ARTIGO

UMA REFLEXÃO SOBRE POSSIBILIDADES DO USO DO BLOCKCHAIN NA ARQUIVOLOGIA

Tânia Barbosa Salles Gava

Pós-Doutora pelo Programa de Pós-Graduação em Ciência da Informação da Universidade Federal Fluminense (PPGCI/UFF) com o projeto de pesquisa intitulado "Preservação Digital Sistêmica" (2022).

Daniel Flores

Doutor em Documentação pela USAL/Espanha - revalidado pela UFRJ como Doutor em Ciência da Informação no Brasil e pós-doutorado na USAL/Fundação Carolina em Documentos Digitais: Gestão e Preservação Digital. Consultor e Assessor em Projetos de Transformação Digital Arquivística.

Simone Perozini

Possui graduação em Arquivologia pela Universidade Federal do Espírito Santo(2023).

Resumo

Este trabalho tem como objetivo geral apresentar uma reflexão sobre possibilidades de uso da tecnologia blockchain na Arquivologia e como objetivos específicos apresentar a mudança de paradigma em relação ao conceito de autenticidade dos documentos arquivísticos no ambiente analógico e digital; apresentar um breve histórico da tecnologia blockchain e apresentar algumas aplicações da tecnologia blockchain na Arquivologia. Como principais resultados, o trabalho apresenta uma reflexão inicial sobre o uso da tecnologia blockchain na Arquivologia, no contexto da mudança de paradigma do conceito de autenticidade do ambiente analógico para o digital, como também algumas aplicações, características, uso potencial, fatores críticos de sucesso, oportunidades e barreiras da tecnologia blockchain. Finalizando, esta pesquisa deixa o tema em aberto propondo que no futuro se realizem novas pesquisas com a finalidade de contextualizar e aprofundar mais o que aqui foi apresentado. Juntamente com possíveis novas pesquisas de contextualização e aprofundamento, sugere-se a realização de estudo de caso.

Palavras-chave: autenticidade; autenticação; blockchain; documentos digitais.

Abstract

This work has the general objective of presenting a reflection on the possibilities of using blockchain technology in Archival Science, and the specific objectives of presenting the paradigm shift in relation to the concept of authenticity of archival documents in the analogue and digital environment; present a brief history of blockchain technology and present some applications of blockchain technology in Archival Science. As main results, the work presents an initial reflection on the use of blockchain technology in Archival Science, in the context of the paradigm shift in the concept of authenticity from the analogue to the digital environment, as well as some applications, characteristics, potential use, critical success factors , opportunities and barriers of blockchain technology. In conclusion, this research leaves the topic open, proposing that new research be carried out in the future with the aim of contextualizing and deepening what was presented here. Along with possible new contextualization and in-depth research, it is suggested to carry out a case study.

Keywords: authenticity; authentication; blockchain; digital documents.

Introdução

Desde 1990 a tecnologia digital no Brasil vem substituindo gradativamente e cada vez mais, a tecnologia analógica no que se refere à produção documental. Essa realidade vem transformando a sociedade como um todo.

> As telecomunicações são quase integralmente digitais desde 1990 e a maioria da nossa memória tecnológica (94%) já estava em formato digital no ano de2007. Se pensarmos que um dos traços marcantes da utilização actual das tecnologias de comunicação e informação consiste em carregar para as várias plataformas disponíveis não só conteúdos novos mas também conteúdos previamente existentes em outros suportes - tornando assim digital a nossa memória colectiva que antes era analógica - concluímos que, para todos os efeitos práticos, a maior parte da nossa memória colectiva registrada tecnologicamente está hoje em formato digital (Manovich, 2001, apud Moreno, 2013, p. 4 e 5).

No contexto tecnológico digital, o documento fica vulnerável à alteração física, seja ela legítima ou ilegítima, assim como sujeito à obsolescência de hardware, software e formatos. Assim, a tecnologia evidenciou um novo paradigma para a preservação – e para a gestão documental – na arquivística, com base na mudança do ambiente analógico para o ambiente digital. Ou seja, o documento deixou de ser uma unidade indissolúvel entre a informação e seu suporte de registro (Santos, 2012, p.118), como acontecia com os documentos produzidos no ambiente analógico, que "[...] se apresentam como um pacote bem amarrado, em que o conteúdo do documento está firmemente fixado em seu suporte, e o próprio documento está arquivado contextualmente com outros documentos a ele relacionados" (InterPARES 2 Project, 2010, p. 04). Rondinelli (2013) reforça esse entendimento quando assevera sobre a relação inextricável do documento de linguagem alfabética e registrado em papel com o suporte. Ao invés disso, no ambiente digital, suporte e cadeias de bits de um documento digital podem mudar com o tempo, porque diferentemente dos documentos analógicos, os documentos digitais não têm sua forma física e conteúdo vinculados ao suporte (Conselho Nacional de Arquivos, 2012). No entanto, essas mudanças devem manter a forma fixa e o conteúdo estável dos documentos, a fim de não comprometer sua autenticidade (InterPARES 2 Project, 2010).

Segundo Gava e Flores (2021), as vulnerabilidades dos documentos digitais advindas da evolução tecnológica trouxeram preocupação no que se refere à autenticidade e confiabilidade desses documentos, visto que, para que eles cumpram suas funções primárias, é preciso que se mantenham autênticos e confiáveis pelo tempo que for necessário.

A Resolução nº 37/2012 do CONARQ considera o conceito de autenticidade a partir da Arquivologia e da Diplomática, e a define como:

> A qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração. A autenticidade é composta de dois elementos, sendo eles: identidade e integridade. A identidade é o conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos e a integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos (Conselho Nacional de Arquivos, 2012, p.37).

Outro conceito importante é o da autenticação, que não se deve confundir com o conceito de autenticidade. Autenticação de acordo com o CONARQ é:

> Autenticação: declaração de autenticidade de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal (Conselho Nacional de Arquivos, 2012, p. 2)

O Projeto InterPARES 2 (2010) define autenticação como "[...] a declaração da autenticidade, resultante da inserção ou da adição de elementos ou afirmações nos documentos arquivísticos em questão, e as normas que a regulam são estabelecidas pela legislação" (InterPARES 2 Project, 2010, p. 04)

A autenticação é o processo de determinar a identidade de um usuário com base nas informações fornecidas a ele. É necessário diferenciar o acesso a dados e serviços. Existem diferentes maneiras de autenticar usuários - senhas, arquivos de chave, chaves eletrônicas, que já se tornaram clássicos e ainda não são muito difundidos, como por exemplo, biometria e métodos não padronizados como a análise das características de tempo de uma frase-chave inserida por um usuário com uma rede neural (Paula; Cordeiro, 2015), sendo as s senhas um dos métodos de autenticação mais simples e comuns.

