Ciência da Informação em Revista
ISSN: 2358-0763

Arquivologia e Blockchain: discussão teórica sobre oportunidades e barreiras

Archival Science and Blockchain: theoretical discussion about opportunities and barriers

Nadynne Cristinne da Silva Gonçalves
Graduanda em Arquivologia
Universidade Federal do Pará
nadynne.arq@gmail.com

Fernando de Assis Rodrigues
Doutor em Ciência da Informação
Universidade Federal do Pará
deassis@ufpa.br

Resumo
Embora tenha sido uma tecnologia criada a fim de solucionar problemas de transações financeiras, o Blockchain possui características que podem contribuir nas atividades arquivísticas referentes à segurança de documentos digitais. Sendo necessário examinar os desafios que esta tecnologia pode trazer à Arquivologia, esta pesquisa tem como objetivo identificar as oportunidades e barreiras apresentadas pelo Blockchain. Trata-se de uma pesquisa bibliográfica qualitativa e quantitativa, realizada por meio da análise de comunicações científicas publicadas em periódicos e em anais de congresso, coletadas durante os meses de abril e maio de 2019, nas bases de conhecimento Google Acadêmico, SciELO e Web of Science. Entre as 108 publicações coletadas, 57 foram descartadas por não atenderem aos critérios definidos. Foi analisado um total de 51 publicações, dentre as quais foram identificadas 12 com temas relacionados com a área de conhecimento. Após a aplicação do critério de qualidade da pesquisa, foram analisadas cinco publicações. Quanto às oportunidades oferecidas pelo Blockchain, a integridade de documentos digitais e acesso à informação estão entre os assuntos mais abordados. Em contrapartida, o tempo elevado para registrar uma informação, a obsolescência tecnológica e questões de privacidade estão entre as barreiras de aplicação do Blockchain. Conclui-se que o Blockchain pode ser importante para a Arquivologia não só para assegurar a autenticidade de documentos, mas também para otimizar e manter a segurança na tramitação e no armazenamento de documentos arquivísticos digitais. Todavia, há que se discutir com mais profundidade acerca da preservação em longo prazo, privacidade de informações e do usuário.

Palavras-Chave
Blockchain. Arquivologia. Documento arquivístico digital. Tecnologia de Informação e Comunicação. Informação.

Abstract
Blockchain has characteristics that can contribute to archival activities related to the security of digital documents, although it was a technology created in order to solve problems of financial transactions. This research aims to identify the opportunities and barriers presented by Blockchain, especially to examine the challenges that this technology can bring to Archival Science. This bibliographic research has a qualitative and quantitative approach, carried out through the analysis of scientific communications published in journals and conference proceedings available in Google Scholar, Sci-

DOI: 10.28998/cirev.2020v7n3b

Submetido em: 24/07/2020
Aceito em: 04/12/2020
Publicado em: 31/12/2020

ELO, and Web of Science knowledge bases. The data was collected during the months of April and May 2019. Among the 108 publications collected, 57 were discarded because they did not meet the defined criteria. A total of 51 publications were analyzed, among which 12 were identified with topics related to the area of knowledge studied. After applying the research quality criterion, five publications were selected to be analyzed. About the opportunities offered by Blockchain, the integrity of digital documents and access to information are among the most addressed issues. On the other hand, the time lag to register information, technological obsolescence, and privacy issues are among the challenges to adopt Blockchain. It is concluded that Blockchain may is an important asset for Archival Science not only to ensure the authenticity of the documents but also to optimize and maintain security in the processing and storage of digital archival documents. However, it is paramount to discuss in more depth about long-term preservation, information privacy, and user privacy.

Keywords
Blockchain. Archival Science. Archival Digital Document. Information and Communication Technology. Information.

1 INTRODUÇÃO

A Arquivologia vive um momento desafiador ocasionado pelo uso de Tecnologias de Informação e Comunicação (TICs), as quais transformaram o mercado de trabalho e o ambiente científico proporcionando facilidade na produção, no compartilhamento e no acesso a informações (SANTOS; FLORES, 2015, 2016).

Encontra-se nesse contexto, uma nova perspectiva do fazer arquivístico, de preservar, organizar, controlar, armazenar e de garantir a autenticidade de documentos digitais. A Câmara Técnica de Documentos Eletrônicos (CTDE, 2014, p. 19) define documento digital como uma "[…] informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.".

Entre os principais problemas dessa nova forma de produção de informação está a dificuldade em reconhecer a autenticidade de documentos arquivísticos digitais. Quanto ao documento arquivístico digital, a CTDE (2014, p. 18) define como um "[…] documento digital reconhecido e tratado como um documento arquivístico […]" este último definido como um "[…] documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência.".

Com base nisso, define-se documento arquivístico digital como uma informação representada por dígitos binários, elaborada durante a realização de uma atividade. Informação esta que se apresenta como resultado ou instrumento da atividade realizada, conservada para ações futuras ou para servir de referência. Além de ser acessível e interpretada por meio de um conjunto de hardwares e softwares.

Santos e Flores (2016, p. 126) afirmam que embora o documento digital tenha uma série de vantagens, "[…] a ausência de procedimentos adequados de segurança e de preservação ameaça sua confiabilidade, autenticidade e acesso.". O Conselho Nacional de Arquivos (CONARQ, 2012) justifica essa vulnerabilidade por conta da facilidade de duplicação, compartilhamento, alteração e falsificação desses documentos, sem deixar evidências aparentes dessas ações. Diante deste cenário, pressupõe-se o uso de novas soluções baseadas em TICs na tentativa de solucionar estes problemas, como o uso do *Blockchain*.

A aplicação do *Blockchain* desperta o interesse da comunidade arquivística por permitir que qualquer usuário monitore as operações realizadas ou atualize-as, e ainda assim assegurar a imutabilidade e a confiança nos dados armazenados; além de não conferir a sua propriedade e controle a ninguém (SWAN, 2015).

Com isso, este estudo levanta a hipótese que o *Blockchain* pode ser uma forma viável para garantir a segurança dos documentos arquivísticos digitais. Por esta razão, levanta-se o problema de pesquisa, verificando se há contribuições que esta tecnologia pode oferecer ao documento arquivístico digital ou seu uso limita-se à garantia de autenticidade de dados.

Se por um lado existem as oportunidades oferecidas pelas TICs, por outro existem as barreiras ocasionadas por sua adoção (FREIRE, 1991). Diante desse cenário, uma das tarefas do arquivista está relacionada com a apropriação de tecnologias como o *Blockchain*, buscando compreender suas vantagens, suas implicações e como podem ser utilizadas na Arquivologia - justificativa desta pesquisa.

