



GARANTIA DE INTEGRIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: uma aplicação prática de blockchain

Guaranteeing the integrity of digital records: a practical application of blockchain

CARLOS EDUARDO CARVALHO AMAND¹
BRENDA COUTO DE BRITO ROCCO²

Resumo

Este trabalho analisa o uso da tecnologia blockchain na preservação digital, com foco na garantia de integridade de documentos arquivísticos. Após revisão conceitual sobre custódia e cadeia de preservação, propõe-se a aplicação prática da blockchain como solução para reforçar a autenticidade e a confiabilidade dos documentos em arquivos públicos, sugerindo modelos de rede eficientes e novas possibilidades de pesquisa.

Palavras-chave

Preservação Digital. Blockchain. Integridade. NFT.

Abstract

This paper analyzes the use of blockchain technology in digital preservation, focusing on ensuring the integrity of archival documents. After a conceptual review of custody and preservation chain, it proposes a practical application of blockchain as a solution to strengthen the authenticity and reliability of records in public archives, suggesting efficient network models and new research possibilities.

Keywords

Digital Preservation. Blockchain. Integrity. NFT.

¹ Mestre em Gestão de Documentos e Arquivos pelo Programa de Pós-Graduação em Gestão de Documentos e Arquivos (PPGARQ) da Universidade Federal do Estado do Rio de Janeiro (UNIRIO).

² Docente Permanente do Programa de Pós-Graduação em Gestão de Documentos e Arquivos (PPGARQ) da Universidade Federal do Estado do Rio de Janeiro (UNIRIO).



1 INTRODUÇÃO

Novos tempos trazem novas tecnologias e estas devem ser exploradas ao máximo possível para que possamos obter delas o maior ganho no menor tempo, até que outras tecnologias apareçam e tornem a anterior obsoleta, nos levando então a migrar a tecnologia antiga para a mais nova. Assim é a vida na preservação digital, temos que ficar atentos, monitorando as evoluções tecnológicas para aplicá-las no melhor momento possível no nosso fazer.

É claro que aplicar novas tecnologias tem seu risco, principalmente no contexto de preservação digital onde temos que manter os documentos sob a custódia de um Arquivo Digital garantindo-lhes o “acesso e interpretação [...] pelo tempo que for necessário” (Conselho Nacional de Arquivos, 2015, p. 7) e este tempo necessário pode ser para sempre. Aplicar uma tecnologia nova antes da adoção do mercado em ambientes de preservação é um erro grave, pode trazer prejuízo para a administração do Arquivo. Esse prejuízo se aplica de forma mais significativa quando uma tecnologia absorvida pelo Arquivo não teve adoção do mercado e por consequência possui um número reduzido de fornecedores e esse número tendendo a zero. Isso implica em uma mudança para uma outra tecnologia mais recente ou para uma mais antiga, porém mais estável em um contexto mercadológico, trazendo um gasto de recursos desnecessário.

Outro problema da adoção precoce é o risco para os documentos digitais preservados por uma tecnologia cujos fornecedores estão se extinguindo do mercado, isso pode levar o Arquivo, por exemplo, a uma situação em que os documentos estão devidamente armazenados em um tipo de mídia de armazenamento, mas não se encontra mais no mercado nem o leitor da mídia novo nem peças de reposição para um leitor defeituoso.

O modelo de preservação Open Archival Information System (OAIS), atualmente recomendado para uso no Brasil pelo Conselho Nacional de Arquivos (CONARQ) através de sua Resolução nº 43, que estabelece diretrizes para a implantação de repositórios arquivísticos digitais confiáveis – RDC-Arq, prevê processos tanto para o monitoramento da tecnologia quando para a prototipação e recomendação de novos padrões tecnológicos. Esses processos são detalhados na ABNT NBR 15.472, quando da descrição da entidade funcional “planejamento de preservação” do modelo.