A área de Arquivologia não foge a esta tendência, da autenticação de documentos à emissão de certificados digitais. O setor de Arquivologia, e particularmente as instituições públicas, enfrenta muitos problemas de segurança de dados. Segundo Silva et al., (2021), existe uma evolução de uma hierarquia arquivística para uma estrutura de rede no setor público. Questões relacionadas à falsificação de dados, perda e roubo de dados digitais, entre outras, levaram as entidades que atuam no setor a buscar novas

formas de promoverem seus processos de forma rápida, segura e eficaz, tendo como cerne a criptografia oferecida pelo *blockchain*.

Segundo Flores (2022), o *blockchain* é uma tecnologia disruptiva com potencial aplicação segura nos Arquivos, porém ao ter uma adoção sem preservação digital sistêmica, ele preserva apenas os *ledger s* de autenticação. De acordo com Rondinelli (2005) a autenticidade do documento digital está diretamente ligada ao modo, à forma e ao status de transmissão. Para Flores (2022) a autenticidade é ampla e contextual e está relacionada ao armazenamento.

Desde o final dos anos 2000 a conceituação do *blockchain* revolucionou muitos setores. Desde os serviços financeiros, com o advento da criptomoeda e do *bitcoin*, ao setor de saúde, para melhor acesso aos dados pessoais dos pacientes, o advento do *blockchain* revela uma necessidade significativa de segurança de dados entre os mais diversos setores.

A tecnologia *blockchain* pode ser resumida como sendo uma base de dados descentralizada, permanente e imutável, mantida por uma rede distribuída de computadores, constituindo-se basicamente como uma tecnologia de autenticação (Moreira; Delgado; Santos, 2021, p. 26). Nas palavras de Mougayar (2017), o *blockchain* é uma tecnologia que grava transações permanentemente de uma maneira que não podem ser apagadas depois. Em suma, a tecnologia *blockchain* é inerentemente resistente à alteração de dados. Portanto, vem despertando grande interesse, por se tratar de uma tecnologia que pode ser útil para facilitar o acesso a dados de pesquisa, armazenar de forma segura dados coletados e fornecer transparência na distribuição de recursos (Gonçalves; Rodrigues, 2020, p.28), por exemplo. Costa (2018) também sugeriu o uso do *blockchain* nas universidades, colaborando para a preservação e autenticidade de documentos acadêmicos. Além de poder até mesmo transformar o serviço financeiro (Deloitte, 2017), visto que tem chamado a atenção das empresas e pode assegurar até mesmo a realização de contratos mais inteligentes e seguros. Logo, o *blockchain* deixa de ser considerado apenas uma tecnologia de autenticação, mas um recurso com inúmeras possibilidades de aplicações arquivísticas.

Nesse sentido, o presente trabalho tem como objetivo geral apresentar uma reflexão sobre possibilidades de uso da tecnologia *blockchain* na Arquivologia e como objetivos específicos apresentar a mudança de paradigma em relação ao conceito de autenticidade dos documentos arquivísticos no ambiente analógico e digital; apresentar um breve histórico da tecnologia *blockchain* e apresentar algumas aplicações da tecnologia *blockchain* na Arquivologia.

Em relação aos procedimentos técnicos, trata-se de uma pesquisa de caráter bibliográfico e documental. De acordo com Gil (2002, p. 44-45), a pesquisa bibliográfica é desenvolvida com material já elaborado, constituído principalmente de livros e artigos científicos e a pesquisa documental se constitui de fontes mais diversificadas, ou seja, documentos que ainda não receberam nenhum tratamento analítico. Para Gil, as pesquisas bibliográfica e documental se assemelham de alguma forma. A primeira porque se utiliza das contribuições de autores sobre determinado assunto e a segunda porque se utiliza de trabalhos que ainda podem ser reelaborados porque ainda não receberam tratamentos analíticos (Gil, 2002, p. 41-45).

Por fim, este trabalho está estruturado da seguinte maneira: a seção 2 apresenta uma breve discussão sobre a mudança de paradigma em relação ao conceito de autenticidade dos documentos arquivísticos no ambiente analógico para o ambiente digital e o conceito de autenticação de documentos. A seção 3 apresenta um breve histórico da tecnologia *blockchain*. A seção 4 apresenta alguns exemplos de aplicação da tecnologia *blockchain* na Arquivologia. A seção 5 apresenta as considerações finais e em seguida estão as referências bibliográficas.

Mudança de paradigma em relação ao conceito de autenticidade dos documentos arquivísticos: do ambiente analógico ao ambiente digital

De acordo com as diretrizes para presunção de autenticidade de documentos arquivísticos digitais (Conselho Nacional de Arquivos, 2020), para que um documento tenha a característica de documento arquivístico, independente do suporte em que foi criado, é preciso que ele seja confiável, autêntico, acessível e compreensível. A autenticidade, ademais dos seus dois componentes: identidade e integridade, tem como três dependências: a custódia, a preservação e a transmissão no tempo. No entanto, é importante destacar que, segundo a resolução nº 43 do CONARQ, a responsabilidade sobre a custódia e preservação dos documentos arquivísticos digitais deve ser de um RDC-Arq (Repositório Arquivístico Digital Confiável), sendo a tecnologia *blockchain*, por suas especificidades, consegue garantir somente a transmissão segura no tempo e espaço.

O e-ARQ Brasil (Conselho Nacional de Arquivos, 2022) define autenticidade como: documento arquivístico autêntico é aquele que diz ser, independentemente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção (Conselho Nacional de Arquivos, 2022, p. 29).

Para Hirtle, no ambiente analógico a transferência física e legal dos documentos de uma instituição produtora para uma instituição arquivística custodiadora (sucessor legítimo), ou seja, do produtor para um custodiador confiável, assegurava uma cadeia de custódia ininterrupta (Hirtle, 2001). Logo, nos documentos arquivísticos analógicos, conteúdo e suporte não se separam, de modo que sua identidade e integridade podem ser constatadas à luz da Diplomática, que diz que a autenticidade se refere a não adulteração do documento após sua produção. A autenticidade dos documentos arquivísticos analógicos está intrinsecamente relacionada com o conceito de documento de arquivo proposto por T.R Schellenberg:

> 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 de 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).

Para Rondinelli, a autenticidade de um documento de arquivo está diretamente ligada ao modo, à forma e ao status de transmissão deste documento, bem como às condições de sua preservação e custódia. Isso quer dizer que o conceito de autenticidade se refere à adoção de métodos que garantem que o documento não foi adulterado após sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento que foi criado (Rondinelli, 2002).

