Fatecnológica
Jahu

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

DEFESA DE REDES IOT COM BLOCKCHAIN: O Uso de Contratos Inteligentes contra ataques DDoS

IOT NETWORK DEFENSE WITH BLOCKCHAIN: THE USE OF SMART CONTRACTS AGAINST DDOS ATTACKS

Thaís de Sousa Silva
Tecnóloga, Fatec Araraquara, thaissousa.advocacia@gmail.com

Leonardo José de Lima Ferrucci
Mestre, Fatec Araraquara, leojau@gmail.com

DOI: https://doi.org/10.54628/issn2763-5600.v19.1.2025.338

RESUMO

A expansão da Internet das Coisas (IoT) em áreas como automação residencial, industrial e urbana trouxe avanços em conectividade, mas também alavancou a exposição das redes a ataques cibernéticos, especialmente os de negação de serviço distribuído (DDoS), que exploram falhas de autenticação em dispositivos com baixa capacidade de processamento e armazenamento, comprometendo a segurança. Este artigo analisa o uso combinado da tecnologia *blockchain* e dos contratos inteligentes como solução para mitigar ataques em redes IoT. Com base em revisão bibliográfica exploratória, são examinadas soluções descentralizadas na rede Ethereum[1]. Tais soluções oferecem vantagens como imutabilidade, descentralização, rastreabilidade e automação de processos de autenticação, o que contribui para reduzir vulnerabilidades e aumentar a resiliência dos sistemas. Além disso, o artigo discute a aplicação dos contratos inteligentes sob a ótica da Lei Geral de Proteção de Dados Pessoais (LGPD), destacando os desafios jurídicos e a importância da conformidade

Palavras-chave: Internet das Coisas; Segurança da Informação; *Blockchain*; Contratos Inteligentes; Ataques DDoS.

ABSTRACT

The expansion of the Internet of Things (IoT) in areas such as residential, industrial, and urban automation has improved connectivity but also increased network exposure to cyber threats, especially distributed denial-of-service (DDoS) attacks. These attacks exploit authentication flaws in devices with limited processing and storage capacity, compromising security. This article analyzes the combined use of blockchain technology and smart contracts as solution to mitigate such attacks in IoT networks. Based on an exploratory literature review, the study examines decentralized solutions on the Ethereum network, highlighting advantages such as immutability, decentralization, traceability, and automated authentication processes. Additionally, the article discusses the legal implications of using smart contracts in light of the Brazilian General Data Protection Law (LGPD), emphasizing regulatory challenges and the importance of compliance.

Keywords: *Internet of Things; Information Security; Blockchain; Smart Contracts; DDoS Attacks.*

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

1 INTRODUÇÃO

Com o avanço da tecnologia digital, a presença de dispositivos inteligentes conectados à Internet tornou-se comum em vários setores da sociedade, como residências, indústrias, hospitais e ambientes urbanos. Essa integração que é conhecida como Internet das Coisas (IoT), permite a automação de processos, ganho de eficiência e novas formas de interação entre sistemas e usuários (Kumar & Mallick, 2018). No entanto, a ampla conectividade também aumenta a superfície de exposição a ameaças cibernéticas, tornando necessária a exploração de novas medidas técnicas visando a segurança da informação.

Um dos ataques mais preocupantes nesse contexto são os chamados ataques de negação de serviço distribuído (DDoS). Eles ocorrem quando uma grande quantidade de dispositivos comprometidos passa a enviar requisições ao mesmo tempo, com o objetivo de sobrecarregar servidores e tirar sistemas do ar. Um exemplo foi o ataque da *botnet* Mirai, em 2016, que comprometeu milhares de dispositivos IoT mal configurados, gerando falhas em serviços como Twitter e Netflix (Antonakakis et al., 2017). Tais dispositivos geralmente possuem autenticação fraca, firmware desatualizado e recursos computacionais limitados (Ibrahim et al., 2022).

As soluções tradicionais de segurança, centradas em servidores, apresentam limitações frente à arquitetura distribuída da IoT. Falhas únicas, baixa escalabilidade e lentidão na detecção de ataques tornam essas abordagens pouco eficazes em redes heterogêneas e dinâmicas (Yakubu et al., 2023).

Nesse contexto, a tecnologia blockchain surge como alternativa promissora. Ela funciona como um banco de dados descentralizado e imutável, permitindo registrar atividades dos dispositivos de forma segura e transparente (Figueiredo & LIMA, 2021). Associados a ela, os contratos inteligentes automatizam regras de controle e autenticação, sem necessidade de intervenção manual, bloqueando dispositivos maliciosos ou não autorizados (Udousoro, 2023).

Este artigo tem como objetivo analisar as principais abordagens que utilizam blockchain pública, em especial a Ethereum, aliada a contratos inteligentes com o objetivo de proteger redes IoT contra ataques DDoS. São discutidas arquiteturas, métodos de autenticação, resultados práticos e desafios como custos de transação e escalabilidade.

Além disso, o estudo também aborda os impactos jurídicos do uso dessas tecnologias à luz da Lei Geral de Proteção de Dados (LGPD), considerando princípios como segurança, transparência e responsabilização. Dessa forma, busca-se contribuir para soluções mais seguras, eficientes e alinhadas à legislação no ecossistema da IoT.

2 FUNDAMENTAÇÃO TEÓRICA

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

2.1. Internet das Coisas (IoT) e Vulnerabilidades

A Internet das Coisas (IoT) refere-se à conexão de objetos físicos à Internet, permitindo que troquem dados entre si e com sistemas centrais. Sua estrutura é geralmente dividida em três camadas: a de percepção (sensores que coletam dados do ambiente), a de rede (que transmite os dados por protocolos como MQTT, CoAP e HTTP), e a de aplicação (que processa e utiliza os dados coletados) (Ibrahim et al., 2022).