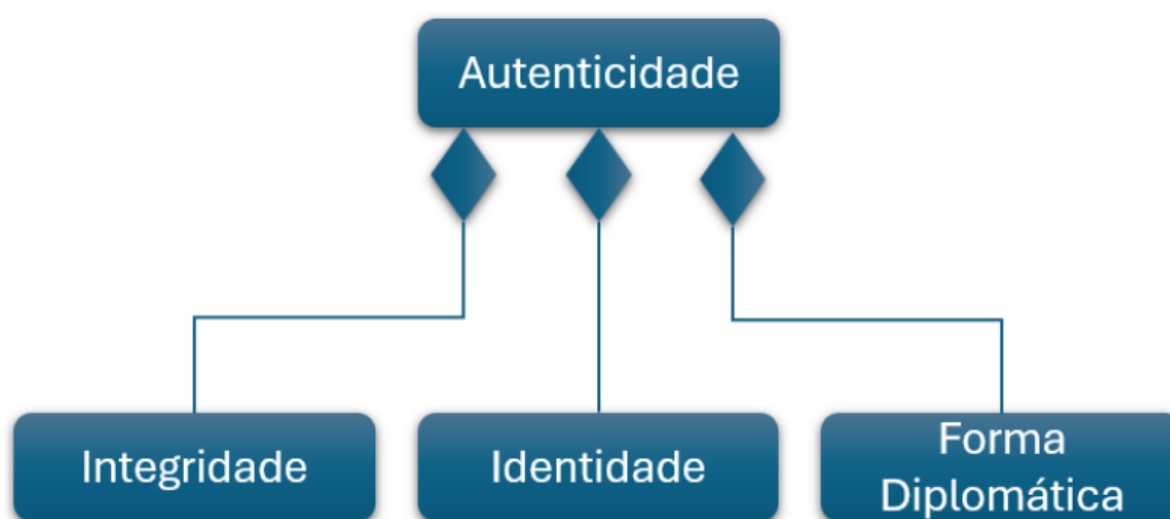
Seguindo a boa prática de monitoramento de tecnologia proposto pelo modelo OAIS (ABNT NBR 15.472, p. 29), vamos analisar aqui a tecnologia “blockchain” e sua aplicação prática na garantia de integridade de documento em meio digital.

A integridade, junto com a identidade, compõe a autenticidade dos documentos arquivísticos (InterPARES 2, 2008, p. 26) e é definida como “a qualidade de ser completo e inalterado em todos os seus aspectos essenciais. [...]” (InterPARES 2, 2008, p. 26, tradução nossa). O CONARQ (2015, p. 7) expande um pouco esta definição dizendo que integridade é o “Estado dos documentos quem se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.”.

Já Amand (2024) expande o conceito de autenticidade acrescentando a ele mais um componente, a forma diplomática, além dos já existentes, integridade e identidade. Essa ontologia é melhor ilustrada na figura 1. Neste contexto se define autenticidade como:

a qualidade de um documento de ser aquele que foi produzido, sem ter sofrido adulterações de qualquer natureza, tendo sido preservados os conjuntos de características que o tornam único no contexto a que pertence e que foram escritos ou produzidos conforme a prática do tempo e do lugar indicado no texto e assinados pela pessoa(s) competente para produzi-lo (Amand, 2024, p. 53)

Figura 1 - Componentes da Autenticidade



Fonte: Amand (2024, p. 53)

Voltando à definição do CONARQ para integridade, a qualidade de ser completo de um documento não está clara, pois esta qualidade pode se referir a completude, um termo que remete diretamente à diplomática clássica e é definido como

Completeness refer to the fact that the record possesses all the elements of intellectual form necessary for it to be capable of archiving the purpose for witch it was created. Such elements – which



include the dates associated with the record, the persons concurring in its formation, the indication of the action or matter, and the classification code[...] (McNeil, 2002, p.42)

Ou pode estar se referindo apenas a ideia de que o documento, entendido como uma unidade complexa, ou seja, composto por vários componentes digitais, como por exemplo um relatório em formato PDF, acompanhado de fotos em alta resolução em formato JPG (Conselho Nacional de Arquivos, 2022), está no momento da análise de sua integridade, com todos os componentes que tinha no momento de sua criação.

A ideia geral da completude gira em torno das necessidades jurídico-administrativas do contexto em que o documento foi criado, ou seja, quais elementos o documento precisa ter para ser efetivo no contexto em que foi criado. Na visão de MacNeil, esses elementos estão mais associados à metadados e componentes textuais do próprio documento.

Já a interpretação que entende como completo aquele documento que se manteve com todos os componentes digitais que o compunham no momento da sua criação, não se distancia tanto da visão diplomática, já que estes componentes podem ser entendidos como elementos necessários para que o documento cumpra a finalidade para o qual foi criado.