Santos (2011) refere-se à autenticidade como sendo um controle do processo de criação, manutenção e custódia do documento arquivístico. Corrobora com esse entendimento o CONARQ quando diz que:

> [...] a confiabilidade está relacionada ao momento da produção, autenticidade está ligada a transmissão do documento e a sua preservação e custódia. Um documento autêntico é aquele que se mantém da mesma forma como foi produzido, e, portanto, apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Assim, o documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico (Conselho Nacional de Arquivos, 2020, p. 37)

Para Rondinelli (2013), o documento analógico está inextricavelmente ligado ao suporte, possui linguagem alfabética, registro em papel e de leitura

direta. Já no paradigma digital, segundo Rondinelli (2013), para que o documento seja acessível aos olhos humanos, faz-se necessário a intermediação de equipamentos tecnológicos passíveis de leitura da linguagem binária, e vai além:

> [...] documento arquivístico digital é um documento, isto é, "uma unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada), com uma sintática estável", "produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades", "codificado em dígitos binários e interpretável por um sistema computacional", em suporte magnético, óptico ou outro" (Rondinelli, 2013, p. 235).

Embora no ambiente analógico a transferência física e legal dos documentos de uma instituição produtora para uma instituição arquivística custodiadora assegurasse uma cadeia de custódia ininterrupta, mantendo a autenticidade dos documentos, no ambiente digital isso não é verdade, pela especificidade e complexidade do documento digital e suas vulnerabilidades (Gava; Flores, 2021). Assim, em relação ao ambiente digital, para o InterPARES 2 Project, 2010, a autenticidade dos documentos é colocada em risco sempre que os documentos são transmitidos através do tempo e do espaço. De acordo com o Conselho Nacional de Arquivos (2020), a presunção de autenticidade do documento arquivístico digital se dá com base na análise da forma e do conteúdo (integridade) e no ambiente de produção, manutenção/ uso e preservação desse documento.

Segundo Rondinelli (2013), de acordo com a Diplomática, um documento arquivístico digital possui as seguintes características: forma fixa, conteúdo estável, relação orgânica, contexto identificável, ação e cinco pessoas envolvidas: autor, redator, destinatário, originador e produtor. Rondinelli ressalta o entendimento de que o documento digital possui forma fixa e conteúdo estável, mesmo ciente de que um documento digital tem seu formato alterado quando da sua apresentação, citando como exemplo os formatos de Word para pdf, que possuem diferentes codificações digitais. Reforça ainda que, para os documentos digitais, por sua natureza dinâmica, certa variabilidade, tanto de forma quanto de conteúdo, deve ser levada em conta (Rondinelli, 2013, p. 245).

Breve histórico da tecnologia *Blockchain*

O termo *blockchain* surgiu em 2008 com a publicação do documento: "*Bitcoin: A Peer-To-PeerEletronci Cash System*" assinado por um autor de codinome Satoshi Nakamoto. Segundo Cesar apud Fernal (2022, p. 34):

> 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, Apud Fernal, 2022, p. 34).

Um *blockchain*, originalmente cadeia de bloco, é uma lista crescente de registros, chamados blocos, que são ligados usando criptografia. Cada bloco contém um *hash* criptográfico do bloco anterior, um registro de data e hora e dados de transação (geralmente representados como um *hash* de raiz de árvore merkle) (Friedrich et al., 2020).

Por ser uma tecnologia que grava transações permanentemente de uma maneira que não podem ser apagadas depois (Mougayar, 2017), em suma, a tecnologia *blockchain* é inerentemente resistente à alteração de dados, sendo "um livro-razão aberto e distribuído que pode registrar de forma eficiente, verificável e permanente as transações entre duas partes". Um *blockchain* é frequentemente administrado por uma rede *peer-to-peer* coletivamente em conformidade com um protocolo para comunicação entre nós e verificação de novos blocos quando usado como um livro-razão distribuído (Moura et al., 2020).

O *Blockchain* foi inventado por uma pessoa usando o nome Satoshi Nakamoto, em 2008, para servir como razão de transação pública da *bitcoin* criptomoeda. A identidade de Satoshi Nakamoto é desconhecida. A invenção do *blockchain* para a *bitcoin* fez dela a primeira moeda digital a resolver o problema do gasto duplo sem a necessidade de uma autoridade confiável ou servidor central (Bovério et al., 2018).

Um *blockchain* é um *ledger* digital descentralizado, distribuído e público que é usado para registrar transações em vários computadores, de forma que qualquer registro envolvido não possa ser alterado retroativamente, sem a alteração de todos os blocos subsequentes. Isso permite aos participantes verificar e auditar transações de forma independente e relativamente barata (Lyra, 2019).

A rede ponto a ponto e um servidor de carimbo de data/hora distribuído são usados para administrar de forma autônoma um banco de dados *blockchain*. A cooperação em massa motivada pelo interesse próprio da comunidade os autentica (Silveira et al., 2021).

Essa arquitetura suporta um processo robusto em que as dúvidas dos participantes sobre a segurança dos dados são mínimas. A implementação de um *blockchain* elimina o atributo de reprodução ilimitada de um ativo. Ele verifica se cada unidade de valor foi transmitida apenas uma vez, resolvendo assim o antigo problema de gastos duplicados (Viana et al., 2020).

Um *blockchain* tem sido caracterizado como um mecanismo de troca de valor. Uma *blockchain* pode preservar os direitos de propriedade porque, quando construída corretamente para especificar o acordo comercial, cria um registro imutável de oferta e aceitação (Greve et al., 2018).

Stuart Haber e W. Scott Stornetta publicaram o primeiro trabalho em um *blockchain* protegido criptograficamente em 1991. Eles queriam construir um sistema que evitasse que os carimbos de data/hora dos documentos fossem alterados. Em 1992, Bayer, Haber e Stornetta integraram as árvores Merkle na arquitetura, o que aumentou sua eficiência ao permitir a coleta de várias certificações de documentos em um único bloco (MOURA et al., 2020).

Em 2008, como dito, uma pessoa ou grupo identificado como Satoshi Nakamoto concebeu o primeiro *blockchain*. Usando uma abordagem semelhante ao *Hash*cash para adicionar blocos à cadeia sem precisar que eles sejam assinados por uma entidade confiável, Nakamoto aprimorou significativamente o conceito. No ano seguinte, Nakamoto implantou o projeto como um componente fundamental da criptomoeda *bitcoin*, onde atua como livro-razão público para todas as transações da rede (Friedrich et al., 2020).

Em agosto de 2014, o arquivo *blockchain* do *bitcoin*, que contém registros de todas as transações da rede, ultrapassou 20 GB de tamanho (gigabytes). Em janeiro de 2015, a capacidade aumentou para cerca de 30 GB e, entre janeiro de 2016 e janeiro de 2017, o tamanho aumentou de 50 GB para 100 GB. As palavras bloco e corrente foram usadas separadamente no artigo original de Satoshi Nakamoto, mas acabaram sendo popularizadas como uma única palavra, *blockchain*, até 2016 (Migliorini et al., 2019).

A tecnologia *blockchain* pode ser integrada em várias áreas. O principal uso de *blockchains* hoje é como um livro distribuído para criptocorrências, mais notavelmente o *bitcoin*. Existem alguns produtos opcionais que vencem a prova de conceito no final de 2016 (Greve et al., 2018).

