ARCHEION ONLINE
ISSN 2318-6186
Revista de Arquivologia da UFPB

Edição Especial CNA 2024

***BLOCKCHAIN, SMART CONTRACTS E NON-FUNGIBLE TOKEN* (NFT):** A tríade Paradigmática no âmbito dos documentos acadêmicos

***BLOCKCHAIN, SMART CONTRACTS AND NON-FUNGIBLE TOKEN* (NFT):** The paradigmatic triad in the context of academic records

Alexandre Fernal*
Rodrigo Eduardo Botelho Francisco**
Gustavo Resende da Costa***
Paula Hara da Silva****
Telma Campanha de Carvalho Madio*****
André Vieira de Freitas Araújo******

RESUMO

As Instituições de Ensino Superior no Brasil foram impelidas a migrar os documentos do ambiente informacional analógico para o informacional digital, conforme disposto na Portaria n.º 613/2023, do Ministério da Educação. Dessa forma, em tempos hodiernos, surgem tecnologias, tais como: *blockchain, smart contracts* e *non-fungible token*. Logo, essas poderão ser aplicadas nos documentos produzidos nas instituições de ensino superior no Brasil e questiona-se, portanto, quais as possíveis aplicações das tecnologias *blockchain*, *smart contracts e non-fungible token* nos documentos arquivísticos digitais no âmbito acadêmico no Brasil. Objetiva-se relacionar as possíveis aplicações das tecnologias *blockchain, smart contracts e non-fungible token* no contexto da arquivologia, especificamente nos documentos de acervos acadêmicos. Para tanto, utilizou-se como metodologia a pesquisa bibliográfica, documental, qualitativa e exploratória. A coleta de dados sucedeu-se por intermédio da literatura nacional e internacional em livros, artigos, dissertações, teses e normativas no idiomas português e inglês. Como resultado, verificou-se que o protocolo *blockchain* criptografa, envia e valida transações, que propiciam registro cronológico inalterável de todas as operações realizadas. Assim, torna-se exequível aplicação da tecnologia *blockchain* em conjunto com os *smart contracts*, em vista de que essa tecnologia poderá produzir documentos de forma automática, por meio de linhas de códigos auto executáveis, as quais produzem tipos documentais específicos do domínio acadêmico. Por fim, a tríade de tecnologias disruptivas é consolidada com aplicação do *non-fungible token*, em concomitância com o conglomerado *blockchain* e *smart contracts*, posto que este garante a originalidade do documento arquivístico digital, por intermédio da tokenização.

Palavras-chave: *Blockchain; Smart Contracts; Non-Fungible Token.*

* Professor. Doutor. E-mail: alexandre.fernal@gmail.com:
** Professor. Doutor. E-mail: rodrigobotelho@ufpr.br
*** Técnico Administrativo. Mestre. E-mail: resende@ufpr.br
**** Técnico Administrativo. Graduada em Gestão da Informação. E-mail: paulah@ufpr.br
***** Professora. Doutora. E-mail: telma.madio@unesp.br
****** Professor. Doutor. E-mail: andre.freitas@ufpr.br

ABSTRACT

Higher Education Institutions in Brazil were forced to migrate the records from the analog information environment to the digital information environment, as provided for in Ordinance no. 613/2023, of the Ministry of Education. Thus, in modern times, technologies such as blockchain, smart contracts and non-fungible tokens have emerged. Therefore, these can be applied to documents produced in higher education institutions in Brazil and, therefore, the question arises as to what are the possible applications of blockchain, smart contracts and non-fungible token technologies in digital records in the academic field in Brazil. The objective is to relate the possible applications of blockchain, smart contracts and non-fungible token technologies in the context of archival science, specifically in documents from academic collections. To this end, bibliographic, documentary, qualitative and exploratory research was used as a methodology. Data collection took place through national and international literature in books, articles, dissertations, theses and regulations in Portuguese and English. As a result, it was found that the blockchain protocol encrypts, sends and validates transactions, which provide an unalterable chronological record of all operations performed. Thus, it becomes feasible to apply blockchain technology in conjunction with smart contracts, since this technology can produce documents automatically, through self-executing lines of code, which produce specific types of records in the academic domain. Finally, the triad of disruptive technologies is consolidated with the application of the non-fungible token, in conjunction with the blockchain and smart contracts conglomerate, since the latter guarantees the originality of the digital archival document, through tokenization.

Keywords: Blockchain; Smart Contracts; Non-Fungible Token.

1 INTRODUÇÂO

Na contemporaneidade, com o advento das tecnologias da informação e comunicação (TIC), emergem tecnologias disruptivas, tais como: o *blockchain, smart contracts* e *non-fungible token* (NFT). A tecnologia *blockchain* possui como cerne a distribuição de registros em sistemas de consenso descentralizados e toma, por base, rede ponto a ponto – *peer to peer* (P2P), a qual opera sem autoridade central, em oposição à arquitetura centralizada, cuja base é o cliente/servidor. A tecnologia *blockchain* apresenta-se como ruptura paradigmática no que diz respeito às questões relacionadas a autenticação, integridade e identidade dos registros, posto que esses encontram-se descentralizados nos ambientes informacionais digitais e armazenados nas nuvens. Nessa direção, os *smart contratcs* são linhas de códigos computacionais, que podem ser armazenados no *blockchain*; são auto executáveis e dispõem de características próprias,

ou seja, é independente de ações das partes interessadas no contrato. Já os NFTs, estes são protocolos, que garantem a unicidade e originalidade de ativos, isto é, são *tokens* utilizados para representar a propriedade de itens exclusivos e podem ser registrados em *blockchain*.