Ambas as interpretações para a qualidade de ser completo do documento apontam de alguma forma para a diplomática clássica e ficam mais bem arranjados como o componente da forma diplomática da autenticidade.

Desta forma, a definição para integridade que o CONARQ faz, se refere então, a proteção contra a adulteração ou corrupção do documento e de todos os seus componentes digitais; sendo o documento digital, se refere diretamente a manutenção da cadeia de bits original ao longo do tempo. O CONARQ explora esse aspecto ainda em 2012 ao definir integridade como:

integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos” (Conselho Nacional de Arquivos, 2012, p. 2).

Em 2015 o CONARQ, conforme citado anteriormente adiciona a ideia de evitar “alteração não autorizada nem documentada” o que nos leva explorar com mais profundidade a cadeia de preservação, antes, porém examinemos o conceito de cadeia de custódia, que é um componente a ser analisado na verificação da autenticidade de um documento.

2 CADEIA DE CUSTÓDIA

Há três abordagens para analisar o termo custódia, que nos interessa neste artigo, léxicos, jurídico e arquivístico. Todas estas são abordadas de forma brilhante pela Dra. Margareth da Silva (2015) em sua Tese intitulada "O arquivo e o lugar: a custódia arquivística como responsabilidade pela proteção aos arquivos". Em sua obra a autora identifica um núcleo comum para o termo que consiste em três elementos essenciais.

O primeiro elemento é a guarda, ou seja, a custódia significa que existe um lugar para preservar arquivos e documentos. A guarda abrange a posse, ou seja, os documentos estão retidos e preservados pelo custodiante[...].

O segundo elemento é a proteção, ou seja, os arquivos são um tipo de material que precisa ser cuidado e estar em segurança, em virtude da sua fragilidade e vulnerabilidade[...].

O terceiro elemento é o aspecto relacional entre o material custodiado e o custodiante, o que nos leva a enfatizar que a custódia é uma relação entre os documentos e as pessoas ou instituições que os preservam. (Silva, 2015, p. 46)

Na Arquivologia o termo custódia foi alvo de discussão teórica na década de 1990, pois havia duas correntes a época, uma defendida por Luciana Duranti, tendo como premissa que os princípios da Arquivologia clássica se aplicam a qualquer tipo de documento, incluindo os digitais. A outra corrente defendida por Terry Cook, onde se buscou revisar os conceitos basilares da Arquivologia clássica numa visão pós-modernista, sendo que essas correntes até hoje não encontram consenso entre si (Silva, 2015).

Analisando esses elementos, e evitando discutir a visão de custódia entre as duas correntes arquivísticas, podemos definir para este artigo que custódia é a responsabilidade legal atribuída a uma pessoa ou instituição de guardar e proteger algo em situação de fragilidade ou vulnerabilidade.

Evoluindo para o termo cadeia de custódia, o *Multilingual Archival Terminology* (MAT), base de dados terminológica do Conselho Nacional de Arquivos em português, o define como "Documento ou trilha que demonstra a sucessão de entidades coletivas ou pessoas que tiveram posse, custódia e controle sobre os documentos". Não foram encontradas referências ao termo no Dicionário Brasileiro de Terminologia Arquivística e nem no glossário publicado pelo projeto InterPARES 2, mesmo pesquisando por sua tradução em inglês (*chain of custody*), no entanto existe a seguinte menção ao termo na Resolução 43 do CONARQ "A partir da destinação para guarda permanente, ocorre



uma alteração da cadeia de custódia, passando a responsabilidade pela preservação dos documentos dos produtores para a instância de guarda.” (Conselho Nacional de Arquivos, 2015), mostrando uma associação do termo a ideia de responsabilidade pela preservação e guarda. O Glossário dos Documentos Digitais (GDD) publicado pelo CONARQ em 2020 associa o termo cadeia de custódia ao termo cadeia de custódia ininterrupta e o define como.

Linha contínua de custodiadores de documentos arquivísticos (desde o seu produtor até seu legítimo sucessor) pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração e, portanto, são autênticos. (Conselho Nacional de Arquivos, 2020)

A definição do GDD parece mesclar a definição de cadeia de custódia do MAT com a definição do termo *unbroken custody*, também dada pelo MAT e descrita como “*A traceable and uninterrupted line of care, control and usually possession of a body of records from creation to preservation that can serve as a means of protecting the authenticity of the record.*”.

