificando quem pode acessar as informações e seu grau de sigilo.

Ao contrário dos registros em museus e bibliotecas, o documento de arquivo é produzido mediante uma "passagem natural, dentro do esquema das três idades" Belloto (2006, p.37). Esta passagem natural se justifica pela sua vinculação as atividades de uma entidade, seja pública ou privada, ao longo do seu curso de funcionamento. O princípio da organicidade segundo a câmara técnica de Documentos eletrônicos (CTDE) (Brasil, 2010, p.18) diz que princípio da organicidade é apresentado como um atributo intrínseco a um conjunto de documentos, resultante da existência de uma relação significativa entre esses documentos. A organicidade é um requisito fundamental para que um conjunto de documentos seja reconhecido e considerado como um arquivo.

Ainda segundo EARQ-Brasil (2011, p.21):

> O documento arquivístico se caracteriza pela organicidade, ou seja, pelas relações que mantem 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 no plano de classificação, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas.

A organicidade representa um elemento crucial para os documentos arquivísticos, a ausência de organicidade pode resultar na perda da funcionalidade do documento, comprometendo, por consequência, a estrutura do arquivo e sua capacidade de refletir adequadamente as funções e atividades da instituição a que está vinculado. (Earq-Brasil, 2011, p.21).

Sobre a **unicidade**, segundo Belloto (2002, p.21), fala que "Não obstante forma, gênero, tipo ou suporte, os documentos de arquivos conservam seu caráter único, em função do contexto em que foram produzidos". Mesmo quando considerados cópias, esses poderão desempenhar funções distintas, influenciadas pela localização e contexto em que se encontram, conforme argumentado por EARQ-Brasil (2011, p.21):

> Documento arquivístico é único no conjunto documental ao qual pertence; podem existir cópias em um ou mais grupos de documentos, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único.

Considerando o exposto, é possível observar que o documento de arquivo, em virtude de sua organicidade, desempenha uma função singular no contexto da estrutura organizacional da instituição, estabelecendo uma conexão intrínseca com as atividades desenvolvidas por esta e com seu acervo documental.

a **auditabilidade** é uma característica importante para garantir a autenticidade e integridade dos documentos arquivísticos digitais. Os metadados fornecidos pelos sistemas de informações são cruciais para verificar as ações envolvidas com os documentos e garantir que eles mantenham suas características originais. É necessário que os metadados sejam verificados para garantir a autenticidade e confiabilidade dos documentos arquivísticos digitais.

Na publicação da revista Techoje, Cassa (2018) afirma que o príncipio da Auditabilidade "*significa a configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividade fisicas e lógicas".*

Conforma Fontes (2006, apud, Rocha 2008, p.25), *"Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o*

acesso e o que foi feito”

Com base nisso, os documentos digitais auditados transformam um documento arquivístico digital em uma prova.

3 SEGURANÇA DA INFORMAÇÃO NA ARQUIVOLOGIA DIGITAL

No contexto da segurança da informação no âmbito arquivístico, ao longo das últimas décadas, observou-se uma significativa evolução. Em épocas anteriores, a presença de documentos digitais nas organizações era inexistente, prevalecendo, predominantemente, a utilização de registros analógicos. Os documentos arquivísticos eram gerenciados de acordo com padrões estabelecidos, abrangendo controles de acesso, métodos de armazenamento regulamentados, protocolos e outros procedimentos arquivísticos convencionais.

À medida que o avanço tecnológico se manifestou, a emergência dos documentos digitais se tornou inelutável. Consequentemente, surgiu a necessidade imperativa de estabelecer sistemas informacionais e mecanismos de segurança que proporcionassem uma

salvaguarda mais robusta das informações. Têm sido desenvolvidos novos mecanismos destinados a automatizar a salvaguarda da segurança das informações em diversos meios de armazenamento, inclusive para documentos tradicionais e no contexto dos documentos arquivísticos digitais, a política de preservação digital se baseia em princípios essenciais, como autenticidade, fidedignidade, integridade, inteligibilidade e usabilidade a longo prazo, visando atender às exigências de valor probatório de tal ato. (The National Archives, [20--?] b).

Em conformidade com NBR ISSO/IEC 17799:2001 (2001, p.2) a segurança da informação “é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software.”. As informações podem adquirir utilidade significativa quando são disponibilizadas em sistemas que garantem a sua produção, utilização, circulação e armazenamento de maneira segura e acessível.

Além disso, é essencial assegurar que as instituições implementem planos que abordem a elaboração de políticas e programas de gestão documental. A interseção entre a segurança da informação e a gestão de documentos é crucial para salvaguardar a

integridade, confidencialidade e disponibilidade das informações arquivísticas. Silva afirma que:

> A gestão da informação desempenha um papel primordial nas organizações, pois ela é a responsável por organizar e gerenciar as informações no mundo corporativo, contribuindo, assim, com a correta comunicação informacional, utilizando-se para isso das ferramentas de tecnologia da informação de comunicações... (SILVA, 2015, p. 37).

E conforme observado por Klettenberg (2016, p.36), os princípios basilares da integridade, confidencialidade e disponibilidade são amplamente reconhecidos como fundamentais no domínio da segurança da informação. A despeito de eliminar as potenciais ameaças e vulnerabilidades que poderiam comprometer os sistemas de informação. Além de que, o profissional arquivista enfrenta uma série de desafios adicionais no que tange aos sistemas de informação que estão interligados à rede mundial de computadores, ou seja, à internet e segundo William Stallings (2008, p.5) expõe que:

> Ao longo do tempo, os ataques na internet e em sistemas conectados à internet se tornaram mais sofisticados, enquanto a habilidade e o conhecimento exigidos para montar um ataque diminuíram. Os ataques se tornaram mais automatizados e podem causar mais danos.

