Blockchain como mecanismo de fortalecimento da segurança da informação: aplicações, riscos e desafios

Vitor Felipe B. A. Carneiro[1], Helio Carrara B. Junior[1], Alan Papafanurakis Heleno[1], Felipe Fonteles Belo[1], Bianca Cristina O. E. S. Silva [1], Josiel M. Figueiredo[1], Nelcileno V. S. Araujo[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCOMP)
Universidade Federal de Mato Grosso (UFMT),
Cuiabá, MT, Brasil

vitorfelip@gmail.com, helio.junior@sou.ufmt.br, alan.heleno@gmail.com
felipebelo@live.com, bianca.ces81@gmail.com, josie@ic.ufmt.br,
nelcileno@ic.ufmt.br

Abstract. *This paper analyzes the relationship between blockchain and information security, highlighting how the technology reinforces the pillars of confidentiality, integrity, and availability. Through a theoretical review, applications in sectors such as finance, healthcare, government, agribusiness, and digital identity are examined. The study also discusses risks and challenges, including scalability, 51% attacks, smart contract vulnerabilities, and energy consumption. Furthermore, it addresses legal implications under LGPD and GDPR, which create tensions between record immutability and the right to be forgotten. The conclusion indicates that blockchain is a promising paradigm but requires technical and legal solutions to enable its responsible adoption.*

Resumo. *Este artigo analisa a relação entre blockchain e segurança da informação, destacando como a tecnologia contribui para os pilares de confidencialidade, integridade e disponibilidade. A partir de uma revisão teórica, são exploradas aplicações em setores como finanças, saúde, governo, agronegócio e identidade digital. Também são discutidos riscos e desafios, como escalabilidade, ataques de 51%, vulnerabilidades em contratos inteligentes e consumo energético. Além disso, são abordadas as implicações legais frente à LGPD e ao GDPR, que geram tensões entre imutabilidade dos registros e o direito ao esquecimento. Conclui-se que o blockchain é um paradigma promissor, mas que demanda soluções técnicas e jurídicas para consolidar sua adoção responsável.*

1. Introdução

Nas últimas décadas, a segurança da informação tornou-se um dos principais desafios da sociedade digital. O avanço das tecnologias de informação e comunicação trouxe inúmeros benefícios para empresas, governos e indivíduos, mas também intensificou a ocorrência de ataques cibernéticos, vazamentos de dados e fraudes digitais. A proteção das informações deixou de ser apenas uma preocupação técnica e passou a assumir papel estratégico nas organizações, pois está diretamente relacionada à confiança dos usuários e à continuidade dos negócios [Stallings et al. 2008]. Nesse cenário, torna-se fundamental investigar novos mecanismos que ofereçam maior confiabilidade, transparência e resiliência, indo além dos modelos centralizados de segurança que historicamente se mostraram vulneráveis a falhas e ataques direcionados.

A tecnologia blockchain desponta como uma das inovações mais promissoras nesse contexto, por apresentar uma arquitetura descentralizada baseada em registros distribuídos e protegidos por criptografia avançada. Diferente das soluções tradicionais, em que um único ponto de falha pode comprometer todo o sistema, o blockchain distribui as informações em uma rede de nós, garantindo maior resiliência contra adulterações e acessos não autorizados [Narayanan et al. 2016]. Suas propriedades de imutabilidade, transparência e rastreabilidade oferecem vantagens significativas para a segurança da informação, uma vez que permitem validar transações de forma confiável, detectar tentativas de fraude e assegurar a integridade dos dados armazenados.

O blockchain reforça os pilares da segurança da informação, abordando conceitos como confidencialidade, integridade e disponibilidade, e tem sido aplicado em setores como o financeiro, a saúde e o agronegócio, promovendo inovação e rastreabilidade [Tapscott and Tapscott 2016]. Contudo, sua adoção enfrenta desafios técnicos e regulatórios, como a escalabilidade, o alto consumo energético e a necessidade de adequação a marcos legais de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR) [BRASIL 2018, Europeia 2016]. Esses fatores evidenciam que o avanço da tecnologia depende de equilíbrio entre inovação, sustentabilidade e conformidade jurídica.