Assim, essa tríade paradigmática supracitada dispõe de essência focada nos sistemas distribuídos. Torna-se, nessa conjuntura, relevante para garantia da transparência e integridade dos documentos arquivísticos digitais (DAD), bem como os documentos digitalizados, isto é, os representantes digitais. A seção 2 apresenta a tríade de tecnologias disruptivas, quais sejam: *blockchain, smart contracts e* NFT.

2 BLOCKCHAIN, SMART CONTRACTS E NON FUNGIBLE TOKEN (NFT)

Essa seção, inicialmente, apresenta os conceitos básicos a respeito da criptografia e função *hash,* que são pré-requisitos altamente desejados e necessários para a compreensão da certificação digital e da tecnologia *blockchain*. O certificado digital para o Instituto Nacional de Tecnologia da Informação (ITI) consiste no registro eletrônico digital assinado, o qual é gerado por intermédio de procedimento da certificação digital, que comprova as relações entre chaves criptográficas (Brasil, 2021).

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

Logo, a assinatura digital é:

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

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

Certificadora (AC), a qual é a entidade responsável por emitir e garantir a validade do certificado.

O certificado digital da Infraestrutura de Chaves Públicas – Brasil (ICP Brasil), além de personificar o cidadão na rede mundial de computadores, garante, por força da Lei n.º 14.063/2020, validade jurídica aos atos praticados com seu uso (Brasil, 2020). A ICP-Brasil trabalha com hierarquia, na qual a Autoridade Certificadora Raiz (AC Raiz) é o ITI, autarquia federal vinculada a Casa Civil da Presidência da República.

Nesse contexto, o ITI é o responsável por gerar as chaves da AC e regulamentação de atividades de cada uma. A série S reúne certificados com sigilo, os quais são utilizados na codificação de documentos de base de dados, mensagens e outras informações eletrônicas sigilosas. Todas as séries são diferenciadas por seu uso, nível de segurança e de validade (Resende, 2009). Segundo Barboza (2018), no Brasil, os tipos de certificados mais usados são os tipos A1 e A3. O certificado digital A1 é o de menor segurança, o qual é gerado e armazenado no próprio computador. Os dados são protegidos por senha de acesso e somente é possível acessar e mover com a chave privada associada. Caso a chave privada seja perdida, novo certificado deverá ser adquirido e todas as etapas deverão ser refeitas pelo usuário.

O certificado do tipo A3 grava-se em dispositivos eletrônicos próprios, como *token* ou *smart card*. Portanto, a chave privada pode ser transportada de maneira segura para realização de transações eletrônicas, com garantia e integridade das informações. A partir do momento que for necessário, quando algo assinado for enviado à AC, com tipo de certificado diferente, tornaria-se um problema administrar todos os formatos diferentes. Para resolver esse problema, foi criado e aprovado pela *International telecomunication Union* (ITU), padrão para certificado, chamado de X-509, cujo uso está bem difundido (Tanebaum, 2003).

Assim como na criptografia assimétrica, a assinatura digital consiste na sequência de números resultantes de determinada operação matemática conhecida como função *hash*. Essa função analisa todo o documento ou arquivo, com a base no algoritmo matemático, que gera tamanho específico em *bytes*, que representa o documento, também conhecido como resumo. A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, posto que os algoritmos de criptografia assimétrica, ainda, são muito lentos (Monteiro; Mignoni 2007).

Archeion Online, João Pessoa, v.13 n. Edição Especial: X CNA - Congresso Nacional de Arquivologia. p. 106-122, jan./mar. 2025.
DOI - 10.22478/ufpb.2318-6186.2025v13nEdição Especial.72550
ISSN 2318-6186. Licença

A Medida Provisória n.° 2.200-2/2001 foi o marco inicial, que possibilitou garantir a validade jurídica dos documentos digitais e a utilização de certificados digitais para atribuir autenticação aos documentos. Esse fato tornou o certificado digital instrumento juridicamente válido em todo território nacional (Brasil, 2001).

O prelúdio da tecnologia *blockchain* ocorreu 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 a *International Busines Machine* (IBM), armazenavam seus dados em grandes bancos de dados (Cesar, 2020). Nessa direção, nos anos 1990, o criptógrafo norte-americano David Lee Chaum foi pioneiro na criação da primeira moeda *on-line* na Holanda (Narayanan *et al*., 2016). Denominada o *DigiCash*, esta consistia na extensão de algoritmo criptográfico conhecido como Rivest, Shamir, Adleman (RSA), que inicialmente despertou o interesse de várias instituições financeiras em seu uso. Porém, o acúmulo de erros administrativos ao longo do ciclo de vida do *DigiCash* culminou na sua decadência e, por conseguinte, no seu desaparecimento do mercado em 1998 (Narayanan *et al*., 2016; Reiff, 2022).

