Uma Arquitetura Baseada em Blockchain para Listas de Bloqueio de E-mail com Integração ao Postfix

Rodrigo Pimentel[1], Eduardo Takeo Ueda[1,2], Anderson Aparecido Alves da Silva[1], Thales Areco Bandiera Paiva[3]

[1]Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT)
Av. Prof. Almeida Prado, 532 - Butantã - São Paulo - SP - Brasil

[2]Departamento de Computação
Universidade Federal de São Carlos (UFSCar) - Sorocaba - SP - Brasil

[3]Departamento de Engenharia de Computação e Sistemas Digitais
Universidade de São Paulo (USP) - São Paulo - SP - Brasil

rodrigo.pimentel@outlook.com, eduardo.takeo@ufscar.br,
anderson@uol.com.br, thalespaiva@larc.usp.br

Abstract. *Email remains one of the primary vectors for cyberattacks, being widely exploited by spam and phishing campaigns. Traditional mechanisms, such as DNS-based blacklists (DNSBL), are widely adopted but present limitations related to centralization and governance. In this context, this paper proposes a permissioned blockchain-based architecture for the decentralized management of blacklists of malicious email senders, integrated with the Postfix email server. The main contribution lies in integrating the proposed architecture into the real SMTP message reception workflow without requiring modifications to the MTA, enabling its adoption in existing environments. The solution leverages Hyperledger Besu and smart contracts to store and query information about malicious senders, enabling cooperation among multiple entities. The experimental evaluation, conducted in a controlled environment, demonstrates the functional viability of the approach, allowing the rejection of malicious messages during the SMTP phase without impacting legitimate emails. Although it does not include a detailed quantitative performance analysis, the study highlights the potential of the approach as a complementary mechanism to traditional solutions, providing increased transparency, traceability, and support for decentralized cooperation.*

Resumo. *O correio eletrônico permanece como um dos principais vetores de ataques cibernéticos, sendo amplamente explorado por campanhas de spam e phishing. Mecanismos tradicionais, como listas de bloqueio baseadas em DNS (DNSBL), são amplamente adotados, porém apresentam limitações relacionadas à centralização e governança. Neste contexto, este artigo propõe uma arquitetura baseada em blockchain permissionada para o gerenciamento descentralizado de listas de bloqueio de remetentes maliciosos, integrada ao servidor de e-mail Postfix. A principal contribuição consiste na integração da arquitetura ao fluxo real de recepção de mensagens SMTP, sem a necessidade de modificações no MTA, permitindo sua adoção em ambientes existentes. A solução utiliza o Hyperledger Besu e contratos inteligentes para armazenar e consultar informações sobre remetentes maliciosos, viabilizando a cooperação entre múltiplas entidades. A avaliação experimental, conduzida em ambiente controlado, demonstra a viabilidade funcional da proposta, permitindo a rejeição de mensagens maliciosas ainda na fase SMTP sem impactar mensagens legítimas. Embora não inclua uma*

análise quantitativa detalhada, o estudo evidencia o potencial da abordagem como mecanismo complementar às soluções tradicionais, oferecendo maior transparência, rastreabilidade e suporte à cooperação descentralizada.

1. Introdução

O correio eletrônico permanece como um dos principais vetores de ataque em segurança digital, sendo amplamente explorado por campanhas de *spam* e *phishing*. Relatórios recentes, como o da Egress (2024), indicam que o volume de mensagens maliciosas continua elevado. Segundo a Barracuda Networks (2025), cerca de um em cada quatro e-mails analisados continha algum tipo de *spam* ou conteúdo malicioso, enquanto a Cisco Talos (2025) apontou o *phishing* como responsável por aproximadamente um terço dos incidentes de segurança observados no período.

Tradicionalmente, o combate a remetentes maliciosos é realizado por meio de listas de bloqueio baseadas em DNS (DNSBLs), utilizadas para identificar e rejeitar mensagens provenientes de endereços associados a spam. Embora amplamente adotadas, essas listas apresentam limitações relacionadas à centralização, dependência de entidades específicas para manutenção e vulnerabilidades à manipulação. Li et al. (2025) destacam riscos que podem comprometer sua confiabilidade, reforçando a necessidade de alternativas mais robustas.

Nesse contexto, tecnologias como blockchain surgem como alternativa para manutenção descentralizada e auditável dessas listas. Embora soluções como bancos de dados replicados ou serviços federados também possam ser consideradas, a adoção de uma blockchain permissionada justifica-se pela possibilidade de governança compartilhada entre entidades independentes, histórico auditável das decisões de bloqueio e menor dependência operacional de uma única organização. Entretanto, sua aplicação em sistemas de correio eletrônico ainda enfrenta desafios relacionados à integração com infraestruturas existentes e ao impacto operacional.

Este trabalho propõe uma arquitetura baseada em Hyperledger Besu para o gerenciamento distribuído de remetentes maliciosos, integrada ao servidor Postfix, um dos MTAs mais utilizados. A principal contribuição consiste na integração da solução ao fluxo real de recepção SMTP, sem necessidade de modificações no MTA, permitindo adoção em ambientes existentes. O estudo concentra-se na viabilidade funcional da abordagem e em suas implicações práticas de integração, governança e operação.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; a Seção 3 descreve a arquitetura proposta; a Seção 4 apresenta o ambiente experimental; a Seção 5 discute os resultados; e a Seção 6 apresenta as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Segundo Zhang (2022) e Choudhari (2021), o uso da tecnologia de blockchain em mecanismos de segurança da informação é explorado em diversos contextos, incluindo controle de acesso, compartilhamento de informações de ameaça e sistemas distribuídos resilientes. No entanto, quando se considera especificamente o problema da detecção e mitigação de *spam* em sistemas de correio eletrônico, observa-se que o número de trabalhos que exploram o uso de blockchain de forma direta ainda é limitado. A maioria das abordagens existentes concentra-se em técnicas de filtragem baseadas em aprendizado de máquina ou em listas centralizadas de bloqueio, enquanto propostas que utilizam blockchain para suportar listas distribuídas ou arquiteturas colaborativas de

mitigação permanecem pouco exploradas. Nesse contexto, esta seção apresenta e discute os principais trabalhos relacionados ao uso de blockchain aplicado à segurança de e-mail, destacando suas abordagens, limitações e diferenças em relação à solução proposta neste artigo.