Os ataquesmais sofisticados podem resultar em danos substanciais às informações armazenadas digitalmente. Além disso, o autor aponta para a democratização das habilidades necessárias para realizar esses ataques, o que, em termos arquivísticos, ressalta a importância da segurança dos dados e da preservação das informações em ambientes digitais. A automatização dos ataques também é um aspecto relevante para a gestão documental, pois implica que os profissionais de arquivologia devem estar preparados para enfrentar ameaças cibernéticas em larga escala. A gestão e a segurança das informações digitais tornam-se ainda mais críticas na era atual, onde os riscos e desafios relacionados à cibersegurança se intensificaram. (William Stallings, 2008, p.5)

3.1 DISPOSITIVO DE CONTROLE DE SEGURANÇA

Conforme previamente demonstrado, é importante ressaltar que qualquer sistema de informação permanece suscetível a ameaças e ataques cibernéticos. Nesse contexto, os especialistas em segurança desempenham um papel crucial na gestão e proteção desses sistemas, empregando uma variedade de mecanismos para mitigar as vulnerabilidades e reduzir o potencial de incidentes de segurança. A seguir, será apresentada uma lista de

medidas que podem ser incorporadas aos sistemas de informação como recursos de segurança.

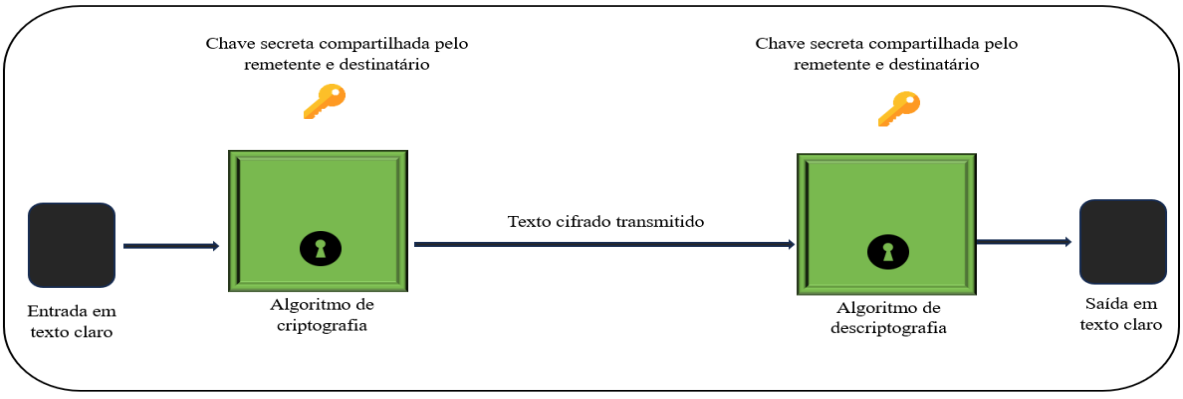
3.2 CRIPTOGRAFIA

A criptografia é um procedimento que se utiliza de um algoritmo específico e de uma chave secreta para codificar dados, assegurando que somente os usuários devidamente autorizados sejam capazes de restaurar a forma original desses dados (EARQ-Brasil 2011, p.127).

Conforme indicado por O'Brien (2007, p. 436), a criptografia desempenha um papel fundamental, ela engloba a aplicação de algoritmos matemáticos específicos, ou seja, chaves, com o propósito de transformar dados digitais em formatos codificados antes de sua transmissão. Esses mesmos algoritmos são empregados para decodificar os dados quando estes são recebidos. Nesse processo, ocorre uma reorganização das informações, tornando-as acessíveis apenas àqueles que detêm a chave de descriptografia.

Existem dois tipos fundamentais de criptografia: a simétrica e a assimétrica. Na criptografia **simétrica**, uma única chave é utilizada tanto para criptografar quanto para descriptografar os dados. Nesse cenário, tanto o remetente quanto o destinatário devem estar cientes dessa chave e mantê-la em sigilo (Turban, Rainer, Potter, 2007, P.73).

Figura 1 - Criptografia Simétrica



Fonte: Stallings (2008, p.18)

A criptografia simétrica, que emprega uma única chave para a cifragem e decifragem de dados, apresenta desafios em relação à segurança. Nessa abordagem, tanto o remetente quanto o destinatário devem compartilhar a mesma chave, o que, por sua vez, expõe as informações a um potencial risco de interceptação. (Stallings, 2008)

Em virtude desse cenário, um intruso que obtivesse acesso à chave de criptografia

poderia facilmente descriptografar mensagens cifradas por meio do sistema simétrico e conforme relatado pela revista Segurança Digital, Oliveira (2012, p. 12), é importante notar que a criptografia, apesar de ser uma ferramenta valiosa para proteger a confidencialidade dos dados, não assegura os princípios fundamentais de autenticidade e não-repúdio. Estes princípios são de extrema relevância no contexto da segurança da informação, especialmente em relação aos documentos arquivísticos.

Por outro lado, a criptografia **assimétrica** adota um par de chaves distintas: uma pública e outra privada. De acordo com a exposição de Turban, Rainer e Potter (2007, p.73), a chave pública e a chave privada são simultaneamente geradas através de um algoritmo matemático específico e essas duas chaves possuem uma relação matemática intrínseca, permitindo que os dados criptografados com uma das chaves possam ser descriptografados de maneira eficaz com a utilização da outra chave.

Além disso, segundo Stallings (2008) a criptografia assimétrica desempenha um papel fundamental na garantia da autenticidade de documentos os sistemas de chave pública desempenham um papel essencial na verificação da autenticidade de mensagens eletrônicas. Quando uma mensagem é criptografada com a chave privada de um remetente e assinada eletronicamente, isso a associa à identidade do remetente, garantindo sua legitimidade. O destinatário, por sua vez, pode confirmar a origem da mensagem ao utilizar a chave pública do remetente para descriptografá-la. Este processo é crucial para preservar a confiabilidade e a integridade das comunicações eletrônicas (Oliveira, 2012).

Neste cenário, de acordo com Stallings (2008, p.272), descreve a **assinatura digital** como um método de autenticação que permite ao remetente de uma mensagem incluir um código que atua como uma assinatura. Esse código é gerado ao aplicar uma função hash à mensagem original e, em seguida, criptografar o resultado usando a chave privada do remetente. Esse processo de criação da assinatura digital tem como objetivo garantir a origem e a integridade da mensagem, fornecendo assim uma forma confiável de verificar a autenticidade da mensagem e a integridade dos dados durante a transmissão.