Já a segunda geração de dinheiro digital na *internet* apropriou-se das experiências do *DigiCash*. Dentre os sistemas para pagamentos monetários baseados na *internet*, destacou-se o *paypal*, que oferecia aos usuários a possibilidade de utilizar dinheiro nas plataformas de navegadores *web* (Perset, 2010; Ningtias *et al*., 2023). O *paypal* foi capaz de realizar, pela primeira vez, a transferência de recursos financeiros *on-line,* por meio de rede *peer to peer* – ponto a ponto (P2P) (Perset, 2010).

Finalmente, o evento que transformou o contexto das criptomoedas foi a crise das hipotecas conhecida como *subprime,* em 2008, nos Estados Unidos da América (EUA), a qual quase neutralizou o sistema financeiro daquele país. Sabe-se, também, que essa provocou problemas significativos para grande maioria das instituições financeiras. Consequentemente, esse evento catastrófico, com viés monetário, despertou o alerta para as principais economias globais, que culminou na conjuntura necessária para o surgimento da tecnologia que viera a ser conhecida como *blockchain* (Barkatullah; Hanke, 2015).

A tecnologia *blockchain* surgiu em 2008, com a publicação do artigo *Bitcoin*: *a peer-to-peer eletronic cash system*. O autor ou seus autores utilizaram o pseudônimo conhecido por Satoshi Nakamoto, para apresentar a tecnologia e cunhou-se, assim, o

conceito de *blockchain* e *bitcoin*. A pesquisa supracitada apresenta os princípios fundamentais e o funcionamento do *blockchain* com sua aplicação em criptomoedas (Nakamoto, 2008).

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

O *blockchain,* enquanto tecnologia, pode ser compreendido em três tipos principais, quais sejam: *blockchain* 1.0, *blockchain* 2.0, *blockchain* 3.0. A primeira categoria refere-se às criptomoedas e atividades no contexto de pagamentos digitais. Já o segundo tipo, refere-se ao setor financeiro com associação da *internet of things* (IoT) – *internet* das coisas, as tecnologias de *smart contracts* – contratos inteligentes com aplicações para ativos econômicos e financeiros. Por fim, a terceira diz respeito a outros domínios, como governo, saúde, cultura e arte (Swan, 2015).

Nessa direção, os *smart contracts* é comumente compreendido como tecnologia disruptiva, entretanto, seu surgimento foi em 1996, proposto por Nicholas Szabo, com a publicação do artigo *Smart contracts: Building blocks for digital markets*. Os *smart contracts* são algoritmos, que definem os requisitos obrigatórios a serem executados por determinada transação, os quais são realizados de forma autônoma para o cumprimento das operações pré estabelecidas, nas linhas de código (Szabo, 2011).

Assim, os *smart contracts* podem ser executados em conjunto com a tecnologia *blockchain*, na qual as linhas de códigos podem gerar *hashes, que, por sua vez,* podem ser armazenados nas bases de dados distribuídas e não sofrem quaisquer modificações. As operações propostas pelo *smart contracts* poderão ser asseguradas pelo protocolo *blockchain,* já que as cadeias de blocos são imutáveis e, como consequência, é praticamente impossível realizar modificações nos blocos validados (Tapscott; Tapscott, 2016).

O NFT configura-se como tipo de certificação digital, a qual poderá ser estabelecida por intermédio da tecnologia *blockchain*, que garante a exclusividade e originalidade. Dessa forma, o NFT consiste em unidade de informação digital, a qual é denominada de *token* e poderá ser armazenada em *blockchain*. Já a terminologia fungível tem sua concepção no domínio econômico e contábil, cuja definição é qualquer elemento que seja intercambiável com objeto semelhante ou idêntico. O conceito de *NFT* emana da tecnologia *blockchain*, que foi utilizado, inicialmente, na primeira aplicação de critptomoedas, denominada *bitcoin* (Chohan, 2021).

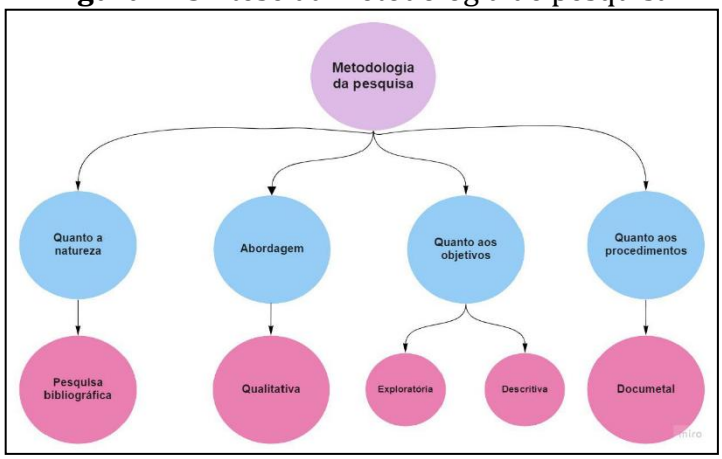
Observa-se que os *fungible tokens* podem ser trocados por outros itens, são idênticos entre si e possibilitam ser divididos em unidades menores. Por outro lado, os NFTs não podem ser substituídos por outro token. O NFT é único com informações e atributos distintos, os quais os tornam diferenciados de outros e são impossíveis de serem trocados (Bal; Ner, 2019).