Os trabalhos relacionados foram identificados por meio de buscas nas bases IEEE Xplore e ACM Digital Library, utilizando a string "blockchain AND (email OR mail OR e-mail) AND spam". Após a aplicação dos critérios de inclusão e exclusão (idioma, período, disponibilidade integral e aderência ao tema), foram selecionados oito artigos relevantes para análise.

2.1 Arquiteturas de e-mail baseadas em blockchain

Alguns trabalhos da literatura propõem a utilização de blockchain como elemento central na construção de novas arquiteturas para sistemas de correio eletrônico, com a finalidade de aprimorar aspectos como segurança, autenticidade e confiabilidade das mensagens. Nesses estudos, a blockchain não atua apenas como um mecanismo auxiliar, mas como parte fundamental da infraestrutura de envio e recebimento de e-mails.

Rachad (2021) propõe uma arquitetura de correio eletrônico baseada em blockchain na qual o processo de envio e recebimento de mensagens é registrado em um banco de dados descentralizado, permitindo maior rastreabilidade e resistência a ataques de falsificação. De forma semelhante, Zhang et al. (2022) apresentam um sistema de e-mail concebido sobre blockchain, no qual transações representam mensagens e metadados associados, buscando reduzir problemas relacionados à confiança entre remetentes e destinatários.

Embora essas abordagens explorem de forma consistente o potencial da blockchain para redefinir a infraestrutura de sistemas de e-mail, elas demandam a substituição ou modificação significativa dos modelos tradicionais de correio eletrônico. Além disso, o tratamento de spam e de remetentes maliciosos não é o foco principal dessas propostas, sendo abordado de maneira indireta ou secundária. Em contraste, o presente trabalho investiga o uso de blockchain como um mecanismo complementar, integrado a um MTA amplamente utilizado, visando especificamente a mitigação de *spam* por meio de uma lista distribuída de remetentes maliciosos, sem a necessidade de reestruturar o ecossistema de e-mail existente.

2.2 Blockchain aplicado à detecção e mitigação de *spam*

Uma segunda linha de pesquisa concentra-se no uso de blockchain como suporte a mecanismos de detecção e mitigação de spam em sistemas de correio eletrônico. Nesses trabalhos, a blockchain é empregada como um meio para registrar informações relacionadas a remetentes maliciosos, eventos de spam ou decisões de classificação, com o propósito de aumentar a confiabilidade, a integridade e o compartilhamento dessas informações entre diferentes entidades.

Choudhari (2021) apresenta uma abordagem para identificação de e-mails de spam que utiliza blockchain como mecanismo de armazenamento e validação dos resultados de classificação. De forma semelhante, Lakhdar (2022) propõe uma solução baseada em blockchain para detecção de *spam*, na qual informações sobre mensagens e remetentes são registradas em um banco de dados descentralizado, buscando reduzir a dependência de listas centralizadas e aumentar a resistência a manipulações.

Embora essas propostas explorem o potencial da blockchain para apoiar a detecção de spam, elas geralmente se concentram no processo de classificação das mensagens ou na validação dos resultados obtidos, sem considerar a integração direta com infraestruturas de e-mail amplamente utilizadas. Além disso, aspectos como compatibilidade com MTAs existentes e impacto no desempenho operacional do sistema de correio eletrônico são frequentemente pouco explorados. Esse aspecto é particularmente relevante, pois soluções de mitigação de spam precisam operar em tempo real e com baixa latência para não comprometer o desempenho do servidor de e-mail. Por sua vez, o presente trabalho investiga a utilização da blockchain como uma lista distribuída de bloqueio de remetentes, integrada a um MTA amplamente adotado, permitindo a mitigação de spam de forma transparente ao fluxo tradicional de entrega de e-mails.

2.3 Abordagens híbridas: blockchain e aprendizado de máquina

Uma terceira categoria de trabalhos combina tecnologias de blockchain com técnicas de aprendizado de máquina para a detecção de *spam* em sistemas de correio eletrônico. Nessas abordagens, algoritmos de classificação são empregados para identificar mensagens maliciosas com base em características de conteúdo ou comportamento, enquanto a blockchain é utilizada como um mecanismo de apoio para garantir a integridade, a rastreabilidade ou o compartilhamento confiável dos resultados de classificação.

Saquib (2023), Rathod (2024) e Saraswathi et al. (2023) exploram modelos de aprendizado supervisionado, como Naïve Bayes e Regressão Logística, aplicados à identificação de spam. Nesses trabalhos, a blockchain é utilizada para registrar decisões de classificação ou validar informações compartilhadas entre participantes. De forma semelhante, Vishwa et al. (2025) propõem integrar técnicas de engenharia de atributos com blockchain, buscando aumentar a confiabilidade do processo de detecção.

Embora essas soluções apresentem bons resultados em termos de precisão de classificação, elas dependem fortemente da qualidade dos dados de treinamento e do ajuste dos modelos de aprendizado de máquina. Além disso, o uso da blockchain nesses trabalhos atua predominantemente como um componente auxiliar, não sendo explorado como um mecanismo direto de mitigação baseado em infraestrutura, como listas distribuídas de bloqueio integradas ao fluxo de entrega de e-mails. O presente trabalho concentra-se na utilização da blockchain como um mecanismo de cooperação entre sistemas de e-mail, independentemente da técnica de detecção empregada, visando a mitigação de *spam* por meio do compartilhamento descentralizado de informações sobre remetentes maliciosos.

A análise dos trabalhos relacionados evidencia que, embora existam propostas que exploram o uso de blockchain no contexto de e-mail e *spam*, a maioria das soluções concentra-se em mecanismos de detecção baseados em aprendizado de máquina ou em modelos conceituais de sistemas de correio eletrônico distribuídos. De forma geral, esses trabalhos não abordam de maneira integrada aspectos fundamentais para adoção prática, como a compatibilidade com infraestruturas de e-mail amplamente utilizadas, o impacto no fluxo SMTP e as implicações operacionais dessas soluções.

Além disso, observa-se que o uso de blockchain frequentemente atua como um componente auxiliar, sem explorar seu potencial como mecanismo direto de mitigação baseado em infraestrutura, como listas distribuídas de bloqueio. Nesse contexto, poucos

trabalhos investigam a integração prática dessas abordagens com MTAs reais, o que limita sua aplicabilidade em cenários operacionais.

Dessa forma, este trabalho diferencia-se ao propor e avaliar a integração de uma lista distribuída baseada em blockchain diretamente ao fluxo de recepção de mensagens de um MTA amplamente utilizado, explorando não apenas a viabilidade técnica, mas também suas implicações práticas em termos de integração e operação. Nesse contexto, o Quadro 1 sintetiza as principais características dos trabalhos analisados, comparando-os à proposta deste artigo, de modo a evidenciar suas diferenças e contribuições específicas.

Quadro 1. Comparação entre os trabalhos relacionados e a proposta deste artigo no contexto de e-mail e *spam*.

Trabalho / Referência	**Blockchain**	**Spam de E-mail**	**Integração com MTA**	**Esforço de Adaptação**	**Observações principais**
Choudhari (2021)	Sim	Sim	Não	Médio	Blockchain como suporte à identificação de *spam*, sem integração com servidores
Vishwa et al. (2025)	Sim	Sim	Não	Médio	Modelo Naïve Bayes com verificação em blockchain
Rachad (2021)	Sim	Parcial	Não	Alto	Sistema de e-mail seguro com foco em confidencialidade e integridade
Zhang (2022)	Sim	Não	Não	Alto	Arquitetura conceitual de correio eletrônico baseado em blockchain
Lakhdar (2022)	Sim	Sim	Não	Médio	Abordagem genérica de detecção de *spam*
Saquib (2023)	Não	Sim	Não	Médio	Aprendizado supervisionado para detecção de spam
Saraswathi et al. (2023)	Não	Sim	Não	Médio	Estudo comparativo de técnicas de aprendizado de máquina
Rathod (2024)	Não	Sim	Não	Médio	Abordagem estatística baseada em Regressão Logística
Este artigo	Sim (Besu)	Sim	Sim (Postfix)	Baixo	Lista distribuída de bloqueio baseada em blockchain.

3. Arquitetura da Solução Proposta

Esta seção descreve a arquitetura proposta para a manutenção e consulta de uma lista distribuída de remetentes maliciosos baseada em blockchain, visando permitir a colaboração entre múltiplas entidades com garantia de descentralização, integridade e transparência.

A arquitetura integra uma rede blockchain permissionada, implementada com o Hyperledger Besu, a um servidor de e-mail Postfix, possibilitando que cada mensagem recebida seja verificada dinamicamente contra a lista distribuída de bloqueio. Diferentemente de abordagens centralizadas, a proposta elimina a dependência de uma autoridade única para manutenção das listas, reduzindo riscos de manipulação e atrasos na atualização.

3.1 Visão Geral da Arquitetura

A arquitetura proposta é composta por três elementos principais: servidores de e-mail responsáveis pelo recebimento e encaminhamento das mensagens, uma camada de integração que realiza a consulta e atualização da lista distribuída de remetentes maliciosos, e uma rede blockchain permissionada utilizada para armazenar e validar as informações de bloqueio. Esses componentes atuam de forma coordenada para permitir a verificação descentralizada de remetentes no momento da recepção das mensagens.

Os servidores de e-mail são implementados utilizando o Postfix. Durante a recepção de uma mensagem, o sistema aciona um módulo externo responsável por verificar o endereço IP ou domínio do remetente, atuando como intermediário entre o MTA e a rede blockchain, sem exigir modificações no funcionamento interno do servidor.

A Figura 1 apresenta uma visão geral da arquitetura proposta, evidenciando a interação entre o servidor de e-mail, a camada de integração e a rede blockchain distribuída. Conforme ilustrado, essa camada estabelece a comunicação com a rede blockchain por meio da Internet, realizando consultas à lista distribuída de bloqueio e, quando aplicável, registrando novas informações sobre remetentes identificados como maliciosos.

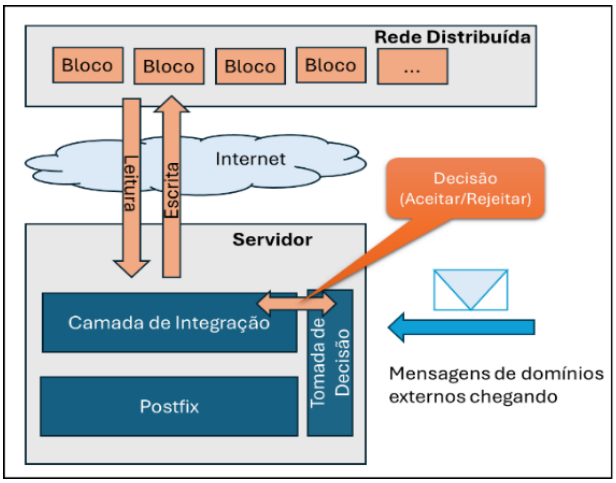

Figura 1. Visão geral da arquitetura proposta para verificação de remetentes de e-mail, na qual a camada de integração consulta uma rede blockchain distribuída e retorna ao servidor de e-mail a decisão de aceitação ou rejeição da mensagem.

Após a consulta, a camada de integração retorna ao servidor de e-mail a decisão de aceitação ou rejeição da mensagem, aplicada pelo Postfix ainda durante o processo de recepção. Ao empregar uma rede blockchain composta por múltiplos nós mantidos por diferentes entidades participantes, a arquitetura evita a centralização do controle da lista de bloqueio e assegura propriedades como integridade, rastreabilidade e consistência das informações compartilhadas. Dessa forma, a solução proposta possibilita a disseminação rápida e confiável de dados sobre ameaças, preservando a modularidade do sistema e facilitando sua integração com infraestruturas de e-mail existentes.

3.2 Infraestrutura Blockchain e Contratos Inteligentes

A solução proposta adota uma blockchain permissionada como infraestrutura para o armazenamento e compartilhamento da lista distribuída de remetentes maliciosos. A escolha por um modelo permissionado deve-se à necessidade de controlar a participação das entidades envolvidas, garantindo que apenas organizações autorizadas possam registrar ou validar informações na rede. Esse modelo é particularmente adequado ao contexto corporativo e institucional, no qual os participantes são conhecidos e há requisitos de governança, desempenho e previsibilidade.

A rede blockchain foi implementada utilizando o Hyperledger Besu, um cliente Ethereum de código aberto que oferece suporte a redes permissionadas e a diferentes mecanismos de consenso. O Hyperledger Besu foi selecionado por sua compatibilidade com a Ethereum Virtual Machine (EVM), permitindo a implementação de contratos inteligentes e integração com aplicações externas por meio de interfaces como JSON-RPC e Web3.

A lista distribuída de remetentes maliciosos é gerenciada por meio de contratos inteligentes, responsáveis por manter os registros associados a endereços IP ou domínios identificados como fontes de *spam* ou *phishing*. Cada registro inclui, além do identificador do remetente, informações adicionais como o instante de inclusão e a entidade responsável pelo registro, permitindo rastreabilidade e auditoria das ações realizadas na rede. A inclusão de novos registros ocorre por meio de transações submetidas pelas entidades participantes, que são validadas conforme as regras de consenso da blockchain antes de serem permanentemente armazenadas.

O contrato inteligente também disponibiliza funções de consulta que permitem à camada de integração verificar, em tempo de execução, se um determinado remetente consta na lista distribuída de bloqueio. Dessa forma, a verificação não depende de repositórios centralizados ou de mecanismos externos de sincronização, uma vez que todos os nós mantêm uma visão consistente do estado da lista. Essa abordagem assegura integridade e transparência no compartilhamento das informações, ao mesmo tempo em que reduz a possibilidade de inconsistências ou manipulações indevidas.

3.3 Integração com o Servidor de E-mail (Postfix) e Fluxo SMTP

A integração da arquitetura proposta com o servidor de e-mail foi realizada por meio do Postfix, utilizando mecanismos padrão de verificação de políticas durante o processo de recepção das mensagens. Essa abordagem permite que a solução seja incorporada ao fluxo normal de processamento do MTA, sem a necessidade de modificações no código-fonte do servidor, preservando compatibilidade e facilitando a adoção em ambientes existentes. A Figura 2 ilustra o fluxo de integração entre o Postfix, a camada de integração e a rede blockchain durante a recepção de uma mensagem SMTP.

Conforme ilustrado na Figura 2, durante a recepção de uma mensagem SMTP, o Postfix aciona a camada de integração por meio de um serviço externo de política (*policy service*), ao qual são repassadas informações relevantes sobre o remetente, como endereço IP e domínio de origem. A camada de integração processa esses dados e realiza a consulta à lista distribuída de bloqueio mantida na rede blockchain, conforme descrito na Subseção 3.2. Esse procedimento ocorre de forma síncrona, permitindo que a verificação seja realizada antes da aceitação definitiva da mensagem pelo servidor de e-mail.

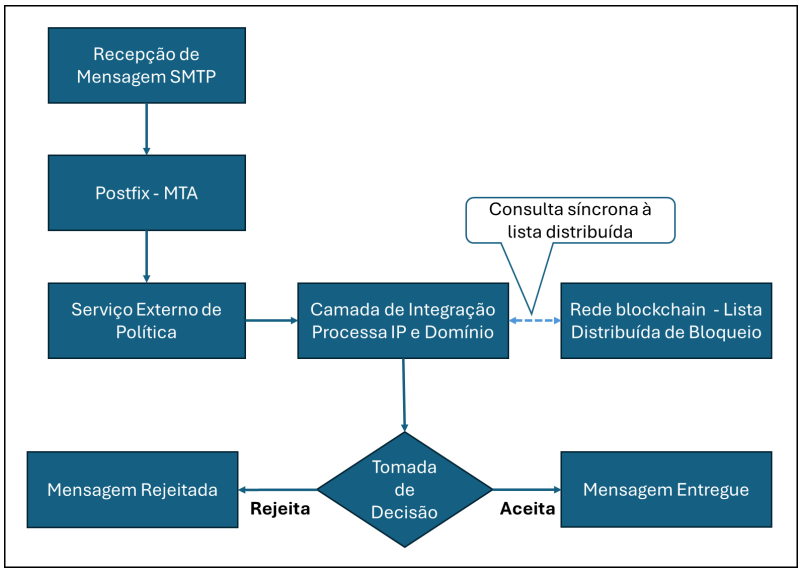

Figura 2. Fluxo de integração entre o servidor de e-mail Postfix, a camada de integração e a rede blockchain durante o processo de recepção de mensagens.