Portanto, estudar a relação entre blockchain e segurança da informação significa compreender não apenas os avanços técnicos e as oportunidades que a tecnologia pode oferecer, mas também os riscos e limitações que precisam ser enfrentados para sua adoção responsável. A análise desse fenômeno revela-se necessária tanto para a comunidade acadêmica quanto para profissionais de tecnologia e gestores públicos, pois o blockchain está situado no ponto de convergência entre inovação, segurança e legislação, sendo capaz de redefinir práticas de confiança digital no futuro próximo.

2. Fundamentação teórica

A consolidação de uma sociedade cada vez mais conectada ampliou os desafios relacionados à proteção e ao controle das informações. Nesse cenário, compreender os fundamentos que sustentam a segurança da informação torna-se essencial para avaliar tecnologias emergentes, como o blockchain, que prometem redefinir a forma como lidamos com confiança e integridade no ambiente digital. A relação entre esses dois campos não é apenas técnica, mas também conceitual e estratégica, uma vez que envolve princípios de criptografia, governança de dados e conformidade legal.

2.1. Segurança da Informação e seus Pilares

A segurança da informação é definida como o conjunto de práticas, políticas e tecnologias destinadas a proteger a confidencialidade, integridade e disponibilidade dos dados, também conhecidos como CIA Triad (Confidentiality, Integrity, Availability). Esses três pilares são amplamente utilizados como referência internacional e representam a base para o desenvolvimento de sistemas seguros [Stallings et al. 2008]. A confidencialidade refere-se à proteção contra acessos não autorizados; a integridade busca garantir que a informação não seja alterada de forma indevida; e a disponibilidade assegura que os dados estejam acessíveis sempre que necessário. Além desses fundamentos, autores como Charles P. Pfleeger ressaltam que conceitos como autenticidade, responsabilidade e não

repúdio também se tornaram centrais no debate sobre segurança em ambientes digitais [Pfleeger and Pfleeger 2015].

A crescente sofisticação dos ataques cibernéticos e a expansão da superfície de exposição digital demonstram que os modelos tradicionais de segurança centralizada têm limitações significativas. Brechas em servidores, ataques distribuídos de negação de serviço (DDoS) e vulnerabilidades em bancos de dados centralizados são exemplos de falhas que podem comprometer milhões de registros sensíveis de uma só vez [Anderson 2010]. Nesse sentido, a busca por alternativas mais resilientes e descentralizadas motivou a atenção da comunidade científica para tecnologias disruptivas como o blockchain.

2.2. Blockchain: Conceito e Funcionamento

O blockchain pode ser definido como um livro-razão distribuído (distributed ledger) que registra transações de forma imutável e verificável em uma rede de nós. Cada bloco da cadeia contém um conjunto de transações que, uma vez validadas por mecanismos de consenso, são criptograficamente ligadas ao bloco anterior, formando uma sequência encadeada e resistente a alterações [Narayanan et al. 2016].

A descentralização é um dos principais diferenciais dessa tecnologia: ao invés de depender de uma autoridade central, a confiança é estabelecida coletivamente pelos participantes da rede, o que reduz a probabilidade de falhas únicas de segurança [Tapscott and Tapscott 2016]. Além disso, a utilização de algoritmos criptográficos de hash garante que qualquer modificação indevida nos registros seja facilmente detectável, reforçando a integridade e a rastreabilidade das informações.

Existem diferentes tipos de blockchain públicos, privados e híbridos que variam quanto ao nível de abertura e controle da rede. Enquanto blockchains públicos, como o Bitcoin, permitem a participação irrestrita de qualquer usuário, blockchains privados ou consórcios são mais adequados para ambientes corporativos e institucionais, em que é necessário maior governança sobre quem pode validar e registrar transações .

2.3. Blockchain e Segurança da Informação

Ao relacionar blockchain e segurança da informação, observa-se que a tecnologia contribui diretamente para os pilares da CIA Triad. A confidencialidade é reforçada pelo uso de criptografia assimétrica e assinaturas digitais, que asseguram que apenas os participantes autorizados tenham acesso aos dados. A integridade é garantida pela imutabilidade dos registros e pelo encadeamento dos blocos, que tornam praticamente impossível a alteração retroativa sem o consenso da rede. Já a disponibilidade é fortalecida pela descentralização, pois os dados são replicados em múltiplos nós, assegurando a continuidade do serviço mesmo em caso de falhas locais [Andoni et al. 2019].