A seção 3, na sequência, apresenta a metodologia definida para essa pesquisa a respeito da tecnologia *blockchain*, *smart contracts* e NFT, a tríade paradigmática no contexto da Arquivologia e nas conjunturas dos documentos acadêmicos.

3 METODOLOGIA

A pesquisa científica, de acordo com Marconi e Lakatos (2008, p. 157), é "considerada um procedimento formal com método de pensamento reflexivo que requer tratamento científico e se constitui no caminho para se conhecer a realidade ou para descobrir verdades parciais". Nessa direção, caracteriza-se o presente estudo como pesquisa teórica, exploratória, de abordagem qualitativa e documental. A Figura 1, a seguir, representa a síntese da metodologia de pesquisa adotada.

Figura 1: Síntese da metodologia de pesquisa



Fonte: Os autores (2024).

Os procedimentos da pesquisa são bibliográficos, posto que buscam aclarar o problema a partir de referências teóricas publicadas em artigos científicos, livros, dissertações e teses. A abordagem é qualitativa, posto que qualquer pesquisa que produza resultados não alcançados por meio de procedimentos estatísticos, considera-se qualitativa (Magalhães, 2007). Quanto aos objetivos, é exploratória, visto que este tipo de pesquisa tem por enfoque familiarizar-se com o fenômeno ou obter nova percepção e descobrir novas ideias. Nesse sentido, Marconi e Lakatos (2008, p. 3) afirmam que "Toda pesquisa deve basear-se em uma teoria, que serve como ponto de partida para a investigação bem sucedida de um problema." A presente pesquisa surgiu com base nesses pressupostos, com o intuito de ampliar o conhecimento acerca da temática dos estudos das tecnologias *blockchain, smart contracts* e NFT, no âmbito documentos acadêmicos das IES no Brasil.

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

A seção 04, a seguir, dispõe da análise e discussão dos resultados acerca da aplicação da tríade paradigmática, a saber: *blockchain, smart contracts* e NFT, no contexto dos documentos acadêmicos das IES no Brasil.

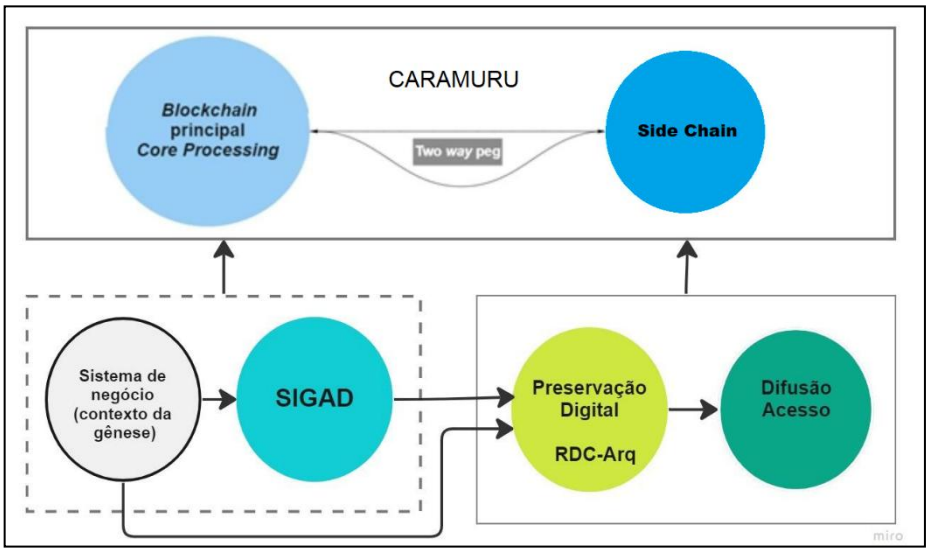
4 A TRÍADE PARADIGMÁTICA NO ÂMBITO DOS DOCUMENTOS ACACÊMICOS: *BLOCKCHAIN, SMART CONTRACTS* E *NON-FUNGIBLE TOKEN* (NFT)

O Ministério da Educação (MEC), instituiu por meio do Decreto n.º 9.235/2017, "[...] o exercício das funções de regulação, supervisão e avaliação das instituições de educação superior e dos cursos superiores de graduação e de pós-graduação no sistema federal de ensino" (Brasil, 2017, p. 01). Esse Decreto determina a obrigatoriedade de migração dos documentos analógicos para o ambiente informacional digital por meio da digitalização, conforme disposto na Portaria n.º 613/2023 (Brasil, 2023). Assim, o contexto da gênese dos documentos deverá ser, obrigatoriamente, o ambiente informacional digital, o que culmina, exclusivamente, na produção de DAD e na digitalização dos documentos analógicos.

A ascensão dos DAD e dos representantes digitais, no contexto das IES no Brasil, implicou o surgimento de paradigmas, ocasionados pelas anomalias das TIC, posto que, nesse cenário, surgem tecnologias disruptivas, as quais impactam o fazer arquivístico no âmbito digital.