A partir de 2016, alguns observadores continuam céticos. Steve Wilson, da *Constellation Research*, acredita que a tecnologia foi anunciada com reivindicações irrealistas. Para mitigar o risco, as empresas relutam em colocar *blockchain* no centro da estrutura de negócios (Viana et al., 2020).

Aplicações da tecnologia *Blockchain* na arquivologia

É praticamente um truísmo dizer que a sociedade tem uma relação difícil com sua história. É igualmente banal dizer e descrever os graves perigos que

ameaçam o patrimônio cultural, monumental e imaterial. Da mesma forma, não há nada de original em mostrar o lugar que os arquivos ocupam na vida administrativa e econômica (Melo et al., 2020).

Com o avanço tecnológico, as Instituições Arquivísticas se viram diante de uma sociedade em busca de direitos demandando uma política organizacional voltada à preservação digital em longo prazo e mantidos em repositórios confiáveis (Santos; Flores, 2018). No Brasil, esses repositórios devem ser Repositórios Arquivísticos Digitais Confiáveis (RCD-Arq), segundo preconiza a Resolução n. 43 do CONARQ (Conselho Nacional de Arquivos, 2015). Embora o cidadão esteja ciente de seu direito de encontrar nos arquivos os documentos que procura, independentemente da sua natureza jurídica, ainda parece haver uma lacuna persistente entre a percepção dos arquivos na sociedade e o papel que às vezes se quer que eles desempenhem na relação entre a administração e os cidadãos (Moura et al., 2020).

Além disso, a última década testemunhou uma ampliação do público. Os arquivistas encontram-se diante de novas restrições e desafios. Devem, portanto, responder às novas necessidades de um público tão diverso quanto uma sociedade pode ser, vendo-se diante de um novo usuário que ocupa cada vez mais espaço e tempo: o cidadão em busca de direitos e da história (Domingues et al., 2022). Compreendendo que a Arquivologia é a disciplina dedicada à análise dos arquivos, também conhecida como arquivística, a Arquivologia investiga todas as questões relacionadas aos arquivos e às instituições dedicadas à sua preservação. Surgindo da Diplomática, a disciplina também se preocupa com as circunstâncias (contexto ou proveniência) sob as quais a informação ou item foi e é usado (Melo et al., 2020).

A Arquivologia também abrange o estudo de esforços anteriores para preservar documentos e itens, correção dessas técnicas nos casos em que esses esforços falharam e o desenvolvimento de novos processos que evitam erros de técnicas anteriores utilizadas. O campo também inclui o estudo de métodos de armazenamento de catálogos tradicionais e eletrônicos, preservação digital e o impacto de longo alcance de todos os tipos de programas de armazenamento. O termo arquivo, por sua vez, refere-se a um documento que uma entidade, uma empresa ou um indivíduo gera no âmbito do desenvolvimento de uma atividade ou função (Moura et al., 2020).

Os arquivos incluem todos os documentos relacionados com a atividade de uma empresa (arquivos privados) ou de uma organização pública (arquivos públicos). Desempenham uma tríplice função administrativa, jurídica e testemunhal. São necessários ao bom funcionamento de uma organização e para contextos históricos (Santos; Flores, 2016). Os arquivos são de grande valor para os historiadores e para a manutenção da memória coletiva. Os arquivos podem ser utilizados como referências para o conhecimento do passado. Em uma organização privada, os arquivos permitem, por exemplo, forjar uma cultura corporativa ou fornecer informações. No âmbito público, os arquivos contribuem para uma melhor compreensão das civilizações e pode auxiliar no desemprenho da gestão (Melo et al., 2020).

Desta forma, a Arquivologia visa promover o uso e a preservação destes arquivos. É comum que a Arquivologia seja enquadrada nas ciências da informação. Gerir recursos, examinar informação em contexto e explorar sua potencial utilidade são alguns dos temas de interesse desta área (Moura et al., 2020). Ademais, a ciência arquivística não trata apenas de promover a preservação e o uso de documentos. A Arquivologia se concentra em como eles devem ser avaliados, classificados, ordenados, geridos, interpretados e divulgados. O arquivamento geralmente está vinculado a grandes arquivos públicos. No entanto, suas contribuições também são importantes nos arquivos de pequenas organizações ou mesmo em registros familiares (Santos; Flores, 2016).

No entanto, todos os documentos são vulneráveis à destruição ou podem ser corrompidos (se forem digitais), seja de forma maliciosa, por acidente ou por um desastre natural, como inundação ou incêndio. Os documentos digitas, por exemplo, podem ser comprometidos por: ameaças à segurança, falha de software ou hardware, falha de energia, mau funcionamento do computador, roubo e erro humano. A Arquivologia correta dos documentos busca evitar tais problemas, garantindo uma maior segurança para os dados (Moura et al., 2020).

Tradicionalmente, a ciência arquivística envolve métodos consagrados pelo tempo para preservar itens e informações em instalações de armazenamento climatizadas. Essa técnica envolvia tanto a catalogação quanto o acesso de itens a um arquivo de coleção, sua recuperação e manuseio seguro. No entanto, as transformações tecnológicas trouxeram novos desafios para as organizações quanto às novas formas de gestão dos documentos arquivísticos e a busca por ferramentas tecnológicas capazes de conferir confiabilidade e segurança aos dados (Moura et al, 2020).

A privacidade dos dados e a segurança da informação também tem sido um aspecto crucial e muito importante, que desafia as instituições. Além disso, à medida que mais dados são digitalizados e mais informações são compartilhadas on-line, a privacidade dos dados se torna ainda mais importante (Souza, 2016). Sendo a prática de impedir o acesso não autorizado, uso, divulgação, distorção, modificação, pesquisa, registro ou destruição de informações, a principal tarefa da segurança da informação é uma proteção equilibrada da confidencialidade, integridade e disponibilidade dos dados, levando em consideração a adequação da aplicação e sem qualquer prejuízo desempenho organizacional. Isso é obtido principalmente por meio de um processo de gerenciamento de risco de várias etapas que identifica ativos fixos e intangíveis, fontes de ameaças, vulnerabilidades, exposição potencial e recursos de gerenciamento de risco. Este processo é acompanhado por uma avaliação da eficácia do plano de gerenciamento de risco (Sousa, 2014).

Neste sentido, as comunidades científica e profissional estão em constante colaboração com o objetivo de desenvolver metodologias, políticas e padrões para a proteção e confiabilidade da informação, responsabilidade legal e padrões de formação de usuários e administradores. Essa padronização é amplamente influenciada por uma ampla gama de leis e regulamentos que governam como os dados são acessados, processados, armazenados e transmitidos (Leonardi, 2012).