Para este artigo consideramos a definição de cadeia de custódia feita no MAT por descrever a cadeia como um documento ou trilha.

Um último termos sobre custódia que faz sentindo revisar no contexto deste artigo é o de custodiador confiável, definido pelo InterPARES 2 Project como:

Preservador que pode demonstrar que não tem motivos para alterar os documentos arquivísticos preservados ou permitir que outros os alterem, e que é capaz de implementar todos os requisitos para a preservação autêntica de documentos arquivísticos. (InterPARES 2, 2011)

O termo custodiador confiável está relacionado a aquele que é “responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação” (InterPARES 2, 2011).

3 CADEIA DE PRESERVAÇÃO

Cadeia de preservação é um modelo que propõe uma sequência de atividades encadeadas desde a produção até preservação dos documentos digitais proposto pelo projeto InterPARES 2 (InterPARES 2, 2011). O modelo COP (do inglês, *Chain of Preservation*) apresenta uma série diagramas que descrevem as atividades, com suas entradas e saídas, para criar, gerir e manter documentos arquivísticos digitais autênticos durante todo se ciclo de vida (InterPARES 2, 2008).

Conforme Silva (2019) a visão do InterPARES Project 2 se baseia na ideia que:

Em virtude da vulnerabilidade intrínseca do material digital e da obsolescência tecnológica, que podem afetar a autenticidade, as ações de preservação, [...] devem ser implementadas desde o momento da criação dos documentos. Portanto todas as atividades para gerenciar os documentos no curso de sua existência estão ligadas como em uma cadeia e são interdependentes. (Silva, 2019)

O MAT em português define cadeia de preservação como um “sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo”, esta definição é a mesma encontrada no GDD.

O Arquivo Nacional do Brasil na sua Resolução n.º 38, traduzindo o material do InterPARES Project 2, prevê que o preservador deve desenvolver procedimentos que possuam controles adequados e que garantam a identidade e a integridade do documento arquivístico, esses controles devem especificamente:

Manter a custódia ininterrupta dos documentos arquivísticos;

Implementar e monitorar procedimento de segurança e controle;

Garantir que o conteúdo dos documentos arquivísticos e as anotações e elementos de forma documental não sofram alterações após a reprodução. (Arquivo Nacional Brasil, 2013)

Em outras palavras, esses procedimentos devem documentar a sucessão das entidades que tiveram custódia dos documentos e sua integridade desde sua criação e pelo tempo que for necessário. Com isso é possível concluir que a cadeia de custódia está inclusa na cadeia de preservação, esta última é responsável pela manutenção da autenticidade do documento arquivístico digital. Exploremos agora a tecnologia de blockchain e em seguida sua aplicação direta na manutenção da cadeia de preservação de documentos digitais.

4 BLOCKCHAIN

Antes de discutir o que é a tecnologia blockchain, precisamos discutir o que é confiança e como esta tecnologia muda a forma como nós confiamos, ou em quem nós confiamos. Segundo o filósofo Clóvis de Barros Filho, “você costura relações de confiança toda vez que é fiel aos valores que afirma respeitar” (Saber Filosófico, 2018), desta forma podemos entender que um custodiante confiável é aquela instituição se mantém fiel aos seus valores e é capaz de demonstrar a todos os interessados essa fidelidade. Agora o objeto desta confiança é uma instituição ou pessoa, mas e se deslocássemos o objeto que é confiável de uma pessoa ou instituição para um consenso entre várias pessoas, instituições ou computadores?



Essa é a uma das revoluções que o blockchain nos proporciona e que de certa maneira pode abalar as relações de confiança na constatação da autenticidade de um documento digital.

Blockchain, de uma forma muito resumida, é uma cadeia de blocos de informação onde cada bloco da cadeia possui um resumo criptográfico de hash do bloco anterior em sua composição. Esta cadeia de informação em blocos está distribuída em cada computador que participa desta rede de informações, isto é, cada componente ou nó desta rede possui uma cópia da cadeia de blocos. Para que um novo bloco de informação seja incluído na cadeia, deve haver um consenso entre os participantes da rede, ou seja uma aprovação distribuída.