Apesar dessas vantagens, desafios ainda persistem. Ataques de 51 por cento em blockchains públicos, vulnerabilidades em contratos inteligentes (smart contracts) e a necessidade de maior escalabilidade são aspectos que limitam sua aplicação plena. Além disso, a compatibilidade da tecnologia com legislações de proteção de dados, como a LGPD no Brasil e o GDPR na União Europeia, gera debates complexos, sobretudo em relação ao princípio da eliminação de dados pessoais, que entra em conflito com a característica de imutabilidade do blockchain [BRASIL 2018, Europeia 2016].

3. Metodologia

O presente estudo caracteriza-se como uma pesquisa exploratória e descritiva, fundamentada em revisão bibliográfica. De acordo com Gil [Gil 2008], a pesquisa exploratória é adequada quando o objetivo consiste em proporcionar maior familiaridade com o problema, visando torná-lo mais explícito ou construir hipóteses. Já a pesquisa descritiva busca descrever as características de determinado fenômeno ou estabelecer relações entre variáveis.

Nesse sentido, foram analisadas obras clássicas e recentes relacionadas à segurança da informação e ao blockchain, bem como artigos científicos indexados em bases acadêmicas como IEEE Xplore, ACM Digital Library, Scopus. O levantamento contemplou publicações que discutem os pilares da segurança da informação confidencialidade, integridade e disponibilidade em sua relação com a tecnologia blockchain, além de estudos que abordam aplicações práticas, riscos, desafios técnicos e implicações legais.

Conforme destacam Marconi e Lakatos [Marconi and Lakatos 2004], a revisão bibliográfica constitui etapa fundamental para identificar, selecionar e analisar contribuições relevantes já produzidas sobre o tema, permitindo situar o estudo no estado da arte. Assim, a metodologia adotada possibilitou a sistematização crítica de referenciais teóricos e normativos, incluindo a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR).

A escolha por essa abordagem justifica-se pela necessidade de mapear, organizar e discutir criticamente o conhecimento existente, sem recorrer à experimentação prática ou análise empírica. Dessa forma, o trabalho busca oferecer uma compreensão interdisciplinar e abrangente da relação entre blockchain e segurança da informação, articulando aspectos técnicos, legais e regulatórios.

4. O papel do blockchain no fortalecimento da segurança da informação

A relação entre blockchain e segurança da informação tem sido objeto de crescente interesse na literatura, especialmente porque a tecnologia reúne características diretamente alinhadas aos pilares clássicos da área. O primeiro aspecto a ser considerado é a confidencialidade, assegurada pelo uso de criptografia de chave pública e privada, que permite que apenas os participantes autorizados realizem transações ou tenham acesso a dados protegidos. As assinaturas digitais utilizadas no blockchain garantem que cada operação esteja vinculada de forma inequívoca a uma identidade criptográfica, dificultando ataques de falsificação ou usurpação de credenciais [Stallings et al. 2008].

O segundo pilar, a integridade, é um dos elementos mais robustos do blockchain. A estrutura encadeada de blocos, combinada com algoritmos de hash criptográfico, torna qualquer tentativa de modificação retroativa de dados praticamente impossível sem o consenso da rede. Isso significa que uma transação, uma vez validada e adicionada à cadeia, torna-se imutável, assegurando a veracidade do histórico de registros. Essa propriedade é fundamental para auditorias e rastreabilidade de dados, garantindo confiança em cenários de negócios, governos e cadeias produtivas [Narayanan et al. 2016, Tapscott and Tapscott 2016].

O terceiro pilar, a disponibilidade, também é fortalecido pelo blockchain. Como os registros são distribuídos em múltiplos nós da rede, não há um ponto único de falha,

característica que confere maior resiliência contra ataques cibernéticos e falhas de infraestrutura. Essa descentralização garante que o sistema continue acessível mesmo diante de falhas locais ou regionais, um avanço em relação a bancos de dados centralizados que podem ser facilmente derrubados por ataques direcionados [Andoni et al. 2019].