Bellotto (2002, p. 37) afirma que a tecnologia:

> [...] 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.

Portanto, esta pesquisa tem como objetivo analisar o potencial de aplicabilidade do *Blockchain*, com o intuito de identificar as oportunidades e barreiras que a Arquivologia pode ter na aplicação desta tecnologia.

Como método se adotou a pesquisa bibliográfica, quantitativa e qualitativa, acerca do *Blockchain,* com base em artigos científicos publicados em canais de comunicação científica. A pesquisa foi realizada durante os meses de abril e maio de 2019 utilizando o termo "Blockchain" e "Blockchain e Arquivologia".

O universo de pesquisa é formado pelas comunicações científicas sobre *Blockchain*, com amostra delimitada a comunicações científicas na língua portuguesa, publicadas na forma de artigo em periódico científico e em anais de congresso. A amostra estudada foi composta pelos resultados de pesquisa nas bases de conhecimento Google Acadêmico, SciELO e *Web of Science*.

Adotou-se estas bases de conhecimento para a amostragem por se tratar de três bases de conhecimento com distintas características de formação de seus conjuntos de comunicações científicas: a) Google Acadêmico, com comunicações científicas de múltiplas áreas de conhecimento, acumuladas a partir de extração de dados de periódicos científicos e editoras acadêmicas que possuem produções disponíveis na Internet; b) SciELO, contendo publicações científicas brasileiras, relacionadas a diferentes áreas do conhecimento, com critérios preestabelecidos para a disponibilização de comunicações científicas em sua base, e c) *Web of Science*, com características similares ao SciELO, porém, abrangendo comunicações científicas brasileiras publicadas em periódicos de abrangência internacional.

As próximas seções estão organizadas da seguinte forma: a seção 2 apresenta as principais características e funcionamento do *Blockchain*, bem como a sua perspectiva histórica (criação e principais áreas de aplicação da tecnologia); a seção 3 apresenta os resultados da revisão de literatura; em seguida, a seção 4 apresenta as possíveis contribuições e limitações do *Blockchain* na Arquivologia a partir dos resultados obtidos; e, por fim, a seção 5 apresenta as considerações finais.

2 BLOCKCHAIN

A tecnologia *Blockchain* foi idealizada por Satoshi Nakamoto e surgiu com o propósito de evitar que um mesmo arquivo computacional (no caso inicial um arquivo computacional

relacionado a criptomoedas) pudesse ser utilizado mais de uma vez, evitando desta forma a falsificação da moeda digital. O objetivo era uma troca do foco centralizador das instituições financeiras para a tecnologia em si, tornando possível, desta maneira, transações mais rápidas, transparentes e informações mais seguras (NAKAMOTO, 2009).

Blockchain é como um livro transparente e descentralizado ou como um banco de dados compartilhado, atualizado e controlado por todos os membros na rede (SWAN, 2015). Uma tecnologia que possibilita registrar transações de forma permanente sem a possibilidade de deletar qualquer registro (MOUGAYAR, 2017).

Tapscott e Tapscott (2016) refere-se à tecnologia como um livro-razão digital, capaz de registrar tudo o que tiver valor e for considerado importante: documentos civis, rastreabilidade de produtos e registro de votos.

Para Lucena e Henriques (2016, p. 2), o *Blockchain* é:

> [...] uma base distribuída de dados que mantém uma lista encadeada com todos os registros dos elementos de uma rede, bem como registros de qualquer criação de novos elementos e modificação destes, impossibilitando revisão e adulteração dos mesmos.

Swan (2015) refere-se ao *Blockchain* como uma tecnologia que tem a capacidade de modificar todos os setores da sociedade. Afirmação que pode ser explicada por se tratar de uma tecnologia inserida em um cenário de alta demanda por informações confiáveis e segurança na tramitação de dados. Partindo desse ponto de vista, Cardozo *et al.* (2018) complementam que o *Blockchain* é um bom recurso para empresas que necessitam de rapidez e segurança na tramitação de informações, bem como para as instituições que precisam ter o controle do fluxo de produtos.

A partir de uma visão de sua estrutura, destaca-se o funcionamento do *Blockchain* pelas seguintes características: cadeia de blocos, identificador único, criptografia assimétrica, validação por consenso, distribuição de dados e controle descentralizado.

O *Blockchain* armazena informações de forma cronológica em uma lista de blocos interligados que possuem um número de identificação próprio e outro de seu antecessor, visando identificar sua origem. Cada bloco armazena um conjunto de informações que também recebem um identificador único e imutável (LUCENA; HENRIQUES, 2016).

O identificador é gerado por meio de uma função *hash* que tem por finalidade transformar informações em um código único de tamanho fixo e faz ser possível manter tanto a integridade da informação quanto da cadeia de blocos (LUCENA; HENRIQUES, 2016). No Quadro 1, apresenta-se um exemplo de identificadores gerados a partir da função *hash* SHA-256.

Quadro 1 – Exemplo de aplicabilidade da 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).

No exemplo, a alteração do caractere “a” minúsculo para maiúsculo na palavra “Arquivologia” apresentará um valor final do *hash* diferente, pois foram gerados a partir de diferentes conjuntos de caracteres. Ou seja, a geração de um *hash* é igual somente se o con-

teúdo informacional inserido na função é o mesmo. Caso contrário, o valor apresentado pela função *hash* mudará e, consequentemente, apresentará discrepância entre as informações inseridas (NARCISO, 2018).

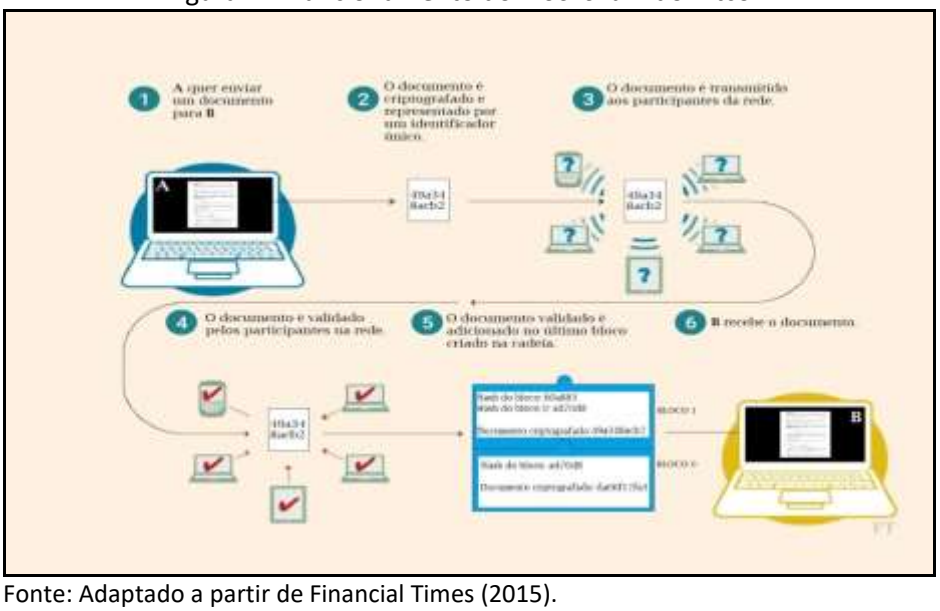
O *hash* é gerado a partir de cálculos em que a decomposição por engenharia reversa (p.ex. descobrir e alterar o conjunto de dados de origem a partir de um *hash*) pode demorar anos para se realizar, mesmo com o uso de computadores de última geração e técnicas matemáticas avançadas, o que torna o custo desta operação relativamente alto.