O crescimento da IoT em setores como cidades inteligentes, agricultura, saúde e indústria trouxe novos desafios de segurança. Muitos dispositivos conectados têm hardware limitado e software desatualizado, com autenticação fraca, protocolos inseguros e configurações padrão (Yakubu et al., 2023). Tais falhas facilitam a atuação de agentes maliciosos, que os transformam em pontos de entrada ou em bots de redes usadas para ataques DDoS.

Segundo Udousoro (2023), é comum que esses dispositivos não possuam proteção contra alterações de firmware nem mecanismos eficazes de detecção de anomalias, tornando-os vulneráveis a ações coordenadas. Além disso, a ausência de padrões unificados de segurança, somada à diversidade de fabricantes e modelos, agrava o risco.

Como muitos desses aparelhos utilizam redes sem fio e acesso via Internet pública, há maior possibilidade de interceptação e manipulação de dados. Isso compromete os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (Silva; Andrade; Oliveira, 2024).

Apesar desses desafios, a IoT continua sendo uma ferramenta estratégica para automação e conectividade. No entanto, para garantir seu uso seguro, é necessário adotar soluções tecnológicas robustas. O uso de blockchain e contratos inteligentes tem sido estudado como alternativa viável para reforçar a segurança, autenticidade e integridade em ambientes distribuídos.

2.2. Ataques DDoS: Conceito e Impacto

Ataques de negação de serviço distribuído (DDoS) consistem em sobrecarregar servidores com grandes volumes de requisições simultâneas, impedindo que usuários legítimos acessem os serviços. Esses ataques são geralmente realizados por botnets — redes de dispositivos infectados — que operam de forma coordenada para gerar tráfego malicioso em larga escala (Yakubu et al., 2023).

Há diferentes tipos de ataques DDoS. Na camada de infraestrutura, há técnicas como SYN Flood e UDP Flood, que consomem largura de banda e recursos do sistema. Já na camada

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

de aplicação, o HTTP Flood é mais difícil de detectar, pois simula o tráfego legítimo, tornando a identificação mais complexa (Silva; Andrade; Oliveira, 2024).

O caso da botnet Mirai em 2016 exemplifica esse tipo de ameaça. Dispositivos IoT vulneráveis, como câmeras IP e roteadores, foram comprometidos e utilizados para lançar ataques contra grandes provedores de serviço, afetando plataformas como Twitter e Netflix (Antonakakis et al., 2017).

Além de afetar a disponibilidade, ataques DDoS causam prejuízos financeiros, danos à reputação e podem servir de cortina de fumaça para outras invasões, como roubo de dados (Ibrahim et al., 2022). No contexto da IoT, esses riscos se intensificam, dada a fragilidade de muitos dispositivos conectados e a ausência de mecanismos eficazes de defesa.

Fabricantes frequentemente negligenciam atualizações de firmware, segurança de autenticação e detecção de anomalias, facilitando a criação de botnets com milhares de aparelhos comprometidos (Udousoro, 2023).

Diante desse cenário, é essencial buscar estratégias inovadoras. O uso de blockchain e contratos inteligentes tem se mostrado promissor, especialmente por permitir automação no controle de tráfego e autenticação, dificultando a propagação de tráfego malicioso em redes distribuídas.

2.3. Blockchain: Conceitos e Aplicações na Segurança

A blockchain é uma tecnologia originalmente concebida para registrar transações de forma segura e transparente. Seu funcionamento baseia-se em blocos encadeados e protegidos por criptografia, formando um registro imutável e compartilhado entre os participantes da rede (Figueiredo & Lima, 2021).

Entre suas principais características estão a descentralização — ausência de uma autoridade central; a imutabilidade — impossibilidade de alterar registros já validados; e a transparência, permitindo auditoria por todos os nós autorizados (Yakubu et al., 2023).

No contexto da Internet das Coisas, a blockchain permite registrar o comportamento de dispositivos, dificultando fraudes e facilitando a rastreabilidade de ações. Essa rastreabilidade é importante para detectar comportamentos suspeitos e reforçar a autenticação em ambientes críticos (Ibrahim et al., 2022).

Além disso, a blockchain contribui para garantir a integridade dos dados trafegados e oferece uma base segura para implementar contratos inteligentes que automatizam decisões de segurança (Udousoro, 2023).

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Há diferentes tipos de blockchain: as públicas, como a Ethereum, permitem que qualquer usuário participe da validação de blocos; as privadas são restritas a entidades específicas. A escolha depende do nível de confiança entre os participantes e do controle desejado sobre os dados (Figueiredo & lima, 2021).

Portanto, a adoção da blockchain em redes IoT oferece um novo paradigma de segurança, especialmente quando associada a contratos inteligentes que automatizam o controle de acesso, autenticação e bloqueio de dispositivos comprometidos.

2.4. Contratos Inteligentes (Smart Contracts)

Contratos inteligentes, ou smart contracts, são programas de computador que executam automaticamente ações previamente definidas, quando determinadas condições são atendidas. Eles operam dentro de plataformas blockchain e foram desenvolvidos para eliminar a necessidade de intermediários, aumentando a eficiência e a confiança nas transações digitais (Figueiredo & lima, 2021).

Esses contratos são particularmente úteis em contextos como a Internet das Coisas (IoT), onde decisões precisam ser tomadas de forma rápida e autônoma. Por exemplo, um contrato inteligente pode autenticar dispositivos automaticamente, permitindo ou bloqueando o acesso com base em regras pré-programadas (IBRAHIM et al., 2022).

Entre os principais benefícios dessa tecnologia estão a segurança, já que o código é executado exatamente como programado; a eficiência, pela eliminação de processos manuais; e a transparência, pois as regras são visíveis e auditáveis por todos os participantes da rede (Yakubu et al., 2023).

No contexto da mitigação de ataques DDoS, contratos inteligentes podem monitorar o comportamento dos dispositivos em tempo real, bloqueando automaticamente aqueles que apresentarem atividades suspeitas ou abusivas (Udousoro, 2023). Isso evita a sobrecarga dos servidores e aumenta a resiliência da rede.

Apesar das vantagens, os contratos inteligentes também enfrentam desafios. Uma vez implantado na blockchain, o código se torna imutável, o que significa que erros de programação não podem ser corrigidos facilmente. Além disso, blockchains públicas como a Ethereum requerem pagamento de taxas (gás) por cada operação executada, o que pode ser um obstáculo para sistemas com alta frequência de transações (Figueiredo & lima, 2021).

Mesmo com essas limitações, o uso de contratos inteligentes tem grande potencial para aprimorar a segurança em ambientes IoT, proporcionando maior automação, confiabilidade e rapidez na resposta a ameaças.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

2.5. Edge Computing e seu Papel na Segurança da IoT

A arquitetura tradicional de computação em nuvem apresenta limitações para o contexto da IoT, especialmente em aplicações que demandam respostas em tempo real. A edge computing surge como uma alternativa, ao processar dados localmente, próximo à origem, ou seja, na borda da rede (Yousefpour et al., 2019).

Ao reduzir a necessidade de envio constante de dados para servidores remotos, a edge computing diminui a latência, melhora a escalabilidade e alivia a carga sobre o núcleo da rede. Esses fatores são críticos para aplicações como veículos autônomos, monitoramento médico e sistemas industriais, onde atrasos podem comprometer a operação (Kumar & Mallick, 2018).

Do ponto de vista da segurança, essa arquitetura permite aplicar políticas de controle diretamente nos gateways locais, identificando padrões de tráfego malicioso antes que atinjam servidores centrais. Dessa forma, atua como uma camada adicional de defesa contra ataques como DDoS (Ibrahim et al., 2022).

Além disso, ao manter parte dos dados sensíveis na borda da rede, reduz-se a exposição de informações críticas durante a transmissão, contribuindo para a confidencialidade e integridade das comunicações.

Quando integrada a soluções baseadas em blockchain, a edge computing pode fortalecer ainda mais a segurança da IoT. É possível, por exemplo, registrar eventos localmente e sincronizá-los com a blockchain, promovendo rastreabilidade e resposta rápida a incidentes (Udousoro, 2023).

Portanto, o uso combinado de edge computing com blockchain e contratos inteligentes representa uma abordagem promissora e distribuída para enfrentar os desafios de segurança na Internet das Coisas.

2.6 Aspectos Jurídicos do Uso de Contratos Inteligentes e sua Relação com a LGPD

A adoção de tecnologias como blockchain e contratos inteligentes em redes IoT levanta importantes questões jurídicas, especialmente no que se refere à conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Essa legislação estabelece princípios como finalidade, necessidade, transparência e segurança para o tratamento de dados pessoais no Brasil.

No contexto da IoT, muitos dispositivos coletam informações sensíveis — como localização, hábitos de consumo e dados de saúde — que, quando associados a uma pessoa natural, configuram dados pessoais. O uso de soluções descentralizadas exige, portanto, atenção

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

redobrada quanto à responsabilização, consentimento e base legal para o tratamento desses dados.

A blockchain, por sua natureza imutável, pode entrar em conflito com direitos previstos na LGPD, como a possibilidade de retificação ou exclusão de dados (art. 18). Por outro lado, oferece vantagens como transparência e rastreabilidade das operações, reforçando o princípio da prestação de contas (accountability) (Figueiredo & lima, 2021).

Já os contratos inteligentes permitem aplicar políticas de segurança de forma automatizada, promovendo controle de acesso, autenticação e registro de eventos. Entretanto, devem ser programados considerando desde o início os princípios da privacidade desde a concepção (privacy by design) e da proteção por padrão (privacy by default).

Além disso, é essencial definir com clareza os papéis de controlador e operador nos ambientes descentralizados, algo ainda carente de regulamentação específica. Sem essa definição, pode haver lacunas na responsabilização em caso de incidentes de segurança.

Assim, a integração entre inovação tecnológica e conformidade jurídica exige um planejamento multidisciplinar. O uso de blockchain e contratos inteligentes na IoT pode ser compatível com a LGPD desde que sejam implementados controles técnicos, administrativos e jurídicos adequados.

3 PROCEDIMENTOS METODOLÓGICOS

Este trabalho adota uma abordagem qualitativa, baseada em revisão bibliográfica exploratória. O objetivo é investigar soluções descentralizadas que utilizam blockchain e contratos inteligentes para mitigar ataques DDoS em redes de Internet das Coisas (IoT), com especial atenção às implicações jurídicas relacionadas à Lei Geral de Proteção de Dados (LGPD).

A pesquisa foi conduzida por meio da análise de artigos científicos, estudos de caso e documentos técnicos disponíveis em bases como *IEEE Xplore, ScienceDirect, SpringerLink, Scopus e o Google Scholar.*

Foram considerados documentos publicados no período de 2018 a 2024, intervalo temporal definido em razão da intensificação das pesquisas sobre blockchain aplicada à segurança de redes IoT e do avanço das plataformas de contratos inteligentes nesse período.

Quanto ao tipo de material analisado, foram considerados: (i) artigos científicos revisados por pares; (ii) trabalhos publicados em anais de conferências internacionais; (iii) teses e dissertações acadêmicas; e (iv) documentos técnicos e normativos relacionados à segurança da informação e à proteção de dados.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Os critérios de inclusão envolveram: (i) proposição de modelos ou arquiteturas de segurança baseados em blockchain; (ii) utilização de contratos inteligentes em ambientes IoT; (iii) discussões técnicas ou normativas sobre conformidade à LGPD no uso dessas tecnologias.

Foram definidos critérios de exclusão para delimitar o escopo da pesquisa exploratória. Foram excluídos: (i) estudos que mencionavam IoT apenas em contextos não relacionados à segurança de redes, como automação doméstica sem abordagem de autenticação ou mitigação de ataques; (ii) trabalhos que tratavam de blockchain de forma meramente conceitual, sem aplicação em IoT ou segurança; (iii) publicações anteriores a 2018; (iv) documentos duplicados entre bases de dados; e (v) materiais sem rigor metodológico ou sem relação direta com o objetivo do estudo. A exclusão ocorreu tanto por filtros automáticos das bases quanto por análise manual de títulos e resumos.

Os termos de busca utilizados incluíram expressões na língua vernácula, como "segurança em IoT", "mitigação de DDoS" e "contratos inteligentes", além de correspondentes em inglês, como IoT security, DDoS mitigation, blockchain in IoT, smart contracts e LGPD. Essa combinação permitiu delimitar o levantamento às abordagens mais relevantes e atuais sobre o tema, o que permitiu delimitar o levantamento às abordagens mais relevantes e atuais sobre o tema.

O levantamento também considerou diretrizes e documentos oficiais emitidos por órgãos reguladores, como a Agência Nacional de Proteção de Dados (ANPD), para embasar o recorte jurídico do estudo.

Por se tratar de um estudo exploratório, não foram realizados experimentos práticos ou simulações computacionais. A proposta metodológica centra-se na sistematização crítica do conhecimento existente, com o intuito de identificar boas práticas, desafios recorrentes e lacunas que possam orientar pesquisas futuras.

Observa-se ainda uma escassez de material técnico produzido por pesquisadores brasileiros sobre a aplicação de blockchain e contratos inteligentes na segurança de redes IoT. Dessa forma, a maior parte das fontes utilizadas nesta pesquisa provém de estudos internacionais, com destaque para publicações originadas nos Estados Unidos, Europa e Ásia, regiões que concentram a produção científica mais consolidada sobre o tema.

4 RESULTADOS E DISCUSSÃO

O levantamento bibliográfico inicial resultou em 214 documentos distribuídos entre as bases de dados consultadas. A quantidade de publicações por base foi a seguinte: IEEE Xplore (58), ScienceDirect (42), SpringerLink (36), Scopus (28) e Google Scholar (50).

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Após a identificação dos resultados, realizou-se o processo de filtragem. Inicialmente, foram excluídos 47 documentos duplicados entre as bases. Em seguida, procedeu-se à triagem de títulos e resumos, resultando na exclusão de 112 trabalhos que não atendiam aos critérios de inclusão definidos na metodologia. Ao final desse processo, 55 estudos foram selecionados para leitura integral e análise.

Quanto à distribuição temporal das publicações selecionadas, observou-se maior concentração de estudos no período entre 2020 e 2023, indicando crescimento recente do interesse científico na aplicação de blockchain e contratos inteligentes para mitigação de ataques DDoS em redes IoT. Esse resultado evidencia a consolidação progressiva do tema na literatura acadêmica.

A análise das abordagens propostas na literatura revela uma diversidade de estratégias para mitigar ataques DDoS em redes IoT utilizando contratos inteligentes. As soluções mais recorrentes incluem: listas brancas (*Whitelists*), que permitem a comunicação apenas de dispositivos previamente autorizados; listas negras (*blacklists*), que bloqueiam o acesso de dispositivos identificados como maliciosos; e sistemas baseados em reputação, que atribuem pontuações aos dispositivos com base em seu comportamento anterior na rede.

Além disso, algumas propostas aplicam o conceito de controle de gás (*Gas control*) um mecanismo característico da *blockchain* Ethereum que limita o número de operações computacionais por transação, funcionando como um sistema de cotas. Com isso, é possível penalizar automaticamente requisições abusivas, já que dispositivos mal-intencionados geralmente consomem mais recursos computacionais (Ibrahim et al., 2022; Yakubu et al., 2023).

Outro elemento importante na segurança de redes baseadas em *blockchain* é o modelo de consenso conhecido como prova de participação (Proof-of-Stake – PoS), que substitui a tradicional prova de trabalho (Proof-of-Work – PoW). Enquanto o PoW exige grande poder computacional e consumo de energia para validar transações, o PoS seleciona validadores com base na quantidade de criptomoedas que possuem e que estão dispostos a "travar" como garantia (*stake),* tornando o processo mais sustentável e eficiente.

Adicionalmente, diversas soluções propõem o uso de armazenamento fora da cadeia (*off-chain*), ou seja, manter os dados sensíveis fora da *blockchain* e utilizar apenas referências registradas na cadeia de blocos. Essa abordagem ajuda a superar limitações relacionadas à privacidade, escalabilidade e custos elevados de armazenamento na *blockchain*.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Algorithm 2: Smart Contract Communication Phase

```
begin
    if (ObjIdExists (sender.id, bc) == false OR ObjIdExists (receiver.id, bc)== false)
     then
        return Error ();
    if (sender.grpId != receiver.grpId) then
        return Error ();
    if (bc.SignVerif (sender.msg) == false) then
        return Error ();
    if (bc.CurrentGaslimitValue >(AllowedGasLimitValue)) then
        return Error ();
        LabelDeviceAsMalicious();
        dropFromWhiteList();
  end
// Communication phase finished with success
```

Listagem 1 – Algoritmo de verificação e controle de comunicação via contrato inteligente

Trecho do algoritmo do processo de validação da comunicação entre dispositivos IoT e a blockchain, incluindo verificação de identidade, grupo e limite de gás.

Fonte: Adaptado de IBRAHIM et al. (2022, p. 10).

Em termos de arquitetura tecnológica, a *blockchain* pública Ethereum é amplamente utilizada, por oferecer suporte a contratos inteligentes e características como descentralização, imutabilidade e transparência. Algumas propostas vão além e sugerem arquiteturas colaborativas entre diferentes domínios administrativos (ASes), onde múltiplas redes IoT compartilham informações de autenticação e reputação por meio de uma *blockchain* comum, aumentando assim a eficácia na identificação e contenção de ataques em larga escala (Udousoro, 2023).

Para ilustrar uma aplicação prática, o trabalho de Rodrigues et al. (2023) propõe um contrato inteligente em Solidity voltado à mitigação colaborativa de ataques DDoS. O contrato é projetado para registrar, verificar e compartilhar IPs maliciosos em uma rede descentralizada baseada em *blockchain* e controladores *Software-Defined Networking* - SDN (ou Rede Definida por Software). A seguir, apresenta-se um trecho relevante desse contrato, com destaque para a função reportIPv4, que permite a inclusão de endereços maliciosos detectados por entidades confiáveis da rede. Vejamos.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Listing 1.1. Smart contract structures and core functionality

```
function reportIPv4(uint32[] src, uint32 expiringBlock) {
  if (msg.sender == owner) {
    for (uint i = 0; i < src.length; i++) {
      drop_src_ipv4.push(ReportIPv4(
        expiringBlock, src[i], dstIPv4));
    }
  }
  DstIPv4 customer = customerIPv4[msg.sender];
  if(customer.dst_ipv4 != 0) {
    for (i = 0; i < src.length; i++) {
      report_src_ipv4.push(ReportIPv4(
        expiringBlock, src[i], customer));
    }
  }
}
```

Listagem 2 – Função reportIPv4() para registro de IPs maliciosos via contrato inteligente

Fonte: Adaptado de RODRIGUES et al. (2023, p. 25–26).

Já o modelo proposto por Yakubu et al. (2023) para mitigar ataques DDoS em ambientes de IoT por meio de uma arquitetura descentralizada baseada em blockchain, é composto por três camadas principais: a camada de autenticação, a de monitoramento e a de consenso. A camada de autenticação gerencia as permissões dos dispositivos IoT, enquanto a de monitoramento observa continuamente o comportamento da rede, gerando alertas para atividades suspeitas. Já a camada de consenso registra as decisões em blockchain, garantindo transparência, imutabilidade e coordenação entre múltiplos domínios. Essa abordagem reforça a resiliência da rede ao dificultar a propagação de ataques em larga escala e permite uma resposta automatizada e auditável frente a comportamentos maliciosos.

A Figura 1 apresenta a proposta de Yakubu et al. (2023) para mitigar ataques DDoS em ambientes de IoT por meio de uma arquitetura descentralizada baseada em blockchain.

Fatecnológica
Jahu
ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

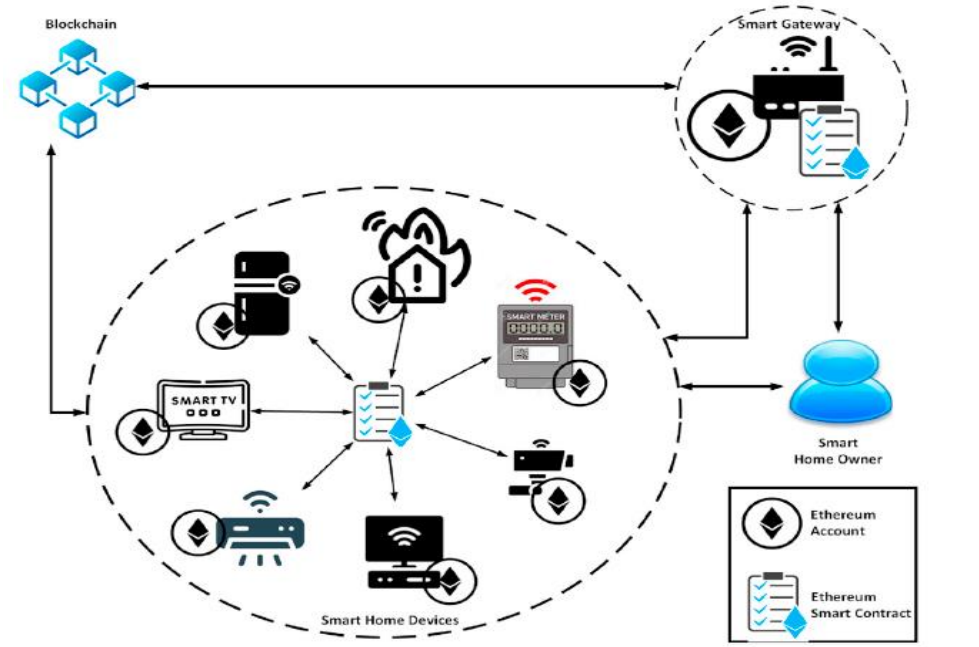

Fig. 1. Smart home network model.

Figura 1 – Arquitetura proposta para mitigação de ataques DDoS baseada em blockchain em ambientes de IoT

Fonte: Adaptado de YAKUBU et al. (2023, p. 386).

O gráfico 1 abaixo relacionado, apresenta a redução estimada de dispositivos maliciosos autenticados após o uso de contratos inteligentes, ilustra a eficácia do uso de contratos inteligentes na redução de dispositivos maliciosos em redes IoT. Inicialmente, 5.000 dispositivos não autorizados foram identificados na rede. Após 30 dias de aplicação dos contratos inteligentes, esse número caiu para 1.200. Ao final de 60 dias, restavam apenas 400 dispositivos com comportamento suspeito. Essa redução demonstra como a automação das regras de controle de acesso, somada à transparência e imutabilidade da *blockchain*, contribui para uma resposta mais ágil e eficaz contra ataques.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

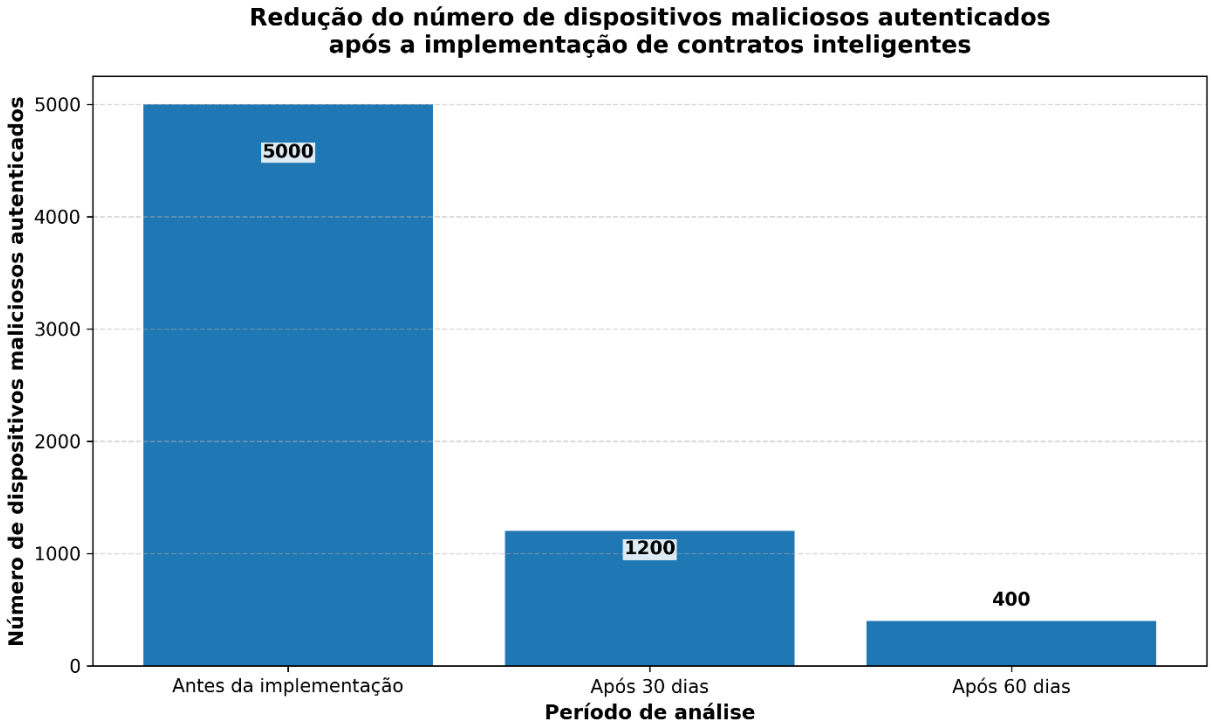

Gráfico 1 – Redução estimada de dispositivos maliciosos autenticados após uso de contratos inteligentes

(Fonte: Elaboração própria com base nas tendências descritas em Ibrahim et al. (2022); Yakubu et al. (2023); Udousoro (2023); valores simulados.); Yakubu et al. (2023); Udousoro (2023))

Yakubu et al. (2023) destacam ganhos expressivos em resiliência da rede, com a filtragem automática de requisições maliciosas, mesmo em cenários com muitos dispositivos comprometidos. A integração com algoritmos de reputação também melhora a capacidade de adaptação do sistema em tempo real.

Essas soluções são especialmente promissoras em ambientes críticos, como hospitais, sistemas de transporte inteligente e infraestruturas urbanas, onde a disponibilidade dos serviços é essencial. A execução automática das regras de segurança reduz a necessidade de intervenção humana e acelera a resposta a ataques, fortalecendo a continuidade operacional.

Além dos aspectos técnicos, o uso de contratos inteligentes em ambientes IoT também levanta questões jurídicas relevantes, principalmente em relação à Lei Geral de Proteção de Dados Pessoais (LGPD). Como as *blockchain*s são imutáveis, a alteração ou exclusão de dados pessoais, conforme previsto na LGPD, torna-se complexa. Isso é especialmente problemático quando informações sensíveis são armazenadas diretamente na *blockchain*. Além disso, a execução automática dos contratos dificulta a identificação de responsáveis, gerando incertezas quanto à atribuição legal (Zanatta, 2021).

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

Assim, é necessário adotar estratégias de conformidade, como o uso de anonimização de dados, armazenamento *off-chain* e a definição clara de papéis entre controladores e operadores de dados (Doneda, 2021), para garantir que a tecnologia seja compatível com as exigências legais.

Em síntese, as soluções baseadas em contratos inteligentes e *blockchain* apresentam vantagens expressivas sobre os modelos centralizados. Elas eliminam pontos únicos de falha, aumentam a resiliência, reduzem o tempo de resposta e favorecem a colaboração entre diferentes redes. Contudo, desafios técnicos, como latência de validação, custos de transação (*Gas fees*) e consumo energético, principalmente no modelo PoW, ainda limitam sua adoção em larga escala. Felizmente, novas abordagens, como *blockchain*s leves, arquiteturas híbridas (pública/privada) e redes 5G com *edge computing,* vêm sendo desenvolvidas para superar essas barreiras.

Conforme destacado por Rouhani e Deters (2019), *blockchains* baseadas em Proof-of-Work (PoW) apresentam alto custo energético, o que inviabiliza sua aplicação direta em redes de dispositivos com recursos limitados, como ambientes IoT. Já o modelo Proof-of-Stake (PoS), ao eliminar a competição computacional e o uso intensivo de hardware, apresenta consumo drasticamente inferior, sendo mais adequado para soluções descentralizadas em larga escala.

O gráfico 2 apresenta dados reais sobre o consumo energético de *blockchains* que utilizam diferentes mecanismos de consenso. Enquanto o Bitcoin, baseado em Proof-of-Work (PoW), consome em média 707 kWh por transação, o Ethereum 2.0, já migrado para Proof-of-Stake (PoS), consome apenas 0,0026 kWh. Essa diferença significativa demonstra a superioridade energética das arquiteturas PoS, especialmente para aplicações em IoT, onde a eficiência é essencial para a sustentabilidade do sistema.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

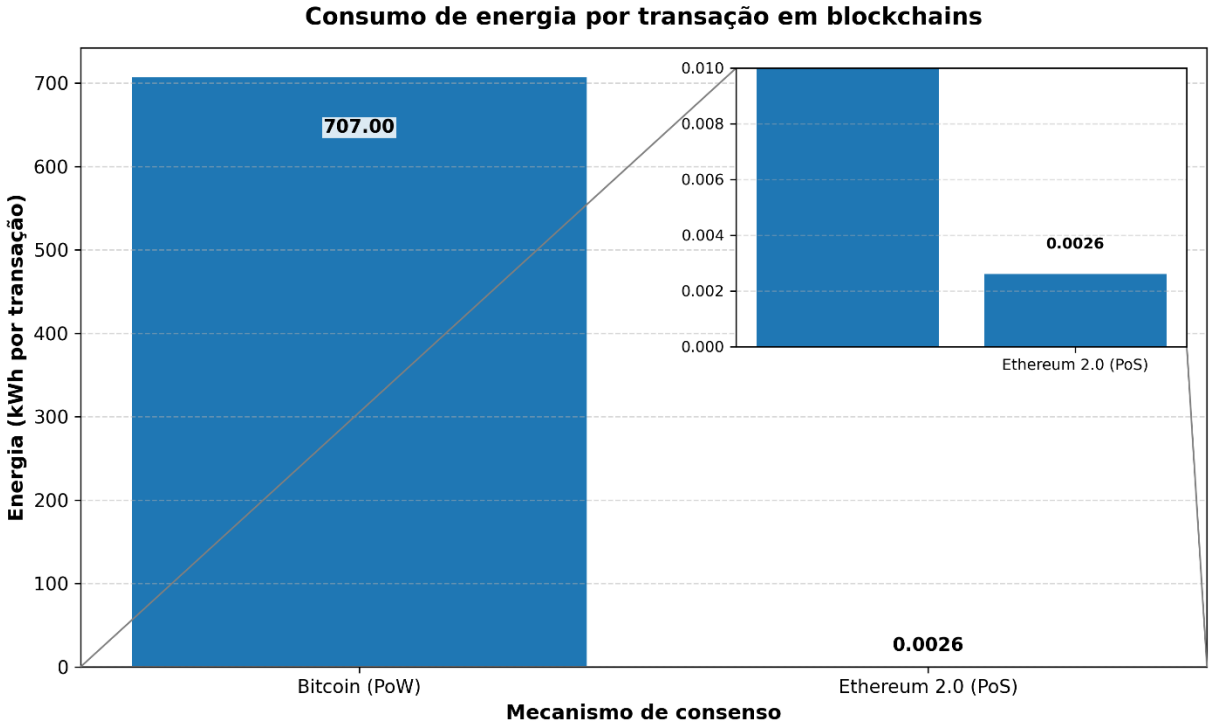

Gráfico 2 – Consumo de energia por transação: comparação entre PoW e PoS em blockchains
Fonte: Adaptado de Digiconomist, BitDegree e Ethereum Foundation (2023).

Portanto, os contratos inteligentes representam uma evolução significativa na proteção de redes IoT contra-ataques DDoS, integrando princípios clássicos da segurança da informação, como disponibilidade, autenticidade e integridade, com tecnologias inovadoras. Seu sucesso prático dependerá da superação dos desafios técnicos e da construção de padrões interoperáveis que permitam sua aplicação segura, eficiente e em conformidade legal.

5 CONSIDERAÇÕES FINAIS

A crescente adoção de dispositivos IoT em ambientes críticos, como cidades inteligentes, indústrias, automação residencial e sistemas de saúde, tem ampliado não apenas a conectividade, mas também os riscos de segurança e conformidade legal, especialmente frente às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD). Neste cenário, os ataques distribuídos de negação de serviço (DDoS) surgem como uma das principais ameaças à disponibilidade e integridade dos sistemas conectados.

Este artigo demonstrou que o uso combinado da tecnologia blockchain pública e dos contratos inteligentes representa uma estratégia robusta para mitigar esses riscos, permitindo a automação de regras de autenticação, controle de acesso e bloqueio de dispositivos maliciosos. Modelos baseados em listas brancas, listas negras, reputação e controle de gás mostraram-se tecnicamente eficazes para detectar e isolar comportamentos suspeitos em tempo real.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

As evidências extraídas da literatura, especialmente dos estudos de Ibrahim et al. (2022), Yakubu et al. (2023) e Udousoro (2023), apontam reduções significativas na presença de dispositivos maliciosos autenticados. Adicionalmente, a adoção de modelos energéticos mais sustentáveis, como o Proof-of-Stake (PoS), mostrou-se vantajosa em termos de eficiência, tornando-se viável para ambientes IoT com recursos limitados.

Além dos ganhos técnicos, a discussão evidenciou os desafios jurídicos que acompanham o uso dessas tecnologias, sobretudo quanto à compatibilidade com a LGPD. A imutabilidade das blockchains, o uso de anonimização, o armazenamento off-chain e a clara definição de papéis entre controladores e operadores são fundamentais para preservar os direitos dos titulares de dados.

Entre as limitações identificadas, destacam-se os custos operacionais em redes públicas, a latência de validação e o consumo energético de blockchains baseadas em Proof-of-Work (PoW). Em contrapartida, soluções como redes híbridas, algoritmos PoS e a integração com edge computing oferecem caminhos promissores para superação desses entraves.

Conclui-se que os contratos inteligentes não apenas fortalecem a segurança em redes IoT, como também promovem uma arquitetura mais resiliente, automatizada e juridicamente consciente. No entanto, sua aplicação efetiva dependerá de um ecossistema com padrões interoperáveis, governança clara e diálogo contínuo entre tecnologia, direito e segurança.

Para pesquisas futuras, recomenda-se a realização de testes empíricos com dispositivos reais, a análise de interoperabilidade entre blockchains, o estudo aprofundado de custos operacionais e o desenvolvimento de diretrizes regulatórias específicas para ambientes descentralizados.

AGRADECIMENTOS

Agradeço a Deus, fonte de toda criação e inspiração, por me conceder o impulso incessante de aprender. À minha família, que é a raiz e a sustentação da minha vida, e aos amigos que se somaram como presentes ao longo do caminho. Sou grato aos mestres que plantaram sementes de conhecimento e abriram horizontes. E ao destino, que entre encontros e desencontros, fez convergir cada estudo e experiência em direção à carreira que hoje abraço como realização de um sonho. Por fim, ao meu orientador, pela generosidade e excelência que iluminaram este percurso.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

REFERÊNCIAS

ANTONAKAKIS, Manos; APRUZZESE, Giovanni; BEARD, Spencer; DAUBE, Jared; ELIE, Marion; GRITA, Valentina. *Understanding the Mirai Botnet*. In: ***USENIX Security Symposium*****,** 26., 2017, Vancouver. Proceedings [...]. Berkeley: USENIX Association, 2017.Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Acesso em: 20 jun. 2025.

BITDEGREE. Most energy efficient cryptocurrency. **BitDegree**, 2023. Disponível em: <https://www.bitdegree.org/crypto/tutorials/most-energy-efficient-cryptocurrency>. Acesso em: 1 jun. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 19 junho 2025.

DIGICONOMIST. Bitcoin Energy Consumption Index. **Digiconomist**, 2023. Disponível em: <https://digiconomist.net/bitcoin-energy-consumption/>. Acesso em: 1 jun. 2025.

DONEDA, Danilo**.** A proteção de dados pessoais: a função e os limites da anonimização na LGPD. ***Revista de Direito, Estado e Telecomunicações***, v. 13, n. 1, p. 9–29, 2021. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/476 Acesso em: 19 junho 2025.

ETHEREUM FOUNDATION. Ethereum Energy Consumption Drops Over 99%. **Ethereum Foundation**, 2023. Disponível em: <https://ethereum.org/en/energy-consumption/>. Acesso em: 1 jun. 2025.

FIGUEIREDO, Jordan E. M.; LIMA, Iremar N**.** Contratos inteligentes com Ethereum. ***Journal of Innovation and Science: Research and Application***, [S. l.], v. 1, n. 1, p. 38–48, 2021. Disponível em: https://joins.emnuvens.com.br/joins/article/view/206. Acesso em: 1 maio 2025.

IBRAHIM, Rahmeh Fawaz et al**.** DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology**.** ***Sensors***, Basel, v. 22, p. 6806, 2022. Disponível em: https://doi.org/10.3390/s22186806. Acesso em: 4 junho 2025.

KUMAR, N.; MALLICK, P. K**.** The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. ***Procedia Computer Science***, v. 132, p. 109–117, 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050918309049. Acesso em: 12 abril 2025.

RODRIGUES, B.; BOCEK, T.; LAREIDA, A.; HAUSHEER, D.; RAFATI, S.; STILLER, B. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In: **IFIP INTERNATIONAL CONFERENCE ON AUTONOMOUS INFRASTRUCTURE, MANAGEMENT AND SECURITY (AIMS)**, 2017, Zurich. Proceedings [...]. Cham: Springer, 2017. p. 16–29. Disponível em: https://doi.org/10.1007/978-3-319-60774-0_2. Acesso em: 30 jun. 2025.

ISSN 1980-8526 (print)
ISSN 2763-5600 (online)

SILVA, Eduardo J. A.; ANDRADE, Gabriel R. L.; OLIVEIRA, Rogério L. S**.** Ataques de negação de serviço distribuído (DDoS): o que é e como prevenir**. VI Jornada Acadêmica, Científica e Tecnológica**, FATEC Jales, 2024. Disponível em: https://ric.cps.sp.gov.br. Acesso em: 3 abril 2025.

UDOUSORO, Isonkobong Christopher**.** Mitigation of IoT Device Based DDoS Attacks Using Blockchain. ***Journal of Research in Engineering and Computer Sciences***, v. 1, n. 4, p. 85–92, 2023. Disponível em: https://hspublishing.org/JRECS/article/view/236/190. Acesso em: 5 abril 2025.

YAKUBU, Bello Musa et al. Blockchain-based DDoS attack mitigation protocol for device-todevice- interaction in smart home. ***Digital Communications and Networks***, v. 9, p. 383–392, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S2352864823000263. Acesso em: 3 março 2025.

YOUSEFPOUR, Ashkan; PENG, Mingyi; SHAHIN, Abbas; GHANEM, Mohamed; MAIER, Martin. *All One Needs to Know about Fog Computing and Related Edge Computing Paradigms: A Complete Survey*. ***Journal of Systems Architecture***, v. 98, p. 289–330, 2019. **Disponível em:** https://arxiv.org/abs/1808.05283**. Acesso em:** 1 jun. 2025.