Para entender melhor essa definição revisemos o conceito de resumo criptográfico, ou hash, que é o resultado da aplicação de uma função de hash unidirecional, estas funções “mapeiam uma massa de dados de tamanho variável para uma sequência de tamanho fixo de bits” (Serafim, 2002, p. 34). É importante lembrar que um resumo criptográfico é único para uma massa de dados, sendo assim qualquer alteração na massa de dados de entrada gera um resumo diferente.

Para exemplificar a aplicação prática dessa técnica criptográfica em uma cadeia de blocos, imaginemos que temos uma cadeia de blocos de informação onde cada bloco possui o registro de uma venda, com isso temos uma simples lista de vendas onde para alguém mal-intencionado alterar alguma informação bastaria apagar a informação e escrever uma nova. Agora, e se cada bloco contivesse além do registro da venda o resumo criptográfico do bloco anterior? Para que uma informação no meio dessa cadeia fosse alterada, seria necessário alterar todas os blocos que foram inseridos depois do bloco alterado, pois todos os resumos criptográficos seriam necessariamente diferentes.

Uma outra dificuldade imposta pelo blockchain para mudança de dados históricos é a distribuição da informação entre vários nós da rede, pois a tecnologia funciona sobre uma rede *Peer-to-Peer* (P2P) que é:

O conjunto de computadores conectados com nós em uma topologia em eterna expansão. [...] Todo nó roda o mesmo software, fornecendo redundâncias inerentes a toda a rede, o que significa que, se um nó para de funcionar ou não responde, o trabalho dos outros nós o compensará. (Mougayar, 2017, p. 137)

Isso significa dizer que para alguém alterar o histórico de um registro é preciso ter acesso não apenas a base de dados de um custodiante da informação, mas também ter acesso a todas as bases de dados dos computadores da rede e ter permissão de

escrita nelas. Neste sentido com essa tecnologia deslocamos a confiança de um custodiante confiável para a tecnológica que mantém os dados de forma distribuída.

Mais uma base do blockchain que devemos explorar é que um nó da rede P2P pode solicitar o registro de mais uma informação nos blocos, isso implica que a rede deve validar se aquele novo bloco de informação está íntegro e pode ser isso inserido no registro imutável de blocos. Esse processo de validação em rede nos leva ao conceito de protocolo de consenso.

Os protocolos de consenso são um conjunto de regras e procedimentos que permitem que uma rede descentralizada, como uma blockchain, alcance um acordo sobre a validade das transações que ocorrem da rede. Eles são essenciais para garantir a integridade da rede, pois permitem que todos os "nós" na rede concordem sobre o estado atual da blockchain, evitando a ocorrência de atividades maliciosas[...] (Montezino, 2023, p.17)

Existem vários tipos de protocolo de consenso, mas não é objetivo deste artigo descrever todas as tecnologias envolvidas no blockchain, neste caso vamos nos ater ao fato que em uma rede blockchain todos os nós precisam entrar em um acordo sobre a validade de uma transação deslocando a confiança de uma única instituição para o consenso entre os componentes da rede.

Outro aspecto da blockchain que precisamos esclarecer é que ativos digitais que não estão em uma rede blockchain podem ter um representante seu dentro da rede. Este representante pode ser alvo de transações dentro da rede, eles são chamados de *Non-Fungible Token* (NFT) ou em uma tradução direta para o português, token não fungível.

Um NFT é um tipo de ativo digital que é registrado em uma blockchain tornando-se uma espécie de certificado de autenticidade e propriedade do item digital.

Por Exemplo, um NFT pode representar um arquivo de áudio, vídeo, imagem arte digital ou qualquer outro tipo de conteúdo digital. Ao possuir o NFT, o proprietário detém a prova de autenticidade e exclusividade do arquivo digital em questão. (Whosoever, 2023)

A característica de um NFT de ser não fungível quer dizer que ele é único, não há algo que se compare a ele, logo não pode ser trocado por algo de igual valor, uma característica que também é associada a um documento arquivístico, que é único dentro de seu contexto.

No que toca a forma como os blockchains se apresentam, existem 4 tipos de redes: blockchains públicas, privadas, *consortium* e híbridas (Montezino, 2023). As públicas são aquelas em que qualquer pessoa ou instituição pode participar, o banco



de dados é compartilhado e as transações usam protocolos de consenso. Uma blockchain privada assim como a pública é descentralizada, no entanto apenas pessoas ou instituições permissionadas podem participar, a gestão da rede é centralizada dentro de uma única instituição que pode participar da rede, quem tem a cópia do banco de dados e quem pode validar ou fazer transações.