A criptografia utilizada no *Blockchain*, denominada como criptografia assimétrica, é composta por um par de chaves distintas: a chave pública para criptografar a mensagem, e a chave privada para descriptografar a mensagem (ABREU, 2019). No *Blockchain* este tipo de criptografia é utilizado no processo de assinaturas digitais, a qual tem a função de autenticar a origem das transações armazenadas nos blocos (LUCENA; HENRIQUES, 2018).

No processo de assinatura digital o remetente utiliza a chave privada para assinar a mensagem a ser enviada, e com a chave pública do remetente, o destinatário verifica se a mensagem de fato foi enviada pela pessoa que assinou a mensagem. Além disso, a assinatura digital garante o não repúdio, ou seja, impede um usuário de alegar que não foi autor da mensagem (DORNELES; CORREA, 2013).

A validação de blocos, na rede *Blockchain*, ocorre por meio de consenso. Greve *et al.* (2018) defendem a utilização do consenso alegando ser um elemento fundamental no desenvolvimento de sistemas seguros e confiáveis, uma vez que possibilita a concordância entre os usuários quanto às ações futuras, visando manter os sistemas estáveis e possibilitando seu progresso. A Figura 1 apresenta um exemplo de funcionamento do *Blockchain*.

Figura 1 – Funcionamento do *Blockchain* do Bitcoin



Fonte: Adaptado a partir de Financial Times (2015).

No caso do *Blockchain*, para que um bloco ou documento seja validado, é necessário que os nós da rede concordem sobre o que será registrado (ABREU, 2019). Para que isso aconteça, os nós (denominados como mineradores) precisam resolver um problema matemático, visando comprovar a veracidade da operação (BATISTA; DIAS; SILVA, 2018). A resolução deste problema requer um esforço computacional da maioria dos nós da rede (ABREU, 2019).

A dificuldade em efetivar um ataque à cadeia de blocos aumenta à medida que são adicionados e validados mais blocos (BATISTA; DIAS; SILVA, 2018). É impossível modificar qualquer operação no *Blockchain* após a adição de seis blocos no topo da cadeia por conta do alto poder de processamento requerido (GATES, 2017). Além disso, a segurança do *Blockchain* pode ser explicada também pela quantidade de locais em que está registrada a informação, característica conhecida no *Blockchain* como distribuição de dados.

As operações realizadas no *Blockchain* são compartilhadas para todos os nós da rede. Portanto, além da necessidade de um grande esforço computacional, para que se tenha sucesso em um ataque à cadeia de blocos, é necessário modificar simultaneamente as informações contidas nos computadores de todos os nós da rede (ABREU, 2019). Por exemplo, um ataque em uma rede com 100.000 locais em que a informação está registrada deverá alterar todos estes locais. Logo, a distribuição das informações dificulta ao usuário intruso essa alteração em massa. Ademais, essa característica distribuída coopera também para a transparência e rápido acesso às informações (a partir do acesso de qualquer nó à rede).

Diferente de um sistema tradicional centralizado (como os servidores de bancos), o *Blockchain* é administrado de forma descentralizada, desse modo a troca de informações pode ser feita sem a necessidade de um intermediário e transações podem ser validadas por qualquer membro na rede. Eliminando a dependência de um servidor único para validação ou a necessidade de um órgão central para controlar transações (MOUGAYAR, 2017).

Greve *et al.* (2018) categoriza o *Blockchain* em dois grupos: *Blockchain* público (sem permissão) e *Blockchain* privado (com permissão). No *Blockchain* público não há proprietário, o acesso é aberto, permite o anonimato dos nós e qualquer pessoa pode participar da rede ou apenas consultar as transações realizadas.

Por ser uma rede totalmente descentralizada, o *Blockchain* público é mais resistente a falhas, pois possui um maior número de nós com a mesma capacidade de validar operações. Contudo, Abreu (2019) destaca que embora seja possível garantir a autenticidade das operações realizadas nessa rede, a não identificação dos participantes pode ser um fator de risco ante a identificação de possíveis fraudes.

No *Blockchain* privado, o acesso é controlado por um proprietário, os membros participantes são identificados e precisam de autorização para participar da rede (GREVE *et al.*, 2018). Um maior nível de segurança pode ser oferecido pela rede privada, dado que as informações são controladas e estão armazenadas de forma centralizada na instituição que utiliza a rede permissionada. Por outro lado, por conta de um menor número de participantes, a utilização de uma rede *Blockchain* privada está mais sujeita a ataques (FURTADO, 2019).

O *Blockchain* tem um grande potencial transformador e aplicação desta tecnologia já está sendo feita no setor financeiro, no setor de saúde, no meio artístico, no governo, bem como na computação (GREVE *et al.*, 2018). No Brasil, é possível encontrar a aplicação do *Blockchain* tanto no setor privado quanto no setor público. No país, a tecnologia *Blockchain* já está sendo utilizada por empresas como a OriginalMy, a qual apresenta soluções com *Blockchain* para assinatura de contratos e registros civis. Outro exemplo de aplicação além de sistemas financeiros, a Agência Nacional de Aviação Civil (ANAC) decidiu pela "[…] gravação de todos os dados de registro obrigatório em banco de dados tipo Blockchain, disponibilizado pela ANAC […]" (ANAC, 2019, p. 1).

Na comunidade científica há discussões sobre *Blockchain* para além da aplicação em criptomoedas. A utilização desta tecnologia já foi analisada, por exemplo, para a segurança de direitos autorais (OLIVEIRA; SEGUNDO, 2018) e na comercialização de energia elétrica

(GABRICH *et al*., 2017). Nesse sentido, a seção seguinte apresenta os artigos analisados nesta pesquisa, que discutem o *Blockchain* com assuntos relacionados à Arquivologia.