De acordo com o EARQ-Brasil (2011, p. 73), a assinatura digital é um conjunto de bits que emprega algoritmos dedicados, chaves criptografadas e certificados digitais com o propósito de autenticar a identidade do signatário e verificar a integridade de um documento. A assinatura digital é uma técnica que garante a autenticidade do remetente e a integridade dos dados em um documento por meio de processos criptográficos e certificação digital. Neste cenário, a criptografia desempenha um papel essencial na segurança da informação, utilizando técnicas simétricas e assimétricas para preservar a

confidencialidade e integridade dos dados. Na abordagem simétrica, uma única chave é usada para cifrar e decifrar, simplificando a gestão, mas apresentando desafios na distribuição segura da chave. Já na criptografia assimétrica, pares de chaves distintas oferecem uma camada adicional de segurança, superando os desafios de distribuição, embora demandando mais recursos computacionais.

A assinatura digital, derivada da criptografia assimétrica, é crucial para verificar a autenticidade de mensagens. O emissor usa sua chave privada para assinar digitalmente, e o destinatário utiliza a chave pública correspondente para validar a assinatura.

A certificação digital, central para confiar em chaves públicas, envolve uma Autoridade Certificadora que emite certificados digitais, atestando a autenticidade das chaves públicas associadas a entidades específicas. Essa prática contribui para a construção de uma infraestrutura de chave pública confiável. Ou seja, a compreensão desses conceitos é crucial no desenvolvimento de sistemas seguros, assegurando a privacidade e autenticidade das comunicações digitais.

4 PRESERVAÇÃO DIGITAL DE DOCUMENTOS ARQUIVÍSTICOS

A preservação digital tem como desiderato assegurar a contínua acessibilidade às informações, preservando, concomitantemente, sua integridade e autenticidade ao longo do tempo, esse imperativo contempla a capacidade de assegurar que as funcionalidades subjacentes a essas informações possam ser adequadamente reproduzidas por tecnologias futuras, as quais, porventura, diferem daquelas que deram origem à informação no passado (Brasil. Conselho Nacional de Arquivos, 2014; Ferreira, 2006; Thomaz; Soares, 2004). Ademais, é imperativo manter, de forma concomitante, uma descrição completa do documento digital que se pretende preservar (Conway, 2001). A preservação digital transcende, portanto, a mera replicação do conteúdo digital,
requerendo a salvaguarda de sua estrutura diplomática e propriedades semânticas de maneira abrangente, tal abordagem deve ser fortemente fundamentada em uma perspectiva interdisciplinar e institucional (INNARELLI, 2007; 2012).

Ao falar dos documentos arquivísticos digitais no meio eletronico, é importante reconhecer a devida significância de sua condição no que diz respeito a maior probabilidade desses documentos serem adulterados sem deixar vestígios e evidenciando a complexidade e a especificidade dos registros (Flores; Dos Santos, 2016). O interPARES 2 Project (2010), desenvolveu um grande trabalho voltado para preservação digital dos

documentos arquivísticos, bem como os conceitos fundamentais de acurácia, confiabilidade e autenticidade.

Ao abordar a temática dos documentos arquivísticos digitais, no meio eletrônico, é imprescindível destacar a relevância significativa de sua natureza, especialmente no que se refere à crescente ameaça de adulterações sem deixar rastros, sublinhando, assim, a complexidade e especificidade intrínsecas a esses registros (Flores; Dos Santos, 2016). Nesse contexto, é importante observar as contribuições significativas do InterPARES 2 Project (2010), desenvolveu uma notável pesquisa a respeito da preservação dos documentos arquivísticos em formato digital, além de ter contribuído para a disseminação dos conceitos fundamentais relacionados à acurácia, confiabilidade e autenticidade.

Segundo InterPARES 2 Project (2010), a **acurácia** é compreendida como o grau de precisão, correção e veracidade dos dados presentes nos materiais arquivísticos digitais, caracterizando-se também pela ausência de erros e distorções. Essa definição reflete a importância da confiabilidade e integridade dos registros digitais na preservação documento digital arquivístico.

No âmbito dos documentos arquivísticos digitais, a **confiabilidade** é definida como a credibilidade do documento como um registro preciso de um fato. Ela é determinada pela capacidade do documento em respaldar o fato ao qual se refere, sendo avaliada com base na completude, forma e controle durante a sua produção (CDTE/CONARQ 2014, p. 13).

A **autenticidade** para InterPARES 2 Project (2010), define a autenticação como a declaração da autenticidade em documentos arquivísticos digitais, resultante da inclusão de elementos ou afirmações, regulada por normas legais. Ela assegura que os documentos se mantenham fiéis à sua identidade inicial. Medidas como assinaturas digitais garantem a autenticidade no momento da recepção, impedindo sua negação, mas não garantem a autenticidade contínua ao longo do tempo, requerendo estratégias adicionais para preservação (Interpares2 Project, 2010).

4.1METADADOS

A fim de adquirir o status de metadado, é essencial que os dados em questão sejam capazes de fornecer descrições e informações sobre outros conjuntos de dados, dando origem a uma abstração conhecida como "esquema" ou "conjunto de metadados". Essa concepção abstrata é meticulosamente delineada com objetivos específicos,

desempenhando um papel crucial na capacidade de identificação, representação, interconexão e gestão das operações e usos relacionados aos conteúdos contidos em um sistema de informação. (De Sordi, 2008; Sayão, 2010).

Os metadados constituem elementos intrínsecos aos documentos arquivísticos digitais, cuja finalidade reside na comunicação de suas características e atributos. Estes elementos revestem-se de fundamental importância no que concerne à preservação, autenticidade e fidelidade desses documentos, implicando, portanto, a imperatividade de um registro preciso e completo de todas as informações de relevância (Interpares, 2007b; Rondinelli, 2005). Em decorrência, os metadados desempenham um papel preponderante na viabilização de uma descrição abrangente do conteúdo do documento digital, configurando-se como uma faceta crítica na sua validação quanto à sua integridade e conformidade. Ademais, é de suma importância que os metadados sejam objeto de padronização, com o intuito de prover informações claras e uniformes aos futuros usuários, permitindo-lhes compreender o contexto em que o documento digital arquivístico que foi gerado, bem como seu histórico de manutenção e evolução. (Innarelli, 2012; Márdero Arellano, 2004). Os padrões estabelecidos permitem o registro da cadeia de custódia dos documentos digitais e seus respectivos componentes. Adicionalmente, os metadados desempenham a função de identificar os documentos de maneira singular, tanto internamente quanto externamente, em relação ao acervo ao qual os metadados estão associados, os metadados de preservação emergem como elementos cruciais na maior parte das estratégias de preservação digital. Sua principal incumbência reside na documentação minuciosa de todas as ações executadas em relação aos documentos. (Saramago, 2004; Thomaz, 2004; Thomaz; Santos, 2003).

