SIMPÓSIO INTERNACIONAL DE ARQUIVOS
Arquivo, documento e informação em cenários híbridos.
5 A 13 DE DEZEMBRO DE 2020

BLOCKCHAIN APLICADO À SEGURANÇA DA INFORMAÇÃO ORGÂNICA

Alexandre Fernal[1]
alexandre.fernal@gmail.com
Telma Campanha de Carvalho Madio[2]
telma.madio@unesp.br

Resumo

O *blockchain* surgiu em 2008 com a publicação do artigo *Bitcoin: a peer-to-peer eletronic cash system*, cuja tecnologia consiste em um banco de dados distribuídos na rede mundial de computadores, no qual todos os registros e saídas de dados são gravadas cronologicamente em uma cadeia de blocos. Nesse sentido, o *blockchain* é um grande banco de dados distribuído, que arquiva todas as movimentações financeiras das transações realizadas de forma irreversível, posto que dispõe de um sistema *ledger* - livro razão com gravação, rastreamento, monitoramento e transferência de ativos. As cadeias de registro são encadeadas uma as outras por intermédio de chaves públicas, entrada e saídas, as quais são consideradas imutáveis, posto que quando um registro é inserido, esse não pode ser modificado. Observa-se que, a primeira aplicação funcional do *blockchain*, foi a cripto moeda denominada *bitcoin*. Todavia, ao longo do tempo desde sua criação, percebeu-se que essa tecnologia poderia ser utilizada para outros fins, tais como: validações de transações financeiras e ativos, *smart contracts* - contratos inteligentes, registro e *records managent* - gestão de documentos, *supply chain* - cadeia de suprimentos. Dessa forma, entende-se que por meio do *ledger* - livro razão, esse algoritmo poderá corroborar com aplicações para segurança da informação orgânica, bem como na autenticidade dos documentos, e, posteriormente, na preservação digital de longa duração. Sendo assim, acerca dos requisitos de segurança da informação, observa-se alguns fatores fundamentais, quais sejam: autenticação, autorização, auditoria e não repúdio, os quais são quesitos fundamentais para segurança de informação. Questiona-se, portanto, quais as possíveis relações e aplicações da tecnologia *blockchain* com a segurança da informação orgânica. Logo, objetiva-se relacionar as possíveis aplicações da tecnologia *blockchain* no contexto da arquivologia, especificamente na segurança da informação orgânica e demonstrar que a tecnologia poderá corroborar com a integridade e identidade dos documentos e na preservação digital. Para tanto, realizou-se uma pesquisa qualitativa, exploratória, bibliográfica e documental acerca da literatura científica em língua portuguesa, espanhola e inglesa publicada em livros, dissertações, teses e artigos. Os resultados obtidos permitiram demonstrar as relações, e, por conseguinte, as aplicações da tecnologia *blockchain* por intermédio do *ledger* no contexto da segurança da informação orgânica. Verificou-se que o protocolo do *blockchain* criptografa, envia e valida transações, que propiciam um registro cronológico inalterável de todas as operações realizadas. Nessa direção, as vantagens de aplicação na autenticidade dos documentos realizadas com o *blockchain* reside na validação de forma distribuída, por um procedimento de validação consensual, quais sejam: *proof of work* - prova de trabalho, *proof of stake* - prova de participação. Essas formas de validações consensuais são realizadas por meio de algoritmos que analisam os metadados dos registros criptografados, os quais verificam a integridade e identidade em vista de que é possível auditar os *hashes* de toda cadeia de blocos até o bloco zero, ou seja, bloco gênese do documento. Sendo assim, torna-se exequível a preservação dos *hashes* das cadeias de registro ao longo do tempo, a qual garante a autenticidade dos documentos ao longo do seu ciclo de vida. A auditoria é realizada por meio do *ledger* dos registros em conjunto com algoritmo denominado árvore de *Merkle*, a qual garante que o documento não tenha sofrido alterações, corrompimento e adulterações. Constata-se que esses procedimentos de auditoria em conjunto com os algoritmos supracitados podem corroborar com a autenticidade dos documentos, uma vez que é possível, com base na tecnologia *blockchain* garantir a integridade e identidade dos documentos contribuindo, assim, com a preservação digital de longa duração, em vista de

[1] Universidade Estadual de Londrina (UEL), Londrina/Paraná, Brasil/ Universidade Estadual Paulista - Campus Marília (UNESP), Marília/São Paulo, Brasil.
[2] Universidade Estadual Paulista – Campus Marília (UNESP), Marília/São Paulo, Brasil.

que essa tem por finalidade garantir o acesso da informação orgânica nos ambientes informacionais digitais. Por fim, a garantia da autenticidade, a qual contempla a integridade e identidade é viabilizada com a aplicação da tecnologia *blockchain.*

Palavras-chave: *Blockchain*. Informação Orgânica. Arquivologia. *Ledger*. Autenticidade.