A confidencialidade da informação é alcançada fornecendo acesso a ela com o mínimo de privilégios com base no princípio do conhecimento mínimo necessário (need-to-know). Em outras palavras, uma pessoa autorizada deve ter acesso apenas às informações de que necessita para o desempenho de suas funções. Uma das medidas mais importantes para garantir o sigilo é a classificação das informações, o que permite que sejam classificadas como estritamente confidenciais ou destinados ao uso público ou interno. A criptografia da informação é um exemplo típico de um dos meios de garantir a confidencialidade (Leonardi, 2012).

Registros que são potencialmente confidenciais são armazenados com segurança até que passe um período predeterminado, quando se tornam disponíveis ao público em geral. Enquanto eles estão sendo armazenados, apenas os profissionais adequados, tais como os arquivistas e outros profissionais da informação, com permissão apropriada podem acessá-los para garantir que os objetos sejam preservados adequadamente. O interesse da tecnologia *blockchain* para arquivamento é que ela permite encadear, compartilhar, carimbar o tempo e proteger qualquer transação, preservando sua integridade, confiabilidade, autenticidade e legibilidade (Iglesias, 2018).

Devido ao uso das tecnologias de informação e comunicação (TICs), que mudaram o mercado de trabalho e o ambiente científico ao possibilitar a criação, o compartilhamento e o acesso à informação, a Arquivologia vive um momento desafiador. O trabalho arquivístico nesse contexto requer preservar, organizar, regular, armazenar e verificar a autenticidade dos recursos digitais sob uma nova perspectiva (Peck, 2017).

Assim como os documentos tradicionais, os documentos de arquivo digital precisam de cuidados

com os registros de suporte (datacenter, disco rígido, fita magnética e memória flash), pois a preservação do documento digital requer requisitos e técnicas para preservar sua autenticidade e integridade. Estes são compostos por seu suporte, substância, forma, ação, pessoas, conexão orgânica e cenário de produção. Em registros arquivísticos gerados digitalmente, esses aspectos são vistos individualmente por meio de metadados ou dados que explicam ou descrevem outros dados (Nascimento et al., 2020).

No contexto de armazenamento distribuído, o *blockchain* garante a imutabilidade e confiabilidade dos dados sem permitir que ninguém os possua ou controle sem autorização. Assim, o uso de *blockchain* para a Arquivologia digital também pode garantir um mecanismo para acessar, gerenciar e proteger o patrimônio cultural diariamente e em momentos de desastres (devido, por exemplo, às mudanças climáticas ou provocadas pelo homem). Graças à propriedade *append-only-register* da *blockchain*, a estrutura fornece uma proteção em camadas e meios de conservação para o patrimônio cultural (Iglesias, 2018). A estrutura também explora algumas vantagens específicas do *blockchain* (integridade, transparência e autenticidade dos registros) para apoiar o armazenamento seguro de patrimônio tangível menor contido em arquivos digitais, desde que esteja associado a uma plataforma de preservação, que deve ser desenvolvido com base no Modelo OAIS (ISO 14721:2012), que é um modelo conceitual que define os componentes funcionais de um sistema de preservação digital. A estrutura integra tecnologias para armazenamento distribuído de registros, a fim de garantir a preservação digital e a transmissão do patrimônio material e imaterial de geração em geração. O uso dessas tecnologias de armazenamento permite o desenvolvimento de uma proteção sustentável e valorização dos arquivos, bem como a gestão a longo prazo do patrimônio cultural em risco (Peck, 2017).

Os *blockchains* podem ser usados em uma variedade de áreas da ciência arquivística. Um exemplo é o prontuário eletrônico do paciente (PEP), um documento que contém informações pessoais sensíveis que, se divulgadas, podem colocar em risco a privacidade, a intimidade, a honra e a reputação de seus titulares. Além de infligir danos monetários ou morais e outras penalidades não só aos indivíduos culpados pela ocorrência, mas também aos responsáveis por zelar pela privacidade de tais dados (Zyskind; Nathan, 2015).

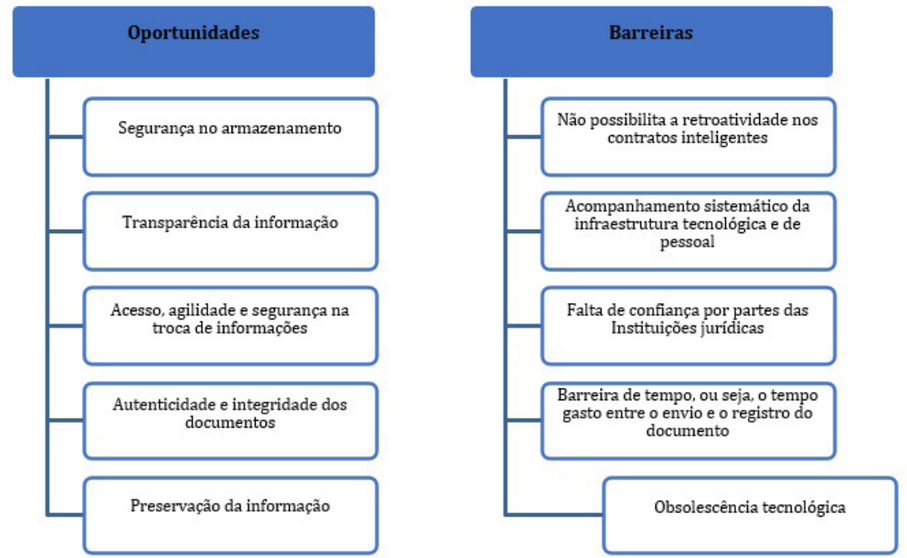
A tecnologia *blockchain* é vista como potencial para uso com PEPs quando for necessário o acesso e compartilhamento de dados pela internet. Isso se deve ao fato de utilizar diversos mecanismos de segurança de dados, incluindo criptografia, assinaturas digitais, armazenamento descentralizado (backup) e auditorias frequentes de novos blocos de dados trazidos para suas redes por mineradores, que são computadores de grande porte. Esses computadores destinam-se a fazer cálculos matemáticos para a validação da operação (Melo et al., 2019). Além disso, o *blockchain* privado pode ser usado para permitir que apenas os usuários confiáveis da instituição validem os documentos (Vaibhav, 2019). Como resultado, a ausência de informações falsas pode ser garantida e o remetente pode ser responsabilizado por qualquer informação incorreta registrada no *blockchain*. Podendo ser uma tecnologia que, aliada às técnicas e estratégias de preservação arquivista de arquivos, resulte em plataformas mais adequadas para auxiliar a preservação (Zyskind; Nathan, 2015).

O interesse da tecnologia *blockchain* para arquivamento é que ela permite encadear, compartilhar, carimbar o tempo e proteger qualquer transação, preservando sua integridade, confiabilidade, autenticidade e legibilidade (Iglesias, 2018). O **Quadro 1** apresenta as principais características, uso potencial e fatores críticos de sucesso na aplicação da tecnologia *blockchain*, de acordo com um estudo realizado pelo Tribunal de Contas da União.