3 RESULTADOS

A coleta de dados recuperou um total de 108 publicações nas bases de conhecimento: 100 foram recuperadas no Google Acadêmico; quatro na Scielo; e quatro na *Web of Science*. A partir dos resultados obtidos, 57 publicações foram descartadas por não se encaixarem nos critérios de seleção definidos, desse modo restaram 51 artigos para análise.

Quadro 2 – Síntese dos artigos analisados

Título	Autores	Congresso	Ano de publicação
Uso não financeiro de Blockchain: um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos	Costa *et al.*	I Workshop em Blockchain	2018
BNDES Token: uma proposta para rastrear o caminho de recursos do BNDES	Arantes Jr. *et al.*	I Workshop em Blockchain	2018
Blockchain e Smart Contracts: um estudo sobre soluções para seguradoras	Cardoso, J. A. A.; Pinto, J. S.	III Congresso de Gestão, Negócios e Tecnologia da Informação	2018
Smart Contracts baseados em Blockchain na cadeia de custódia digital: uma proposta de arquitetura	Gonçalves, R. F.; Petroni, B. C. A.	X Conferência Internacional de Ciência Computacional e Direito Cibernético	2018
Tecnologia Blockchain: um novo paradigma nas Ciências Abertas	Cruz *et al*.	XIX Encontro Nacional de Pesquisa em Ciência da Informação	2018

Fonte: Dados da pesquisa (2019).

A partir dos termos utilizados como estratégia para recuperação das comunicações científicas nas bases de conhecimento, não foi recuperado nenhum artigo relacionado diretamente com periódicos ou congressos de Arquivologia, conforme mostra o Quadro 2. No entanto, o processo de análise desta pesquisa identificou 12 artigos com discussões de temas próximos à Arquivologia, estabelecendo as seguintes categorias (definidas pelos autores a partir da leitura dos artigos):

I - *Preservação de documentos digitais*: artigos que propõem a aplicação do *Blockchain* para preservação de documentos digitais;

II - *Autenticidade de documentos digitais*: artigos que consideram o *Blockchain* uma tecnologia capaz de manter a autenticidade de documentos digitais;

III - *Integridade de documentos digitais*: artigos que identificaram na aplicação do *Blockchain* uma forma segura de garantir a integridade do documento;

IV - *Acesso à informação*: artigos que consideram o *Blockchain* uma tecnologia para obter fácil acesso à informação;

V - *Transparência informacional*: artigos que consideram o *Blockchain* uma tecnologia capaz de oferecer transparência informacional.

Contudo, sete artigos foram descartados após a utilização do critério de qualidade da pesquisa, restando cinco publicações para análise. O critério de qualidade da pesquisa foi realizado a partir do descarte de resumos e resumos expandidos, pois entende-se que este

tipo de comunicação científica está relacionado com pesquisas ainda em estágio inicial. Destaca-se que entre as cinco publicações analisadas, não foi identificada nenhuma publicação em periódico científico.

Costa *et al*. (2018) analisam a utilização do *Blockchain* para autenticação e preservação de documentos acadêmicos. Os autores propõem uma plataforma a partir da combinação de tecnologias do *Blockchain* e tecnologias de certificação e preservação digital, visando fornecer um ambiente seguro para armazenar os registros e preservá-los em longo prazo, além de otimizar o processo de autenticação e validação dos documentos, garantindo sua veracidade, integridade e autenticidade.

Visando à transparência da informação, Arantes Jr. *et al*. (2018) estudam a aplicação de um mecanismo de rastreamento de recursos públicos em projetos financiados pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), optando pela utilização de uma rede *Blockchain* pública. A escolha, segundo os autores, se dá por conta do nível de segurança da rede, a qual dificulta a realização de alterações por ser composta de um maior número de membros para validar transações. Ademais, por meio de software de monitoramento, qualquer pessoa pode conectar-se a rede e acompanhar as movimentações realizadas.

Cardoso e Pinto (2018) discutem sobre a utilização da tecnologia como recurso para seguradoras. Segundo os autores, com a aplicação do *Blockchain* junto aos *Smart Contracts*[1] é possível reduzir custos em processos de autenticação documental, agilizar acordos e garantir a transparência, acesso às informações, autenticidade e integridade dos documentos registrados. Além disso, justificam o uso do *Blockchain* por ser um recurso que oferece às organizações a confiança pretendida para armazenar dados.

Também com base nessa confiança, Petroni e Gonçalves (2018) sugerem a aplicação de *Blockchain* aliado a *Smart Contracts* para utilização em cadeias de custódia digital, objetivando a integridade de evidências digitais a serem apresentadas em processos judiciais. Os autores afirmam ser possível tratar de todas as questões que envolvem estes processos, devido à característica descentralizada e à segurança fornecida pela tecnologia.

Para Cruz *et al*. (2018), a tecnologia pode ser útil também no campo científico por possibilitar: facilidade no acesso a dados de pesquisa, por meio da disponibilidade dos dados; armazenamento seguro para os dados coletados, garantindo a autenticidade e integridade dos documentos; além de facilitar e fornecer transparência na distribuição de recursos para pesquisas.

No Quadro 3 apresenta-se uma síntese das oportunidades da utilização de *Blockchain* (de acordo com as categorias apresentadas no início desta seção) e as barreiras encontradas pelos autores ante a aplicação da tecnologia *Blockchain*.

Quadro 3 – Oportunidades e Barreiras do uso de *Blockchain* por publicação

(continua)

Publicações	Síntese das oportunidades da aplicabilidade do *Blockchain*	Síntese das barreiras identificadas para a aplicabilidade do *Blockchain*
Costa *et al*. (2018)	Segurança no armazenamento de documentos digitais, capacidade de preservar os documentos, garante a veracidade, integridade e autenticidade de documentos digitais.	Não trata sobre
Arantes Jr. *et al*. (2018)	Segurança de informações, Integridade de dados, transparência de informações, acesso a informações.	Não trata sobre

Fonte: Dados da pesquisa (2019).

[1] *Smart Contracts* ou Contratos Inteligentes são contratos digitais autoexecutáveis escritos em linguagem de programação (STOKES; RAMOS, 2017).