1 INTRODUÇÂO

Na Arquivologia em tempos hodiernos, as tecnologias da informação e comunicação (TIC), estão gerando mudanças profundas no fazer arquivístico. Nesse cenário, os constructos consagrados outrora no contexto clássico perdem a sua produção de sentido nos ambientes informacionais digitais. As rupturas paradigmáticas com advento das TIC propiciam o surgimento de tecnologias disruptivas, que descontroem as fundamentações da tradição arquivística.

Logo, é de extrema relevância que a Arquivologia entre em debate acerca da tecnologia *Blockchain* e que analise sua possível adoção, em vista de que os impactos proporcionados poderão ser significativos nos arquivos e por conseguinte surgem excelentes oportunidades para Arquivologia nos ambientes informacionais digitais.

A tecnologia *blockchain* possui como característica fundamental a imutabilidade dos dados gravados em seus blocos, posto que uma vez registrado os dados em um bloco, esses não podem ser modificados. Essas cadeias de blocos funcionam como um *ledger* – livro razão aberto e distribuído ponto a ponto, o qual armazena as operações realizadas de ativos de forma permanente e auditável ao longo do tempo.

Logo. essa tecnologia tem com base a segurança da informação das operações realizadas, ou seja, baseia-se em padrões de tolerância a falhas, que permite o funcionamento e integridade plena dos registros de forma distribuída.

A segurança da informação orgânica é garantida por meio do *hash*, o qual é um resumo criptográfico obtido com o uso de uma função matemática complexa, que garante integridade dos registros.

Nesse sentido, o *blockchain* utiliza-se de protocolos de validação consensual como, por exemplo, o *proof of work* – prova de trabalho e *proof of stake – prova de*

validação, que garantem a integridade e identidade dos documentos, os quais podem corroborar com a preservação digital, em vista de que com o uso da arvore de *merkle* podem checar todas cadeias de blocos até o bloco zero, isto é, o bloco gênesis e consequentemente auditar todas as alterações ocorridas nos documentos arquivísticos digitais ao longo do tempo ocasionadas pelas migrações, que podem deformar o objeto digital em questão.

2 CERTIFICADO DIGITAL

Essa seção apresenta os conceitos básicos a respeito da criptografia e função *hash*, os quais são pré requisitos altamente desejados e necessários para a compreensão do certificado digital e o funcionamento da tecnologia *blockchain*.

O certificado digital para o Instituto Nacional de Tecnologia da Informação (ITI) (BRASIL, 2021), é um registro eletrônico digital assinado, o qual é gerado por intermédio de um procedimento da certificação digital, que comprova as relações entre chaves criptográficas.

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 consistem de 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, utilizada uma única chave para cifra e decifrar (KOBAYASHI, 2007).

O certificado digital no Brasil, deve ser emitido por uma 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 nº 14.063 de 23 de setembro de 2020 , validade jurídica aos atos praticados com seu uso (BRASIL, 2020).

A ICP-Brasil trabalha com uma hierarquia, na qual a Autoridade Certificadora Raiz (AC Raiz) é o ITI, autarquia federal vinculada a Casa Civil da Presidência da República. O ITI é responsável por gerar as chaves da AC e regulamentam as atividades de cada uma.

Para uma assinatura, em suporte papel, geralmente é usado algum tipo de marca física para identificação de autenticação do documento, ou também para firmar o acordo entre as partes interessadas com que esta dita em um documento, no qual é feito uma assinatura manuscrita com validade jurídica, reconhecida em cartório (NUNES, 2007).

Já no documento digital, a autenticação é realizada por meio de um certificado digital emitido por alguma autoridade certificadora que faz ligação entre o certificado e o assinante, garantindo assim, o princípio da integridade.