Entretanto, apesar dessas vantagens, a adoção do blockchain na segurança da informação não está isenta de riscos e limitações. Um dos principais problemas apontados é a possibilidade de ataques de 51%, em que agentes maliciosos controlam a maioria do poder de mineração e podem comprometer a confiabilidade da rede. Além disso, vulnerabilidades em contratos inteligentes (smart contracts) têm se mostrado pontos críticos de exploração, uma vez que códigos inseguros podem ser explorados para fraudes e perdas financeiras [Zheng et al. 2017]. Outro desafio relevante diz respeito à escalabilidade, pois blockchains públicos como o Bitcoin e o Ethereum ainda enfrentam dificuldades para lidar com um grande volume de transações sem comprometer o desempenho.

No campo jurídico, surgem discussões complexas quanto à compatibilidade do blockchain com legislações de proteção de dados. A Lei Geral de Proteção de Dados e o Regulamento Geral sobre a Proteção de Dados estabelecem o direito à eliminação de dados pessoais, mas essa prerrogativa entra em conflito direto com a imutabilidade característica da tecnologia. Nesse sentido, pesquisadores apontam a necessidade de novas soluções técnicas e modelos híbridos de governança que conciliem a inovação com a conformidade legal [BRASIL 2018, Europeia 2016].

5. Aplicações e exemplos práticos

O potencial do blockchain extrapola o universo das criptomoedas, sendo cada vez mais explorado em diferentes setores que demandam altos níveis de segurança e confiabilidade. A tecnologia, ao aliar descentralização, imutabilidade e rastreabilidade, tem possibilitado novos modelos de proteção de dados, mitigação de fraudes e fortalecimento da governança digital.

5.1. Setor Financeiro

O setor financeiro foi o primeiro a adotar o blockchain em larga escala, por meio das criptomoedas, como o Bitcoin. Entretanto, a aplicação da tecnologia vai além das moedas digitais. Bancos e instituições financeiras têm explorado o uso de blockchains privados para liquidação de transações, sistemas de pagamento interbancário e prevenção à lavagem de dinheiro. A rastreabilidade das operações e a eliminação de intermediários tornam as transações mais rápidas, transparentes e menos suscetíveis a fraudes [Narayanan et al. 2016, Tapscott and Tapscott 2016].

5.2. Saúde

Na área da saúde, o blockchain é aplicado no gerenciamento de prontuários eletrônicos, assegurando que os dados dos pacientes sejam armazenados de forma íntegra, acessível e rastreável apenas por profissionais autorizados. Essa abordagem reduz o risco de adulterações e acessos indevidos, além de facilitar a interoperabilidade entre diferentes sistemas hospitalares e laboratórios. Estudos apontam que o uso do blockchain nesse setor contribui para maior confiança, tanto dos pacientes quanto das instituições de saúde [Zheng et al. 2017, Andoni et al. 2019].

5.3. Governo e Transparência Pública

Governos em diversos países têm adotado soluções baseadas em blockchain para aumentar a transparência e reduzir práticas de corrupção. Aplicações incluem o registro de contratos públicos, sistemas de votação eletrônica e gestão de identidades digitais. No Brasil, discute-se a possibilidade de adoção dessa tecnologia em portais de transparência e no acompanhamento de licitações, de modo a assegurar maior integridade e rastreabilidade dos processos administrativos [Anderson 2010, BRASIL 2018].

5.4. Agronegócio

No agronegócio, o blockchain tem sido amplamente explorado para promover rastreabilidade, transparência e eficiência nas cadeias produtivas [Tapscott and Tapscott 2016, Andoni et al. 2019]. Pesquisas demonstram que sistemas de rastreabilidade baseados em blockchain aumentam a segurança e a confiabilidade das transações comerciais agrícolas, especialmente na cadeia da soja [Salah et al. 2019]. Esses sistemas permitem verificar a procedência dos produtos e garantir conformidade com padrões de sustentabilidade e normas sanitárias internacionais, além de reforçar a confiança do consumidor [Kamble et al. 2020].