No entanto, de acordo com Cardoso e Pinto (2018), ainda há muitas incertezas nos usos e impactos que a tecnologia *blockchaim* pode causar devido a sua inflexibilidade e irretroatividade no que diz respeito aos contratos inteligentes. Para Gonçalves e

Características	Uso potencial	Fatores críticos de Sucesso
- Hipertransparência e auditabilidade - Distribuído e descentralizado - Desintermediação - Disponibilidade - Imutabilidade - Integridade - Irrefutabilidade	- Repositório compartilhado - Múltiplos participantes têm direito a escrita - Baixa confiança ou conflito de interesses - Intermediários desnecessários - Dependências de transações - Rastreabilidade e procedências das informações - Concordância entre os participantes sobre os dados e transações	- Conhecimento da tecnologia - É necessário justificar o uso Integração com ambiente computacional - Implementação gradual - Os benefícios são potencializados com mais colaboração Mudança cultural

Quadro 1 – Características, uso potencial e fatores críticos de sucesso na aplicação da tecnologia *blockchain*.
Fonte: Adaptado de Tribunal de Contas da União (2019).



Quadro 2 – Oportunidades e barreiras na aplicação da tecnologia *blockchain*.
Fonte: Adaptado dos dados de pesquisa obtidos em Gonçalves e Rodrigues (2020).

Camargo (2017) esse fator distancia seu uso mais diversificado no dia a dia das instituições.

Conforme estudo realizado por Gonçalves e Rodrigues (2020), podemos destacar ainda outras barreiras que se impõem ao uso mais abrangente da tecnologia *blockchain*. São elas: acompanhamento sistemático da infraestrutura tecnológica e de pessoal; falta de confiança por partes das Instituições jurídicas. Seguem demonstradas no **Quadro 2** algumas possibilidades e barreiras na aplicação da tecnologia *blockchain*.

Considerações finais

Este artigo teve como objetivo apresentar uma reflexão sobre a possibilidade de uso da tecnologia *blockchain* na Arquivologia, apresentando a mudança de paradigma em relação ao conceito de autenticidade dos documentos arquivísticos no ambiente analógico e digital, um breve histórico da tecnologia *blockchain*, bem como apresentando algumas características, uso potencial, fatores críticos de sucesso, oportunidades e barreiras da tecnologia *blockchain* na Arquivologia.

Essa reflexão demonstrou que o conceito de autenticidade do documento arquivístico no ambiente analógico precisou ser ressignificado para o ambiente digital. Nos estudos realizados constatou-se que a presunção de autenticidade dos documentos arquivísticos no ambiente analógico, onde conteúdo e suporte não se separam, refere-se à não adulteração do documento após sua produção. Diferentemente do documento arquivístico no ambiente digital, que por não possuir vinculação com o suporte e ter sua cadeia de bits alterada com o tempo quando da aplicação de estratégias de preservação como a conversão de formatos, por exemplo, permite tais alterações desde que se mantenham a forma fixa e o conteúdo estável dos documentos.

Identificou-se também que, diante do avanço tecnológico, os Arquivos se viram diante de uma sociedade em busca de direitos que demandam uma política organizacional voltada à preservação digital em longo prazo e mantidos em um ambiente de preservação. No entanto, o uso do *blockchain* tem ganhado força à medida que seu uso avança, sendo um modelo para autenticação descentralizada automatizada que já contempla o contexto da gênese do documento arquivístico digital. Dessa forma, se torna possível que os dados sejam armazenados de forma descentralizada e com acessos disponíveis somente por quem é autorizado para tal. Todavia, se faz necessário recuperar que a tecnologia *blockchain* tem como foco principal a autenticação dos documentos, ou seja, uma declaração de sua autenticidade. Isso porque essa tecnologia envia *ledger s* de autenticação para serem minerados na sua rede, não sendo, portanto, uma tecnologia adequada para a custódia e preservação dos documentos, que são dependências fundamentais para a garantia da autenticidade, sendo, portanto, uma tecnologia de autenticação, que apoia a transmissão dos documentos de forma segura ao logo do tempo, mas não de garantia de autenticidade. Ao invés disso, para a custódia e preservação dos documentos, o ideal é adotar a implantação de um RDC-Arq. Assim, pode-se dizer que a tecnologia *blockchain* colabora com a autenticidade, mas não a garante.

Essa reflexão nos mostrou que a tecnologia *blockchain* pode se tornar futuramente uma grande aliada para a Arquivologia no contexto digital, trazendo grandes modelos de inovação e de mudanças, elevando assim o ambiente e o nível de prestação de serviço no setor. E que, atualmente, a utilização dessa tecnologia representa acima de tudo uma vantagem considerável de autenticação segura e duradoura.

Concluiu-se ainda que, a aplicação do *blockchain*, colabora, se aplicada juntamente com um ambiente de preservação (RDC-Arq), para um armazenamento seguro de documentos digitais correntes, com uso de chaves assimétricas, distribuição de registro e verificação da origem e destino da informação, além de ser um grande aliado para verificação de autenticação.

Essa tecnologia se torna mais interessante à medida que reduz os processos burocráticos nas instituições e se transforma numa plataforma sólida para consulta e tramitação segura de documentos em sua fase corrente. Sendo assim, diante de tantas possibilidades do uso da tecnologia *blockchain*, principalmente no contexto da arquivística, neste artigo entendemos a tecnologia de *blockchain* como uma ferramenta promissora para a autenticação dos documentos arquivísticos. No entanto, por ser uma tecnologia de autenticação, e de controle das transações realizadas, não permitindo a alteração de dados, entendemos que esta tecnologia não pode ser confundida com uma ferramenta de garantia de autenticidade.

Por fim, sugere-se manter o tema em aberto propondo que no futuro se realizem novas pesquisas e discussões, com a finalidade de verificar, avaliar e validar não somente possíveis usos e aplicações da tecnologia *blockchain*, mas a eficácia delas em relação à proteção dos documentos digitais, mantendo-os sempre autênticos e confiáveis ao longo do tempo.

Referências

BOVÉRIO, M. A.; SILVA, V. A. F. da. ***BLOCKCHAIN*: uma tecnologia além da criptomoeda virtual.** Revista Interface Tecnológica, [S. l.], v. 15, n. 1, p. 109–121, 2018. DOI: 10.31510/infa. v15i1.326. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/326. Acesso em: 20 jan. 2023.

CARDOSO, J. A. A.; PINTO, J. de S**. *BLOCKCHAIN* E SMART CONTRACTS**: UM ESTUDO SOBRE SOLUÇÕES DISPONÍVEIS PARA SEGURADORAS. Ideias e Inovação - Lato Sensu, [S. l.], v. 5, n. 2, p. 29, 2019. Disponível em: https://periodicos.set.edu.br/ideiaseinovacao/article/view/7908. Acesso em: 4 jan. 2023.