Nesse cenário, os metadados desempenham um papel fundamental ao fornecer informações de apoio à preservação em longo prazo, contribuindo para a criação de um registro histórico das transformações ocorridas ao longo do tempo. É importante destacar que a finalidade primordial dos metadados é assegurar a capacidade de reconstrução da integridade e da autenticidade dos documentos (Saramago, 2004).

Conforme mencionado por EARQ (2011), é apresentada uma base composta por alguns elementos que devem integrar os metadados de um SIGAD (Sistema informalizado de Gestão Arquivística de Documentos). Cabe ressaltar que a composição desses elementos varia de acordo com as particularidades de cada instituição. No entanto, tais elementos são expostos a fim de proporcionar uma visão mais abrangente da vasta gama de informações contidas nos sistemas de informação, muitas das quais podem não ser

necessariamente acessadas ou consultadas pelos interessados da instituição.

Quadro 1 – Elemento de metadados

DOCUMENTO	1. Identificador do documento 2. Número do documento 3. Numero do protocolo 4. Identificador do processo/dossiê 5. Número do processo/dossiê 6. Identificado do volume 7. Número do volume 8. Tipo de meio 9. Status 10. Identificador de versão 11. Título 12. Descrição 13. Assunto 14. Autor 15. Destinatário 16. Originador 17. Redator	18. Interessado 19. Procedência 20. Identificador do componente digital 21. Gênero 22. Espécie 23. Tipo 24. Idioma 25. Quantidade de folhas – páginas 26. Numeração seqüencial dos documentos 27. Identificação de anexos 28. Relação com outros documentos 29. Níveis de acesso 30. Data de produção 31. Classe 32. Destinação 33. Prazo de guarda 34. Localização
EVENTO DE GESTÃO	1. Captura 2. Tramitação 3. Transferência 4. Recolhimento 5. Eliminação 6. Abertura_processo – dossiê	10. Encerramento volume 11. Juntada anexação 12. Juntada apensação 13. Desapensação 14. Desentranhamento 15. Desmembramento
	7. Encerramento processo dossiê 8. Reabertura processo dossiê 9. Abertura volume	16. Classificação sigilo 17. Desclassificação sigilo 18. Reclassificação sigilo
CLASSE	1. Classe nome 2. Classe código 3. Classe subordinação 4. Registro de Reabertura 5. Registro de desativação 6. Reativação de classe 7. Registro de mudança de classe 8. Registro de deslocamento de classe	9. Registro de extinção 10. Indicador de classe ativa – inativa 11. Prazo de guarda na fase intermediaria 12. Evento que determina a contagem do prazo de guarda na fase intermediaria 13. Destinação final 14. Registro de alterações 15. Observações
AGENTE	1. Nome 2. Identificador 3. Autorização de acesso	4. Credenciais de autenticação 5. Relação 6. Status do agente
COMPONENTE DIGITAL	1. Identificador do componente digital 2. Nome original 3. Características técnicas 4. Formato de arquivo 5. Armazenamento	6. Ambiente de software 7. Ambiente de *hardware* 8. Dependências 9. Relação com outros componentes digitais 10. Fixidade
EVENTO DE PRESERVAÇÃO	1. Compressão 2. Decifração 3. Validação 4. Verificação de fixidade 5. Cálculo hash	6. Migração 7. Replicação 8. Verificação de vírus 9. Validação

Fonte: e-ARQ Brasil (2011, p.93, 94, 95)

Esses metadados são apresentados como um recurso fundamental para a eficiente gestão arquivística de documentos digitais. No entanto, é importante destacar que eles não estão prontamente acessíveis durante a visualização do conteúdo dos documentos digitais. Em vez disso, esses metadados geralmente permanecem em segundo plano, o que se relaciona com a natureza dinâmica dos documentos digitais, que frequentemente contêm uma quantidade maior de informações do que aquelas que estão sendo atualmente exibidas ou acessadas.

5 BLOCKCHAIN NA ARQUIVOLOGIA DIGITAL

O advento do blockchain teve sua origem em 2008, quando o artigo intitulado "Bitcoin: a peer-to-peer electronic cash system" foi publicado. No referido documento, os autores optaram pelo uso do pseudônimo amplamente reconhecido como Satoshi Nakamoto para introduzir a tecnologia, estabelecendo, assim, os fundamentos dos conceitos de blockchain e bitcoin. Esta pesquisa seminal não apenas descreve os princípios essenciais subjacentes a essa tecnologia, mas também detalha minuciosamente o funcionamento do blockchain, destacando sua aplicabilidade no contexto das criptomoedas. (Nakamoto, 2008)

Segundo Lemieux (2017, p.118) O blockchain é definido como um sistema de banco de dados de transações distribuídas, no qual diversos computadores, denominados nós (nodes), colaboram para o armazenamento de sequências de bits que são criptografadas como uma única unidade ou bloco.

O blockchain é fundamentado na configuração de uma sequência de registros inalteráveis e de acesso público, os quais se encontram distribuídos de forma descentralizada. Essas sequências de registros são articuladas por meio de chaves públicas, operações de entrada e saída. A característica preeminente desse sistema reside na sua imutabilidade, pois, uma vez que um registro é incorporado, torna-se imune a qualquer forma de alteração.

Para Narayanan et al. (2016), é compreendido que as cadeias de registros são de natureza pública e estão acessíveis por meio da infraestrutura da internet. Para que assim garanta a disseminação efetiva e a redundância desses registros, sendo eles armazenados e replicados em várias máquinas interconectadas na ampla rede global de computadores. Este design tem o propósito de evitar a dependência de um único servidor centralizado, promovendo, assim, a descentralização e fortalecendo a segurança no armazenamento e gerenciamento dos registros.

Dessa maneira, o blockchain, representa um extenso banco de dados distribuído, responsável por armazenar de maneira irrevogável todas as transações financeiras. Este sistema inclui um mecanismo de inventário que incorpora funções de registro, rastreamento, monitoramento e transferência de ativos. É pertinente mencionar que a pioneira aplicação prática do blockchain se materializou na forma da criptomoeda conhecida como Bitcoin (Swan, 2015).