Além disso, estudos recentes apontam que a adoção do blockchain pode contribuir para o cumprimento dos Objetivos de Desenvolvimento Sustentável da ONU, ao oferecer maior transparência e controle nas operações da cadeia alimentar [Chandan et al. 2023]. A integração de contratos inteligentes automatiza processos de exportação e comercialização, reduzindo custos operacionais e mitigando riscos de fraude em cadeias globais de fornecimento [Azevedo et al. 2023].

5.5. Identidade Digital e Autenticação

Outra aplicação relevante do blockchain é na gestão de identidades digitais. Soluções baseadas em blockchain permitem que indivíduos controlem de forma autônoma suas informações pessoais, compartilhando apenas os dados estritamente necessários com terceiros. Esse modelo, conhecido como Self-Sovereign Identity (SSI), está em consonância com legislações de proteção de dados, como a LGPD e o GDPR, e representa um avanço frente aos modelos tradicionais de autenticação centralizada [Europeia 2016, Stallings et al. 2008].

A análise dos diferentes setores mostra que, apesar das aplicações específicas, todos convergem no fortalecimento da segurança da informação. O blockchain destaca-se por oferecer confiança, resiliência e transparência, unindo áreas diversas sob a lógica da descentralização e da imutabilidade. Sua relevância ultrapassa nichos e o consolida como elemento central nas discussões sobre segurança e governança digital. A Tabela 1 apresenta um resumo das principais aplicações por setor.

Setor	Principais Aplicações e Benefícios
Setor Financeiro	Uso inicial com criptomoedas e posterior expansão para liquidação de transações, sistemas interbancários e prevenção à lavagem de dinheiro. Destacam-se a rastreabilidade, transparência e redução de fraudes [Narayanan et al. 2016, Tapscott and Tapscott 2016].
Saúde	Gerenciamento seguro de prontuários eletrônicos, com integridade e controle de acesso. Facilita interoperabilidade entre sistemas e aumenta a confiança de pacientes e instituições [Zheng et al. 2017, Andoni et al. 2019].
Governo e Transparência Pública	Registro de contratos públicos, votação eletrônica e gestão de identidades digitais. Foco na transparência, integridade e rastreabilidade administrativa [Anderson 2010, BRASIL 2018].
Agronegócio	Rastreabilidade da cadeia produtiva, certificação de origem e sustentabilidade dos produtos. Uso de contratos inteligentes para automatizar exportação e comercialização [Tapscott and Tapscott 2016, Andoni et al. 2019].
Identidade Digital e Autenticação	Implementação de identidades digitais autônomas (Self-Sovereign Identity), alinhadas à LGPD e ao GDPR, com controle descentralizado dos dados pessoais [Europeia 2016, Stallings et al. 2008].

Tabela 1. Resumo das aplicações práticas do blockchain por setor

6. Desafios e riscos

Apesar do potencial do blockchain para fortalecer a segurança da informação em diferentes setores, sua adoção em larga escala apresenta desafios e riscos que não podem ser ignorados. Um dos principais pontos de atenção refere-se à escalabilidade. Blockchains públicos, como o Bitcoin e o Ethereum, ainda enfrentam dificuldades para processar um grande volume de transações de forma rápida e eficiente. A necessidade de validação distribuída e o consumo energético elevado de mecanismos de consenso como Proof of Work tornam a tecnologia menos viável em contextos que exigem alta velocidade e baixo custo [Zheng et al. 2017].

Outro risco importante está relacionado aos ataques de 51%, em que um grupo de mineradores ou participantes maliciosos controla a maioria do poder computacional da rede, podendo manipular transações, criar registros duplos ou comprometer a confiança no sistema. Embora esse cenário seja mais difícil em redes de grande porte, blockchains menores ou de nicho estão mais suscetíveis a esse tipo de ataque [Narayanan et al. 2016].

Além disso, os contratos inteligentes (smart contracts) introduzem novas vulnerabilidades. Como esses contratos são executados automaticamente com base em código previamente definido, erros de programação ou brechas de segurança podem ser explorados por atacantes, resultando em perdas financeiras significativas ou comprometimento de dados sensíveis. Casos reais de falhas em contratos inteligentes, como os ataques à plataforma DAO em 2016, demonstram que a imutabilidade do blockchain, embora seja uma vantagem, também dificulta a correção de erros e a reversão de danos [Anderson 2010].