Um certificado possui um período de validade, normalmente com duração entre alguns meses e anos. Um certificado só tem validade durante um período determinado, após esse período ele é expirado e se torna inválido. Segundo Monteiro e Mignoni (2007, p. 40) os certificados digitais apresentam um ciclo de vida, composto por estes seis (06) itens, que executam todo processo da certificação, que é apresentado em detalhes, a seguir:

> 1. Solicitação – Os procedimentos incluem exigências referentes à geração, proteção do par de chaves e lista de informações necessárias para cada classe de certificado e o preenchimento de uma solicitação e seu envio à AC. Informações no qual são mantidas em regime de confidencialidade pela AC;
> 2. Validação – Ao receber uma solicitação de certificados, a AR, deverá efetuar as validações obrigatórias, estabelecidas como pré-requisitos para emissão. AR verificar se as informações são verdadeiras ou não para então enviar à AC, caso contrário a solicitação é rejeitada;
> 3. Emissão – A emissão de um certificado ocorrerá após receber uma solicitação aprovada pela AR. A emissão do certificado significa aprovação final da solicitação pela AC. O certificado passa ser válido a partir do momento em que a assinante aceita; Os meios de aceitação de um certificado variam de acordo com a sua classe. Aceito o certificado, o assinante deverá garantir a integridade de sua chave privada, a veracidade de suas informações e o usuário será exclusivo para sua finalidade;
> 4. Uso dos Certificados – A garantia que os certificados estão sendo usados corretamente é realizada pela conferência da assinatura Digital da cópia com o original;
> 5. Suspensão/ Revogação de Certificado – Poderão ocorrer por vários motivos, tais como: comprometimento, roubo, perda, modificações,

> divulgação, violação de obrigações, pelo assinante, faltas de pagamentos de tarifas e taxas entre outras ações consideradas relevantes ela AC;
> 6. Vencimento – O certificado digital tem validade de 1 a 3 anos, a partir do vencimento, o certificado não implica na validade das obrigações contratuais. A utilização de certificados vencidos é de inteira responsabilidade da pessoa que se utiliza ou nele confia; a AC não se responsabiliza pelo uso de certificados vencidos (MONTEIRO; MIGNONI, 2007, p. 40).

Na ICP-Brasil existe oito (08) tipos de certificados, separados por duas (02) séries. Série A, a qual é dividida em quatro tipos (A1, A2, A3, A4), e a série S, que também é separada em quatro tipos (S1, S2, S3, S4).

A série A, reúne certificados de assinatura digital utilizados na confirmação de identidade na *web*, em *e-mail*, em redes privadas e em documentos digitais com verificação da integridade de suas informações (RESENDE, 2009).

A série S reúne certificados com sigilo, os quais são utilizados na codificação de documentos de base de dados, de mensagens e de outras informações eletrônicas sigilosas. Todas as séries são diferenciadas pelo o uso, pelo 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 que ele foi solicitado. Os dados são protegidos por uma senha de acesso. Somente é possível acessa e mover com a chave privada a ele associada. Caso a chave privada seja perdida, um 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 realizando transações eletrônicas, com garantia e integridade das informações. A partir do momento que for necessário, que algo assinado fosse enviado a AC , com um tipo de certificado diferente, logo se tornaria um problema administrar todos os formatos diferentes. Para resolver esse problema, foi criado e aprovado pela *International telecomunication Union* (ITU), um padrão para certificado. O padrão chamado é X-509 e seu uso está bem difundido (TANENBAUM, 2003).

Assim como na criptografia assimétrica, a assinatura digital é uma sequência de números resultantes de uma operação matemática conhecida como função *hashing*.

Essa função analisa todo o documento ou arquivo, com a base no algoritmo matemático, que geram tamanho específico para ele, conhecido como resumo. Com base nesse resumo fica impossível relizar qualquer alteração. A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, posto que os algoritmos de criptografia assimétrica são muito lentos (MONTEIRO; MIGNONI 2007).

A submissão de resumos criptográficos ao processo de decifragem com a chave privada reduz o tempo de operação para gerar uma assinatura, por serem os resumos, em geral, muito menores que o documentos. Assim, consomem um tempo menor e uniforme, independentemente do tamanho do documento a ser assinado.

A autenticação dos algoritmos de criptografia de chave pública opera em conjunto com uma função resumo, também conhecida como função de *hash.*

O resumo criptográfico é o resultado retornado por uma função de *hash.* Esse pode ser comparado a uma impressão digital, cada documento possui um valor único de resumo e uma pequena alteração no documento, como a inserção de um espaço em branco resulta em um resumo completamente diferente.

O emissor que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela *Internet*. O sigilo é garantido, já que somente o destinatário que possuir a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais.

A Medida Provisória n° 2.200-2, de 24 de agosto de 2001 foi o marco inicial que garantiu a validade jurídica dos documentos digitais e a utilização de certificados digitais para atribuir autenticidade e integridade aos documentos. Esse fato tornou o certificado digital um instrumento válido juridicamente em todo território nacional (BRASIL, 2001).