CONSELHO NACIONAL DE ARQUIVOS. **Glossário Documentos Arquivísticos Digitais**. Anexo: Diretrizes para a presunção de autenticidade dos documentos arquivísticos digitais. Rio de Janeiro: Conselho Nacional de Arquivos, 2012. p.1-6.

CONSELHO NACIONAL DE ARQUIVOS. Resolução nº 37, de 19 de dezembro de 2012. Aprova as diretrizes de presunção de autenticidade dos documentos arquivísticos digitais. Anexo: Diretrizes para a presunção de autenticidade dos documentos arquivísticos digitais. Rio de Janeiro: Conselho Nacional de Arquivos, 2012. p.1-6. Disponível em: Acesso: 12 set. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq.** Rio de Janeiro: Arquivo Nacional, 2015. 31 p. Disponível em: http://conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf Acesso em: 04 nov. 2019.

CONSELHO NACIONAL DE ARQUIVOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil.** Rio de Janeiro: Arquivo Nacional, 2020. v. 2. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/noticias/conarq-abre-consulta-publica-visando-a-atualizacao-do-e-arq-brasil/EARQ_v2_2020_final.pdf. Acesso em: 24 mar. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário.** Brasília: Conselho Nacional de Justiça, 2009. Disponível em: https://www.cnj.jus.br/programas-e-acoes/gestao-documental-e-memoria-proname/gestao-documental/moreq-jus-e-sistemas-informatizados/. Acesso em: 23 jun. 2021.

CONSELHO NACIONAL DE ARQUIVOS. Resolução nº 37, de 19 de dezembro de 2012. Aprova as diretrizes de presunção de autenticidade dos documentos arquivísticos digitais. Anexo: Diretrizes para a presunção de autenticidade dos documentos arquivísticos digitais. Rio de Janeiro: Conselho Nacional de Arquivos, 2012. p.1-6. Disponível em: Acesso: 12 set. 2022.

COSTA, R. et al. **Uso Não Financeiro de *Blockchain***: Um Estudo de Caso Sobre o Registro, Autenticaçãoe Preservação de Documentos Digitais Acadêmicos. In: WORKSHOP EM *BLOCKCHAIN*,1, 2018, Campos do Jordão. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação,2018. Disponível em:https://sol.sbc.org.br/index.php/w*blockchain*/article/view/2356/2320. Acesso em: 18 dez. 2022.

FERNAL, A. ***Blockchain* e os impactos na arquivologia:** um modelo lógico para autenticação distribuída dos documentos arquivísticos digitais. Universidade Estadual Paulista (Unesp), 2022. Disponível em: <http://hdl.handle.net/11449/237524>. Acesso em: 20 jan. 2023.

FLORES, D. **A Transformação Digital Compulsória Que Vem Acometendo os Arquivos, os Documentos e Arquivistas. Quais Subsídios temos para uma tomada de decisão: Disruptiva ou Inovação sustentada?** Boletim Digital de laAssociacionLatinoamericana de Archivos, Lima, Edicíon 65, ano 2022, disponível em: <https://www.alaarchivos.org/wp-content/uploads/2022/03/Artigo-Daniel-Flores.pdf> Acesso em: 20 dez. 2022.

FRIEDRICH, D. B., & PHILIPPI, J. H. M. (2020). **Inclusão digital e *Blockchain* como instrumentos para o desenvolvimento econômico:** Digital inclusion and *Blockchain* as instruments for economic development. International Journal of Digital Law, 1(1), 97-116.

GAVA, T. B. S.; FLORES, D. **Auditoria e certificação ao longo da cadeia de custódia digital arquivística. Informação & Informação**, v. 26, n. 4, p. 424-449, 2021. DOI:10.5433/1981-8920.2021v26n4p424 Acesso em: 15dez. 2022.

GAVA, T. B. S.; FLORES, D. Problematizando a Pós-Custódia com a contemporaneidade da Cadeia de Custódia Digital Arquivística compartilhada e distribuída na Preservação Digital Sistêmica. **InCID: Revista de Ciência da Informação e Documentação**, [S. l.], v. 13, n. 2, p. 222-243, 2022. DOI: 10.11606/issn.2178-2075.

v13i2p222-243. Disponível em: https://www.revistas.usp.br/incid/article/view/191654. Acesso em: 18 abr. 2023.

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

GONÇALVES, N.C; RODRIGUES, F.A. **Arquivologia e *blockchain***: discussão teórica sobre oportunidades e barreiras. [TESTE] Ciência da Informação em Revista, Maceió, v. 7, n. 3, p. 21-38, dez. 2020. ISSN 2358-0763. Disponível em: https://www.seer.ufal.br/ojs-2-somente-consulta/index.php/cir/article/view/10673. Acesso em: 24 nov. 2022. doi:https://doi.org/10.28998/cirev.2020v7n3b.

GREVE, F. G., SAMPAIO, L. S., ABIJAUDE, J. A., COUTINHO, A. C., VALCY, Í. V., & QUEIROZ, S. Q. (2018). ***Blockchain* e a Revolução do Consenso sob Demanda**. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos.

HIRTLE, P. B. Archival authenticity in a digital age. **Páginas A&B, Arquivos e Bibliotecas (Portugal)**, n. 6, p. 73-90, 2001. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/136/128. Acesso em: 29 jun. 2021.

IGLESIAS, D.**Privacidadeemperspectivas**: Nudging Privacy: Benefits and Limits of Persuading Human Behaviour Online. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

InterPARES 2 PROJECT. **Diretrizes do produtor: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos.** Tradução Arquivo Nacional e Câmara dos Deputados. TEAM Brasil, 2010. Disponível em: http://www.interpares.org/ip3/display_file.cfm?doc=ip2_creator_guidelines_booklet-- portuguese.pdf. Acesso em: 26 jul. 2021.

InterPARES 3 PROJECT. **Estudo de Caso BR08** – Câmara dos Deputados –Dossiê digital das proposições legislativas: Relatório final. TEAM Brasil, 2012.Disponível em:http://www.interpares.org/ip3/display_file.cfm?doc=ip3_brazil_cs08_Final_Report.pdf.

LACOMBE, C.; RONDINELLI, R.C. **Gestão e preservação de documentos arquivísticos digitais:** revisando alguns dos conceitos que as precedem. Acervo, [S; l.], v.29, n. 2, p. 61-73. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/709. Acesso em: 20 out. 2023.

LEBRE, O. C. das N.; ANDRADE, E. R.; MIRANDA, M. R. **A Tecnologia *Blockchain* nos Tribunais de Contas do Brasil.** Cadernos de Prospecção, [S. l.], v. 15, n. 4, p. 1056–1074, 2022. DOI: 10.9771/cp.v15i4.49749. Disponível em: https://periodicos.ufba.br/index.php/nit/article/view/49749. Acesso em: 7 dez. 2022.