Sendo assim, Tapscott e Tapscott (2016), define que a tecnologia blockchain pode ser caracterizada como um livro razão digital que tem a capacidade de registrar tudo o que

possui valor e é considerado significativo, abrangendo desde documentos civis até a rastreabilidade de produtos e o registro de votos. Já de acordo com Bellotto (2002), a tecnologia é conceituada como um livro de operações de contas correntes, devidamente rubricadas e organizadas em ordens de débito e crédito, que é distribuído e compartilhado por participantes de uma rede peer-to-peer (P2P).

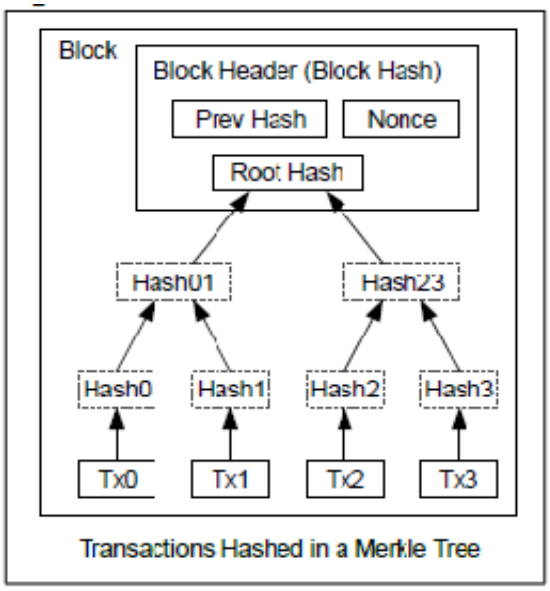
Nesse contexto, em relação à tecnologia, Bellotto (2002, p. 37) afirma que:

> [...] não causará danos à informação arquivística se os arquivistas tiverem plena consciência e conhecimento teórico e metodológico suficientes para saber servir-se das vantagens modalizadoras que lhes são oferecidas, podendo assim otimizar seu trabalho.

Dessa forma, destaca-se que a implementação de tecnologia e mudanças no ambiente arquivístico não resultarão em prejuízos para a preservação da informação arquivística, desde que os arquivistas possuam um entendimento sólido e conhecimento teórico e metodológico adequado. Isso permite que eles aproveitem as vantagens oferecidas por essas modificações de maneira eficaz, otimizando, desse modo, seu desempenho profissional no âmbito da gestão de documentos e arquivos (Bellotto, 2002).

Nesse contexto, é relevante observar que, no ano de 2008, Nakamoto concebeu a tecnologia blockchain, a qual representa uma sinergia de várias tecnologias, cuja exposição detalhada será provida na Figura 1.

Figura 1 – Anatomia do block



Fonte: Nakamoto, 2008.

Ao notarmos na Figura 1, é apresentada a anatomia de um bloco, o qual integra a cadeia de blocos. Esse bloco é estruturado em diversas camadas distintas, a saber: o Bloco (Current_block_header_version), o Cabeçalho do Bloco (Block Header) com seu respectivo hash (Block hash), a Referência ao Bloco Anterior (Reference Prev Block) com seu hash anterior (prev hash - Hash_Prev_Block), o nonce (Nonce), bem como o Nó Raiz (Root node) e seu hash raiz que é o Hash_Merkle_Root (Nakamoto, 2008).

O termo "Block" refere-se à versão do bloco, correspondendo, assim, ao número sequencial que identifica cada bloco na cadeia. Enquanto isso, o "Header" designa o resumo criptográfico associado ao bloco em questão. O terceiro elemento, denominado "Reference Prev Block," é o hash do bloco imediatamente anterior na sequência. A "Nonce" consiste em um valor numérico sequencial atribuído aleatoriamente ao bloco. Por fim, o "Root Hash" detém a raiz dos resumos criptográficos, e seu propósito primordial reside em conferir integridade aos blocos (Nakamoto, 2008).

Quadro 1 – Exemplo de uma função hash

Identificador da palavra “Arquivologia” com a letra “A” maiúscula.	6b2d7f5feb446bad70d88757c55248fe10c40390 9061369af6497cda06f12fa3
Identificador da palavra “arquivologia” com a letra “a” minúscula.	df2ae460a883cbfd6040d66d0f91c1406915df22 e444ad201541be967b230723

Fonte: Adaptado de Narciso (2018, p.324).

Segundo Narciso (2018), ao analisar o trecho fornecido, percebe-se que a função hash, ao sujeitar pequenas variações nos dados de entrada, destaca a sua precisão e capacidade de produzir resultados distintos para informações bastante diferentes. Essa característica é, de certa forma, crucial na área de Arquivologia, onde a integridade e autenticidade dos dados e informações são fundamentais para a segurança da documentação. Assim como é mencionado por Dorneles:

> A segurança é um ativo essencial para que as instituições possam salvaguardar seus acervos. No caso da informação em meio digital há necessidade de tecnologias que garantam a sua integridade, autenticidade e confidencialidade (Dorneles et. al 2013).

Com base nos autores, entende-se que a utilização de funções de hash na blockchain contribui para a imutabilidade dos registros, uma vez que alterações nos dados de um bloco exigiriam a modificação de todos os blocos subsequentes, o que é computacionalmente inviável. Isso reforça a confiança na integridade do histórico de transações e dados armazenados na blockchain. Em resumo, a aplicação de funções de

hash na blockchain é crucial para a preservação da integridade, segurança e confiabilidade do sistema distribuído.

Além disso, a compreensão de que até mesmo uma única mudança, como a troca de uma letra minúscula por maiúscula, pode gerar um hash totalmente diferente ressalta a sensibilidade dessa técnica e a importância de sua aplicação em garantir a segurança e consistência das informações armazenadas (Narciso, 2018).

Dentro das configurações da tecnologia blockchain, segundo Nakamoto (2008), destaca que o Proof of Work (PoW) se configura como um mecanismo fundamental dentro das redes blockchain, onde cada participante, chamados mineiros, são incumbidos de resolver enigmas criptográficos complexos, conhecidos como "provas de trabalho." Essa atividade tem como objetivo validar transações e criar novos blocos na cadeia de blocos (Nakamoto, 2008).