Os Criptossistemas provêm técnicas para embaralhar ou cifrar mensagens de forma que, aparentemente, tornam ilegíveis, e, que posteriormente, possam obter novamente a mensagem original por meio do texto embaralhado. Quaisquer Criptossistemas deve garantir que as mensagens que trafegam em um canal de

comunicação tenham privacidade e que a mensagem seja autentica sem alteração (MARTINI, 2001). O criptossistema pode ser dividido em dois tipos distintos, segundo o método que realizam: criptografia simétrica e assimétrica.

Segundo Train (2007) a criptografia simétrica é o tipo mais simples de criptografia, pois o emissor e o receptor fazem o uso de uma única chave para codificar e decodificar uma determinada informação. Portanto, a chave que o emissor usa para codificar a informação é a usada pelo receptor para decodificá-la. Na seção 3, é apresentada as conjunturas do surgimento da tecnologia *blockchain* e seus conceitos.

3 BLOCKCHAIN

O *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 assim, cunhou-se o conceito de *blockchain* e *bitcoin*, essa pesquisa supracitada apresenta os princípios fundamentais, bem como o funcionamento do *blockchain* com sua aplicação em criptomoedas (NAKAMOTO, 2008).

A tecnologia *blockchain* consiste em um banco de dados distribuído na rede mundial de computadores, no qual todos os registros e saídas de dados são gravados cronologicamente em uma cadeia de blocos. Alguns participantes, isto é, os mineradores dessas redes ofertam esforços computacionais para gravação de novos blocos, e ao realizar essas operações, esses efetuam cálculos de *hash* para solucionar os problemas criptográficos apresentados, e, por conseguinte obtêm uma parte do valor transacionado nas operações, que são entendidas como mineração (NAKAMOTO, 2008).

O *blockchain* é composto por uma cadeia de registros imutáveis públicos e distribuídos, cujas cadeias de registro são encadeadas uma as outras por intermédio de chaves públicas, entrada e saídas. São consideradas imutáveis, em vista de que quando um registro é inserido, esse não pode ser alterado. As cadeias são públicas, visto que o acesso poderá ser realizado por meio da *internet*. E por fim, as cadeias de registro estão armazenadas e replicadas em várias máquinas conectadas na rede mundial de

computadores, isto é, o sistema não é armazenado em um único servidor central (NARAYANAN, BONNEAU, FELTEN, MILLER, GOLDFEDER,; OKURPSKI, 2016).

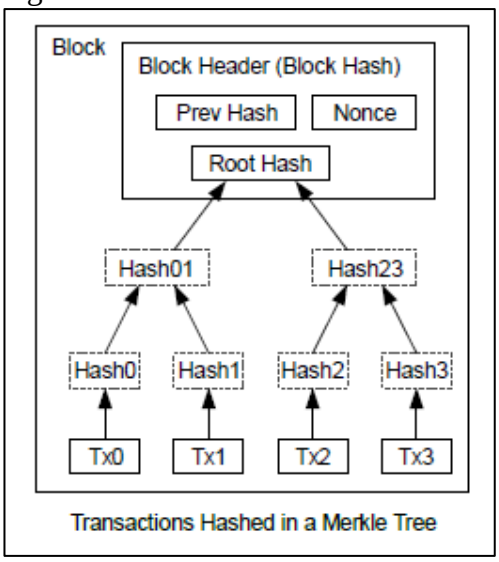
Dessa forma, o *blockchain* é um grande banco de dados distribuído, que arquiva todas as movimentações financeiras das transações de forma irreversível. Dispõe de um sistema de inventário com gravação, rastreamento, monitoramento e transferência de ativos. A primeira aplicação funcional do *blockchain* foi a *cripto* moeda denominada *bitcoin* (SWAN, 2015).

Assim, o blockchain é um *ledger* - livro razão distribuído e imutável, que forma um banco de dados distribuído por intermédio de uma rede *peer to peer* (P2P), na qual são registradas operações com ativos e transações, que podem ser: tangíveis e intangíveis. O primeiro pode ser, por exemplo, os registros de imóveis como propriedades. Já o segundo são marcas, diretos autorais. Os sistemas atuais de *ledger* centralizados tradicionais podem apresentar certas deficiências, tais como: custo operacional elevado, pouca transparência e dificuldade na execução de auditabilidade, que podem culminar em fraude e resultados equivocados. Dessa forma, o *blockchain* se configura em um sistema *ledger* descentralizado e apresenta certas vantagens ao modelo centralizado como as redes baseadas em cliente servidor, em vista de que podem reduzir os custos operacionas, bem como prover transparência nos processos de auditoria evitando-se as atividades fraudulentas.