Do ponto de vista regulatório, o blockchain enfrenta um dos dilemas mais complexos: a compatibilidade com legislações de proteção de dados pessoais. Normas como a LGPD no Brasil e o GDPR na União Europeia garantem direitos como a portabilidade e a exclusão de dados pessoais, mas essas exigências entram em conflito com a imutabilidade característica da tecnologia. Isso gera um paradoxo entre o direito ao esquecimento e a impossibilidade técnica de apagar registros já validados na cadeia. Pesquisadores e órgãos reguladores têm discutido soluções híbridas, como o armazenamento off-chain de dados pessoais sensíveis, de modo que apenas referências criptográficas permaneçam na blockchain [BRASIL 2018, Europeia 2016].

Outro desafio relevante está ligado à adoção institucional e cultural. Organizações muitas vezes encontram resistência em migrar de sistemas centralizados, já estabelecidos, para estruturas descentralizadas que exigem novas competências técnicas, adaptações regulatórias e mudanças de governança. Além disso, o custo inicial de implementação e a falta de profissionais especializados podem dificultar a integração do blockchain em ambientes corporativos e governamentais [Stallings et al. 2008].

Dessa forma, embora o blockchain represente avanços notáveis para a segurança da informação, é fundamental reconhecer que seus riscos e limitações ainda exigem soluções técnicas, legais e organizacionais. A superação desses obstáculos será determinante para que a tecnologia se consolide como base confiável para ecossistemas digitais mais seguros e transparentes.

7. Considerações legais

O uso do blockchain em ambientes corporativos, governamentais e sociais não pode ser analisado de forma isolada de seu contexto jurídico. A tecnologia, por sua característica descentralizada e imutável, apresenta desafios específicos para sua compatibilidade com legislações de proteção de dados pessoais, como a LGPD no Brasil e o GDPR na União Europeia [Zafar 2025]. Ambas as legislações estabelecem direitos fundamentais aos titulares, entre os quais se destacam o direito ao esquecimento, a portabilidade dos dados e a eliminação de informações pessoais quando solicitado. Esses princípios, contudo, entram em choque com a natureza do blockchain, uma vez que os dados registrados em blocos são projetados para serem permanentes e inalteráveis [BRASIL 2018, Europeia 2016].

No caso brasileiro, a LGPD reforça a importância da finalidade e da minimização do tratamento de dados pessoais. Ou seja, somente devem ser coletados os dados estritamente necessários para a execução de uma finalidade legítima. Essa exigência se mostra desafiadora em blockchains públicos, em que os dados ficam acessíveis a todos os participantes da rede, mesmo que de forma pseudonimizada. Além disso, a definição de quem seria o controlador e o operador dos dados dentro de uma rede distribuída é um ponto controverso, pois a responsabilidade jurídica pode se diluir entre múltiplos atores, dificultando a aplicação de sanções ou a responsabilização por incidentes de segurança [BRASIL 2018].

Na União Europeia, o GDPR é ainda mais rigoroso ao tratar de direitos relacionados ao apagamento e à retificação de informações. Esse ponto entra em conflito direto com a imutabilidade do blockchain, levantando debates sobre até que ponto a pseudonimização e a anonimização dos dados podem ser consideradas soluções compatíveis [Finck 2018]. Alguns autores defendem que o uso de técnicas como o armazenamento off-chain, em

que dados pessoais não são gravados diretamente na blockchain, mas sim armazenados em bases externas com apenas referências criptográficas na cadeia, pode ser um caminho viável para mitigar o problema [Zheng et al. 2017].

A natureza global das redes blockchain impõe desafios significativos de jurisdição, pois transações e registros podem estar distribuídos em múltiplos países submetidos a legislações divergentes [Anderson 2010]. Essa fragmentação gera insegurança jurídica e evidencia que a compatibilidade entre blockchain e normas de proteção de dados ainda está em amadurecimento. O avanço seguro dessa tecnologia depende da cooperação entre reguladores, pesquisadores e profissionais da área, a fim de desenvolver modelos que conciliem inovação, segurança e efetiva proteção dos direitos dos titulares de dados pessoais.