A blockchain *consortium* é uma rede privada que é administrada por mais de uma instituição e a blockchain híbrida combina uma rede privada com uma pública, permitindo a participação pública e de membros selecionados, cabe a gestão da rede definir quais processos são públicos e quais processos podem se executados apenas por membros selecionados.

5 UMA APLICAÇÃO PRÁTICA

De maneira prática, a tecnologia de blockchain pode ser usada para incrementar o nível de garantia da autenticidade de documentos arquivísticos digitais sendo usada para registrar a cadeia de preservação dos documentos digitais. A estratégia para aplicação seria a seguinte:

- a) criar um NFT em uma rede blockchain para cada componente digital de um documento arquivístico e um NFT para cada documento em si;
- b) Registrar cada evento de preservação em um componente digital que compõe o documento arquivístico e/ou separadamente dentro da blockchain.
- c) Gerir cadeia de custódia do documento através de transações com as NFTs dos documentos.

Para criar a NFT de um componente digital de um documento deve-se escolher uma plataforma de blockchain e criar uma carteira digital na plataforma sob responsabilidade da instituição que possui a custódia legal do documento em questão. Essa carteira virtual é um registro que associa a identidade de alguém na rede blockchain as posses desse mesmo alguém.

Uma instituição que tenha uma carteira digital pode fazer o upload dos componentes digitais de um documento digital e a partir deles gerar um conjunto de NFTs que representam esses componentes sob sua posse. Um último componente digital deve ser gerado representando o documento digital como um todo, isto é, a soma de seus componentes digitais. Este componente deve conter a lista de resumos criptográficos de hash de cada componente digital do documento a ser representado. Por fim um NFT é gerado para este último componente.

A cadeia de preservação pode ser implementada como um componente digital que lista os eventos de preservação, atualmente o padrão usado para esse registro é um

documento em XML seguindo o dicionário de dados para metadados de preservação PREMIS construído pela *Library of Congress*. Cada evento descrito nesta trilha pode ser registrado em uma blockchain de maneira isolada ou pode-se gerar um NFT novo do componente com a cadeia de preservação e do componente que representa o documento arquivístico como um todo a cada nova atualização dos eventos de preservação.

A cadeia de custódia pode ser registrada dentro da própria blockchain, como o documento passa a ser representado por um NFT dentro da rede, o NFT possui um proprietário associado a carteira digital onde o NFT está alocado. Para que a custódia legal do documento mude e seja registrada de forma permanente, basta a realização de uma transação que transfere um conjunto de NFT de uma carteira digital para outra.

As transações com NFTs representando documentos digitais podem aumentar a confiança na autenticidade de documento digitais tirando a responsabilidade da manutenção dos registros que sustentam a autenticidade do documento de um custodiante confiável para a uma rede de confiança distribuída entre os nós de uma rede blockchain. A cadeia de preservação não estaria apenas sendo protegida pela instituição que detém a custódia legal do documento, a proteção desta cadeia seria feita pelo consenso entre uma rede P2P, criando assim uma cadeia de preservação compartilhada.

6 CONSIDERAÇÕES FINAIS

A aplicação prática deste artigo é apenas uma introdução de como a blockchain pode contribuir para os processos de gestão e preservação documento arquivísticos digitais, muitas outras aplicações podem ser levantadas para aplicação da tecnologia em documentos de arquivo. Pode-se pensar por exemplo em uma rede privada entre instituições de arquivo para criar NFTs ou registrar transações, reduzindo o custo de energia por transação.

A rede privada poderia ser expandida para uma rede híbrida onde qualquer usuário poderia consultar a autenticidade de um documento, mas apenas as instituições produtoras podem criar ou transferir as NFTs de documentos. Esta última configuração pode eliminar a atuação de cartórios na autenticação de documentos.

Pessoas podem usar a blockchain para assinar documentos com irrefutabilidade garantida pela própria rede sem a necessidade de usar uma infraestrutura de chaves públicas para isso. A rede registraria as assinaturas de forma permanente estando a conferência da assinatura disponível a todos os participantes da rede, além dos dados da assinatura estarem separados fisicamente do documento.