Logo, com o advento da tecnologia *blockchain* viabilizou-se inicialmente os registros distribuídos por meio de criptografias para uso em moedas digitais. Entretanto, percebeu-se que a tecnologia poderia ser utilizada para outros fins diferentes da proposta original, quais sejam: validações de transações financeiras e ativos, *smart contracts* – contratos inteligentes, registros e *records management* – gestão de documentos e *supply chain* – cadeia de suprimentos, em sistemas descentralizados de consenso ponto a ponto.

Nesse sentido, Nakamoto, em 2008, concebeu a tecnologia *blockchain*, a qual é composta pela convergência de várias tecnologias, que será apresentada na figura 1.

Figura 1 - Anatomia do bloco.



Fonte: Nakamoto, 2008.

A figura 01 apresentou anatomia de um bloco, que fará parte da cadeia de blocos. O bloco é composto de várias camadas, a saber: *Block (Current_ block_header_version), Block Header - Block hash, Reference Prev Block - prev hash (Hash_Prev_Block), nonce (nNonce), Root node - Root hash (Hash_Merkle_Root).*

O *block* é a versão do bloco, ou seja, o número de cada bloco. Já o *Header* é o resumo criptográfico do bloco. O terceiro o *Reference Prev Block* é o *hash* do bloco anterior. O *Nonce* é sequencial numérico atribuído para o bloco de forma aleatória. E por fim, *Root Hash*, que armazena a raiz dos resumos criptográficos, a qual é utilizada para prover integridade aos blocos (NAKAMOTO, 2008).

Nessa direção, o *blockchain* surge como uma proposta que dispõe de um mecanismo de consenso baseado no modelo de *proof of work*, que foi inicialmente sinalizada por Cynthia Dwork e Moni Naor em 1992, no artigo intitulado *Pricing via processing or combatting junk mail*, o qual não utilizou o termo *proof of work* (PoW). Todavia, já apresentava que o usuário deveria provar que realizou alguma tarefa para viabilizar a utilização de um determinado serviço, com o objetivo final de inviabilizar o uso de serviços desprovido de serventia (DWORK; NAOR, 1993).

O termo PoW foi cunhado, posteriormente, em 1999, por Markus Jakobsson e Ari Juels, formalizado por intermédio do trabalho *Proffs of Works and a bread*

pudding protocols (JUELS; JAKOBSSON, 1999).

O consenso distribuído em uma rede *peer to peer* (P2P), do tipo distribuída é o processo realizado por meio de algoritmos pelos quais os nós participantes da rede ponto a ponto estão de acordo acerca de um conjunto de dados, que representa um valor único (BASHIR, 2017). Dessa forma, o procedimento de consenso é formado por uma sequência lógica de ações, ou seja, um algoritmo de consenso que permite a validação dos valores propostos pela maioria dos nós (BASHIR, 2017).

Sendo assim, a tecnologia *blockchain* atualmente utiliza-se dos principais métodos de validação consensual, tais como: *proof of work* e *proof of stake*.

O primeiro consiste em um mecanismo de consenso, no qual cada nó participante da rede busca uma possível solução para o enigma criptográfico com objetivo de adicionar um novo bloco a cadeia de blocos existentes. Paa criação de blocos novos pressupõe a participação dos mineradores, os quais empenham-se em conseguir uma solução ao desafio critptográfico.

Para algumas aplicações com a tecnologia *blockchain*, o procedimento de consenso consiste em propor um valor pré determinado denominado de *nonce*, que está contido no cabeçalho do bloco *Head*, e, por conseguinte, quando o valor do *hash* seja inferior ao parâmetro dificuldade *threshold* estabelecido, ocorre a inserção de um novo bloco.

A figura 2 demonstra por meio de um algoritmo a condição para inserção de novos, nas cadeias de blocos pré existentes.

Figura 2 - Condição para inserção de novo bloco

Se *HASH* < menor que < *NONCE*
Adicionar novo bloco

Fonte: Baseado em Nakamoto (2008)

A figura 2, apresentou como os minerados realizam a inserção de novos blocos, que é realizada quando se obtém uma solução criptográfica. Tomando-se por base um *threshold* global (dificuldade) e o maior índice de bloco conhecido pelo minerador, este seleciona um *nonce* (número aleatório) e aplica um algoritmo com uma função aleatória para o *hash*, nos campos do *header* – cabeçalho.

Assim, enquanto o resultado do *hash* não for menor que o *threshold*, o *nonce* é substituído por outro *hash*. Logo, quando o *hash* for menor que o *nonce*, um novo bloco será adicionado, em vista de que a condição pré estabelecida com o algoritmo proposto será contemplada.

Por fim, o mecanismo de consenso *proof of stake* (PoS) – prova de participação consiste na seleção do nó participante de forma aleatória, que poderá inserir um bloco novo a cadeia de blocos pré existente. Esse algoritmo de validação consensual foi proposto por Nick Szabo (2011), o grande diferencial do PoS em relação ao PoW, versa na validação e aprovação de novos blocos, de forma distinta da mineração de *hashes* propostas pelos PoW.

A seção 4 apresenta a segurança da informação orgânica com o uso da tecnologia *blockchain*, que se configura como uma possibilidade de aplicação para fins de autenticidade e corrobora com a preservação digital de longa duração.

4 SEGURANÇA DA INFORMAÇÃO ORGÂNICA COM *BLOCKCHAIN*

A segurança da informação pressupõe alguns quesitos fundamentais, tais como: autenticação, autorização, auditoria e não repúdio. Nessa direção, a *International organization for Standartization/International eletrotehcnical comission* (ISO/IEC) (2005), estabelece os requisitos da segurança da informação, a saber: confidencialidade, integridade, autenticidade, disponibilidade, não repúdio, conformidade e tempestividade.

No contexto da Arquivologia para as questões relacionadas aos requisitos de presunção da autenticidade para documentos arquivísticos digitais, a câmara técnica de documentos arquivísticos digitais (CTDE), do Conselho Nacional de Arquivos (CONARQ), do Arquivo Nacional aponta que a autenticidade dos documentos arquivísticos digitais é constantemente comprometida devido a obsolescência tecnológica. Dessa forma, a presunção da autenticidade deve ter como base a utilização de tecnologias e métodos administrativos, que possam garantir a identidade e integridade documental (BRASIL, 2002).

De acordo com o CONARQ (BRASIL, 2020, p.12) a autenticidade é a "Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade".

A identidade é o conjunto de atributos de um documento de arquivo, o qual se manifesta como único diferenciando-se de outros documentos. Já a integridade é a qualidade de transmitir a mensagem que propiciou o seu contexto da gênese para cumprir com seus objetivos (BRASIL, 2002).

Para garantir a autenticidade dos documentos arquivísticos digitais, é necessário a utilização de tecnologias para autenticação documental como, por exemplo, a assinatura digital, que podem declarar a autenticidade documental em determinadas situações.

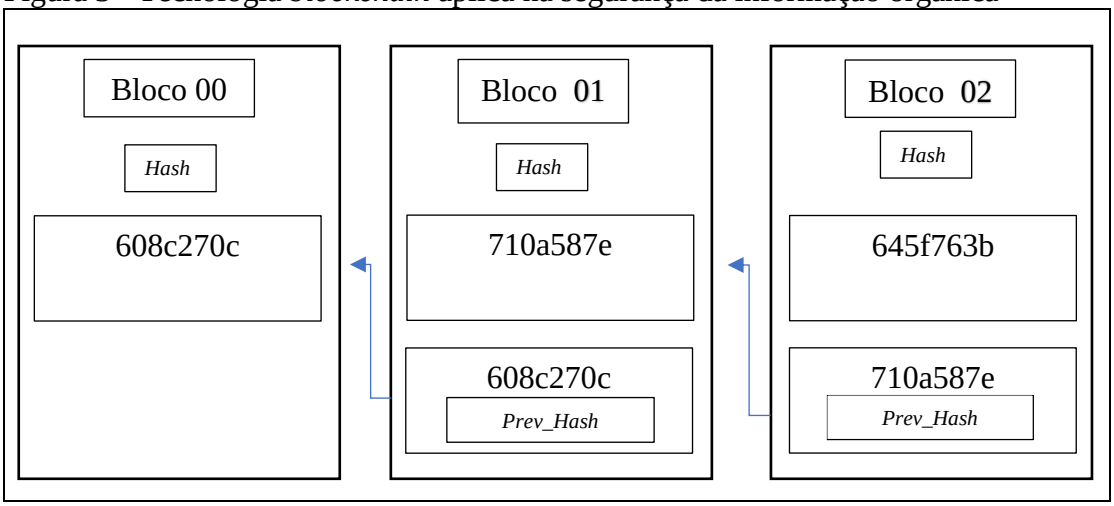
A CTDE, do CONARQ (BRASIL, 2002, p. 5), manifesta a distinção entre autenticidade e autenticação: aquelas se referem à "[...] qualidade do documento ser verdadeiro, isto é, ser exatamente aquele que foi produzido.", enquanto essa "[...] é a declaração da autenticidade feita em um dado momento por uma pessoa autorizada para tal."

Ainda, de acordo com CTDE (BRASIL, 2002), os métodos de autenticação com o uso tecnologias não são seguras ao longo do tempo, isto é, a utilização de tecnologias a longo prazo tem a sua validade comprometida ou quando são migrados os arquivos, posto que as assinaturas digitais não podem ser transferidas para as novas cadeias de *bits*. Dessa forma, as migrações sucessivas nos documentos arquivísticos digitais ao longo do tempo não viabilizam que a assinatura digital seja preservada na nova cadeia de *bits*, comprometendo a garantia de autenticidade. Entretanto, em 2008, surge uma possibilidade de solução para esse problema, a tecnologia *Blockchain*.

Em tempos hodiernos, a tecnologia *blockchain* emerge como uma alternativa, que poderá ser utilizada para sanar as problemáticas referentes a autenticidade documental a longo prazo em um contexto descentralizado, bem como corroborar com a preservação digital de forma duradoura.

A Figura 3 demonstra a aplicação da tecnologia *blockchain* na segurança da informação orgânica.

Figura 3 - Tecnologia *blockchain* aplica na segurança da informação orgânica



Fonte: Elaborado pelos autores 2021

A figura 3 apresentou aplicação da tecnologia *blockchain* na segurança da informação orgânica.

O bloco 00 é o bloco gênesis, bloco inicial que contém o *Root hash* referente ao objeto digital, no caso a função *hash*, isto é, o resumo critptográfico do documento arquivístico digital, representado por meio de um metadado, qual seja: 608c270c. O bloco 01, seguinte do *blokchain*, 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 validados por meio dos algoritmos de validação consensual, a saber: *proof of work* e *proof of stake*. Já o bloco 02 tem acesso ao *Prev Hash* (710a587e) do bloco 01, no caso o bloco 02 aponta para o bloco anterior, nesse caso o bloco 01, após a validação consensual, assim inicia-se a formação do *blockchain.*

Nesse sentido, demonstra-se por intermédio da figura 3, as questões da segurança da informação orgânica no âmbito da Arquivologia, especificamente no quesito de como garantir a autenticidade dos documentos arquivísticos digitais de forma descentralizada, bem como corroborar com a garantia das trilhas de auditorias para fins de preservação digital de forma duradoura.

O resumo inicial – *Root Hash*, é obtido por intermédio de um algoritmo de função *hash*, o qual foi aplicado no documento arquivístico digital. Com base no metadado em questão, isto é, 608c270c referente ao bloco 00 - gênesis é possível

garantir a integridade, identidade, e, por sua vez, autenticidade documental, em vista de que ao comparar o documento arquivístico digital com o resumo *hash*, esse será válido. Todavia, quando o documento arquivístico digital sofrer quaisquer modificações como, por exemplo, migração da sua extensão em decorrência da obsolescência tecnológica, de um arquivo de texto (TXT), com o *hash* inicial de 608c270c convertido para *portable document format* (PDF), esse sofrerá alteração em seu resumo, posto que ocorreram modificações na camada lógica do objeto digital. O documento arquivístico digital receberá um novo resumo, tal como: 710a587e, posteriormente esse objeto digital com extensão em pdf sofrerá uma nova migração, da extensão pdf para pdf/a, alterando novamente sua camada lógica, e, consequentemente seu resumo, a qual será modificada para 745f763b.

Nesse cenário, a tecnologia *blockchain*, fornece a solução para problemática da autenticidade em ambientes descentralizados, bem como corrobora com a preservação digital de longa duração, uma vez que poderá garantir que essas migrações realizadas no documento arquivístico digital, são modificações autorizadas com uso de algoritmos de validação consensual, que propiciam um registro cronológico inalterável, na 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.

5 CONSIDERAÇÕES FINAIS

Os resultados obtidos permitiram demonstrar as relações, e, por conseguinte, as aplicações da tecnologia *blockchain* por intermédio do *ledger* no contexto da segurança da informação orgânica. Verificou-se que o protocolo do *blockchain* criptografa, envia e valida transações, que propiciam um registro cronológico inalterável de todas as operações realizadas.

Nessa direção, as vantagens de aplicação na autenticidade dos documentos realizadas com o *blockchain* reside na validação de forma distribuída, por um procedimento de validação consensual, quais sejam: *proof of work* - prova de trabalho, *proof of stake* - prova de participação. Essas formas de validações consensuais são

realizadas por meio de algoritmos que analisam os metadados dos registros criptografados, os quais verificam a integridade e identidade em vista de que é possível auditar os *hashes* de toda cadeia de blocos até o bloco zero, ou seja, bloco gênese do documento.