O funcionamento da solução ocorre de forma integrada ao fluxo de recepção de mensagens. Ao receber uma mensagem, o Postfix aciona a camada de integração, que consulta a lista distribuída na blockchain para verificar se o remetente consta como malicioso. Com base no resultado, a mensagem é aceita ou rejeitada ainda durante a fase SMTP.

Com base no resultado da consulta, a camada de integração retorna ao Postfix a decisão de aceitação ou rejeição da mensagem. Caso o remetente esteja presente na lista distribuída de bloqueio, a mensagem é rejeitada ainda durante a fase SMTP, evitando processamento desnecessário. Caso contrário, o processamento prossegue normalmente pelo servidor de e-mail.

Adicionalmente, quando uma entidade participante identifica um novo remetente como malicioso, essa informação pode ser registrada na blockchain. Após validação pela rede, o novo registro passa a compor a lista distribuída de bloqueio e torna-se imediatamente disponível para consulta pelos demais participantes, permitindo resposta rápida e compartilhada frente a novas ameaças.

Embora a arquitetura permita o registro distribuído de remetentes maliciosos, o processo de identificação desses remetentes depende dos mecanismos locais adotados por cada entidade participante, como filtros de *spam*, análise de reputação ou políticas internas. Nesse contexto, a veracidade das informações registradas não é garantida apenas pelo mecanismo de consenso da blockchain, que assegura integridade, mas não necessariamente correção dos dados inseridos.

Para mitigar riscos associados a registros incorretos ou maliciosos, a arquitetura pode ser complementada com estratégias de governança, como validação por múltiplas entidades, uso de mecanismos de reputação ou auditoria dos registros realizados. Além disso, a natureza permissionada da rede permite o controle dos participantes autorizados, reduzindo a probabilidade de comportamento malicioso. Esses aspectos evidenciam que, além da infraestrutura tecnológica, a definição de políticas de governança é fundamental para a adoção segura da solução proposta.

4. Avaliação Experimental

Esta seção apresenta a avaliação experimental da arquitetura proposta, com foco na verificação da viabilidade funcional da solução e de sua integração ao fluxo de processamento de mensagens de correio eletrônico. Os experimentos foram conduzidos em ambiente controlado, permitindo observar o comportamento do sistema em cenários representativos de envio de mensagens.

Inicialmente, descrevemos o ambiente experimental utilizado, incluindo a configuração do servidor de e-mail, da camada de integração e da rede blockchain. Em seguida, são apresentados os cenários de avaliação e as métricas adotadas. Por fim, os resultados obtidos são discutidos à luz dos mecanismos tradicionais de bloqueio de remetentes, destacando as principais características e implicações da abordagem proposta.

4.1 Ambiente Experimental

Os experimentos foram conduzidos em um ambiente controlado, com o propósito de avaliar a viabilidade funcional da arquitetura proposta e seu comportamento no processamento de mensagens de correio eletrônico. O ambiente experimental foi composto por um servidor de e-mail responsável pela recepção das mensagens, uma

camada de integração encarregada da consulta e atualização da lista distribuída de remetentes maliciosos e uma rede blockchain permissionada utilizada para o armazenamento e validação das informações de bloqueio.

O servidor de e-mail responsável pela recepção das mensagens foi implementado utilizando o Postfix, amplamente adotado em ambientes corporativos e acadêmicos. Durante o processo de recepção de mensagens SMTP, o Postfix aciona um serviço externo de política (*policy service*), responsável por consultar a camada de integração e aplicar a decisão de aceitação ou rejeição da mensagem ainda durante a fase SMTP, antes de sua entrega ao sistema.

Além do servidor de recepção, o ambiente experimental incluiu um servidor emissor de e-mails, também configurado com o Postfix, utilizado para o envio controlado de mensagens durante os experimentos. Esse servidor foi empregado exclusivamente para a simulação de remetentes legítimos e maliciosos, possibilitando a geração de tráfego de e-mail em um ambiente isolado, reproduzível e livre de dependências de infraestruturas externas.

A camada de integração foi implementada como um serviço independente, executado de forma desacoplada do servidor de e-mail. Esse componente é responsável por processar as informações do remetente fornecidas pelo Postfix e realizar consultas e registros na lista distribuída de bloqueio por meio de chamadas a contratos inteligentes. A comunicação com a rede blockchain foi realizada utilizando bibliotecas compatíveis com a Ethereum Virtual Machine, por meio de interfaces Web3.

A rede blockchain foi composta por múltiplos nós executando o cliente Hyperledger Besu, configurados em um ambiente permissionado. Os nós participantes mantêm cópias sincronizadas do livro-razão distribuído e utilizam um mecanismo de consenso adequado a ambientes com participantes conhecidos, garantindo integridade, consistência e rastreabilidade das informações armazenadas. O contrato inteligente responsável pela manutenção da lista de remetentes maliciosos foi implantado nessa rede e acessado pela camada de integração durante a execução dos experimentos. A organização e a interação entre esses componentes no ambiente experimental são apresentadas na Figura 3, que ilustra a topologia utilizada e o fluxo de comunicação entre os elementos da solução durante os experimentos.

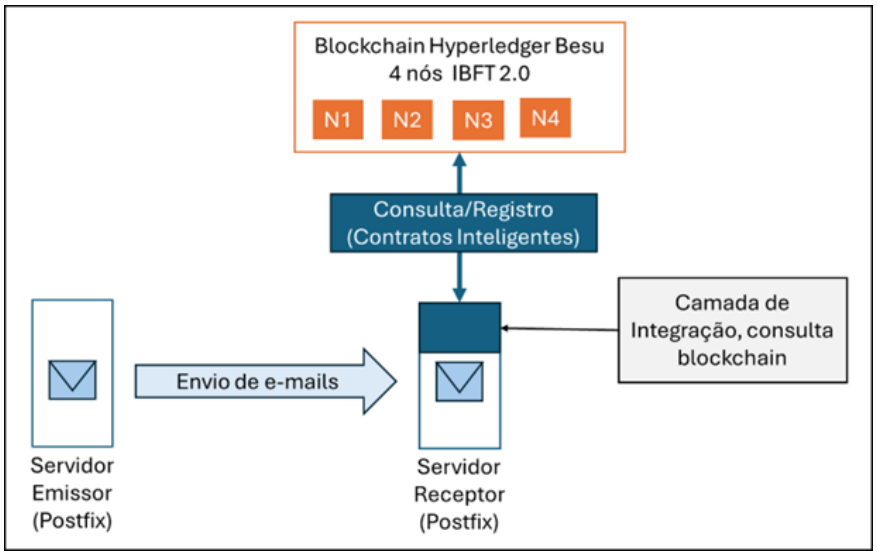

Figura 3. Topologia do ambiente experimental e fluxo de comunicação entre o servidor emissor, o servidor receptor Postfix, a camada de integração e a rede blockchain Hyperledger Besu, composta por quatro nós e utilizando o algoritmo de consenso IBFT 2.0.

Conforme ilustrado na Figura 3, mensagens provenientes de domínios externos são enviadas pelo servidor emissor ao servidor de e-mail receptor. Ao receber cada mensagem, o Postfix delega à camada de integração a verificação do remetente, que consulta a lista distribuída de bloqueio mantida na rede blockchain e retorna a decisão de aceitação ou rejeição da mensagem, aplicada ainda durante o processo de recepção.

O ambiente experimental foi configurado de modo a permitir a avaliação da integração entre os componentes da solução e a verificação do comportamento do sistema durante o processamento de mensagens, priorizando aspectos funcionais da arquitetura proposta.

4.2 Cenários de Avaliação Funcional

Com base no ambiente experimental descrito na Subseção 4.1, foram definidos cenários de avaliação com o propósito de analisar o comportamento da arquitetura proposta durante o processo de recepção de mensagens de correio eletrônico. Esses cenários foram elaborados de forma a simular condições controladas de envio de mensagens, permitindo observar o comportamento da consulta à lista distribuída de remetentes maliciosos no fluxo de processamento do servidor de e-mail.

Para complementar essa descrição, o Quadro 2 resume as principais configurações adotadas no ambiente experimental, incluindo os componentes utilizados, suas funções e as tecnologias empregadas. Essa descrição detalhada permite a compreensão do contexto em que os cenários foram executados e favorece a reprodutibilidade dos experimentos realizados.

Quadro 2. Configuração do ambiente experimental.

Componente	Tecnologia / Ferramenta	Função no ambiente experimental
Servidor emissor de e-mails	Postfix	Envio controlado de mensagens SMTP para simulação de remetentes legítimos e maliciosos
Servidor receptor de e-mails	Postfix	Recepção das mensagens e aplicação das decisões de aceitação ou rejeição com base na lista distribuída
Camada de integração	Serviço externo de política (Policy Service)	Intermedia a comunicação entre o servidor de e-mail e a blockchain, realizando consultas e registros na lista de bloqueio
Rede blockchain	Hyperledger Besu	Armazenamento distribuído da lista de remetentes maliciosos
Tipo de blockchain	Permissionada	Controle de participação e validação entre entidades conhecidas
Número de nós blockchain	4 nós	Garantia de descentralização e tolerância a falhas
Algoritmo de consenso	IBFT 2.0	Validação das transações e consistência do livro-razão distribuído
Ambiente de hospedagem da blockchain	Amazon AWS	Execução dos nós blockchain em infraestrutura de nuvem
Interface de comunicação	Web3 / Contratos inteligentes	Consulta e atualização da lista distribuída de bloqueio

A partir dessa configuração, foram conduzidos cenários de avaliação em ambiente controlado, utilizando o servidor emissor para gerar tráfego de e-mail de forma reproduzível e permitir observar o comportamento da consulta à lista distribuída de bloqueio no processo de recepção das mensagens.

No primeiro cenário, o servidor emissor enviou mensagens simulando remetentes legítimos, cujos endereços IP e domínios não estavam registrados na lista distribuída de bloqueio. Esse cenário teve como finalidade avaliar o comportamento do sistema em

condições normais de operação, considerando situações em que o remetente não é identificado como malicioso.

No segundo cenário, o servidor emissor foi configurado para enviar mensagens simulando remetentes maliciosos, previamente registrados na lista distribuída de bloqueio mantida na blockchain. Nesse caso, a finalidade foi analisar a capacidade da solução em identificar e bloquear mensagens indesejadas ainda durante a fase SMTP, impedindo sua aceitação pelo servidor de e-mail e evitando o processamento desnecessário dessas mensagens.

Esses cenários permitem avaliar, de forma comparativa, o comportamento da arquitetura proposta em situações distintas de envio, servindo de base para a análise das métricas e dos resultados apresentados na próxima seção.