Logo, propõe-se um possível modelo lógico para autenticação distribuída, denominado *Caramuru*, que surge com base na tecnologia *blockchain* no âmbito da arquivologia, desde o contexto da gênese dos documentos, até a sua destinação final. A Figura 2 apresenta o modelo lógico de aplicação da tecnologia *blockchain* na autenticação descentralizada de documentos acadêmicos

. **Figura 2:** Modelo lógico *Caramuru*



Fonte: Os autores (2024).

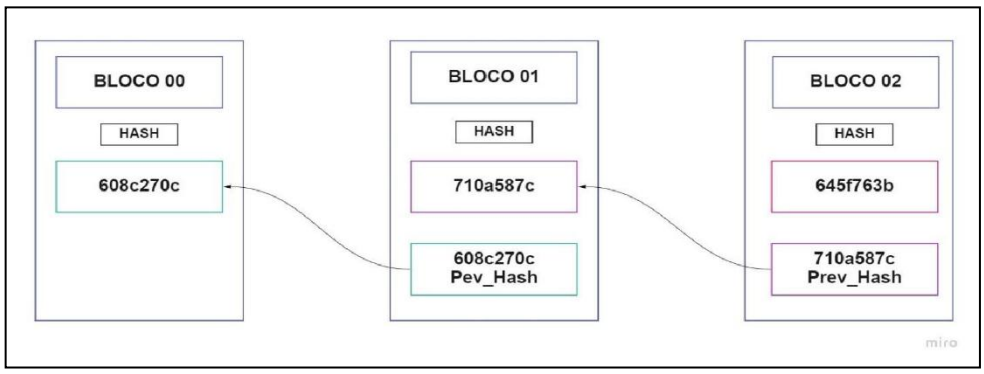
Conforme representado na Figura 2, o modelo proposto para autenticação inicia-se no contexto de gênese, isto é, quando é produzido documento nato-digital na conjectura dos sistemas de negócios, o qual gera resumo criptográfico para o DAD por meio de função *hash.* Esse resumo consiste em metadado do tipo *string*, em que inicia o bloco gênesis, o *root hash;* o bloco 00 fica armazenado no *core processing*.

Após o DAD ser produzido nos ambientes de negócios, faz-se necessário realizar a gestão documental no Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), o qual segue os requisitos do e-ARQ Brasil. Posteriormente, é realizado o recolhimento do DAD para o ambiente de preservação, o repositório arquivístico digital confiável (RDC-Arq) e acesso/difusão.

Logo, gera-se o *root hash* na gênese documental, e, ao longo do ciclo de vida do documento, são gerados outros *hashes*, principalmente no momento em que há o recolhimento do SIGAD para o ambiente de preservação, cujos *hashes* constituem blocos. Esses, por sua vez, serão validados e adicionados na cadeia de blocos de forma permanente, com o objetivo final de criar a trilha de auditoria.

A Figura 3 demonstra a aplicação detalhada do modelo lógico *Caramuru*, com base na tecnologia *blockchain* na autenticação distribuída dos documentos acadêmicos em seu ciclo de vida, o qual compreende o *main blockchain* – *core processing* e o *sidechain.*

Figura 3: Aplicação detalhada do modelo lógico *Caramuru* na autenticação distribuída



Fonte: Os autores (2024).

A Figura 3, cujo objetivo é produzir a trilha de auditoria ininterrupta e imutável ao longo do ciclo de vida dos documentos, poderá ser utilizada, ainda, para verificação da proveniência. O bloco 00 é o bloco gênesis, bloco inicial que contém o *root hash* referente

ao DAD nos sistemas de negócio, no caso a função *hash.* Isto é, o resumo criptográfico do DAD, representado por meio de metadado, qual seja: 608c270c.

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

Nesse sentido, demonstrou-se, por intermédio da Figura 3, as questões relacionadas à autenticação distribuída de documentos acadêmicos, a qual poderá utilizar-se dos *sidechains,* com intuito de auxiliar na construção das cadeias de blocos, bem como produzir as trilhas de auditorias para fins de verificação da proveniência. O resumo inicial – *root hash,* é obtido por intermédio de algoritmo de função *hash,* que foi aplicado no DAD.