LEONARDI, M.**Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LEHMKUHL, C. S.; MINTEGUI, E. M.; SILVA, E. C. L.; BRÄSCHER, M.; LEHMKUHL, C. S.; MINTEGUI, E. M.; SILVA, E. C. L. **Diálogos entre a função arquivística de avaliação e a representação da informação**. Informação & Informação, v. 24, n. 2, p. 163-181, 2019. DOI: 10.5433/1981-8920.2019v24n2p163 Acesso em: 22 dez. 2022.

LYRA, J. G. ***Blockchain* e organizações descentralizadas**. Rio de Janeiro, editora Brasport, 2019.

MELO, J. H.; CARNEIRO, N. S.; BANDEIRA, P. M. **Por dentro do arquivo público da paraíba.** Pesquisa Brasileira em Ciência da Informação e Biblioteconomia, v. 15, n. 3, p. 172-179, 2020. DOI: 10.22478/ufpb.1981-0695.2020v15n3.55432 Acesso em: 12 jan. 2023.

MIGLIORINI, I. B.; DA ROCHA, E. **Estudo de viabilidade sobre a utilização do *blockchain* na contabilidade.**CAFI , [S. l.], v. 2, n. 1, p. 99–111, 2019. DOI: 10.23925/cafi.v2i1.40601. Disponível em: https://revistas.pucsp.br/index.php/CAFI/article/view/40601. Acesso em: 20 jan. 2023.

MOREIRA, Arthur Salles de Paula; CHAGAS, Ciro Costa; SANTANA, Mariana Damiani**. Repensando a tecnologia *blockchain*: por que nem tudo o que você leu até hoje era verdade?** In: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coord.). Direito, Tecnologia e Inovação – v. III: Aplicações Jurídicas de *Blockchain*. Belo Horizonte: Expert Editora Digital, 2021. Disponível em: https://pos.direito.ufmg.br/wp-content/uploads/2021/05/Direito-tecnologia-e-Inovacao.pdf. Acesso em: 04 ago. 2022.

MORENO, J.C.**Do Analógico ao Digital: Como a digitalização afeta a produção, distribuição e consumo de informação, conhecimento e cultura na Sociedade em Rede**. Observatório (OBS*), *[S. l.]*, v. 7, n. 4, 2013. DOI: 10.15847/obsOBS742013695. Disponívelem: https://obs.obercom.pt/index.php/obs/article/view/695. Acesso em: 6 dec. 2022.

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

MOURA, L. M. F. D., BRAUNER, D. F., & JANISSEK-MUNIZ, R. (2020). ***Blockchain* e a perspectiva tecnológica para a administração pública: uma revisão sistemática**. Revista de Administração Contemporânea, 24, 259-274.

PAULA; Lorena Pires de; CORDEIRO, Douglas Farias. **Políticas de segurança da informação em instituições públicas.** Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica. 2015; v. 6, n. 2; p. 58-69.

PECK, M. E. ***Blockchains*:** How they work and why they'll change the world. IEEE spectrum, IEEE, v. 54, n. 10, p. 26–35, 2017.

RONDINELLI, Rosely Curi. **O documento arquivistico ante a realidade digital uma revisão conceitual necessária.** Rio de Janeiro; Editora FGV, 2013.

SANTOS, V. B. D. **Preservação de documentos arquivísticos digitais**. Ciência da Informação, v. 41, n. 1, 2012. DOI: 10.18225/ci.inf.. v41i1.1357 Acesso em: 12 dez. 2022.

SANTOS, H. M.; FLORES, D. **A Obsolescência do Conhecimento em Preservação Digital.** Ciência da Informação em Revista, [S. l.], v. 5, n. 1, p. 41–58, 2018. DOI: 10.28998/cirev.2018v5n1d. Disponível em: https://www.seer.ufal.br/index.php/cir/article/view/3337. Acesso em: 12 jan. 2023.

SANTOS, H.M; FLORES, D. **Preservação de documentos arquivísticos digitais autênticos reflexões e perspectivas**. BIBLOS - Revista do Instituto de Ciências Humanas e da Informação, v. 30, n. 2, p. 64-85, 2016. Disponível em: http://hdl.handle.net/20.500.11959/brapci/22829. Acesso em: 05 jul. 2022. Revista ACERVO, v. 28, N. 1, p. 241-253. Disponível em: https://revista.

an.gov.br/index.php/revistaacervo/article/view/603/601, Acesso em: 28 jun. 2022

SANTOS, H. M; FLORES, D. BIBLOS - Revista do Instituto de Ciências Humanas e da Informação, v. 30, n. 2, p. 64-85, 2016. Disponível em: http://hdl.handle.net/20.500.11959/brapci/22829. Acesso em: 05 jul. 2022.

SCHELLENBERG, T. R. **Arquivos modernos – Princípios e Técnicas**; Tradução de Nilza teixeira Soares – 6ª. ed. Rio de Janeiro; Editora FGV, 2006.

SILVA, E. C. C. E.; MARQUES, R. M. ***Blockchain* no setor público: uma revisão sistemática de literatura.** AtoZ: Novas Práticas em Informação e Conhecimento, v. 10, n. 3, p. 1-11, 2021. DOI: 10.5380/atoz.v10i3.79903.Disponível em: https://revistas.ufpr.br/atoz/article/view/79903. Acesso em: 29 set. 2022.

SILVEIRA, G. M., SILVA, M. R. D. S. D., LUFT, M. C. M. S., & DUARTE, R. G. (2021). **Aplicações e Possibilidades do *Blockchain*:** Uma Revisão Sistemática da Produção Científica Brasileira.

SOUSA, P. M. C. **Gestão da Informação: do modelo de segurança e preservação ao repositório confiável**. PÁGINAS a&b. S.3, 1 (2014) 03- 13.

SOUZA, J. G. S. et al. **Gestão de riscos da segurança da informação em uma instituição pública federal: um estudo de caso**. ENIAC Projetos, Guarulhos (SP), v.5, n.2, jun.- dez. 2016.

TRIBUNAL DE CONTAS DA UNIÃO. **Relatório de Levantamento**. 2019. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-realiza-estudo-inovador-sobre-a-tecnologia-*blockchain*-e-elabora-guia-para-orientar-os-gestores.htm. Acesso-em: 19 dez. 2022.

VAIBHAV, S. (2019) **"Understanding IPFS in Depth**: A Beginner to Advanced Guide",

VIANA, C., BRANDAO, A., DIAS, D., & CASTELLANO, G. (2020). ***Blockchain* para gerenciamento de prontuários.** RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, 177-187.

ZYSKIND, G.; NATHAN, O. et al. **Decentralizing privacy**: Using *blockchain* to protect personal data. In: IEEE. 2015 IEEE Security and Privacy Workshops. [S.l.], 2015. p. 180–184.