4.3 Procedimento Experimental e Execução dos Testes

Os experimentos foram conduzidos considerando diferentes cenários de envio de mensagens, incluindo remetentes legítimos e remetentes previamente identificados como maliciosos. Para os cenários maliciosos, os endereços IP ou domínios correspondentes foram previamente registrados na lista distribuída mantida na blockchain.

Durante os testes, mensagens SMTP foram enviadas a partir de um servidor Postfix configurado para simular domínios legítimos e maliciosos. No momento da recepção, o servidor Postfix receptor acionou a camada de integração, que realizou a consulta à blockchain e retornou a decisão de aceitação ou rejeição da mensagem.

Esse procedimento permitiu verificar a consistência das decisões aplicadas pelo servidor de e-mail e a correta consulta à lista distribuída de bloqueio, evidenciando a viabilidade funcional da arquitetura proposta nos cenários considerados.

5. Análise e Discussão dos Resultados

5.1 Análise dos Resultados

Os experimentos realizados permitiram avaliar o comportamento da arquitetura proposta em cenários controlados de envio de mensagens de correio eletrônico, considerando tanto remetentes legítimos quanto remetentes previamente identificados como maliciosos. Em todos os testes conduzidos, o servidor de e-mail Postfix aplicou corretamente as decisões de aceitação ou rejeição das mensagens com base nas informações armazenadas na lista distribuída de bloqueio mantida na blockchain.

Nos cenários envolvendo remetentes previamente registrados como maliciosos, as mensagens foram rejeitadas ainda durante a fase SMTP, impedindo sua aceitação pelo servidor de e-mail. Esse comportamento foi consistente em todos os testes realizados, indicando que a consulta à lista distribuída de bloqueio ocorreu de forma correta e sincronizada com o fluxo de recepção de mensagens.

Nos cenários envolvendo remetentes legítimos, cujos endereços IP ou domínios não constavam na lista distribuída, as mensagens foram aceitas normalmente pelo servidor Postfix. Esse resultado evidencia que a integração com a blockchain não interferiu de forma indevida no processamento de mensagens válidas, preservando o funcionamento esperado do sistema de correio eletrônico.

Além disso, foi observado que a atualização da lista distribuída de bloqueio, por meio do registro de novos remetentes maliciosos na blockchain, refletiu-se de forma imediata nas decisões aplicadas pelo servidor de e-mail. Mensagens subsequentes

provenientes desses remetentes passaram a ser corretamente rejeitadas, demonstrando a consistência das informações compartilhadas entre os nós da rede blockchain e a camada de integração. O Quadro 3 apresenta os comportamentos observados durante os experimentos realizados, considerando diferentes tipos de remetentes e o resultado da verificação realizada pela arquitetura proposta.

Quadro 3. Descrição dos comportamentos observados durante os experimentos realizados.

Cenário avaliado	Situação do remetente	Resultado esperado	Comportamento observado
Envio de mensagem de domínio malicioso	IP/Domínio presente na blockchain	Rejeição da mensagem	Mensagem rejeitada na fase SMTP
Envio de mensagem de domínio legítimo	IP/Domínio ausente da blockchain	Aceitação da mensagem	Mensagem aceita normalmente
Atualização da lista distribuída	Novo remetente malicioso registrado	Bloqueio imediato	Bloqueio aplicado em mensagens subsequentes

Embora a consulta à lista distribuída de bloqueio introduza um tempo adicional no processo de recepção das mensagens, não foram realizadas medições quantitativas desse impacto, restringindo-se a análise à verificação do funcionamento da arquitetura nos cenários avaliados.

5.2 Discussão

Os resultados obtidos indicam a viabilidade do uso de uma blockchain permissionada como mecanismo de compartilhamento descentralizado de informações sobre remetentes maliciosos no contexto de sistemas de correio eletrônico. A arquitetura proposta integrou-se de forma adequada ao fluxo de recepção de mensagens do servidor Postfix, aplicando decisões de aceitação ou rejeição de acordo com as informações armazenadas na lista distribuída de bloqueio.

Mecanismos tradicionais baseados em DNSBL constituem o estado da prática para o bloqueio de remetentes maliciosos. Nesse contexto, a proposta apresentada neste trabalho não busca substituir diretamente essas soluções, mas atuar como um mecanismo complementar, especialmente em cenários que demandam maior transparência, rastreabilidade e cooperação entre múltiplas entidades.

Do ponto de vista operacional, a solução proposta apresenta funcionamento semelhante ao de DNSBLs tradicionais, realizando consultas síncronas durante a fase SMTP. Contudo, ao empregar uma blockchain permissionada, a proposta permite governança distribuída, maior transparência e rastreabilidade das ações de bloqueio, características não presentes em listas centralizadas.

Sob a perspectiva arquitetural, é útil distinguir dois tipos de custo operacional na solução proposta: o plano de dados e o plano de controle. O plano de dados corresponde às consultas realizadas durante a fase SMTP para cada mensagem recebida, impactando diretamente a latência de processamento e o desempenho operacional do servidor de e-mail. Já o plano de controle está associado às operações de inclusão, remoção e propagação de registros na lista distribuída de bloqueio, envolvendo transações validadas pela rede blockchain. Essa distinção permite compreender que os custos associados à atualização colaborativa da lista não necessariamente coincidem com os custos observados no processamento individual de mensagens.

A avaliação experimental concentrou-se nos aspectos funcionais e de integração da arquitetura proposta, com a finalidade de verificar sua correta operação no fluxo de mensagens de correio eletrônico. Dessa forma, os experimentos priorizaram a observação

do comportamento do sistema, em vez da coleta de métricas quantitativas detalhadas, como latência média por consulta ou vazão sob cargas elevadas.