Sendo assim, torna-se exequível a preservação dos *hashes* das cadeias de registro ao longo do tempo, a qual garante a autenticidade dos documentos ao longo do seu ciclo de vida. A auditoria é realizada por meio do *ledger*, dos registros em conjunto com algoritmo denominado árvore de *merkle*, a qual garante que o documento não tenha sofrido alterações, corrompimento e adulterações.

Constata-se que esses procedimentos de auditoria em conjunto com os algoritmos supracitados podem corroborar com a autenticidade dos documentos, uma vez que, é possível, com base na tecnologia *blockchain*, garantir a integridade e identidade dos documentos, contribuindo, assim, com a preservação digital de longa duração, em vista de que essa tem por finalidade garantir o acesso da informação orgânica nos ambientes informacionais digitais. Por fim, a garantia da autenticidade, a qual contempla a integridade e identidade viabiliza-se com a aplicação da tecnologia *blockchain.*

REFERÊNCIAS

BARBOZA, E.S. **Autenticação multifatorial em hardaware para o processo de assinatura digital da nota fiscal eletrônica (NF-e)**. Orientador: Manoel Eusebio de Lima. 2018. 155f. Dissertação (Mestrado em Ciência da Computação), Universidade Federal de Pernambuco, Recife. 2018. Disponível em: https://attena.ufpe.br/bitstream/123456789/32403/1/DISSERTA%C3%87%C3%83O%20Eudes%20da%20Silva%20Barboza.pdf. Acesso em 20 dez. 2020.

BASHIR, I. **Mastering Blockchain**. 1. ed. Packt Publishing Ltd. 2017.

BRASIL. Ministério da Justiça (MJ). Arquivo Nacional (AN). Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Glossário de Documentos Arquivísticos Digitais.** 2020. Disponível em: http://antigo.conarq.gov.br/images/ctde/Glossario/glosctde_2020_08_07.pdf. Acesso em: 09 jan. 2021.

BRASIL. Ministério da Justiça (MJ). Arquivo Nacional (AN). Conselho Nacional de Arquivos (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE).

Resolução nº 37, de 19 de Dezembro de 2002 – Diretrizes para presunção da autenticidade de documentos arquivísticos digitais. 2002. Disponível em: http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf. Acesso em: 09 jan. 2021.

BRASIL. Casa Civil. Presidência da República. Instituto Nacional de Tecnologia da Informação (ITI). **Glossário**. 2021. Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/glossario. Acesso em: 03 jan. 2021.

BRASIL. Casa Civil. Presidência da República. Subchefia para assuntos jurídicos. **Lei nº 14.063, de 23 de setembro de 2020.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 23 dez. 2020.

BRASIL. Casa Civil. Presidência da República. Subchefia para assuntos jurídicos. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 23 nov. 2020.

DWORK, C.; NAOR, M. Pricing via processing or combatting junk mail. **CRYPTO .**1992. Advances in Cryptology - CRYPTO' 92, v. 740, p. 139–147, 1992.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/ INTERNATIONAL ELETROTECHNICAL COMISSION (ISO/IEC) 17799:2005 (E). 2005. Information technology. Security techniques. **Code of practice for information security management**. 2005.

JUELS. A.; JAKOBSSON. Proofs of works and bread pudding protocols. **Springer Science Bussines Media Dordrecht**, Boston, MA. v.23, 258–272, 1999. Disponível em: https://link.springer.com/content/pdf/10.1007%2F978-0-387-35568-9_18.pdf. Acesso em: 05 jan. 2021.

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: 04 jan. 2021.

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. 2020.

MARTINI, R. **Criptografia e cidadania digital**. Rio de Janeiro: Editora Ciência Moderna Ltda. 2001.

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

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: 01 nov. 2019.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. **Bitcoin and Cryptocurrency Technologies**‖. 2016. Princeton University Press.

NUNES, N. S. **Public Key Infrastructure** *(PKI)*, 2007. Disponível em: http://www.gta.ufrj.br/grad/07_2/delio/index.html. Acesso em 20 nov. 2020.

RESENDE. A. D. **Certificação Digital**. 2009. Disponível em: http://www.unigran.br/revistas/juridica/ed_anteriores/22/artigos/artigo09.pdf. Acesso em: 05 jan. 2021.

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: 20 dez. 2020.

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

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

TRAIN, S. **Como os Certificados Digitais estão Facilitando a Vida das Pessoas**. Identidade Digital. 2 ed. Revista e ampliada – São Paulo, 2007.