Quadro 3 – Oportunidades e Barreiras do uso de *Blockchain* por publicação

(continuação)

Publicações	Síntese das oportunidades da aplicabilidade do *Blockchain*	Síntese das barreiras identificadas para a aplicabilidade do *Blockchain*
Cardoso e Pinto (2018)	Segurança no armazenamento, transparência de informações, acesso, agilidade e segurança na troca de informações, garante a autenticidade e integridade dos documentos.	O *Blockchain* não possibilita a reversão de contratos inteligentes, o que impede a adoção da tecnologia por grande parte das empresas do direito contratual.
Petroni e Gonçalves (2018)	Garantia da integridade e autenticidade de informações, facilidade no acesso, transparência de informações, preservação de informação.	Necessidade de analisar sistematicamente a infraestrutura tecnológica e de pessoal. A falta de confiança de instituições jurídicas para que as aplicações de redes distribuídas deixem de sofrer restrições.
Cruz *et al*. (2018)	Garante a autenticidade e integridade dos documentos, facilita o acesso à informação, possibilita a preservação de informações e a transparência informacional.	Não trata sobre

Fonte: Dados da pesquisa (2019).

O Quadro 4 apresenta a relação entre as categorias e as publicações. Em cada categoria, as colunas de 2 a 7 representam aderência ao tema da categoria por publicação. A última coluna mostra o percentual que as publicações apresentam com discussões sobre a categoria.

Quadro 4 – Distribuição de Publicações em Categorias

Categorias	Costa *et al*. (2018)	Arantes Jr. *et al*. (2018)	Cardoso e Pinto (2018)	Petroni e Gonçalves (2018)	Cruz *et al*. (2018)	Percentual de publicações que abordam cada categoria
I. Preservação de documentos digitais	X			X	X	**60,00 %**
II. Autenticidade de documentos digitais	X		X	X	X	**80,00%**
III. Integridade de documentos digitais	X	X	X	X	X	**100,00 %**
IV. Acesso à informação	X	X	X	X	X	**100,00 %**
V. Transparência informacional		X	X	X	X	**80,00%**
Percentual de categorias que cada publicação aborda	**80,00%**	**60,00%**	**80,00%**	**100,00%**	**100,00%**	**-**

Fonte: Dados da pesquisa (2019).

O percentual de publicações que abordam cada categoria está relacionado com o número de pesquisas que discutem as categorias. Ou seja, quão maior o percentual da última coluna, significa que mais publicações apresentam o tema da categoria. Já a última linha

do quadro apresenta o total de categorias que cada publicação aborda. Neste caso, quão maior o percentual, maior o número de categorias abordadas em cada publicação.

4 DISCUSSÃO: OPORTUNIDADES E BARREIRAS NA ARQUIVOLOGIA

Petroni e Gonçalves (2018) e Cruz *et al*. (2018) discutem em suas pesquisas um total de 100% das categorias apresentadas no Quadro 4. Já Costa *et al*. (2018), Cardoso e Pinto (2018) discutem quatro das cinco categorias, resultando em um total de 80% em cada pesquisa. Arantes Jr. *et al*. (2018) é o que menos discute categorias em sua publicação, onde há apenas três das cinco categorias, com um percentual de 60%.

Quanto às categorias mais discutidas, destacam-se apenas duas: III. *Integridade de documentos digitais* e IV. *Acesso à informação*, as quais aparecem em 100% das publicações. Por outro lado, a categoria I. *Preservação de documentos digitais*, com um percentual de 60%, é a categoria menos abordada nas publicações.

Tendo como base as categorias apresentadas na seção anterior, discute-se nesta seção cada uma das categorias, visando compreender as oportunidades que a Arquivologia pode encontrar na aplicação da tecnologia *Blockchain*. Ademais, apresenta-se as barreiras identificadas pelos autores com a aplicação do *Blockchain*, bem com as barreiras na comunicação da informação que a cadeia de blocos pode apresentar.

4.1 Oportunidades

I – Preservação de documentos digitais

A preservação digital tem como objetivo garantir a autenticidade e o acesso permanente de documentos digitais, bem como a possibilidade de interpretar o conteúdo do documento independente da plataforma tecnológica (BAGGIO; FLORES, 2013). Estratégias de preservação devem ser aplicadas em um ambiente que monitore as ações realizadas nos documentos. Ambiente este que possa assegurar confiança para o armazenamento de documentos digitais (FLORES; SANTOS, 2015).

Cardoso e Goya (2018) afirmam que plataformas baseadas em *Blockchain* podem armazenar documentos e informações de forma segura, tornando-as disponíveis e confiáveis. Essa afirmativa pode ser justificada pelo nível de segurança que a cadeia de blocos oferece, por meio da utilização de criptografia, validação por consenso e distribuição de registros (MARQUES; MENDES, 2019). Esta última característica deve ser considerada para armazenamento permanente de dados de qualquer natureza (LUCENA; HENRIQUES, 2016).

Em relação à preservação digital, Flores e Santos (2015, p. 200) ressaltam ainda que "[...] deverá efetuar a manutenção da integridade e da autenticidade dos documentos arquivísticos digitais em virtude da necessidade de garantir que o patrimônio documental mantido sob custódia é autêntico e permanecerá íntegro no decorrer do tempo.". Estas atribuições da preservação (autenticidade e integridade) serão discutidas a seguir.

II – Autenticidade de documentos digitais

A autenticidade é a qualidade de o documento ser exatamente o que aparenta ser, não ter sofrido qualquer tipo de alteração desde sua produção (CONARQ, 2014). Quanto aos documentos arquivísticos eletrônicos considera-se autêntico "[…] aquele que é transmitido de maneira segura, cujo status de transmissão pode ser determinado, que é preservado de

maneira segura e cuja proveniência pode ser verificada." (MACNEIL *apud* RONDINELLI, 2002, p. 66).

Com a aplicação do *Blockchain* pode ser possível garantir a autenticidade dos documentos digitais tendo como base as seguintes características da cadeia de blocos: a) utilização de chave assimétrica que garante que os dados possam ser enviados de um ponto a outro sem que sejam alterados; b) distribuição de registro visando impedir a eliminação ou alteração dos dados armazenados na cadeia; c) possibilidade de verificar a origem e o destino da informação (MOUGAYAR, 2017).

III – Integridade de documentos digitais

Para Bellotto (2002, p. 21), a integridade ou indivisibilidade é um princípio arquivístico onde "Os fundos de arquivo devem ser preservados sem dispersão, mutilação, alienação, destruição não autorizada ou adição indevida.".

Nesse sentido, no *Blockchain* a integridade do documento digital pode ser garantida por conta da característica encadeada imutável da rede. Não permite a alteração do conteúdo, eliminação da informação, nem a troca do bloco de armazenamento. Arantes Jr. *et al*. (2018, p. 3) afirmam que "O uso da tecnologia *Blockchain* permite que a sociedade confie na inviolabilidade das informações de forma irrefutável, sem a necessidade de uma relação de confiança com a entidade centralizadora.".