8. Conclusão

O presente trabalho buscou analisar a relação entre o blockchain e a segurança da informação, explorando seus fundamentos, aplicações práticas em diferentes setores, riscos e desafios, bem como suas implicações legais. A revisão teórica mostrou que a tecnologia se conecta diretamente aos pilares clássicos da segurança confidencialidade, integridade e disponibilidade ao oferecer um modelo descentralizado, resistente a adulterações e capaz de proporcionar maior resiliência em sistemas críticos [Stallings et al. 2008, Narayanan et al. 2016].

A análise das aplicações práticas evidenciou que setores distintos, como o financeiro, a saúde, o governo, o agronegócio e a gestão de identidades digitais, convergem na adoção do blockchain com o objetivo de fortalecer a confiança, a rastreabilidade e a transparência dos dados. Esse caráter transversal indica que a tecnologia não se limita a um nicho, mas atua como um paradigma de inovação, capaz de remodelar ecossistemas informacionais ao redor do mundo [Tapscott and Tapscott 2016, Andoni et al. 2019].

Entretanto, os desafios e riscos identificados demonstram que a adoção do blockchain não é uma solução absoluta. Questões como a escalabilidade, os ataques de 51%, a vulnerabilidade dos contratos inteligentes e os elevados custos energéticos ainda limitam sua aplicação em larga escala. Além disso, o conflito entre a imutabilidade dos registros e as exigências de legislações de proteção de dados pessoais como a LGPD no Brasil e o GDPR na União Europeia revela tensões entre o potencial técnico da tecnologia e as normas jurídicas que buscam resguardar direitos fundamentais [BRASIL 2018, Europeia 2016].

Do ponto de vista legal e regulatório, a discussão mostra-se ainda em construção, exigindo diálogo interdisciplinar entre tecnologia, direito e governança. Soluções como o armazenamento off-chain, o uso de técnicas de anonimização e novos modelos de consenso regulatório podem oferecer caminhos para compatibilizar inovação e proteção de dados.

Diante disso, pode-se afirmar que o blockchain representa um instrumento promissor, mas que deve ser compreendido dentro de um contexto mais amplo, que inclua riscos técnicos, desafios de implementação e barreiras regulatórias. Mais do que uma ferramenta tecnológica, trata-se de um campo de pesquisa e prática interdisciplinar, cujo impacto dependerá da capacidade de alinhar sua evolução aos princípios éticos, legais e sociais que regem a era digital.

Referências

Anderson, R. (2010). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, 100:143–174.

Azevedo, P., Gomes, J., and Romão, M. (2023). Supply chain traceability using blockchain. *Operations Management Research*, 16(3):1359–1381.

BRASIL, G. d. (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). *Diário oficial da União*, 155(157 seção 1):59–64.

Chandan, A., John, M., and Potdar, V. (2023). Achieving un sdgs in food supply chain using blockchain technology. *Sustainability*, 15(3):2109.

Europeia, U. (2016). Regulamento (ue) 2016/679 do parlamento europeu e do conselho. *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva*, 95:46.

Finck, M. (2018). Blockchains and data protection in the european union. *Eur. Data Prot. L. Rev.*, 4:17.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social*. 6. ed. Ediitora Atlas SA.

Kamble, S. S., Gunasekaran, A., and Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International journal of information management*, 52:101967.

Marconi, M. d. A. and Lakatos, E. M. (2004). *Metodologia científica*, volume 4. Atlas São Paulo.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Pfleeger, C. P. and Pfleeger, S. L. (2015). *Security in Computing*. Pearson Education, London, 5th edition.

Salah, K., Nizamuddin, N., Jayaraman, R., and Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. *Ieee Access*, 7:73295–73305.

Stallings, W., Bressan, G., and Barbosa, A. (2008). *Criptografia e segurança de redes* . Pearson Educacion.

Tapscott, D. and Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Zafar, A. (2025). Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. *Journal of Cybersecurity*, 11(1):tyaf002.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee.