

**BLOCKCHAIN PERMISSIONADA NA ADMINISTRAÇÃO PÚBLICA BRASILEIRA:
UMA ANÁLISE SOBRE OS IMPACTOS NA TRANSPARÊNCIA DE PROCESSOS
GOVERNAMENTAIS E NA SEGURANÇA DE DADOS PÚBLICOS DIGITAIS**

***PERMISSIONED BLOCKCHAIN IN BRAZILIAN PUBLIC ADMINISTRATION: AN
ANALYSIS OF THE IMPACTS ON THE TRANSPARENCY OF GOVERNMENT PROCESSES AND
ON THE SECURITY OF DIGITAL PUBLIC DATA***

Guilherme Anaia Costa¹
Alessandro Firmiano de Jesus²

RESUMO

O trabalho propõe-se a analisar os impactos da implementação da tecnologia de blockchain permissionada na transparência de processos governamentais e segurança de dados na administração pública brasileira. A tecnologia, que opera como um livro-razão distribuído e imutável cujos dados são gerenciados por um mecanismo de consenso pré-definido, demonstra resultados positivos no campo da segurança de dados e governança digital. Diversos estudos de caso referenciam seu potencial em otimizar e automatizar processos burocráticos e introduzir soluções inovadoras voltadas ao armazenamento seguro e eficiente de dados. Para a concretização desta análise, o método de pesquisa incluirá a revisão da literatura, visando à compreensão do funcionamento da blockchain e a análise de estudos de caso sobre sua implementação no setor público, abrangendo experiências internacionais, em países como Estônia, Geórgia, Estados Unidos e no Brasil, para exposição dos resultados esquematicamente em quadros e tabelas, considerando as diferenças políticas, econômicas e tecnológicas entre os casos internacionais em relação ao Brasil e seu ordenamento jurídico. Dessa forma, pela identificação dos conceitos relacionados à tecnologia, descrição do funcionamento de redes blockchain permissionadas, análise de estudos de caso nacionais e internacionais foi realizada a análise dos impactos causados pela implementação da blockchain permissionada na administração pública brasileira. O objetivo do estudo, portanto, consiste em fornecer uma análise crítica sobre o impacto da implementação dessa tecnologia na segurança de dados e na transparência administrativa, aplicada ao contexto da administração pública brasileira com base nas iniciativas nacionais que se encontram em fase de estudo, desenvolvimento ou operação.

Palavras-chave: blockchain; administração pública; segurança cibernética; livro-razão distribuído; dados.

¹ Cadete Intendente do 4º Esquadrão (Turma *Ártemis*, 2025).

² Prof. Titular de Matemática na Academia da Força Aérea e integrante do Grupo de Pesquisa em Modelagem Matemática e Computacional - GMMC. E-mail: firmianoafj@fab.mil.br

ABSTRACT

This paper aims to analyze the impacts of implementing permissioned blockchain technology on the transparency of government processes and data security in the Brazilian public administration. The technology, which operates as a distributed and immutable ledger whose data is managed by a predefined consensus mechanism, has demonstrated positive results in the field of data security and digital governance. Several case studies reference its potential to optimize and automate bureaucratic processes and introduce innovative solutions aimed at the safe and efficient storage of data. To carry out this analysis, the research method will include a literature review, aiming at understanding how blockchain works and the analysis of case studies on its implementation in the public sector, covering international experiences in countries such as Estonia, Georgia, the United States and Brazil, to present the results schematically in charts and tables, considering the political, economic and technological differences between international cases in relation to Brazil and its legal system. Thus, by identifying concepts related to technology, describing how permissioned blockchain networks work, and analyzing national and international case studies, an analysis of the impacts caused by the implementation of permissioned blockchain in the Brazilian public administration was carried out. The objective of the study, therefore, is to provide a critical analysis of the impact of the implementation of this technology on data security and administrative transparency, applied to the context of the Brazilian public administration based on national initiatives that are in the study, development, or operation phase.

Keywords: blockchain; public administration; cybersecurity; distributed ledger; data.

INTRODUÇÃO

1 CONTEXTUALIZAÇÃO DA PESQUISA

Em 2008, uma pessoa ou um grupo de pessoas, sob o pseudônimo de Satoshi Nakamoto, disponibilizaram publicamente o White Paper: “*Bitcoin: A Peer-to-Peer Electronic Cash System*”. O documento revelava informações técnicas sobre o funcionamento da estrutura subjacente necessária ao funcionamento da criptomoeda bitcoin: a *blockchain*, um livro-razão distribuído e imutável (Nakamoto, 2008). A tecnologia inicialmente atendia estritamente ao propósito de registrar transações financeiras de forma descentralizada e segura, com a finalidade de substituir o papel de instituições financeiras tradicionais como bancos e sem a necessidade de intermediários no processo (Antonopoulos, 2018). Como afirma Antonopoulos (2018), a compreensão aprofundada do funcionamento da blockchain deu origem a modelos com diversas outras finalidades e áreas de aplicação, como o modelo permissionado, mais adequado ao setor público e empresarial.

Segundo o Tribunal de Contas da União (Acórdão TCU nº 1613/2020), a tecnologia de livro-razão distribuído tem o potencial de ter um efeito transformador na administração pública brasileira

tanto por apresentar as características não encontradas nos sistemas convencionais quanto por ser capaz de reduzir o tempo requerido para a conclusão de processos burocráticos.

Como pontua Amorim e Malagolli (2022), há, no Brasil, muitos processos burocráticos, dentre eles, a confecção de documentos oficiais, processo composto por diversas etapas burocráticas, que envolvem a participação de muitos agentes intermediários. Para que documentos simples, como um contrato de cobrança de dívidas, adquiram validade legal no Brasil, é necessária a assinatura de três vias fiscais pelas partes envolvidas e testemunhas, além do registro em cartório. Devido às etapas demandadas, tal processo leva vários dias para ser completado e exemplifica tanto o cenário burocrático quanto a necessidade de tecnologias que podem tornar esse processo mais ágil, eficiente, transparente e seguro tal como exige a legislação nacional vigente.

Com base na contextualização apresentada, este trabalho tem como objeto de estudo o impacto da implementação da blockchain permissionada na administração pública brasileira. A aplicação de uma abordagem quali quantitativa torna-se imprescindível para a compreensão do potencial impacto da aplicação da tecnologia no cenário burocrático atual do Brasil, quanto a eficiência operacional, segurança cibernética, integridade, rastreabilidade e auditabilidade de dados públicos.

1.1 Justificativa

A blockchain permissionada tem um número limitado e conhecido de nós participantes autorizados. Essas características permitem o controle mais centralizado de uma rede e menor necessidade de confiança nos usuários, o que, de acordo com Bakos e Halaburda (2021), viabiliza a inserção de algoritmos incomparavelmente menos custosos e menos robustos que os utilizados em uma rede blockchain pública como a do bitcoin, na qual qualquer pessoa pode se tornar um participante. O resultado obtido na aplicação desses algoritmos menos complexos é a maximização da escalabilidade e da eficiência em termos de escrita de dados por segundo, que são características vantajosas para sistemas governamentais e empresariais (Bakos; Halaburda, 2021).

Os projetos baseados no modelo de blockchain permissionada na administração pública brasileira incluem o B-Connect, ferramenta criada pelo Serviço Federal de Processamento de Dados (SERPRO) para armazenar os dados do Certificado de Operador Econômico Autorizado (OEA) de empresas; o Drex, uma moeda digital em desenvolvimento pelo Banco Central do Brasil que tem o objetivo de funcionar como a versão digital do Real (Souza; Bezerra, 2024); o TruBudget, um sistema que permite a rastreabilidade de recursos do Fundo Amazonia a clientes e empresas, e o SOL, uma plataforma digital que permite a execução de licitações públicas.

Ademais, estudos de caso conduzidos na Estônia (Jalakas, 2018), na Geórgia (Shang; Price, 2019) e implementações no âmbito militar de países como os Estados Unidos, na Agência de Projetos de Pesquisa Avançada de Defesa (DARPA) e na Organização do Tratado do Atlântico Norte (OTAN), demonstram que a adoção da tecnologia em ambientes governamentais está em análise devido ao potencial aumento da eficiência dos processos burocráticos e introdução de uma sólida camada de segurança contra ataques cibernéticos que a tecnologia pode proporcionar (Ahmad *et al.* 2021).

Os estudos de caso citados e analisados revelam o impacto prático que o uso de sistemas baseados em blockchain permissionada podem trazer ao setor público em relação ao aprimoramento da segurança de dados, governança digital, economia de recursos, rastreabilidade e celeridade na elaboração de documentos oficiais e na tramitação de processos burocráticos. Tais análises buscaram identificar os impactos causados no setor público de países que aderiram à tecnologia para comparativamente descrever o impacto da tecnologia na administração pública do Brasil e, por meio da revisão de estudos de caso das iniciativas nacionais, apresentar uma análise das implicações observáveis.

Portanto, o estudo se justifica por contribuir para pesquisas futuras sobre o tema ao apresentar, por meio da revisão bibliográfica de estudos de caso nacionais e internacionais, uma análise crítica abrangente e de abordagem quali-quantitativa sobre os impactos concretos observáveis, na segurança de dados públicos e transparência de processos governamentais, decorrentes da implementação da disruptiva e promissora blockchain permissionada na administração pública brasileira e aplicação do conceito de livro-razão distribuído em sistemas.

1.2 Estrutura do trabalho

Este estudo, fundamentado nas aplicações práticas da tecnologia em diversos países e nas iniciativas desenvolvidas no Brasil, explora como a blockchain pode impactar a transparência de processos governamentais e a segurança de dados digitais. A pesquisa estruturou-se em uma análise quali-quantitativa comparativa dos estudos de caso nacionais e internacionais publicados a respeito do tema, baseando-se na identificação, descrição e exposição esquemática em quadros e tabelas dos impactos observados no setor público de diversos países com a implementação da blockchain permissionada, com foco na segurança de dados digitais e transparência de processos governamentais.

Portanto, este trabalho se estruturou na descrição do funcionamento da tecnologia e na análise crítica dos dados obtidos na literatura acadêmica disponível sobre o tema, comparação dos resultados dos estudos de caso internacionais e nacionais e estudo do impacto da implementação da tecnologia

na administração pública brasileira. Desse modo, este estudo buscou responder: “**Quais são os possíveis impactos da implementação da blockchain permissionada no âmbito da administração pública brasileira em relação à transparência de processos governamentais e segurança de dados público digitais?**”

OBJETIVOS

1.3 OBJETIVO GERAL

Avaliar o potencial impacto da implementação da tecnologia blockchain permissionada na administração pública brasileira, com foco na transparência de processos governamentais e na segurança de dados digitais, mediante a revisão da literatura acadêmica disponível e exploração de estudos de caso nacionais e internacionais de forma comparativa, visando identificar desafios, métricas de transparência, como número de auditorias bem-sucedidas, redução de fraudes; métricas de segurança de dados, como integridade dos dados, número de violações de dados; e avaliação de processos governamentais específicos como registro de imóveis, licitações e emissão de documentos.

1.4 OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral, são definidos os seguintes objetivos específicos:

- A) **Identificar** conceitos relacionados ao modelo de blockchain permissionada.
- B) **Descrever** o funcionamento de uma blockchain permissionada.
- C) **Analisar** estudos de caso internacionais e aplicações práticas nacionais da blockchain permissionada na administração pública.
- D) **Identificar** os possíveis impactos decorrentes da implementação da tecnologia na administração pública brasileira com ênfase na transparência de processos governamentais e segurança de dados digitais.

2 A BLOCKCHAIN PERMISSIONADA NA ADMINISTRAÇÃO PÚBLICA BRASILEIRA

2.1 REFERENCIAL TEÓRICO

2.1.1 O mecanismo de consenso e a segurança em uma blockchain

Segundo Antonopoulos (2018), a blockchain pode ser rigorosamente definida como um livro-razão distribuído e imutável constituído por uma cadeia de blocos de dados encadeada por criptografia, distribuída e atualizada pelo protocolo de rede Peer-to-Peer (Ponto a Ponto) e gerenciada por um mecanismo de consenso, que define os critérios de validação, aceitação, rejeição e inclusão de novos blocos para um subconjunto de usuários que possuem uma cópia local completa da blockchain, os nós completos, e reúnem os requisitos de hardware e rede necessários para executar plenamente o mecanismo.

Em uma rede descentralizada, surge o problema da confiança para todo usuário, que pode potencialmente apresentar comportamento malicioso, denominado nó bizantino (Nakamoto, 2008). O conceito surge de um dilema clássico da computação: o Problema dos Generais Bizantinos. Nele, um grupo de generais precisa entrar em consenso sobre atacar uma cidade simultaneamente, porém encontram-se geograficamente afastados e dependentes de mensageiros para se comunicarem por meio de cartas e entrarem em consenso sobre a data e hora exatas do ataque (Antonopoulos, 2018). Caso os generais não entrem em consenso sobre atacar a cidade simultaneamente, o plano falhará. O problema surge devido à incerteza quanto a veracidade das mensagens, que podem ter sido adulteradas por mensageiros ou generais traidores, criando o dilema, que consiste em como estabelecer o consenso sem a necessidade de confiança em todos os participantes de uma rede de comunicação (Antonopoulos, 2018).

Nesse contexto, uma solução para o problema advém da lógica empregada no funcionamento do mecanismo de consenso, o qual atua na forma de um algoritmo para atingir o consenso sobre a validade de uma transação sem a necessidade de confiança em todos os participantes, viabilizando sua implementação em sistemas de acesso público de forma segura (Bashir, 2018).

O Algoritmo de Hash Seguro, ou Secure Hash Algorithm (SHA)-256, criado pela Agência Nacional de Segurança dos Estados Unidos (NSA) é responsável por viabilizar o funcionamento do mecanismo de consenso. Ele gera uma saída única para quaisquer entradas de dados, representada pelo conjunto de 64 caracteres denominada hash (NIST, 2015). A saída, de acordo com o National Institute of Standards and Technology (NIST) (2015), vale-se intrinsecamente de três características,

que tornam esse algoritmo apropriado para o uso em uma rede do tipo blockchain, sendo elas: Irreversibilidade, Resistência à Colisão e Efeito Avalanche. A primeira implica que os dados de saída não podem ser revertidos para os dados de entrada; a segunda, que dados de entrada distintos nunca geram a mesma saída; a terceira, que quaisquer alterações nos dados de entrada, geram uma mudança completa nos dados de saída.

Em resumo, o mecanismo de consenso transforma a blockchain em uma tecnologia robusta no âmbito da segurança digital e da administração pública, como aponta Taylor (2020). Ele evita ataques cibernéticos e alteração nos dados armazenados, tornando essas ações extremamente custosas por exigirem o recálculo dos hashes de todos os blocos da cadeia que precedem o bloco a ser alterado, devido ao encadeamento criado pelo SHA-256. Isso define fundamentalmente o critério para o consenso da rede sobre a validade de uma transação, como sendo a aceitação pela maioria dos nós participantes da rede (51% do poder computacional) de que ela é legítima, conforme descreve Antonopoulos (2018).

2.1.2 O modelo permissionado de Blockchain na administração pública

Toda blockchain pode ser criada com base na maximização de apenas duas das três características essenciais num sistema distribuído: escalabilidade, segurança e descentralização. Essa restrição é conhecida como trilema das blockchains, uma limitação da tecnologia, que impede a maximização simultânea das três características. Ou seja, quando duas estão otimizadas, uma fica comprometida (Antonopoulos, 2018).

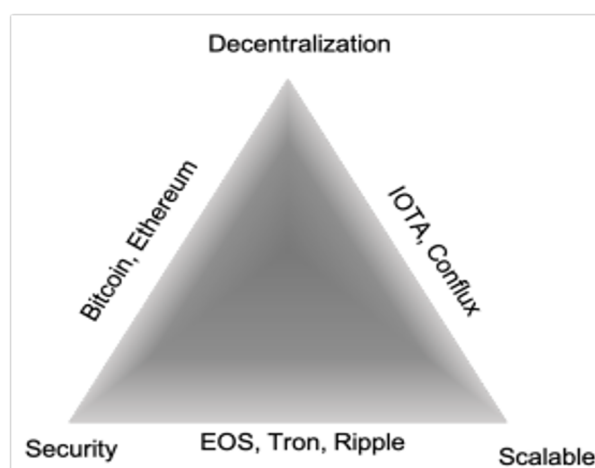


Figura 1 - Trilema das blockchains

Fonte: Trifecta Team (2019)

Desse modo, de acordo com a Figura 1, uma blockchain, ao se propor a ser simultaneamente segura e descentralizada, apresenta baixa escalabilidade. Na rede bitcoin, cada bloco de dados é gerado num intervalo variável de 5 (cinco) a 15 (quinze) minutos (Antonopoulos, 2018) devido à execução de um mecanismo de consenso complexo, que viabiliza a maximização da descentralização sem o comprometimento da segurança da rede, exigindo, entretanto, o comprometimento da escalabilidade.

Em uma blockchain permissionada e projetada para atender aos requisitos de maximização da escalabilidade e segurança para sua implementação na administração pública, como a Blockchain do modelo industrial de Infraestrutura de Assinaturas Sem Chave (KSI) e Hyperledger Fabric, a descentralização é propositalmente reduzida para compensação do trade-off postulado pelo trilema das blockchains, pois o número de nós completos é restringido a um grupo pré-definido e conhecido de participantes autorizados, de forma a exigir um mecanismo de consenso menos robusto, aumentando a escalabilidade e a segurança do sistema (Bashir, 2018).

Para Amorim e Malagolli (2022), a aplicação do modelo permissionado considera o trilema num cenário em que há o armazenamento de grandes volumes de dados e um conjunto limitado de agentes verificadores e validadores dos blocos a serem consolidados na rede. Esses fatores, junto a implementação de um mecanismo de consenso menos robusto em comparação ao da Prova de Trabalho, promovem a escalabilidade em detrimento da descentralização, aspecto menos relevante num cenário em que a blockchain serve ao único propósito de armazenar digitalmente dados e documentos da administração pública de forma imutável, transparente e segura.

Segundo Bakos e Halaburda (2021), o consumo de energia das blockchains permissionadas é consideravelmente menor por requererem uma quantidade menor de nós completos pré-determinados e proporcionalmente mais confiáveis associados à rede, além do uso de um mecanismo de consenso mais eficiente e escalável.

Fatores como a escalabilidade, segurança e eficiência energética justificam a escolha por blockchains permissionadas no ambiente empresarial e na administração pública (Arão, 2024).

2.1.3 Árvore de Merkle e arquitetura técnica da KSI Blockchain e Hyperledger Fabric

Antonopoulos (2018) define a Árvore de Merkle como uma estrutura que sumariza todos os hashes de dados registrados em uma blockchain e os resume num único hash para cada bloco, de modo a facilitar a verificação da integridade de grandes volumes de dados por meio da Raiz de Merkle. A árvore é o resultado da função SHA-256 aplicada sucessivamente às combinações dois a

dois dos hashes de cada dado armazenado, gerando a estrutura de mesmo nome, que encontra seu fim na própria Raiz de Merkle, o hash final único, de acordo com a figura 2.

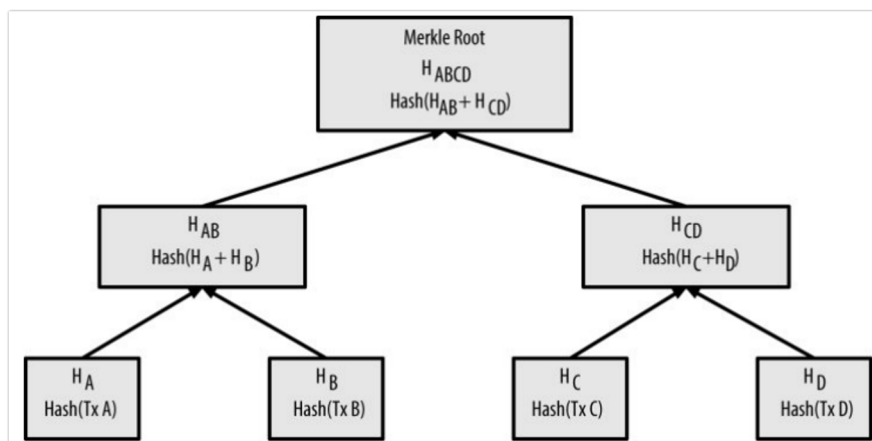


Figura 2 - Esquema simplificado de Árvore de Merkle

Fonte: Antonopoulos (2018)

A partir da estrutura esquematizada na Figura 2, a autenticação e verificação de integridade passa a exigir apenas que qualquer um dos nós calcule o hash da concatenação do Merkle Path, definido pelo conjunto de hashes intermediários que conectam o hash do dado a ser verificado à Raiz de Merkle, com o hash do dado solicitado (Antonopoulos, 2018). A saída do re-hasheamento comprova a integridade dos dados contidos na Árvore de Merkle, e deve resultar na Raiz de Merkle. O armazenamento dos hashes, ao invés dos documentos completos, proporciona uma redução significativa do espaço a ser ocupado em unidades físicas de armazenamento como Unidades de Estado Sólido (SSD) e Discos Rígidos (HDD) (Antonopoulos, 2018).

Lemieux (2017) identifica três níveis de modelos de blockchain direcionadas para o armazenamento de dados. O primeiro deles, denominado “Mirror”, permite que apenas os hashes dos documentos sejam armazenados na blockchain, em uma estrutura que combina um banco de dados externo, como o Oracle DB, no qual os documentos digitais são de fato integralmente armazenados, enquanto o AuditLog realiza os registros de eventos de auditoria nos dados, os quais são gerenciados pelo RsysLog. Os dados são armazenados na RsysLog Signature Storage e encaminhados à KSI Gateway para que as assinaturas sejam geradas e os hashes, criados e armazenados na KSI Blockchain, organizados na Árvore de Merkle, que responde a chamadas diretas do Oracle DB para verificações de integridade dos documentos e da árvore de dados. O documento sofre um re-hasheamento e é comparado com o respectivo hash armazenado na KSI Blockchain, como mostrado na Figura 3, a seguir.

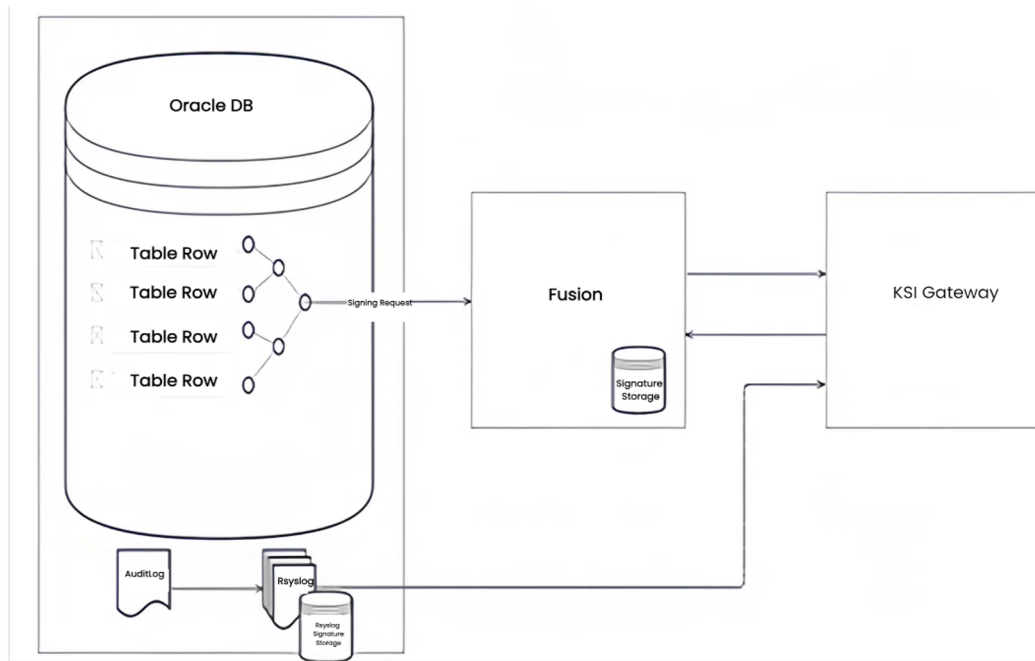


Figura 3 - Esquema genérico KSI Blockchain

Fonte: Lemieux (2017)

Conforme a figura 3, a KSI Blockchain é um exemplo de blockchain voltada apenas para o armazenamento eficiente de dados e documentos, evidenciando de forma prática a possibilidade de desemparelhar a tecnologia de sua função inicial, de servir apenas como um livro-razão distribuído, imutável que registra e armazena hashes de transações financeiras, para transformá-la em um banco de dados robusto e eficiente, com alto grau de rastreabilidade e segurança, características asseguradas por meio da tecnologia de criptografia empregada e mediante a forma com a qual os dados são armazenados, na estrutura que origina a Raiz de Merkle (Lemieux, 2017).

Enquanto isso, a Hyperledger Fabric se trata de uma plataforma baseada na tecnologia de livro-razão distribuído permissionado de código aberto voltada para o nível empresarial. A gestão de identidade é feita pelo Membership Service Provider (MSP), que fornece o controle ao acesso granular dos participantes da rede, assegurando que apenas entidades autorizadas possam submeter transações, ler dados específicos ou executar determinadas ações dentro da rede, além de servir como componente responsável pela emissão e validação de certificados digitais (Gangula *et al.* 2021).

Na rede Fabric, Gangula *et al.* (2021) afirmam que há dois tipos principais de nós com funções especializadas: Peers e Orderers, conforme a representação esquemática do funcionamento genérico de uma rede Hyperledger Fabric na figura 4.

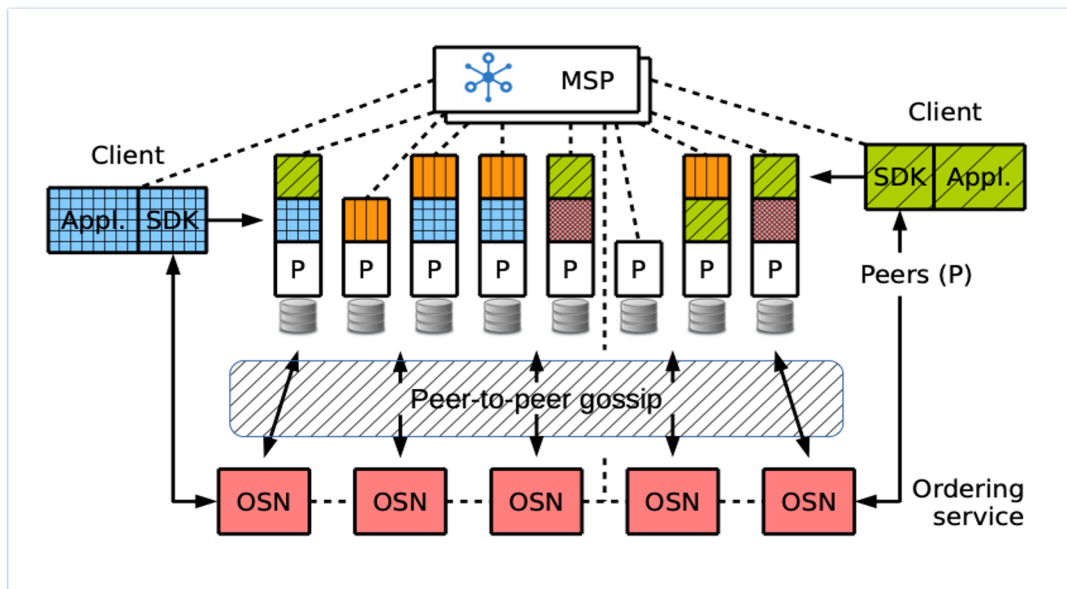


Figura 4 - Esquema genérico Hyperledger Fabric

Fonte: Androulaki *et al.* (2018)

Os nós do tipo peers hospedam cópias do livro-razão distribuído e do código que encapsula a lógica de negócios (chaincode), sendo responsáveis pela execução e validação das transações de dados. Os Orderers recebem as transações, estabelecem um consenso sobre a ordem total delas dentro de um canal, empacotam-nas em blocos e as distribuem aos peers (Gangula *et al.*, 2021).

Outro mecanismo fundamental na Hyperledger Fabric, de acordo com Androulaki *et al.* (2018), são os canais. Eles atuam como uma sub-rede privada, as quais contêm um subconjunto específico de participantes com seu próprio livro-razão distribuído independente. De maneira complementar, o mecanismo Private Data Collections permite que um subconjunto de organizações dentro de um mesmo canal mantenha certos dados privados entre si, sem necessidade de criação de um canal separado, enquanto apenas um hash dos dados privados compartilhados é registrado no livro público como evidência da transação. Esses dois mecanismos oferecem um método mais granular de controle de privacidade interno.

Portanto, a análise da arquitetura técnica, tanto da Hyperledger Fabric quanto da KSI Blockchain, revela, como sustentado por Androulaki *et al.* (2018) e Gangula *et al.* (2021), características que se alinham aos requisitos técnicos de segurança e escalabilidade necessários para

sistemas destinados ao uso na administração pública e justificam seu emprego nas diversas iniciativas abordadas nos estudos de caso.

2.1.4 Estudos de caso internacionais

Sistemas baseados em blockchain, implementados ou em fase de implementação e estudo na administração pública de países como Geórgia, Estônia e Estados Unidos, de acordo com os estudos de caso analisados, trouxeram mais transparência, segurança e eficiência aos processos administrativos. A seguir, são apresentados quatro estudos de caso que destacam o impacto da tecnologia na administração pública: o registro de títulos de terra na Geórgia, a gestão documental na Estônia e a aplicação da tecnologia para o aprimoramento da segurança cibernética e rastreabilidade de dados na DARPA.

2.1.5 Caso da Geórgia

O antigo sistema de registro de terras da Geórgia, inicialmente gerenciado pelo Bureau of Technical Inventory e pelo State Department of Land Management através de um sistema generalizadamente pouco transparente, permitia que oficiais ilegalmente alterassem registros de títulos de terra para benefício próprio através de uma conduta difícil de ser detectada. Em 2004, o NAPR (National Agency of Public Registry) foi criado para substituir as duas instituições responsáveis pelo gerenciamento dos títulos de terra no país. A nova agência introduziu políticas para simplificar esse processo junto a um banco de dados centralizado que, segundo Shang e Price (2019), era vulnerável a ataques de hackers e manipulações internas e externas do sistema.

O governo da Geórgia demonstrou interesse pela tecnologia blockchain em um esforço para restaurar a confiança nas agências governamentais. Para suportar o projeto, foi firmada uma parceria entre o governo do país e a empresa Bitfury, para que ocorresse o lançamento do projeto piloto de um sistema de registro de títulos de terra baseado em blockchain em 2016.

O projeto consistia em aplicar a tecnologia blockchain no sistema antigo de registro de terras da Geórgia. Os usuários realizariam os registros entrando no sistema da NAPR, no qual os certificados seriam convertidos em hashes criptográficos e receberiam um carimbo de data e hora, depois seriam armazenados na blockchain do Bitcoin. Tal processo garantiria a imutabilidade dos registros e aumentando a segurança contra fraudes.

2.1.6 Caso da Estônia

O estudo de caso realizado na Estônia por Jalakas (2018), concluiu que, com a inserção da KSI Blockchain ao x-Road, uma aplicação de serviços e depósito de dados extensivamente aberta ao setor público, responsável por armazenar informações e documentos de diversas naturezas, os serviços públicos receberam a adição de uma camada maior de segurança, que melhorou a confiança dos cidadãos nos processos governamentais e aprimorou de forma significativa a governança digital.

Segundo Espinoza (2024), a blockchain atualmente assegura a imutabilidade dos dados de diversos serviços digitais na Estônia como e-Health, e-Residency, e-Voting e e-Land Registry. Ainda segundo o autor, os principais resultados obtidos com a tecnologia foram o aumento da confiança, segurança e melhoria da transparência, pois com o acesso e imutabilidade dos dados, os cidadãos podem confiar que as informações fornecidas pelas autoridades não foram alteradas de maneira fraudulenta.

2.1.7 Caso dos Estados Unidos

Segundo Wouters *et al.* (2020), a adoção da tecnologia blockchain tem se expandido nas instituições militares dos Estados Unidos, em parceria com a DARPA, que passou a investir em iniciativas baseadas na tecnologia para proteger dados sensíveis e a cadeia de suprimentos contra ataques cibernéticos, firmando parcerias com empresas como Guardtime e Galois em um contrato de 1,8 milhão de dólares para o desenvolvimento de ferramentas de verificação e de sistemas de monitoramento de integridade, de acordo com Hillberry, Monaghan e Tripop (2025). Além disso, em 2017 a DARPA concedeu uma bolsa à Technology and Manufacturing Companies para a construção de uma plataforma de mensagens segura e invulnerável a ataques de hackers para uso militar.

2.1.8 Estudos de caso nacionais

Diversas iniciativas nacionais têm surgido no cenário da administração pública brasileira, evidenciando a aplicabilidade da blockchain em diversas áreas. A seguir, algumas dessas iniciativas serão detalhadas e exploradas.

2.1.9 TruBudget

Produzido pelo KfW, Banco de Desenvolvimento do governo da Alemanha, a premissa do TruBudget é estabelecer uma rede de diferentes doadores de recursos permitindo uma gestão clara, transparente e auditável dos recursos alocados no Fundo Amazonia. A ferramenta é relevante para manter a transparência na aplicação dos recursos e a confiança dos stakeholders envolvidos (Divino, 2024).

2.1.10 SOL (Solução online de Licitação)

O SOL é uma ferramenta desenvolvida pelos Estados da Bahia e do Rio Grande do Norte para facilitar a elaboração e tramite de licitações por meio do uso de software livre e blockchain. Dessa forma, o sistema permite que haja aumento da transparência e segurança das compras no setor público por possibilitar que tentativas de corromper dados sejam detectadas e reportadas facilmente (Cardoso et al., 2021).

2.1.11 B-Connect

No Brasil, a blockchain vêm sendo gradualmente implementada em diversos setores. Um exemplo é o B-Connect, sistema desenvolvido pelo Serviço Federal de Processamento de Dados (SERPRO), a pedido da Receita Federal do Brasil em parceria com os demais países. De acordo com Medeiros *et al.* (2024), ele atende ao propósito de armazenar os dados do Certificado de Operador Econômico Autorizado (OEA) de empresas, facilitando a comunicação entre as aduanas do Brasil, Argentina, Paraguai e Uruguai e conferindo celeridade ao processo burocrático que antes envolvia a atualização, inclusão e exclusão de empresas que possuíam direito ao certificado OEA, que atribui às empresas a classificação de seguras e confiáveis no aspecto do risco à integridade física das cargas transportadas e conformidade tributária e aduaneira. Eles são transmitidos à rede e armazenados de forma imutável, após o consenso de todos os países (nós), no livro-razão distribuído.

2.1.12 DREX

O DREX é uma iniciativa do Banco Central do Brasil que pretende digitalizar o Real brasileiro por meio de tecnologias emergentes como contratos inteligentes e blockchain para aprimorar a eficiência, segurança e transparência do sistema financeiro brasileiro. A digitalização pode resultar

na redução dos custos operacionais do Banco Central associados à emissão da moeda física, além de expandir o acesso aos serviços financeiros a grupos sub-bancarizados e tradicionalmente excluídos (Silva *et al.*, 2024).

2.1.13 bCPF e bCNPJ

Os projetos bCPF e o bCNPJ tratam-se de iniciativas baseadas em blockchain permissionada realizadas pela Receita Federal do Brasil (RFB). O principal objetivo das iniciativas foi proporcionar a desburocratização do acesso e compartilhamento da base de dados da RFB de modo a facilitar a integração entre os órgãos e entidades da Administração Pública Federal (Thompson, 2019).

Os participantes da rede foram divididos em proprietário do dado e colaborador do dado. O proprietário do dado é aquele responsável por alterar o dado na blockchain, enquanto o colaborador é a entidade não detentora dos dados capaz de enviar sugestões de alteração dos dados na rede para validação do proprietário e posterior alteração do dado. O comportamento e as permissões são incorporados à rede através de um contrato inteligente, que materializa a regra de governança (Thompson, 2019).

O exemplo hipotético fornecido por Thompson (2019) envolve o Tribunal Superior Eleitoral, proprietário da base de título de eleitor, que receberia uma chamada de colaboração da RFB sobre o campo “Endereço Título de Eleitor”. A colaboração é escrita na rede e propagada aos participantes pelo protocolo “peer-to-peer”, oferecendo ao TSE, possuidor da prerrogativa de tomada de decisão sobre a validação e alteração dos dados, a sugestão de modificação proposta pela entidade governamental.

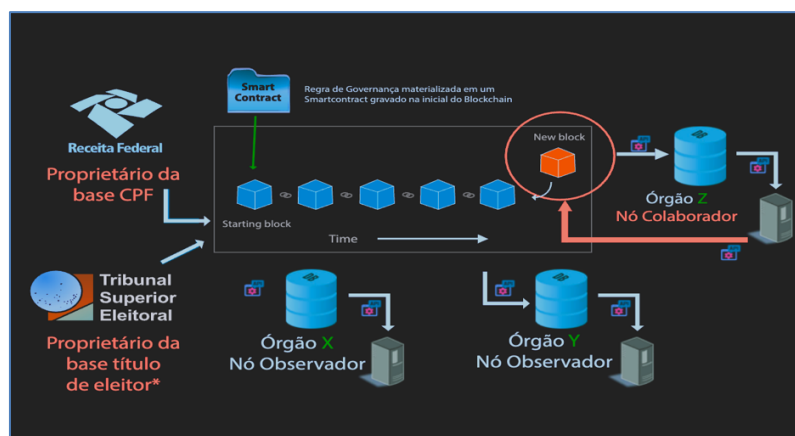


Figura 5 – Funcionamento das iniciativas bCPF e bCNPJ

Fonte: Thompson (2019)

2.1.14 Auditabilidade e transparência

Quanto à auditabilidade e transparência de sistemas baseados em blockchain, Zang, Ma e Meng (2025) abordam quatro estudos de caso de firmas de auditoria que utilizam a tecnologia: PricewaterhouseCoopers (PwC) Ernst and Young, Deloitte e KPMG. Segundo Zang, Ma e Meng (2025), a eficiência de auditoria foi aprimorada com a aplicação da PwC, pois enquanto a auditoria tradicional se ocupa de até 10% do custo das transações a blockchain permite uma auditoria integral dos dados, além de colaborar para a redução do ciclo de auditoria de 3 meses para 6 semanas e do custo de mão de obra em 40%, conforme o reporte anual de uma companhia multinacional (Zang; Ma; Meng, 2025). Da mesma forma, a Deloitte ChainFinance encurtou o ciclo de auditabilidade de 14 para 2 dias e reduziu a taxa de erro para 75%, aproximadamente (Zang; Ma; Meng, 2025).

O aumento da transparência promovido pela blockchain KPMG desenvolvida para o rastreamento de cadeia de suprimentos auxiliou o time de auditoria de uma marca global a localizar comportamento suspeito de um fornecedor e prevenir a perda de U\$ 8 milhões (Zang; Ma; Meng, 2025).

Da mesma forma, o estudo de Kukman e Gricar (2025) revela dados quantitativos positivos relacionados à blockchain e o aumento da segurança dos dados digitais armazenados em contraste ao modelo tradicional, apontando que, segundo a Association of Certified Fraud Examiners, enquanto fraudes na blockchain geram em torno de 4 bilhões de dólares anualmente em prejuízo, fraudes no sistema bancário tradicional geram um prejuízo em torno de 125 bilhões de dólares, sugerindo uma diminuição de 80% nos casos de fraude com a implementação de sistemas baseados em blockchain.

3 MÉTODOS DE ANÁLISE

A pesquisa baseou-se em uma revisão documental e análise de estudos de caso múltiplos, com enfoque em exemplos práticos de implementação da blockchain permissionada tanto no Brasil quanto em outros países, bem como no impacto apresentado na administração pública. A coleta de dados envolveu o uso de fontes primárias, como documentos oficiais, relatórios de instituições, publicações de instituições técnicas e acadêmicas, publicações de organizações técnicas ou acadêmicas diretamente relacionadas aos projetos brasileiros e de fontes secundárias como artigos científicos e técnicos, livros e publicações que exploram a relação entre blockchain e gestão pública.

Os dados coletados foram apresentados em dois quadros para a comparação dos estudos de caso utilizados para o desenvolvimento da pesquisa e representação esquemática da análise dos

resultados. Dados quantitativos de outros estudos para a sustentação dos resultados teóricos esperados para a tecnologia foram esquematizados na forma de tabela. A disposição esquemática dos dados em quadros e tabelas atendeu ao propósito de facilitar a análise do impacto da implementação da blockchain permissionada no grau de transparência dos processos governamentais e no nível de segurança dos dados digitais.

Foi adotada uma abordagem mista e majoritariamente qualitativa na medida em que integra dados da análise interpretativa de estudos de casos de forma crítica e adota a abordagem quantitativa ao utilizar dados numéricos para a sustentação dos achados e do potencial teórico da tecnologia. A abordagem mista permitiu a identificação de padrões, desafios e oportunidades relacionadas à adoção da tecnologia blockchain na administração pública, com foco na segurança de dados públicos e na transparência de processos administrativos governamentais.

3.1 REVISÃO DOCUMENTAL

O desenvolvimento da pesquisa foi baseado na revisão documental da literatura científica disponível sobre o tema blockchain, para a produção de uma descrição concisa e técnica a respeito dos fundamentos e conceitos teóricos básicos que alicerçam a tecnologia, definem suas limitações e permitem a compreensão de seu modo de funcionamento.

Os dados obtidos na análise do conteúdo técnico de artigos e obras científicas foram utilizados para a fundamentação teórica da pesquisa qualitativa proposta, que abordou os impactos da adoção da blockchain na administração pública, com foco na segurança de dados e transparência de processos governamentais, mediante a comparação de estudos de caso nacionais e internacionais.

3.2 ESTUDOS DE CASO

A pesquisa utilizou estudos de caso nacionais e internacionais que abarcam a implementação da tecnologia blockchain, para a identificação e descrição de seu impacto real e potencial - ocasionado pela implementação da tecnologia blockchain em setores da administração pública brasileira -, com ênfase na segurança de dados e transparência de processos governamentais.

Os dois quadros comparativos foram feitos com base nos dados coletados, com o objetivo de expor a aplicação e o modelo de blockchain permissionada utilizada, assim como o impacto real e os desafios observados antes, durante ou após sua implementação.

3.3 LIMITAÇÕES

Apesar do rigor e abrangência direcionados à pesquisa, o estudo demonstrou algumas limitações. Primeiramente, a seleção dos estudos dependeu de sua disponibilidade e qualidade, o que restringiu o acesso a pesquisas mais recentes ou pouco divulgadas. Em segundo lugar, os estudos de caso envolvendo outros países podem não representar fielmente a realidade do Brasil, por refletirem realidades específicas, o que dificultou a generalização dos resultados pela diversidade dos aspectos econômico, tecnológico e social, únicos de cada país. Apesar disso, as limitações não invalidam os achados do estudo, apenas sugerem que futuras pesquisas podem aprofundar as análises feitas.

A maioria das iniciativas e projetos utilizados no trabalho encontram-se em fase de implementação ou em estudos, o que gera uma significativa limitação sobre dados quantitativos disponíveis, que se encontram escassos para a apresentação de uma comparação puramente quantitativa sem o uso de uma abordagem qualitativa.

Portanto, ao adotar os métodos citados, considerando as limitações da pesquisa, pretendeu-se desenvolver uma análise técnica e bem fundamentada, que reflète integralmente o objetivo proposto através de uma pesquisa de abordagem qualitativa, de natureza exploratória, baseada em objetivos explicativos.

4 ANÁLISE E DISCUSSÃO

A adoção da tecnologia blockchain na administração pública tem sido vista por diversos países como uma alternativa para aumentar a transparência, a segurança e a eficiência da administração pública. A partir da análise dos estudos de caso internacionais da Geórgia, Estônia e EUA e iniciativas nacionais, foi possível avaliar o potencial impacto da tecnologia blockchain na administração pública brasileira, revelar objetivamente as diferentes abordagens aplicáveis à tecnologia e destacar os principais benefícios alcançados e desafios a serem enfrentados.

4.1 COMPARAÇÃO DOS ESTUDOS DE CASO INTERNACIONAIS

A partir da análise realizada nos estudos de caso, foi observado que cada um dos países adotou a blockchain para resolver problemas distintos no âmbito da administrativo:

- **Geórgia:** Apresentou um sistema blockchain para armazenamento de títulos de terra, para contornar problemas existentes do antigo sistema de titulação, como transparência, integridade e segurança dos dados armazenados (Shang; Price, 2019).
- **EUA:** Com foco na segurança cibernética, a DARPA tem desempenhado um importante papel para a compreensão e aplicação da tecnologia para a proteção de dados militares e governamentais sensíveis, explorando as características intrínsecas da blockchain para aumentar a resistência a ataques de hackers e garantir a imutabilidade e confiabilidade das informações armazenadas. Através do financiamento e parcerias estratégicas estimulou projetos conduzidos por empresas como ITAMCO (mensagens seguras), conforme Doskey e Johnson (2018), Guardtime (monitoramento de integridade de dados) e, de acordo com Daf Woodfield (2019), a SIMBA Chain (segurança da cadeia de suprimentos).
- **Estônia:** Utiliza a KSI Blockchain para armazenar dados de sistemas públicos de todo o país e fornecer um nível avançado de segurança e prevenção contra alterações (Espinosa; Pino, 2024).

O Quadro 1, apresentado a seguir, evidencia os principais impactos trazidos pela blockchain na segurança e transparência nos casos internacionais analisados.

Quadro 1 Comparativo de estudos de caso internacionais

País	Aplicação	Tecnologia	Impactos esperados na transparência	Impactos esperados na segurança de dados	Desafios observados
Geórgia	Registro de terras	BitFury Blockchain	Aumento da transparência para os proprietários e partes interessadas no processo, permitindo a verificação de status e histórico das propriedades, reduzindo a opacidade associada ao antigo sistema burocrático de registro de imóveis	Reduziu significativamente o risco de fraude em documentações e adulteração de títulos de propriedade. Uso da ancoragem na blockchain do bitcoin serve como prova pública adicional da integridade e do momento de registro do imóvel, dificultando disputas e contestações.	Planejamento da infraestrutura necessária e aceitação pública
			Aumento da confiança na integridade dos dados	A KSI fornece forte proteção contra adulteração de	Complexidad e técnica e

Estônia	Segurança de dados públicos	KSI Blockchain	governamentais, permitindo a verificabilidade da integridade do registro	dados, tanto por ataques externos quanto internos. Permite a detecção imediata de qualquer modificação não autorizada, dissuadindo tentativas de fraude ou encobrimento.	aceitação pública
EUA (DARPA)	Mensagens seguras (ITAMCO), monitoramento de integridade de dados de alta garantia com verificação formal (Guardtime/Galois) e conceitos de segurança da cadeia de suprimentos (SIMBA Chain/AFRL)	Projetos DARPA	Maior transparência interna, com foco na garantia de trilhas de auditoria seguras e imutáveis para logística e gerenciamento de dados e manutenção da confidencialidade em relação ao público externo	Sistemas de informação e de comunicação mais resilientes a ataques cibernéticos e tentativas de manipulação de dados. Capacidade de criar registros imutáveis e fornecer trilhas de auditoria criptografadas e seguras	Regulamentação e complexidade técnica

Fonte: elaboração própria, com base em Doskey e Johnson (2018), Daf Woodfield (2019), Shang e Price (2019) e Jalakas (2018)

Os impactos identificados com a implementação da blockchain no setor público dos países analisados na questão da transparência de processos governamentais e segurança de dados se manifestam de diferentes formas.

Na Geórgia, a implementação do sistema de registro de terras baseado em blockchain, conforme apontado por Shang e Price (2019), restaurou a confiança da população ao proporcionar maior eficiência e segurança ao processo de registro fundiário.

Na Estônia, a tecnologia serviu como uma resposta robusta aos ataques cibernéticos ocorridos em 2007 e como uma forma de melhoramento da governança digital, com a introdução da KSI Blockchain, uma infraestrutura conhecida por sua resistência a invasões, garantiu um ambiente seguro contra ataques de hackers, conforme destacado por Jalakas (2018).

Nos Estados Unidos, a blockchain encontra-se em fase de estudo para implementação em diversos estudos apoiados pela DARPA, que vê a tecnologia como um meio para aprimorar a transparência, rastreabilidade da cadeia de suprimentos e a segurança de dados militares sensíveis (Ahmad *et al.* 2021).

Através dessas experiências, observa-se um padrão na adoção da blockchain internacionalmente. A sua implementação busca geralmente impactar principalmente a eficiência administrativa, auxiliando na proteção contra fraudes e ataques cibernéticos, para o fortalecimento da confiança institucional e redução de processos burocráticos mediante a implementação de um sistema que reduz o nível de confiança individual necessário da instituição em cada agente atuante no processo administrativo.

4.2 COMPARAÇÃO DOS ESTUDOS DE CASO NACIONAIS

A nível nacional, muitas soluções baseadas em blockchain com objetivos, infraestruturas, impactos e desafios distintos tem sido adotadas pela administração pública brasileira, conforme evidenciado pelo Quadro 2.

Quadro 2 Comparativo de estudos de caso nacionais

Iniciativa	Aplicação	Tecnologia	Impactos esperados na transparência	Impactos esperados na segurança de dados	Desafios Observados
B-Connect	Facilitar a troca de informações entre aduanas internacionais para a rastreabilidade e atualização do certificado OEA.	Blockchain permissionada desenvolvida pelo SERPRO.	Melhoria da transparência entre os países do Mercosul conectados e redução do tempo para atualizações de certificados OEA.	Integridade dos certificados armazenados e alta permissividade para inclusão de dados devido à utilização do modelo permissionado.	Infraestrutura tecnológica limitada que não permite alto nível de interoperabilidade e que necessita de aceitação por mais países parceiros.
SOL (Solução Online de Licitação)	Garantir maior transparência e confiabilidade em processos licitatórios.	Blockchain permissionada para registro imutável de dados (Hyperledger Fabric).	Todos os contratos são disponibilizados publicamente e armazenados de forma imutável. As etapas e resultados são exibidos e podem ser acompanhados abertamente.	Redução de fraudes e aumento da transparência nos processos de licitação.	Necessidade de integração com os sistemas existentes e resistência de usuários acostumados com processos tradicionais.
TruBudget	Auxiliar na gestão de recursos públicos, garantindo segurança e transparência na execução orçamentária.	Blockchain permissionada em parceria com o Banco de Desenvolvimento da Alemanha (KfW).	Registro imutável das transações financeiras realizadas por instituições para o Fundo Amazônia e identificação dos participantes doadores através de certificados digitais	Maior controle sobre a destinação de recursos públicos, evitando desvios e ineficiência administrativa.	Interoperabilidade com sistemas governamentais existentes e desafios na adesão por órgãos públicos.

		Baseada na Hyperledger Fabric.	para pessoas jurídicas.		
DREX (Real Digital)	Digitalizar a moeda nacional, promovendo segurança e rastreabilidade de transações financeiras.	Infraestrutura de blockchain permissionada desenvolvida pelo Banco Central do Brasil. Baseada em Hyperledger Besu.	Manutenção de um ambiente controlado, com identificação rigorosa de participantes para evitar fraudes, lavagem de dinheiro e financiamentos ilegais por meio da imutabilidade dos dados, que contribui para a integridade dos registros, transações e saldos.	O registro único, compartilhado e imutável de transações financeiras e execução programada de contratos inteligentes aumentam a visibilidade e a auditabilidade das operações financeiras. A transparência, entretanto, seria regulada pela Lei de Proteção Geral de Dados Pessoais (LGPD). O impacto então residiria na melhora da rastreabilidade e a supervisão dentro do sistema financeiro.	Regulamentação e adesão por parte dos bancos e instituições financeiras, além da aceitação do público em geral.
bCPF e bCNPJ	Facilitar o acesso e compartilhamento da base de dados de CPF e CNPJ da Receita Federal.	Blockchain permissionada criada pela RFB.	As regras de governança são públicas e imutáveis, gravadas na blockchain por meio de um contrato inteligente, permitindo que os participantes tenham conhecimento do comportamento da rede. Além disso, no modelo federativo e colaborativo nenhum participante perde a prerrogativa sobre seus próprios dados.	A adesão de novos membros depende da aprovação da RFB, reduzindo a chance de um participante mal intencionado participar da rede. As regras de governança são imutáveis e garantem que o comportamento da rede não seja alterado de forma maliciosa.	Risco de fracasso do projeto e complexidade técnica da manutenção de um serviço em um país de dimensão continental, onde alguns municípios possuem comunicação de dados precária.

Fonte: elaboração própria, com base em Cardoso et al. (2021), Medeiros *et al.* (2024), Divino (2024), Thompson (2019) e Silva *et al.* (2024)

A partir do Quadro 2 é notável a preferência pela utilização de blockchains permissionadas consolidadas como a Hyperledger Fabric, reforçando sua adequabilidade técnica ao cenário da administração pública. Além disso, a implementação da tecnologia através da análise dos estudos de caso provou gerar um impacto positivo em relação a segurança de dados e na transparência, reduzindo fraudes e proporcionando um nível de transparência financeira maior (SOL, TruBudget, b-CPF, b-

CNPJ e B-Connect). Em contrapartida, há problemas como o aumento da complexidade técnica, necessidade de investimento inicial para a adoção da tecnologia e ausência de um arcabouço legal que regule e normatize o uso da blockchain no Brasil, da mesma forma, a própria barreira cultural, política e a dificuldade de interoperabilidade com os sistemas já existentes se tornam problemas relevantes.

4.3 IMPACTOS E DESAFIOS

De acordo com os Quadros 1 e 2, na comparação entre as iniciativas nacionais e internacionais analisadas e exploradas durante a pesquisa, similaridades e distinções sobre a implementação da blockchain podem ser observadas. Tanto na Geórgia quanto na Estônia, a blockchain foi utilizada para aumentar a segurança de dados e registros públicos, enquanto os Estados Unidos utilizaram-na principalmente para a proteção de informações sensíveis no campo militar. No Brasil, as iniciativas possuem um foco maior em aprimorar os processos da administração pública para garantir maior nível de transparência e segurança, de forma menos integrada e mais experimental.

Além disso, é possível identificar desafios semelhantes. Enquanto a Geórgia precisa enfrentar barreiras como a aceitação pública; A Estônia lida com questões relativas à interoperabilidade dos sistemas e a DARPA, com a complexidade técnica. Da mesma forma, o Brasil precisa ainda superar obstáculos relacionados a falta de regulamentação da tecnologia, aceitação por parte de usuários e instituições públicas e infraestrutura tecnológica ainda pouco desenvolvida.