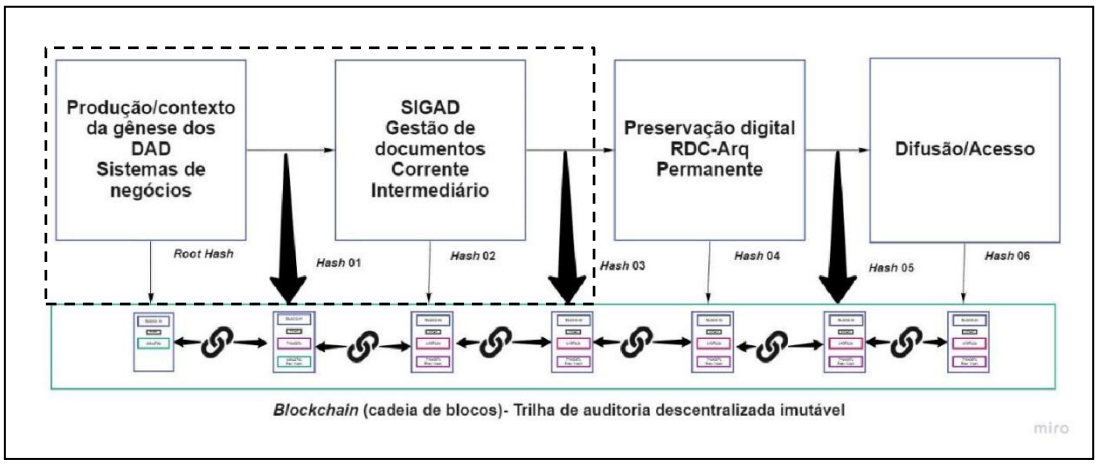
Com base no metadado supracitado, isto é, 608c270c, referente ao bloco 00 – gênesis, é possível garantir autenticação, em vista de que, ao comparar o DAD com o resumo *hash,* esse será válido. Todavia, quando o DAD sofrer quaisquer modificações, a exemplo da migração da sua extensão em decorrência da obsolescência tecnológica de arquivo de texto (TXT), com o *hash* inicial de 608c270c, convertido para *Portable Document Format* (PDF), este sofrerá alteração em seu resumo, já que ocorreram modificações na camada lógica do documento.

Logo, o DAD receberá novo resumo, tal como 710a587, cujo objeto digital com extensão em pdf, posteriormente, sofrerá nova migração da extensão pdf para pdf/a. Seguidamente, haverá alteração de sua camada lógica, e, por conseguinte, de seu resumo, o qual será modificado para 745f763b.

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

A Figura 4 apresenta a síntese de aplicação do modelo lógico *Caramuru* no âmbito dos documentos acadêmicos por intermédio de um diagrama de blocos.

Figura 4: Diagrama de blocos do funcionamento da aplicação do modelo lógico *Caramuru* no âmbito dos acervos acadêmicos



Fonte: Os autores (2024).

Conforme observado, a Figura 4 apresentou o diagrama de aplicação do modelo lógico *Caramuru* para autenticação descentralizada de documentos acadêmicos, desde a sua produção até a preservação/acesso de longa duração. Ademais, nota-se a eficiência do *blockchain* na autenticação descentralizada nos ambientes informacionais digitas, já que o processo de gerar os resumos criptográficos podem ser realizados de forma automatizada e descentralizada, nas migrações a serem realizadas no SIGAD, RDC-Arq e plataformas de difusão e acesso.

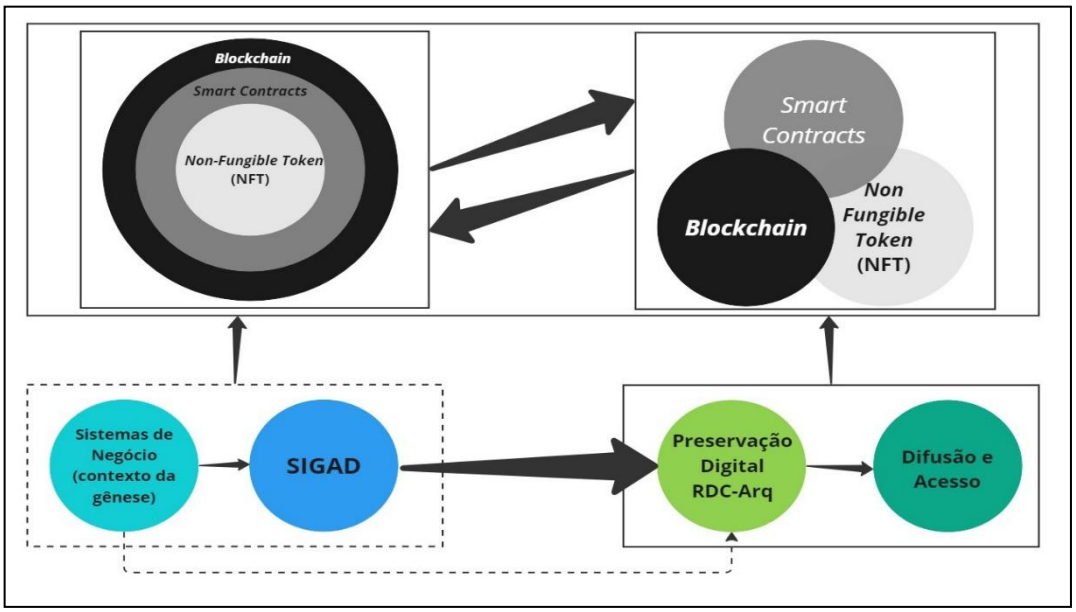
Por fim, em todos os eventos ao longo do ciclo de vida do DAD, podem ser gerados *hashes*, que serão validados e adicionados à cadeia de blocos, para constituição de trilha de auditoria descentralizada e imutável. Portanto, a tecnologia *blockchain* fornece a solução para problemática da autenticação em ambientes descentralizados, bem como auxílio às questões relacionadas à preservação digital de longa duração.

Dessa forma, o *blockchain* poderá garantir que as migrações realizadas no DAD sejam modificações autorizadas com uso de algoritmos de validação consensual. Por sua vez, esses devem propiciar o registro cronológico inalterável, no qual as trilhas de auditorias são realizadas com os registros dos metadados criptografados com o uso do algoritmo árvore de *merkle,* que realiza auditoria desde o último *hash* do bloco até o bloco gênesis.