Nesse contexto, o autor diz:

> [...] O protocolo PoW envolve escanear um valor utilizando a função hash5, como a função SHA-256, onde o hash começa com n bits 0. O trabalho médio requerido é exponencial ao número de bits 0 e podem ser verificados utilizando um único hash. (Nakamoto, 2008, p.3).

Percebe-se que o consenso na rede PoW é alcançado pela mensuração do esforço computacional empregado, conferindo-lhe uma robustez considerável contra possíveis tentativas de ataque. Todavia, é importante notar que esse método é caracterizado por uma demanda energética significativa (Nakamoto, 2008).

Ao observar o texto, o autor apresenta o protocolo Proof of Work (PoW), sendo assim um método utilizado em sistemas blockchain para alcançar consenso entre os participantes da rede. Consiste na resolução de problemas computacionais complexos, conhecidos como "provas de trabalho", por parte dos mineradores. Essas provas demandam considerável poder computacional e consomem bastante energia, o que contribui para a segurança da rede, uma vez que a modificação retroativa de blocos anteriores exigiria uma quantidade impraticável de poder de computação. Ou seja, o Proof of Work (PoW) é um método que usa a mineração para validar as transações e gerar novas moedas. Esse método é mais seguro e resistente a ataques, mas também é mais lento e consome mais energia

Por outro lado, o Proof of Stake (PoS) opera de maneira diferente, eliminando a necessidade de mineração intensiva. Nesse modelo, os validadores são escolhidos para criar novos blocos com base na quantidade de moeda que possuem e estão dispostos a

"apostar" como garantia. Quanto mais moedas alguém possui, maior a probabilidade de ser escolhido como validador. O PoS busca ser mais eficiente em termos energéticos, sendo considerado uma alternativa mais sustentável em comparação com o PoW.

Essa abordagem visa reduzir significativamente o consumo de energia, uma vez que não há necessidade de realizar cálculos intensivos. Através da implementação da Prova de Participação (PoS), segundo Saleh (2015) Diferentemente do processo convencional de mineração que envolve computadores, hardware, e dispositivos de armazenamento, a PoS propõe uma abordagem inovadora. Nesse sentido, a moeda não é minerada por meio de hardware, HD e afins, mas sim por outras moedas, estabelecendo assim um mecanismo em que estas validam umas às outras. Esse paradigma implica uma transição de hardware para software, proporcionando não apenas maior celeridade no processo, mas também uma expressiva economia de recursos. A mudança para o software (softwere) não apenas otimiza a eficiência da mineração, mas também democratiza o acesso a esse processo, permitindo que um maior número de indivíduos participe ativamente. Já segundo Sunny King at al. (2012) o PoS (Proof of Stake), os direitos de validação são atribuídos com base na quantidade de criptomoeda que um validador possui e está disposto a "apostar" como garantia de sua integridade no sistema. Validadores com uma participação mais substancial na rede têm maiores chances de serem selecionados para a criação de blocos e, consequentemente, para a validação de transações.

Por outro lado, para Thompson (2017), diz que mecanismo de Prova de Participação (PoS) opera de maneira análoga a um supercomputador, implementado sob a forma de software. Este supercomputador é constituído pelo nó principal, cuja função é a execução de contratos inteligentes e aplicações descentralizadas. Nesse contexto, os usuários desempenham um papel crucial ao assinar e publicar blocos, proporcionando assim a validação proporcional em termos de tokens.

Trazendo para o contexto arquivístico, Thompson (2017, p.4-5) continua e menciona que a tecnologia blockchain, aliada aos algoritmos de consenso, desempenha um papel de extrema relevância na preservação de assinaturas digitais.

Dessa forma, a tecnologia emprega mecanismos fundamentais para a confirmação e validação dos blocos, nos quais, para cada bloco imutável, é gerado um código hash por meio de um algoritmo de criptografia. Este algoritmo mapeia os dados de entrada em uma sequência de números na base hexadecimal, de tamanho predefinido, identificando de maneira permanente a transação em questão. Esta abordagem difere das assinaturas digitais tradicionais, as quais são inseridas diretamente no documento de arquivo. A

utilização desses mecanismos assegura a integridade e autenticidade dos registros, garantindo, assim, um ambiente confiável e imutável para transações digitais.

Conforme definido pelo Dicionário Online de Português, o termo consenso denota um estado de pensamento compartilhado, consentimento mútuo ou a ação de aprovação. Segundo o Digital Assets Holdings (2016) percebe-se que um algoritmo de consenso é uma sequência de procedimentos que viabiliza a obtenção de um acordo dentro de um sistema distribuído.

Dessa maneira, para Bodkhe et al. (2020), a tecnologia opera por meio de uma rede estruturada na verificação das cadeias, incumbindo-se da validação e verificação das transações através de mecanismos de consenso. Esses mecanismos de consenso garantem a persistência dos dados em um banco de dados distribuído, que é compartilhado entre todos os nós participantes do sistema. Assim de acordo com Blodhe(2020):

> [...] Transações são interligadas a chaves criptográficas e ao livro-razão imutável que dificultam ataques para manipular ou excluir informação registrada. Dados são sempre armazenados de forma imutável junto aos seus carimbos de data/hora, auditoria pública e mecanismos de consenso. O uso destes mecanismos torna a arquitetura de segurança robusta e garante a integridade e privacidade dos dados (Bodkhe et al., 2020, p. 79766, tradução nossa).

O Com base nas informações fornecidas pelos autores, é possível afirmar que o consenso dentro da blockchain é um dos elementos fundamentais para garantir a validação e aceitação unânime das transações em uma rede descentralizada. Em ambientes tradicionais, como sistemas centralizados, uma autoridade central é responsável por validar transações e manter a integridade do sistema. No entanto, em blockchains, que operam de maneira descentralizada, é necessária uma forma de os participantes chegarem a um acordo sobre a validade das transações, uma vez que não há uma autoridade central.

Existem diferentes mecanismos de consenso, e dois dos mais conhecidos, que já foram mencionados, são o Proof of Work (PoW) e o Proof of Stake (PoS). No PoW, os participantes (mineradores) resolvem problemas matemáticos complexos para adicionar novos blocos à blockchain. O primeiro a resolver o problema é recompensado e seu bloco é adicionado à cadeia. Isso garante que a maioria dos participantes concorde sobre a ordem das transações e a validade dos blocos.

No caso do PoS, em vez de resolver problemas computacionais, os participantes (validadores) são escolhidos para criar novos blocos com base na quantidade de criptomoedas que possuem e estão dispostos a "apostar" como garantia. Esse método busca

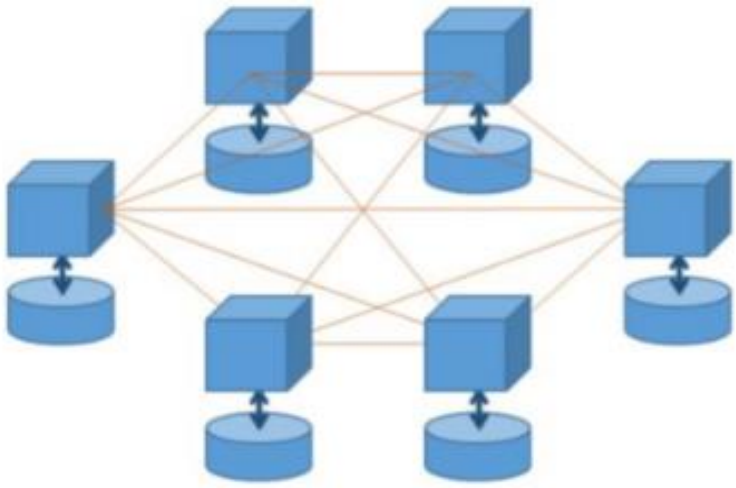
alcançar consenso de forma mais eficiente e sustentável em termos de consumo energético.

O consenso, seja por PoW, PoS ou outros mecanismos, é essencial para evitar fraudes e assegurar que todas as cópias da blockchain mantenham um registro consistente e confiável das transações. Ele é a espinha dorsal da confiabilidade e segurança das blockchains, permitindo que múltiplos participantes, muitas vezes desconhecidos entre si, concordem sobre o estado atual da rede.

Nesse Cenário, conforme apontado por David Schwartz (2014), os sistemas de registro distribuído podem ser classificados em três categorias distintas de desafios, a saber: corretude, acordo e utilidade. A corretude refere-se à capacidade do sistema de discernir eficazmente entre transações fraudulentas e transações legítimas. O acordo diz respeito à necessidade de assegurar a integridade e singularidade do sistema em questão. E a utilidade, que alude ao grau de eficácia do sistema para seus usuários, medindo seu valor e relevância para os mesmos.

A figura 3 apresenta visualmente a definição de François Zaninotto (2011) demostra que cada entidade de processamento, representada como um nó, se interconecta com múltiplos outros nós, configurando assim uma estrutura semelhante a uma rede peer-to-peer. Além disso, cada nó mantém uma cópia da blockchain, a qual é representada simbolicamente por um cilindro. O grau de replicação, seja total ou parcial, é determinado em consonância com as exigências específicas do sistema em questão.

Figura 3 - Blockchain em uma rede peer-to-peer



Fonte: Can We Reach Consensus on Blockchain (2016)?

O consenso distribuído em uma rede peer to peer (P2P) de natureza distribuída é

um processo que se efetua por meio de algoritmos, nos quais os nós participantes da rede ponto a ponto alcançam um acordo unânime acerca de um conjunto de dados, o qual representa um valor único (Bashir, 2017). Portanto, o procedimento de consenso consiste em uma sequência lógica de operações, ou seja, um algoritmo de consenso que possibilita a validação dos valores propostos pela maioria dos nós (Bashir, 2017).

Para assegurar a autenticidade dos documentos arquivísticos digitais, é imperativo o uso de consensos da plataforma blockchain, Esta tecnologia garante os princípios da segurança da informação e a preservação dos documentos digitais, fornecendo confiabilidade e veracidade ao longo do tempo, permitindo que os indivíduos confiem em seus documentos digitais para provas verificas. A utilização da blockchain fortalece a integridade dos dados, dando mais confiabilidade registros arquivísticos digitais destacando-se, como exemplo, a assinatura digital, a qual se revela capaz de atestar a autenticidade dos registros documentais em circunstâncias específicas (Stallings, 2008).

Dessa forma, evidencia-se a relevância da tecnologia blockchain para a preservação e segurança da informação, conferindo, assim, maior veracidade aos documentos arquivísticos digitais. A utilização dos consensos Proof of Work (PoW) e Proof of Stake (PoS) no blockchain contribui para a garantia da integridade e autenticidade, estabelecendo uma robusta base de confiança na preservação dos registros digitais.

6 CONSIDERAÇÕES FINAIS

Tendo em vista o objetivo proposto, a presente pesquisa conduziu uma reflexão abrangente embasada em uma revisão de literatura que abordou as cadeias de registro através do blockchain na arquivologia. Dentre os pontos abordados, destacam-se aspectos como a autenticidade do documento arquivístico digital; a devida atenção aos metadados; a salvaguarda da informação mediante medidas de segurança; bem como a preservação adequada do referido documento; ademais, é pertinente abordar a blockchain como um protocolo inserido no contexto da segurança da informação, dada sua influência e potencial contribuição para a integridade e autenticidade dos registros digitais.

Conforme apresentado, a preservação da autenticidade do documento arquivístico digital é imperativa para assegurar sua confiabilidade e integridade. Este processo engloba a verificação da origem e a inalterabilidade ao longo do tempo, frequentemente realizada por meio de tecnologias como assinaturas digitais e blockchain.

Além disso, conforme mencionado, os metadados: enquanto informações sobre dados, desempenham um papel fundamental ao oferecer contextos relacionados a documentos arquivísticos digitais. Sua relevância se destaca na facilitação da recuperação, autenticação e preservação efetiva desses documentos ao longo do tempo.

Percebe-se que a tecnologia blockchain, quando considerada como um protocolo integrado no âmbito da segurança da informação, desempenha um papel significativo no fortalecimento da integridade, autenticidade e confidencialidade dos dados digitais e traz mais veracidade aos documentos arquivísticos digitais. Como profissionais arquivistas, devemos estar em constante aprendizado e abertos a inovações tecnológicas, quando princípois e regras são semelhantes, aplicando nossos conhecimentos e desenvolvendo novas ideias para a melhoria dos documentos arquivísticos digitais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISSO|IEC 17799 Tecnologia da informação – Código de prática para gestão da segurança da informação**. Rio de Janeiro, 2001.