Outros aspectos da tecnologia, como contratos inteligentes, que são blocos de informação programáveis podem ser explorados para programar nos próprios documentos ações de preservação a serem executadas no futuro.

A própria definição de documento arquivístico digital pode ser posta à prova quando confrontada com um contrato inteligente programado em uma blockchain, pois este contrato deixa de ser algo estático, cuja ação para se executar alguma de suas cláusulas depende uma pessoa, para ser algo dinâmico onde suas cláusulas são executadas de forma automática sem a necessidade de interferência humana.

Muitas são as possíveis aplicações desta tecnologia que podemos aguardar para o futuro, mas destas talvez a mais impactante seja uma conceitual: o deslocamento do objeto de confiança de uma pessoa ou instituição para o consenso entre uma rede de pessoas e instituições.

REFERÊNCIAS

ABNT. **ABNT NBR 15.472:2007** – Sistemas especiais de dados e informações – Modelo de referência para um sistema aberto de arquivamento e informação (SAAI). Rio de Janeiro: ABNT, 2007.

AMAND, Carlos Eduardo Carvalho. **Proposta para um modelo de requisitos para sistemas gerenciadores de repositórios arquivísticos digitais confiáveis**. Dissertação (Mestrado em Gestão de Documentos e Arquivos) Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2024.

CONSELHO NACIONAL DE ARQUIVOS (BRASIL). **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Arquivo Nacional, 2012.

_____. **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq**. Rio de Janeiro: Arquivo Nacional, 2015.

_____. **E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos Versão 2**. Rio de Janeiro: Arquivo Nacional, 2022.

DURANTI, L, EASTWOOD, T.; MACNEIL, H. **Preservation of the Integrity of Electronic Records**. Dordrecht: Kluwer Academic Publishers Group, 2002.

INTERNATIONAL COUNCIL ON ARCHIVES. **Multilingual archival terminology**. Disponível em: <http://www.ciscra.org/mat/>. Acesso em: 14 jul. 2023.

INTERPARES 2 Project. **Diretrizes do produtor** – A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Tradução de Câmara de Deputados e Arquivo Nacional. Rio de Janeiro: Arquivo Nacional, 2011b.

_____. "The InterPARES 2 Project Glossary," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008). Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_book_glossary.pdf. Acesso em: 14 jul. 2023.

MONTEZINO, Richard. **Blockchain - Da teoria à prática**: Tudo o que você precisa saber sobre a tecnologia que está revolucionando o mundo. Edição do Kindle, 2023.

MOUGAYAR, William. **Blockcahin para negócios**: Promessa, Prática e Aplicação da Nova Tecnologia da Internet. Rio de Janeiro: Alta Books, 2017.

PREMIS EDITORIAL COMMITTEE. **Data Dictionary for Preservation Metadata**: PREMIS version 3.0, 2015. Disponível em: <http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf>. Acesso em: 21 jul. 2023.

SABER FILOSÓFICO, **Como construir relação de confiança – Clóvis de Barros Filho**. YouTube, 14 de junho de 2018. Disponível em https://www.youtube.com/watch?v=A_Mb7I7vPN8. Acesso em: 21 de jul. de 2023.

SERAFIM, Vinícius da Silveira. **Um verificador seguro de integridade de arquivos**, 2012. Disponível em: <http://hdl.handle.net/10183/2756>, Acesso em: 21 de jul. de 2023.

SILVA, Margareth da. **O arquivo e o lugar**: a custódia arquivística como responsabilidade pela proteção aos arquivos. 2015. Tese (Doutorado em História Social) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2015. Disponível em: <https://doi.org/10.11606/T.8.2015.tde-22122015-093801>. Acesso em: 13 jul. 2023.

_____. Custodia, cadeia de preservação e custodiante confiável: conceitos para a preservação de documentos digitais autênticos. **Revista Conhecimento em Ação**, 4(2), 46-64. Disponível em: <https://doi.org/10.47681/rca.v4i2.30291>. Acesso em: 21 jul. 2023.

WHOSOEVER, Angelo. **NFT OPEN BOX**: do Zero ao mercado multimilionário da WEB3. Edição do Kindle, 2023.

Recebido em 31/10/2025

Aprovado em 14/11/2025



Licença de Atribuição BY do Creative Commons
<https://creativecommons.org/licenses/by/4.0>