Nesse contexto, a caracterização quantitativa detalhada, incluindo métricas de latência, vazão e comportamento sob carga, constitui etapa subsequente de investigação. Os experimentos realizados indicaram que mensagens provenientes de remetentes maliciosos foram corretamente rejeitadas ainda durante a fase SMTP, enquanto mensagens legítimas foram aceitas normalmente. Embora a consulta à lista distribuída introduza tempo adicional ao processamento, nos cenários avaliados não foram observados indícios de comprometimento do funcionamento esperado do servidor de e-mail.

A análise quantitativa de desempenho da solução, incluindo comparações com DNSBLs tradicionais e avaliações sob diferentes níveis de carga, constitui uma direção relevante para trabalhos futuros. Ainda assim, os resultados obtidos neste estudo são suficientes para demonstrar a viabilidade técnica da abordagem como um mecanismo complementar às soluções tradicionais de mitigação de *spam*.

Adicionalmente, aspectos relacionados à governança da rede, como critérios para registro e remoção de remetentes maliciosos e mecanismos para mitigação de registros incorretos ou maliciosos, representam desafios relevantes e reforçam a necessidade de políticas complementares à infraestrutura proposta.

Em termos práticos, modelos de governança para esse tipo de arquitetura podem incluir requisitos de validação por múltiplas entidades antes da inclusão de novos registros, mecanismos de contestação e revisão de bloqueios, políticas de expiração periódica dos registros e auditorias regulares das ações realizadas pelos participantes. Tais mecanismos podem contribuir para elevar a confiabilidade operacional da lista distribuída e reduzir riscos de uso indevido.

6. Conclusão e Trabalhos Futuros

Este trabalho apresentou uma arquitetura baseada em blockchain para o gerenciamento descentralizado de uma lista de bloqueio de remetentes maliciosos no contexto de sistemas de correio eletrônico. A solução proposta integra uma rede blockchain permissionada, implementada com o Hyperledger Besu, a um servidor de e-mail amplamente utilizado, o Postfix, por meio de uma camada de integração desacoplada, permitindo a verificação de remetentes durante a fase SMTP.

Os resultados obtidos em ambiente controlado indicam a viabilidade da abordagem, evidenciando a correta identificação e rejeição de mensagens provenientes de remetentes maliciosos, bem como a aceitação normal de mensagens legítimas. Nesse contexto, a proposta pode ser compreendida como um mecanismo complementar às soluções tradicionais baseadas em DNSBL, contribuindo para a redução da dependência de mecanismos centralizados e oferecendo maior transparência e rastreabilidade na manutenção das informações.

Como trabalhos futuros, destacam-se a realização de uma avaliação quantitativa abrangente da arquitetura, incluindo métricas de latência, vazão, tempo de resposta e comportamento sob diferentes níveis de carga, bem como a análise da solução em cenários corporativos de maior escala. Adicionalmente, pretende-se investigar mecanismos complementares de governança, reputação e consenso, visando aprimorar a confiabilidade e a integridade das informações compartilhadas entre as entidades participantes.

Referências

Barracuda Networks (2025). “Email Threats Report, 2025”. Disponível em: https://assets.barracuda.com/assets/docs/dms/2025-email-threats-report.pdf. Acesso em: nov. 2025.

Choudhari, S. (2021). “Spam E-mail Identification Using Blockchain Technology”. International Journal of Computer Applications, vol. 183, no. 43, pp. 1–5.

Cisco Talos Intelligence Group (2025). “Incident Response Trends Q1 2025”. Disponível em: https://blog.talosintelligence.com/ir-trends-q1-2025. Acesso em: nov. 2025.

Egress (2024). “Email Security Risk Report, 2024”. Disponível em: https://www.egress.com/blog/company-news/stats-from-the-email-security-risk-report. Acesso em: nov. 2025.

Lakhdar, H. (2022). “Blockchain-Based Spam Detection Approach”. In Proceedings of the International Conference on Cyber Security and Blockchain.

Levine, J. and Galvin, J. (2010). “DNS Blacklists”. RFC 5782, IETF. Disponível em: https://datatracker.ietf.org/doc/html/rfc5782. Acesso em: nov. 2025.

Li, R., et al. (2025). “HADES Attack: Understanding and Evaluating Manipulation Risks of Email Blocklists”. In Proceedings of the Network and Distributed System Security Symposium (NDSS).

Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: dez. 2025.

Rachad, A. (2021). “Sending and Receiving Secure Email Based on Blockchain”. In Proceedings of the International Conference on Information Technology and Communications.

Rathod, S. (2024). “Detecting Email Spam with Precision: A Logistic Regression Approach”. In Proceedings of the International Conference on Data Science and Applications.

Vishwa, R., Kamalin, D., Vanaja, S., Ramesh, C. H., Gotlur, K., and Sabarinathan, G. (2025). “Enhanced Naïve Bayes Model for Intelligent and Secure Email Spam Detection Using Hybrid Feature Engineering and Blockchain-Based Verification”. In Proceedings of the International Conference on Machine Computing and Technology Convergence (ICMCTC). doi:10.1109/ICMCTC62214.2025.11196588.

Saquib, N. U. (2023). “Content Based Email Spam Filtering and Detection Using Hybrid Supervised Learning Approach”. International Journal of Computer Science and Information Security, vol. 21, no. 3, pp. 45–52.

Saraswathi, D. and Karthik, S. (2023). “Machine Learning Approaches for Email and IoT Spam Detection: Analysis and Challenges”. Journal of Network and Computer Applications, vol. 214, pp. 103–118.

Zhang, L. (2022). “A Blockchain-Envisioned Mailing System”. IEEE Access, vol. 10, pp. 45678–45689.