O uso de blockchains como a KSI na Estônia e Hyperledger Fabric pela maioria das soluções implementadas e em fase de estudo para implementação no Brasil evidenciam uma preferência por tecnologias tecnicamente robustas, voltadas para o ambiente empresarial e alinhadas com os requisitos de segurança e transparência do modelo permissionado. Tanto a KSI quanto a Hyperledger Fabric possuem alto nível de rastreabilidade e transparência, como detalhado em seu modo de funcionamento anteriormente, permitindo a identificação de alterações em documentos e garantindo maior transparência devido à sua estrutura imutável e aplicação do mecanismo de consenso para a garantia da segurança.

Além disso, conforme os dados apresentados por Zang, Ma e Meng (2025) e Kukman e Gricar (2025) em seus estudos, a aplicação de blockchain é capaz de trazer do ponto de vista quantitativo e no aspecto da segurança de dados e transparência uma redução da carga de trabalho em auditorias e aumento da eficiência em decorrência da redução no número de erros, na mão de obra e no tempo de ciclo de auditoria, redução de fraudes e um ganho na eficiência operacional. Tais impactos positivos

revelam os efeitos práticos da aplicação da tecnologia para a segurança e transparência de dados, conforme pode ser observado na Tabela 1, a seguir.

Tabela 1 Impacto na segurança, transparência e eficiência administrativa

Setor	Métrica	Valor (% ou unidade)
Auditoria (Financeira - PwC)	Redução do Ciclo de Auditoria (Relatório Anual)	de 3 meses para 6 semanas
Auditoria (Financeira - PwC)	Redução do Custo de Mão de Obra na Auditoria	40%
Auditoria (Financeira - Deloitte)	Redução do Ciclo de Auditoria	de 14 dias para 2 dias
Auditoria (Financeira - Deloitte)	Redução da Taxa de Erro na Auditoria	75%
Serviços Financeiros (Comparativo)	Taxa de Fraude (Blockchain vs. Tradicional)	0.15% vs. 0.8% (80% menor)

Fonte: elaboração própria, com base em Zang, Ma e Meng (2025) e Kukman e Gricar (2025)

Portanto, os dados qualitativos e quantitativos apresentados, extraídos a partir da Tabela 1 e dos estudos de caso nacionais e internacionais analisados e esquematizados no Quadro 1 e Quadro 2, sugerem que o impacto da blockchain, quanto ao aumento da segurança de dados e da transparência de processos é positivo, havendo ainda, um considerável incremento da eficiência operacional em contraste ao sistema tradicional em auditorias, rastreamento e fiscalização financeira e de cadeias de suprimento. Os dados apresentados sustentam as expectativas teóricas para a tecnologia no aspecto da transparência e segurança de dados, reforçando o impacto positivo no ambiente da administração pública brasileira.

5 CONSIDERAÇÕES FINAIS

A análise realizada confirma que a blockchain permissionada já impacta a administração pública brasileira, promovendo mais transparência e segurança aos processos governamentais, ao passo que as iniciativas analisadas como o B-Connect, SOL, TruBudget, bCPF, bCNPJ e DREX

comprovam essa tendência, ao refletirem a gradual aceitação e adoção da blockchain pelo setor público com o objetivo de reduzir a burocracia e promover mais segurança, eficiência e transparência a esses processos. Da mesma forma, os estudos de caso internacionais demonstram a capacidade da tecnologia de reduzir fraudes, agilizar processos burocráticos e aprimorar a rastreabilidade de dados e evidenciam outros potenciais usos e aplicações.

A implementação da blockchain na administração pública brasileira apresenta impactos concretos nas áreas da segurança digital e transparência de processos governamentais. No caso do B-Connect, a blockchain permitiu o aprimoramento da rastreabilidade de certificações de OEA, reduzindo fraudes e facilitando consideravelmente a troca de informações entre as aduanas dos países do Mercosul em decorrência da transparência da rede. Enquanto o TruBudget, introduzido na gestão de recursos do Fundo Amazônia, aumentou a transparência na execução orçamentária ao garantir a rastreabilidade de recursos. Da mesma forma a Solução Online de Licitação (SOL) em fase de implementação gradual demonstrou, a partir de sua aplicação regional, o potencial de tornar processos licitatórios mais seguros e auditáveis, e o DREX, ainda em fase de testes, promete trazer maior segurança e rastreabilidade às transações financeiras nacionais. Ainda em território nacional, o bCPF e o bCNPJ são soluções materializadas pela RFB com o objetivo de promover mais eficiência operacional no compartilhamento desses dados públicos e simultaneamente promover segurança, rastreabilidade e transparência, algo que foi evidentemente alcançado com o projeto quando os impactos positivos identificados na segurança e transparência de dados, no Quadro 2, são observados, assim como ocorre nos demais projetos em âmbito nacional mencionados.

Internacionalmente, no campo da Defesa, o estudo de caso da DARPA demonstra o potencial da tecnologia no campo das comunicações e do Gerenciamento da Cadeia de Suprimento. Enquanto isso, o caso da Georgia sugere o potencial de sua aplicação como base para um sistema de registro de terras, capaz de aumentar a transparência, reduzir a corrupção e aumentar a confiança da população. Por fim, o caso da Estônia propõe o uso da blockchain como uma camada assentada a um sistema maior de registro de dados geral massivamente aplicado ao setor público (X-Road), assegurando a imutabilidade e transparência dos dados registrados.

Entretanto, tecnologias baseadas na tecnologia de livro-razão distribuído não estão isentas de problemas fundamentais como má qualidade dos dados que alimentam o sistema – em alguns casos a imutabilidade pode até mesmo se tornar um problema para a correção de erros legítimos não intencionais. Além disso, a transparência radical através da inscrição imutável de dados fornecida pela blockchain pode sofrer resistência política e cultural dentro de organizações governamentais,

levantando a questão de que o principal valor de uma blockchain estaria mais na capacidade de gerar confiança na informação e nos processos realizados e menos na transparência total dos dados armazenados.

Existe também uma lacuna entre o potencial anunciado baseado no aspecto técnico e teórico da arquitetura de uma blockchain permissionada e o impacto comprovado e quantificado em larga escala. A maioria dos projetos encontram-se em fase piloto ou em implementações limitadas e necessitam ainda demonstrar seu valor e a dificuldade em isolar e medir os benefícios de forma quantitativa e atribuíveis exclusivamente às blockchains contribui para essa lacuna.

Desse modo, o estudo contribui, através de uma abordagem quali-quantitativa, para a compreensão dos possíveis impactos da implementação da tecnologia de blockchain permissionada na administração pública brasileira. Foi ilustrado, pela análise de iniciativas nacionais e internacionais e através da explicação teórica sobre o funcionamento da tecnologia, que a blockchain permissionada é capaz de fortalecer significativamente a segurança digital, ao fazer uso de algoritmos de criptografia e um modelo de livro-razão distribuído e imutável, que reduz a necessidade de confiança direta nos usuários do sistema. A fragmentação de permissões e o uso do mecanismo de consenso impedem alterações maliciosas ou indesejadas, ao passo que garantem a imutabilidade dos dados armazenados e reduzem o número de fraudes. Entretanto, desafios como restrições regulatórias, limitações culturais, aceitação institucional, dificuldade de interoperabilidade com sistemas legado e a necessidade de uma infraestrutura tecnológica mais adequada são barreiras que impedem o uso mais amplo da tecnologia, a serem transpostas pela criação de mais políticas públicas de incentivo à inovação, capacitação profissional e novas regulamentações que garantam o uso eficiente da tecnologia.

REFERÊNCIAS

AHMAD, Raja Wasim *et al.* Blockchain for aerospace and defense: Opportunities and open research challenges. **Computers & Industrial Engineering**, v. 151, p. 106982, 2021. Acesso em: 30 set. 2024.

AMORIM, Deivid T.; MALAGOLLI, Guilherme A. Análise sobre o uso de smart contracts e da blockchain para a confecção de documentos oficiais no Brasil. **Revista Interface Tecnológica**, v. 19, n. 2, p. 213-222, 2022. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/download/1517/803>. Acesso em: 30 set. 2024.

ANDROULAKI, Elli. *et al.* Hyperledger fabric: A Distributed Operating System for Permissioned Blockchains. **Proceedings of the Thirteenth EuroSys Conference on EuroSys '18, 2018**. Disponível em: <https://doi.org/10.1145/3190508.3190538>. Acesso em: 20 fev. 2025

ANTONOPOULOS, Andreas M. **Mastering Bitcoin: programming the open blockchain**. Beijing; Boston; Farnham; Sebastopol; Tokyo: O'Reilly, 2018.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. **Mastering Ethereum: building smart contracts and Dapps**. Beijing; Boston; Farnham; Sebastopol; Tokyo: O'Reilly, 2019.

ARÃO, Gabriel. Blockchain na Indústria 4.0: definição, aplicabilidade e desenvolvimento. In: **CONGRESSO BRASILEIRO DE ENGENHARIA DE FABRICAÇÃO (COBEF)**, 12., 2023, Brasília. Anais [...]. Brasília: COBEF, 2023. Disponível em: https://www.researchgate.net/profile/GabrielArao2/publication/370972277_BLOCKCHAIN_NA_INDUSTRIA_40_DEFINICAO_APLICABILIDADE_E_DESENVOLVIMENTO/links/6477d7df9a722376501c972/BLOCKCHAIN-NA-INDUSTRIA-40-DEFINICAO-APLICABILIDADE-E-DESENVOLVIMENTO.pdf. Acesso em: 30 set. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 14724**: informação e documentação – trabalhos acadêmicos – apresentação. Rio de Janeiro: ABNT, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 6024**: informação e documentação – numeração progressiva das seções de um documento – apresentação. Rio de Janeiro: ABNT, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 6022**: informação e documentação – artigo em publicação periódica técnica e/ou científica – apresentação. Rio de Janeiro: ABNT, 2018a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 6023**: informação e documentação – referências – elaboração. Rio de Janeiro: ABNT, 2018b [2020].

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 6028**: informação e documentação – resumo, resenha e recensão – apresentação. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR 10520**: informação e documentação – citações em documentos – apresentação. Rio de Janeiro: ABNT, 2023.

BAKOS, Yannis; HALABURDA, Hanna. *Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance*. **NYU Stern School of Business working paper, 2021**. Disponível em: https://questromworld.bu.edu/platformstrategy/wp-content/uploads/sites/49/2022/07/PlatStrat2022_paper_14.pdf. Acesso em: 30 set. 2024.

BASHIR, I. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. [s.l.] **Birmingham - Mumbai Packt March**, 2018. Acesso em: 20 fev. 2025

CARDOSO, Henrique Ribeiro; DE CERQUEIRA, Rafael Soares; DE ANDRADE, Anne Beatriz Costa. *A aplicabilidade da tecnologia blockchain às licitações públicas*. *Revista do CEJUR/TJSC: Prestação Jurisdicional*, v. 9, n. 1, p. e0368-e0368, 2021.

DIVINO, Sthéfano B. S. *Diretrizes de governança e compliance para aplicações jurídicas da plataforma blockchain na administração pública e na administração de empresas*. **Administração de Empresas em Revista**, v. 3, n. 36, p. 194-223, 2024. Acesso em: 20 fev. 2025

DOSKEY, Teresa; JOHNSON, Stacylee. **Blockchain technology in the department of defense. 2018**. Disponível em: <https://calhoun.nps.edu/bitstream/handle/10945/61880/NPS-LM-19-024.pdf?sequence=1>. Acesso em: 26 fev. 2025

ESPINOSA, Victor I.; PINO, Antonia. *E-Government as a Development Strategy: The Case of Estonia*. **International Journal of Public Administration**, 2024. Disponível em: <https://doi.org/10.1080/01900692.2024.2316128>. Acesso em: 20 fev. 2025

GANGULA, Ramya. *et al.* *Leveraging the Hyperledger Fabric for Enhancing the Efficacy of Clinical Decision Support Systems*. **Blockchain in Healthcare Today**, 18 fev. 2021. Disponível em: <https://doi.org/10.30953/bhty.v4.154>. Acesso em: 26 abr. 2025.

HILLBERRY, Jeremy; MONAGHAN, Maynard; TRIPOP, Tyle. **ISO9001: 2015 and ISO21001: 2018 Certification Opportunities for Quality Education at the Naval Postgraduate School. 2025**. Tese de Doutorado. Acquisition Research Program. Acesso em: 20 fev. 2025

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 6. ed. São Paulo: Atlas, 2000. Acesso em: 20 fev. 2025

LEMIEUX, Victoria L. *A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation*. In: 2017 IEEE international conference on big data (Big Data). **IEEE**, 2017. p. 2271-2278. Disponível em: <https://ai-collaboratory.net/wp-content/uploads/2020/04/Lemieux.pdf>. Acesso em: 30 set. 2024.

JALAKAS, Parol. **Blockchain from public administration perspective: case of Estonia**. Tallinn: Tallinn University of Technology, 2018. Disponível em: <https://digikogu.taltech.ee/en/Download/d591ed87-3350-44a1-acb3-f0e184f9dc18/PlokkahelavalikuhaldusevaatenurgastEestiKaas.pdf>. Acesso em: 19 jul. 2024.

Keyless Signature Infrastructure® (KSITM) Technology An Introduction to KSI Blockchain Technology and Its Benefits. [s.l.: s.n.]. Disponível em: https://blockchain.machetemag.com/wp-content/uploads/2017/11/Guardtime_WhitePaper_KSI.pdf. Acesso em: 25 set. 2024.

KUKMAN, Tomaž; GRIČAR, Sergej. Blockchain for Quality: Advancing Security, Efficiency, and Transparency in Financial Systems. **FinTech**, v. 4, n. 1, p. 7, 2025.

MEDEIROS, Camila Q. *et al.* Blockchain no Comércio Exterior. **InGeTec-Inovação, Gestão & Tecnologia**, v. 3, n. 6, p. 67-81, 2024. Disponível em: <https://www.fatecbarueri.edu.br/revista/index.php/ingetec/article/view/121>. Acesso em: 24 set. 2024.

MENEZES, Pedro. Referencial Teórico: o que é e como fazer. **Significados**. Disponível em: <https://www.significados.com.br/referencial-teorico/>. Acesso em: 12 jan. 2025.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system.** [S.l.: s.n.], 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 24 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **FIPS PUB 180-4: Secure Hash Standard (SHS).** Gaithersburg: NIST, 2015. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>. Acesso em: 11 out. 2024.

SERPRO. **Serpro desenvolve rede BlockChain para a Receita Federal.** Disponível em: https://www.serpro.gov.br/acl_users/credentials_cookie_auth/require_login?came_from=https%3A/www.serpro.gov.br/menu/imprensa-bkp/Releases/serpro-desenvolve-rede-blockchain-para-a-receita-federal. Acesso em: 25 set. 2024.

SHANG, Qiuyun; PRICE, Allison. A blockchain-based land titling project in the Republic of Georgia: rebuilding public trust and lessons for future pilot projects. **Innovations: Technology, Governance, Globalization**, v. 12, n. 3-4, p. 72-78, 2019. Disponível em: <https://direct.mit.edu/itgg/article/12/3-4/72/9852/A-Blockchain-Based-Land-Titling-Project-in-the>. Acesso em: 19 jul. 2024.

SOUZA, Richelle Santos; BEZERRA, Fábio Luiz de Oliveira. Drex: a moeda digital brasileira e as consequentes inovações contratuais. **Revista Insigne de Humanidades**, Natal, v. 1, n. 1, p. 39-49, jan./abr. 2024. Disponível em: <https://insigneacademica.com.br/ojs/index.php/revistainsignedehumanidades/article/view/4>. Acesso em: 21 set. 2024.

SILVA, Adriano Rodrigues da *et al.* **Moedas digitais dos bancos centrais: inovações, desafios e os caminhos do Brasil com o DREX.** 2024. Disponível em: <https://bdtd.ucb.br:8443/jspui/handle/tede/3567>. Acesso em: 21 set. 2024.

TAYLOR, Paul J. *et al.* A systematic literature review of blockchain cyber security. **Digital Communications and Networks**, v. 6, n. 2, p. 147-156, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352864818301536>. Acesso em: 21 set. 2024.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1619/2020**. 24 jun. 2020. Processo nº 031.044/2019-0. Relator: Ministro Aroldo Cedraz. Disponível em: <https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/1613%252F2020/%2520%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0>. Acesso em: 24 set. 2024.

TRIFECTA TEAM. Trifecta: the blockchain trilemma solved. **White Paper**, 2019. Disponível em: <https://pramodv.ece.illinois.edu/pubs/Whitepaper2019-9.pdf>. Acesso em: 09 out. 2024

THOMPSON, Ronald Cesar. **1º lugar: Projeto b-CPF e b-CNPJ: Blockchain das bases de cadastro fiscal**. 2019. Acesso em: 30 jun. 2025

WOUTERS, G. *et al.* **An expertise forum contributing to European armies interoperability since 1953: blockchain in defence: a breakthrough?** [S.l.: s.n.], 2020. Disponível em: https://finabel.org/wp-content/uploads/2020/09/FFT_Blockchain_Web.pdf. Acesso em: 25 set. 2024.

DAF WOODFIELD, Mr Daryl. **THE EMERGING IMPACTS OF BLOCKCHAIN TECHNOLOGY ON**. 2019. Tese de Doutorado. AIR UNIVERSITY. Disponível em: <https://apps.dtic.mil/sti/pdfs/AD1107534.pdf>. Acesso em: 25 set. 2024.

SARACEVIC, Tefko. Ciência da informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, p. 41-62, jan./jun. 1996. Acesso em: 25 set. 2024.

SEVERINO, Antonio Joaquim. **Metodologia do trabalho científico**. 23. ed. São Paulo: Cortez, 2007. Acesso em: 25 set. 2024.

VOLPATO, Gilson Luiz. Como escrever um artigo científico. **Anais da Academia Pernambucana de Ciência Agronômica**, Recife, v. 4, p. 97-115, 2007. Disponível em: <http://www.journals.ufrpe.br/index.php/apca/article/view/93>. Acesso em 04 abr. 2025.

ZHANG, Yunfan; MA, Zifei; MENG, Jiaming. **Auditing in the blockchain: a literature review**. **Frontiers in Blockchain**, v. 8, p. 1549729, 2025.