No caso de um repositório digital confiável, o CONARQ (2014) estabelece que o sistema deve possuir "[...] mecanismos para garantir o sincronismo entre as cópias de um mesmo documento, ou seja, garantir que as mudanças intencionais feitas em uma cópia sejam propagadas para todas as outras.". Grosso modo, a integridade do *Blockchain* não permite que um documento original ou a cópia deste seja alterado intencionalmente ou não. É possível atualizar o documento apenas por meio de um novo registro e distribuir aos nós da rede.

IV – Acesso à informação

No Dicionário Brasileiro de Terminologia Arquivística (ARQUIVO NACIONAL, 2005) o acesso refere-se a uma função arquivística que visa promover o acesso e a utilização dos documentos. O acesso à informação é um direito assegurado pela Constituição Federal da República de 1988 (Art. 5º inciso XXXIII), a qual estabelece que:

> […] todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Este direito é regulamentado pela Lei 12.527/2011, a qual dispõe sobre os procedimentos necessários para garantir o direito de acesso à informação.

No *Blockchain* o acesso é disponibilizado para qualquer pessoa que se conecte à rede, mas nesse caso o acesso refere-se à possibilidade de verificar as transações que já foram ou estão sendo realizadas, incluindo o endereço do remetente e do destinatário (MOUGAYAR, 2017). Para o acesso mais detalhado da informação, é preciso ter autorização de acesso.

Considerando que os critérios de acesso no *Blockchain* devem estar de acordo com as regulamentações e normas estabelecidas, vale destacar a proposta de Cardoso e Goya (2018) quanto à utilização simultânea do *Blockchain* público e do *Blockchain* privado. Os autores propõem a utilização do *Blockchain* público para confirmar a veracidade do documen-

to, acessando apenas o código gerado pela função *hash*. No *Blockchain* privado, o acesso às informações detalhadas deve ser restrito e controlado pelas instituições reguladoras, obedecendo ao disposto na Lei 12.527/2011 (Art. 6º, inciso III) quanto à função do poder público de assegurar a proteção da informação pessoal e da informação sigilosa (BRASIL, 2011).

V – Transparência informacional

A Lei de Acesso à Informação também estabelece que a informação deve ser gerenciada de forma transparente, disponibilizando seu acesso e divulgação (Art. 6º, inciso I). No *Blockchain*, a transparência se deve ao fato de todas as operações validadas serem visíveis e replicadas para os demais nós da rede (ABREU, 2019).

Assim como o acesso, o nível de transparência oferecida pelo *Blockchain* depende de qual rede será utilizada. No *Blockchain* público, o nível de transparência é maior. Por exemplo, as operações realizadas na rede para tramitação de documentos podem ser facilmente verificadas por qualquer pessoa, acompanhando o fluxo que os documentos percorrem e visualizando dados de origem e destino do documento. No *Blockchain* privado, não há este nível de transparência, uma vez que o acesso é restrito.

4.2 Barreiras

Entre os artigos analisados, apenas dois tratam sobre as barreiras da aplicação do *Blockchain*.

Para Cardoso e Pinto (2018), a irretroatividade do *Blockchain* limita a adoção desta tecnologia frente aos requerimentos do direito contratual, bem como por parte da população. Esta barreira evidencia a impossibilidade de adequar o *Blockchain* ante o princípio arquivístico da reversibilidade, onde, segundo o Dicionário Brasileiro de Terminologia Arquivística, deve haver a possibilidade de reverter qualquer procedimento ou tratamento feito em arquivos (ARQUIVO NACIONAL, 2005).

Em relação à utilização de redes distribuídas como o *Blockchain*, Petroni e Gonçalves (2018) afirmam que ainda há necessidade de analisar a infraestrutura, tanto tecnológica quanto de pessoal, e a confiança das instituições nessas redes, para que se tornem aliados tecnológicos, visando beneficiar a sociedade. Referente à falta de confiança, Marques e Mendes (2019) explicam que só pode ser superada a partir de testes que comprovem a segurança do *Blockchain*.

Quanto à autenticidade de documentos, o CONARQ (2012) ressalta que um documento pode ser considerado diplomaticamente autêntico, ainda que seu conteúdo não seja verdadeiro. Ressalta-se nesse sentido que o *Blockchain* ainda não é capaz de assegurar a veracidade do conteúdo documental. Na Argentina, por exemplo, um documento falso referente à pandemia da COVID-19 foi validado na plataforma "Blockchain Federal da Argentina (BFA)", mesmo quando o governo já havia classificado o documento como falso (RODRIGUES, 2020). Com esta lacuna que a cadeia de blocos deixa para registro de informações falsas, percebe-se que a veracidade da informação depende da honestidade dos membros da rede.

Com a análise do funcionamento do *Blockchain*, além das barreiras já apresentadas, foram identificadas algumas das barreiras apresentadas por Freire (1991):

I – *Barreiras legais (refere-se às restrições de acesso e uso da informação)*

Para o acesso às informações privadas, a LAI estabelece que "Poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem." (Art. 31, § 1º, inciso II). É necessário estabelecer como será disponibilizada a permissão de um terceiro para visualizar a informação registrada na rede, pois no *Blockchain* apenas o proprietário (detentor da chave privada) do documento registrado na rede pode visualizar o conteúdo em sua totalidade, fator que coopera para manter a privacidade dos dados.

II – *Barreiras de tempo (refere-se ao intervalo de tempo entre a produção e a disponibilização da informação)*

a) Na rede *Blockchain* do Bitcoin, por exemplo, o tempo para validar um registro leva cerca de 60 minutos (LUCENA; HENRIQUES, 2016) e não há o registro do momento de envio do documento, apenas o registro do momento em que o documento foi adicionado na cadeia (SWAN, 2015). Isso acarreta a demora em acessar a informação e pode evidenciar uma falha quanto à transparência do *Blockchain*.

b) Por conta da obsolescência tecnológica, Swan (2015) ressalta que em relação ao arquivamento ainda não há garantias concretas de que o *Blockchain* pode preservar informações por um longo prazo. A partir disso, se torna possível compreender a criação de um protótipo de autenticação e preservação de documentos digitais, proposto por Costa *et al.* (2018), a partir da utilização da tecnologia *Blockchain* com repositórios digitais, visando à autenticação e à preservação em longo prazo. Desta forma, apesar das condições supracitadas, considera-se que o Blockchain ainda pode ser melhor explorado neste contexto, unido às estratégias de preservação de documentos digitais.

5 CONSIDERAÇÕES FINAIS

Embora o conceito da tecnologia *Blockchain* tenha sido criado há mais de 10 anos, esta pesquisa evidencia a lacuna de estudos sobre *Blockchain* no âmbito arquivístico. Ressalta-se uma demanda considerável de discussões em eventos científicos ligados às Ciências Exatas acerca da segurança de documentos e informações em meio digital. Contudo, apesar de haver uma preocupação na comunidade científica relacionada aos documentos digitais, o resultado apresentou a *Categoria I. Preservação de documentos digitais* como a categoria menos discutida nas publicações, o que pode ser explicado pela incerteza quanto à capacidade do *Blockchain* na preservação em longo prazo.