BELLOTTO, H. L. Arquivística: objetos, princípios e rumos. São Paulo: Associação de Arquivistas de São Paulo, 2002

BELLOTTO, H. L. Como fazer análise diplomática e análise tipológica de documento de arquivo. São Paulo: Arquivo do Estado, 2002.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes – Tratamento documental.** Rio de Janeiro: FGV, 2006.

COLLOMOSSE, John et al. ARCHANGEL: Trusted archives of digital public documents. In: **Proceedings of the ACM Symposium on Document Engineering 2018**. 2018. p. 1-4.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos** – Câmara Técnica de Documentos Eletrônicos. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2005.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos** – Câmara Técnica de Documentos Eletrônicos. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2011.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais** – Câmara Técnica de Documentos Eletrônicos. CTDE. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2012.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Glossário**. Rio de Janeiro, 2014. Disponível em: < http:<//www.conarq.arquivonacional.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf>. Acesso em: 08 ago. 2023

CONWAY, P. Preservação no universo digital. 2. ed. Rio de Janeiro: Arquivo Nacional, 2001.

DIGITAL LIBRARY FEDERATION. A working definition of digital library, 1998. Disponível em: http://www.dlib.org/dlib/september99/09lynch.html. Acesso em: 18 de Setembro 2023.

FERREIRA, M. Introdução à preservação digital: conceitos, estratégias e atuais consensos, Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. Acesso em: 24 Set. 2023.
FLORES, Daniel; DE BRITO ROCCO, Brenda Couto; DOS SANTOS, Henrique Machado. Cadeia de custódia para documentos arquivísticos digitais. 2016.

INNARELLI, H. C. Preservação digital e seus dez mandamentos. In: SANTOS, V. B. (Org.).

Arquivística: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. Distrito Federal: SENAC, 2007. p. 21-75.

INNARELLI, H. C. Instrumenta 2: preservação de documentos digitais. São Paulo: ARQ-SP, 2012.

INTERPARES 2 PROJECT. Diretrizes do preservador. A preservação de documentos arquivísticos digitais: diretrizes para organizações. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002–2007a. Disponível em: <http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>. Acesso em: 27 Set. 2023.

KLETTENBERG, Josiane. Segurança da informação: um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal de Santa Catarina, Florianópolis, 2016, 160 f. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=3696851. Acesso em: 31 jul. 2023.

LEMIEUX, V. L. Trusting records: is Blockchain technology the answer?. **Records Management Journal**, Vol. 26 No. 2, pp. 110-139, 2016. Disponível em: https://doi.org/10.1108/RMJ-12-2015-0042. Acesso em: 03 Out 2023

LUCENA, A. U.; HENRIQUES, M. A. A. Estudo preliminar da adoção de assinaturas baseadas em hash no blockchain do Bitcoin. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 18., 2018, Natal. **Anais** [...]. Rio Grande do Norte: Sociedade Brasileira de Computação, 2018. p. 65-72. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/4271. Acesso em: 10 Out. 2023.

MARAKAS, George M.; O'BRIEN James A. **Administração de Sistema da Informação – Uma introdução**. São Paulo: Mc Graw-Hill, 2007.

MÁRDERO ARELLANO, M. Á. Preservação de documentos digitais. Ciência da Informação, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: <http://revista.ibict.br/ciinf/index.php/ciinf/article/view/305>. Acesso em: 26 Set. 2023.

MOUGAYAR, W. **Blockchain para negócios**: promessa, prática e aplicação da nova tecnologia da internet. Tradução: Vivian Sbravatti. Rio de Janeiro: Alta Books, 2018.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **Decentralized business review**, 2008.

RABELO, Natália Bruno. **Uso de blockchain nos arquivos:** da autenticidade à autenticação de documentos. 2023. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal Fluminense – PPGCI do Rio de Janeiro, Niterói, 2023.

RONDINELLI, Rosely Curi. **O documento arquivístico ante a realidade digital.** Rio de Janeiro: Editora FGV, 2013.

RONDINELLI, Rosely Curi. **Gerenciamento Arquivístico de Documentos Eletrônicos.** São Paulo: Editora FGV, 2007.

SCHELLENBERG, T.R. **Arquivos Modernos**: princípios e técnicas. 6.ed. Rio de Janeiro:

Ed. Da FGV, 2006.

SHARMA, Chetan; SHARMA, Shamneesh; SAKSHI. Latent DIRICHLET allocation (LDA) based information modelling on BLOCKCHAIN technology: a review of trends and research patterns used in integration. **Multimedia Tools and Applications**, v. 81, n. 25, p. 36805-36831, 2022

SILVA, Bruna Guedes Martins da; SILVA, Márcio Bezerra da. Análise da produção científica em tecnologia da informação: Estudo panorâmico dos artigos publicados pelos professores de biblioteconomia da UnB. Biblios (Peru), n. 59, p. 18-33, 2015. Disponível em: https://www.brapci.inf.br/index.php/res/v/70152. Acesso em: 22 mar. 2019.

STALLINGS, William. **Criptografia e Segurança de Redes**. São Paulo: Pearson Prentice Hall, 2008.

SWAN, M. **Blockchain**: Blueprint for a New Economy. 1. ed. Sebastopol, California: O'Reilly Media Inc., 2015.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution**: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI – SP Editora, 2016.

TECHOJE. A importância e a implementação da segurança da informação no âmbito das atividades de negócios. 2018. Disponível em: < http://www.techoje.com.brlsite/techoje/categorialdetalhe_artigo/221 > Acesso em 18 Setembro 2023.

THOMPSON, S. The preservation of digital signatures on the blockchain. See Also: the University of British Columbia iSchool Student Journal, v. 3, 2017. Disponível em: https://ojs.library.ubc.ca/index.php/seealso/article/view/188841. Acesso em: 26 jun. 2020.

TURBAN, Efraim; RAINER, JR Kelly; POTTER, Richard E. **Introdução a Sistemas de Informação - Uma Abordagem Gerencial**. Rio de Janeiro: Elsevier, 2007.

UNITED KINGDOM. **The National Archives** [20--?]b Digital Preservation Policy. [Em linha]. [Consult. 15 Set. 2023]. Disponível em : https://www.nationalarchives.gov.uk/archives-sector/advice-and guidance/managing-your-collection/preserving-digital-collections/developing-a-digital-preservation-strategy-and-policy/