Nessa direção, em tempos hodiernos surgiram outras tecnologias disruptivas, além do *blockchain*, tais como: *smart contracts* e NFTs, essas tecnologias poderão ser

aplicadas nos documentos produzidos nas IES no Brasil. A Figura 05, apresenta o uso das tecnologias *smart contracts,* NFT em conjunto com o *blockchain*, no âmbito das IES no Brasil, com a perspectiva da Arquivologia.

Figura 5: Aplicação das tecnologias *smart contracts,* NFT em concomitância com *blockchain* nos documentos das instituições de ensino superior no Brasil.



Fonte: Os autores (2024).

A Figura 5 apresentou o modelo para aplicação da tecnologia *blockchain, smart contracts* e NFT sob o viés da Arquivologia, especificamente nos documentos acadêmicos das IES no Brasil, desde o contexto da gênese até sua destinação final.

O procedimento da gênese documental poderá ser automatizado com uso do *smart contracts,* posto que por meio de linhas de código é viabilizada a produção de tipos documentais autoexecutáveis, a exemplo da matrícula no curso de educação superior de graduação.

O NFT poderá ser aplicado no contexto gênese documental e até o final do seu ciclo de vida, de acordo com as necessidades e especificidades, estabelecidas por meio das políticas de arquivo, a qual deve constar nos planos de ações de cada instituição, seja pública ou privada. Nesse sentido, com o uso do NFT, pode-se garantir a originalidade e unicidade dos DAD.

Assim, gera-se o *root hash* na gênese documental. Ao longo do ciclo de vida do DAD, são gerados outros *hashes*, principalmente no momento do recolhimento do DAD do

SIGAD para o ambiente de preservação, cujos *hashes* constituem blocos, que serão validados e adicionados na cadeia de blocos de forma permanente com o objetivo final de criar a trilha de auditoria ininterrupta e auditável. Na conjuntura de geração do *root hash,* a produção documental poderá utilizar-se do *smart contracts*, automatizando os procedimentos da gênese, bem como aplicar o NFT, para garantir a originalidade dos DAD.

5 CONSIDERAÇÕES FINAIS

Na contemporaneidade, a Arquivologia poderá utilizar-se da tecnologia *blockchain* para apoiar a autenticação distribuída de documentos e, assim, corroborar com a cadeia de custódia digital arquivística de forma automatizada. Nessa perspectiva, emerge a proposta de um modelo lógico nacional, qual seja: *Caramuru*, que tem por base a aplicação da tecnologia *blockchain* no âmbito da Arquivologia, para proceder a autenticação distribuída ao longo do ciclo de vida dos documentos acadêmicos das IES no Brasil.

Demonstrou-se as aplicações da tecnologia *blockchain* no contexto da autenticação distribuída para fins arquivísticos, com a proposta de um modelo lógico denominado *Caramuru*, que criptografa, envia e valida transações, as quais propiciam o registro cronológico inalterável de todas as operações realizadas. A auditoria é realizada por meio do *ledger,* dos registros em conjunto com algoritmo denominado árvore de *merkle,* que poderá verificar se o documento sofreu alterações, corrompimento e adulterações não autorizadas.

A tríade tecnológica *blockchain, smart contracts e* NFT fornece a solução para as problemáticas da autenticação, gênese documental automatizada e originalidade dos DAD em ambientes descentralizados, bem como auxílio às questões relacionadas à preservação digital de longa duração. Nesse sentido, poderá garantir que as migrações realizadas no DAD sejam modificações autorizadas mediante o uso de algoritmos de validação consensual, que propiciam registro cronológico inalterável, pela qual as trilhas de auditorias são realizadas com os registros dos metadados criptografados com o uso do algoritmo, que realiza auditoria desde o último *hash* do bloco até o bloco gênesis.

Verificou-se que as tecnologias *blockchain*, *smart contracts* e NFT podem, ser

aplicadas no âmbito arquivístico, em especial nos documentos acadêmicos das IES, em vista de que podem garantir rastreabilidade da proveniência, infungibilidade, autenticação, imutabilidade e unicidade, em abordagem descentralizada e automatizada dos DAD.

Assim, observa-se que os novos desafios dos sistemas distribuídos, que surgem nos ambientes informacionais digitais com uso das TIC e dos aparatos institucionais, em especial as tecnologias *blockchain, smart contracts* e *NFT* fazem um convite para discutir e debater seus impactos na Arquivologia. Sobretudo, na autenticação automatizada e distribuída de documentos nato-digitais e representantes digitais, que compõem os acervos acadêmicos digitais.

REFERÊNCIAS

BAL, M.; NER, C. **NFT Tracer**: a non-fungible token tracing roof-of-concept using hyperledger fabric. 2019. Disponível em: https://arxiv.org/pdf/1905.04795. Acesso em: 10 dez. 2024.

BARBOZA, E. S. **Autenticação multifatorial em hardware para o processo de assinatura digital da Nf-e**. Orientador: Manoel Eusébio de Lima. 2018. 154p. Dissertação (Mestrado) – Universidade Federal de Pernambuco. CC, Ciência da Computação, Recife, 2018. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/32403/1/DISSERTA%c3%87%c3%83O%20Eudes%20da%20Silva%20Barboza.pdf. Acesso em: 10 dez. 2024.