As *Categorias III. Integridade de documentos digitais* e *IV. Acesso à informação* aparecem como as categorias mais discutidas. Isto porque, uma vez que a informação atualmente é vista como matéria-prima, convém que tanto pessoas físicas quanto pessoas jurídicas possam confiar nas informações que são digitalmente compartilhadas. Quanto ao acesso, as publicações tratam do *Blockchain* para o acesso imediato à informação, visando cooperar na tomada de decisões e no desenvolvimento das instituições, objetivos estes que podem ser alcançados com a aplicação da tecnologia *Blockchain*.

Entre as publicações, observou-se que 40% das comunicações científicas abordam quase todas as categorias e outras 40% das publicações estudam elementos relacionados com todas as categorias apresentadas. Quanto à publicação que menos trata das categorias estabelecidas, pode ser justificada por abordar a tecnologia *Blockchain* em questões mais

ligadas ao rastreamento de recursos financeiros. Não havendo discussões sobre as *Categorias I. Preservação de documentos digitais e II. Autenticidade de documentos digitais.*

Por conta da obsolescência tecnológica, o *Blockchain* pode não atender de forma completa aos requisitos de acesso a documentos digitais por longo prazo. Além disso, mostrou-se necessária a criação de políticas de acesso às informações pessoais registradas em plataformas que utilizarão como base o *Blockchain*, seja em sua aplicação pública ou privada.

Se para informações detalhadas é necessário ter posse da chave privada, é importante definir como essa chave será compartilhada. Além disso, sendo o *Blockchain* uma tecnologia que reduz o processo burocrático de instituições, há que examinar com mais detalhes como o acesso às informações privadas pode ser resolvido com mais facilidade sem colocar em risco a privacidade do usuário. Dado que ainda há muito a se pesquisar sobre o *Blockchain*, principalmente na Arquivologia, as questões de acesso e privacidade podem e devem ser analisadas com mais detalhes em estudos futuros.

Outra questão que deve ser discutida é o tempo gasto durante o envio e o registro do documento. Na fase corrente dos documentos, onde a tramitação precisa acontecer com rapidez, é inviável que um documento leve cerca de uma hora para ser registrado na cadeia de blocos. Quanto à veracidade das informações registradas na rede, sugere-se a aplicação do *Blockchain* privado, onde será possível permitir que apenas usuários confiáveis, escolhidos pela instituição, possam validar os documentos na cadeia de blocos. Desta forma, há a possibilidade de garantir a ausência de informações falsas e responsabilizar o remetente por qualquer conteúdo falso registrado no *Blockchain*.

Com base no que foi apresentado, verificou-se a hipótese desta pesquisa identificando que há potencial no uso do *Blockchain* para o armazenamento seguro de documentos digitais, devido às suas características. Podendo ser uma tecnologia que, aliada às técnicas e estratégias de preservação arquivística de documentos digitais, resulte em plataformas mais adequadas para auxiliar na preservação de documentos digitais.

Verificou-se que as possibilidades de utilização do *Blockchain* na Arquivologia podem ir além da autenticidade de documentos digitais (problema levantado nesta pesquisa). O *Blockchain* pode ser uma base sólida para tramitação segura de documentos na fase corrente e um aliado para verificação de autenticidade de informações no combate a *fake news*, problema persistente no momento da elaboração desta pesquisa. Questões que poderão ser verificadas com mais detalhes em trabalhos futuros.

REFERÊNCIAS

ABREU, J. A. B. M. **A validade jurídica das provas registradas em redes blockchain no processo civil**. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/23547. Acesso em: 16 jun. 2019.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Resolução nº 511, de 11 de abril de 2019**. Altera a Resolução nº 458, de 20 de dezembro de 2017. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/2019. Acesso em: 20 maio 2020.

ARANTES JUNIOR, G. M. *et al*. BNDESToken: Uma Proposta para Rastrear o Caminho de Recursos do BNDES. *In*: Workshop em Blockchain: Teoria, Tecnologias e Aplicações, 1., 2018, Campos do Jordão. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018. Disponível em: https://sol.sbc.org.br/index.php/wblockchain/article/view/2355. Acesso em: 05 abr. 2019.

ARQUIVO NACIONAL (Brasil). **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. 232p. Publicações Técnicas; nº 51. Disponível em: http://www.arquivonacional.gov.br/images/pdf/Dicion_Term_Arquiv.pdf. Acesso em: 23 jun. 2020.

BAGGIO, C. C.; FLORES, D. Documentos digitais: preservação e estratégias. **Biblos,** v. 27, n. 1., p. 11-24, 2013. Disponível em: https://periodicos.furg.br/biblos/article/view/2654. Acesso em: 26 jun. 2020.

BATISTA, A. O. A.; DIAS, E. R. B.; SILVA, M. B; ROCHA, C. Identificação digital baseada em blockchain:Um conceito disruptivo no ciberespaço. *In*: Simpósio Internacional de Inovação em Mídias Interativas, 5., 2018, Goiânia. **Anais** [...], p. 307-320. Goiânia: Media Lab/UFG, 2018. Disponível em: https://files.cercomp.ufg.br/weby/up/777/o/28_-_Alex_Batista.pdf. Acesso em: 28 abr. 2019.

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

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 jun. 2020.

BRASIL. **Lei nº 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 29 jun. 2020.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Glossário**. 2014. Disponível em: http://conarq.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf. Acesso em: 24 jun. 2020.

CARDOSO, J. A. A.; PINTO, J. S. Blockchain e Smart Contracts: Um Estudo Sobre Soluções para Seguradoras. *In*: CONGRESSO DE GESTÃO, NEGÓCIOS E TECNOLOGIA DA INFORMAÇÃO, 2., 2018. **Anais** [...]. Sergipe: Universidade Tiradentes, 2018. Disponível em: https://eventos.set.edu.br/index.php/congenti/article/view/9618/4325. Acesso em: 06 abr. 2019.

CARDOSO, R.P.; GOYA, D. Um framework para interoperabilidade de instituições heterogêneas de ensino utilizando Blockchain. *In:* WORKSHOP @NUVEM, 2., 2018, Santo André.

Anais [...] São Paulo: Universidade Federal do ABC, 2018. Disponível em: http://nuvem.ufabc.edu.br/certificados/ii-workshop/2-workshop-nuvem-ufabc_paper_21.pdf. Acesso em: 06 abr. 2019.