BARKATULLAH, J.; HANKE, T. Goldstrike 1: CoinTerra's First-Generation Cryptocurrency Mining Processor for Bitcoin. **IEEE Micro**, v. 35, n. 2, p. 68-76, 2015, DOI: 10.1109/MM.2015.13. Acesso em: 10 dez. 2024.

BRASIL. Casa Civil. Presidência da República. Instituto Nacional de Tecnologia da Informação (ITI). **Instrução normativa ITI nº19, de 10 novembro de 2021**. 2021. Disponível em: https://www.in.gov.br/web/dou/-/instrucao-normativa-iti-n-19-de-10-de-novembro-de-2021-359443482. Acesso em: 10 dez. 2024.

BRASIL. Casa Civil. Presidência da República. Subchefia para assuntos jurídicos. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 10 dez. 2024.

Archeion Online, João Pessoa, v.13 n. Edição Especial: X CNA - Congresso Nacional de Arquivologia. p. 106-122, jan./mar. 2025.
DOI - 10.22478/ufpb.2318-6186.2025v13nEdição Especial.72550
ISSN 2318-6186. Licença

BRASIL. Ministério da Educação (MEC). **Portaria nº 613, de 18 de agosto de 2023.** Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-613-de-18-de-agosto-de-2022-423583397. Acesso em: 10 dez. 2024.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para assuntos jurídicos. **Lei nº 14.063 de 23 setembro de 2020** - Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos. (2020) Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 10 dez. 2024.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos. **Decreto n.º 9.235 de 15 de dezembro de 2017.** Dispõe sobre o exercício das funções de regulação, supervisão e avaliação das instituições de educação superior e dos cursos superiores de graduação e de pós-graduação no sistema federal de ensino. Brasília, DF. 2017. Acesso em: 10 dez. 2024.

CESAR, D. M. F. ***Blockchain* aplicado à aviação:** uma revisão integrativa da literatura. 2020. 144 f. Dissertação (Mestrado em Aeronáutica) – Escola de Aeronáutica – Instituto Superior de Educação e Ciências, Lisboa. 2020. Acesso em: 10 dez. 2024.

CHOHAN, U. W. Non-fungible tokens (NFTs): Early Thoughts and a Research Agenda. **Ssrn Electronic Journal**, v.1, n.1, p. 1-14, mar. 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822743. Acesso em: 10 dez. 2024.

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

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

KOBAYASHI, L. O. M. **Abordagem criptográfica para integridade e autenticidade em imagens médicas**. Orientador: Sergio Shiguemi Furuie. 2007. 136 p. Tese (Doutorado Engenharia de telecomunicações e controle). Escola politécnica, Universidade de São Paulo, São Paulo, 2007. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-14012008-122458/publico/Kobayashi_Tese_Revisado.pdf. Acesso em: 10 dez. 2024.

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

MARCACINI, A. T. R. **O documento eletrônico como meio de prova**. 2002 Disponível em: http://augustomarcacini. cjb. net/textos/docelet2. html. Acesso em: 10 dez. 2024.
MARCONI, M. A.; LAKATOS, E. M. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 7. ed. São Paulo: Atlas. 2008. 296 p.

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

Archeion Online, João Pessoa, v.13 n. Edição Especial: X CNA - Congresso Nacional de Arquivologia. p. 106-122, jan./mar. 2025.
DOI - 10.22478/ufpb.2318-6186.2025v13nEdição Especial.72550
ISSN 2318-6186. Licença

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

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 dez. 2024.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. Bitcoin and Cryptocurrency Technologies. 2016. Princeton University Press. **Network (DLnet)**. n. 20, p. 1-12, 2001. Disponível em: https://www.uio.no/studier/emner/matnat/ifi/IN5420/v18/timeplan/resources/bitcoinand-cryptocurrency-techniques.pdf. Acesso em: 10 dez. 2024.

NINGTIAS, A. D. et al. Enforcement of the Crime of Money Laundering in Digital Financial Transactions. **Jornal Independent**, v. 11, n. 2, p. 575-585, 2023. DOI: 10.30736/ji.v11i2.265. Acesso em: 10 dez. 2024.

PERSET, K. The economic and social role of Internet intermediaries. **OECD Digital Economy Papers**, n. 171, 2010. DOI: 10.1787/5kmh79zzs8vb-en. Acesso em: 10 dez. 2024.

REIFF, N. **What Was the First Cryptocurrency?**. Investopedia, 23 jul. 2022. Disponível em: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/. Acesso em: 10 dez. 2024.

RESENDE. A. D. **Certificação Digital.** 2009. Disponível em: http://www.unigran.br/revistas/juridica/ed_anteriores/22/artigos/artigo09.pdf. Acesso em: 10 dez. 2024.

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

SZABO, N. **Bitcoin, what took ye so long?** 2011. Disponível em: http://unenumerated.blogspot.com.br/2011/05/bitcoin-what-took-ye-so-long.html. Acesso em: 10 dez. 2024.

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

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution**. New York: Penguin Random House LLC, 2016.