CONSELHO NACIONAL DE ARQUIVOS. **Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq**. 2014. Arquivo Nacional, Rio de Janeiro. Disponível em: http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf. Acesso em: 25 jun. 2020.

CONSELHO NACIONAL DE ARQUIVOS. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf. Acesso em: 15 jun. 2020.

COSTA, R. *et al*. Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e 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/wblockchain/article/view/2356/2320. Acesso em: 03 abr. 2019.

CRUZ, J. C. *et al*. Tecnologia blockchain: um novo paradigma nas ciências abertas. *In***:** ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19., 2018, Londrina. **Anais** [...]. Paraná: Universidade Estadual de Londrina, 2018. p. 2768-2784. Disponível em: http://enancib.marilia.unesp.br/index.php/XIX_ENANCIB/xixenancib/paper/view/1522/1591. Acesso em: 05 abr. 2019.

DORNELES, S. L.; CORRÊA, R. F. Gestão de documentos digitais em aplicações de certificação digital. **Informação Arquivística**, v. 2, n. 2, p. 3-31, 2014. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/28. Acesso em 30 jun. 2020.

FREIRE, I. M. Barreiras na comunicação da informação tecnológica. **Ciência da Informação**, v. 20, n. 1, p. 51-54, 1991. Disponível em: https://brapci.inf.br/index.php/res/v/21471. Acesso em: 18 jun. 2020.

FURTADO, F. R. **L7SP**: serviços para otimizar o gerenciamento e o desempenho de Blockchain Privados. 2019. Dissertação (Mestrado em Computação Aplicada) - Universidade do Vale do Rio dos Sinos, São Leopoldo, 2019. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/8706. Acesso em: 29 jun. 2020.

GABRICH, Y. B.; COELHO, I. M.; COELHO, V. N. Tendências para sistemas microgrids em cidades inteligentes: Uma visão sobre a blockchain. *In*: SIMPÓSIO BRASILEIRO DE PESQUISA OPERACIONAL**,** 49.**,** 2017, Blumenau. **Anais** [...]. Santa Catarina, 2017. p. 1-12. Disponível em: http://www.sbpo2017.iltc.br/pdf/169695.pdf. Acesso em: 05 abr. 2019.

GATES, M. **Blockchain**: ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. 1 ed. Createspace Independent Publishing Platform, 2017. *E-book*.

GREVE, F. *et al*. Blockchain e a Revolução do Consenso sob Demanda. *IN*: VERDI, F.; UEYAMA, J.; ROSSETO, S. (Org.). **Livro de Minicursos do SBRC 2018**. 1. ed. Porto Alegre: Sociedade Brasileira de Computação, 2018. v. 1, cap. 5, p. 1-52. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770. Acesso em 30 maio 2019.

LUCENA, A. U.; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum. *In*: ENCONTRO DOS ALUNOS E DOCENTES DO DEPARTAMENTO DE ENGENHARIA DE COMPUTAÇÃO E AUTOMAÇÃO INDUSTRIAL, 9., 2016, Campinas. **Anais** [...]. São Paulo: FEEC - Unicamp, 2016. p. 1-4. Disponível em: https://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf. Acesso em: 04 abr. 2019.

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: 06 abr. 2019.

MARQUES, F. P.; MENDES, J. M. O Impacto da blockchain: desafios para a ordem jurídica e para os mercados energéticos. **Revista Videre**, v. 11, n. 22, p. 277-293, 2019. Disponível em: http://ojs.ufgd.edu.br/index.php/videre/article/view/10460/5783. Acesso em: 22 jun. 2020.

OLIVEIRA, J. A. M. M.; SEGUNDO, J. E. S. A possibilidade de identificação de violações a direitos autorais com base em metadados gerados na blockchain: avaliação da plataforma original.my. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19, 2018, Londrina. **Anais** [...]. Paraná: Universidade Estadual de Londrina, 2018. p. 5370-5378. Disponível em: http://enancib.marilia.unesp.br/index.php/XIX_ENANCIB/xixenancib/paper/view/1327. Acesso em: 21 mar. 2019.

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

NAKAMOTO, S. **Bitcoin**: A Peer-to-Peer Electronic Cash System. 2009. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 out. 2019.

NARCISO, P. H. D.; ROCHA, C. (Org). Blockchain como garantia de direitos autorais. *In*: SIMPÓSIO INTERNACIONAL DE INOVAÇÃO EM MÍDIAS INTERATIVAS, 5., 2018, Goiânia. **Anais** [...]. Goiânia: Media Lab/UFG, 2018. p. 321-325. Disponível em: https://files.cercomp.ufg.br/weby/up/777/o/29_-_Paulo_Narciso.pdf. Acesso em: 12 maio 2019.

PETRONI, B. C. A.; GONÇALVES, R. F. **Smart Contracts baseados em blockchain na cadeia de custódia digital**: uma proposta de arquitetura. *In*: The Tenth International Conference on Forensic Computer Science and Cyber Law, 2018, São Paulo. **Anais** [...] 2018. p. 23-30. Disponível em: http://icofcs.org/2018/ICoFCS-2018-003.pdf. Acesso em: 06 abr. 2019.

RODRIGUES, L. Sistema em blockchain na Argentina registra documento falso com dados do Coronavírus. **CriptoFácil**, 2020. Disponível em: https://www.criptofacil.com/sistema-blockchain-argentina-registra-documento-falso-com-dados-coronavirus/. Acesso em: 26 jun. 2020.

RONDINELLI, R. C. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2002.

SANTOS, H. M.; FLORES, D. O documento arquivístico digital enquanto fonte de pesquisa. **Perspectivas em Ciência da Informação**, v. 21, n. 4, p. 121-137, 2016. Disponível em: https://www.scielo.br/scielo.php?pid=S1413-99362016000400121&script=sci_arttext&tlng=pt. Acesso em: 30 jun. 2020.

SANTOS, H. M.; FLORES, D. Políticas de preservação digital para documentos arquivísticos. **Perspectivas em Ciência da Informação**, v. 20, n. 4, p. 197-217, 2015. Disponível em: https://www.scielo.br/pdf/pci/v20n4/1413-9936-pci-20-04-00197.pdf. Acesso em: 19 fev. 2020.

STOKES, M.; RAMOS, G. F. Smart Contracts. **Actualidad Juridica,** n. 46, p. 124-127, 2017. Disponível em: https://www.uria.com/documentos/publicaciones/5459/documento/foro_port02.pdf?id=7139. Acesso em: 05 abr. 2019.

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.

WILD, J.; ARNOLD, M.; STAFFORD, P. **Technology**: Banks seek the key to blockchain. *In*: Financial Times. 2015. Disponível em: https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64. Acesso em: 22 jun. 2020.