ANÁLISE DA INTEGRAÇÃO ENTRE BLOCKCHAIN E IOT PARA SEGURANÇA CIBERNÉTICA

Autor:
Angela Aparecida Pereira Cândido
afiliação institucional autor
angela.candido@fatec.sp.gov.br

Orientador:
Cleber Henrique de Oliveira
afiliação institucional orientador
cleber.oliveira16@fatec.sp.gov.br

RESUMO

Este estudo explora a integração da Internet das Coisas (IoT) e a tecnologia Blockchain para melhorar a segurança dos dados e enfrentar desafios de escalabilidade. Destaca-se o uso crescente de dispositivos IoT nas empresas e a vulnerabilidade desses dispositivos a ataques cibernéticos. A pesquisa enfatiza o papel do Blockchain na garantia da integridade e confidencialidade dos dados. Através de uma revisão bibliográfica abrangente e análise corporativas, investiga-se tecnologias que podem assegurar a segurança dos dados processados pela IoT. Avalia-se também o impacto do Blockchain na imutabilidade dos dados, um aspecto crucial para a segurança dos dados organizacionais.

Palavras-chave: Internet das Coisas; Blockchain; Segurança de dados; Escalabilidade; Organizações.

ABSTRACT

This study explores the integration of the Internet of Things (IoT) and Blockchain technology to enhance data security and address scalability challenges. It highlights the increasing use of IoT devices in businesses and the vulnerability of these devices to cyber-attacks. The research emphasizes the role of Blockchain in ensuring data integrity and confidentiality. Through a comprehensive literature review and analysis corporate, we investigate technologies that can secure the data processed by IoT. We also evaluate the impact of Blockchain on data immutability, a crucial aspect for data security in an organizational context.

Keywords: Internet of Things; Blockchain; Data security; Scalability; Organizations.

1. INTRODUÇÃO

Em meio à rápida digitalização da sociedade contemporânea, a Internet das Coisas (IoT) surge como uma tecnologia emergente que permeia diversos aspectos de nossas vidas. A IoT representa uma rede de objetos físicos, ou "coisas", que possuem tecnologia embarcada para se conectar e trocar dados com a internet (Sakamoto, 2020). Esses objetos variam desde dispositivos domésticos, como geladeiras e Smart TVs, até dispositivos pessoais, como Smartwatches (Santos et al., 2016).

A IoT tem experimentado um crescimento exponencial no ambiente corporativo devido à sua capacidade de oferecer uma gama diversificada de aplicações práticas. Dentro das organizações, esses dispositivos podem se comunicar entre si e com os usuários, desempenhando uma infinidade de funções e atribuições. Este fenômeno tem o potencial de revolucionar a maneira como as empresas operam e interagem com sua base de clientes (Cernev et al., 2021).

No entanto, à medida que os dispositivos conectados à internet (IoT) continuam a evoluir e seu uso se torna cada vez mais difundido, eles se tornam alvos cada vez mais atraentes para os cibercriminosos. Isso coloca em risco a segurança dos dados compartilhados por meio desses dispositivos (Sakamoto, 2020). A problemática central deste estudo reside nesse desafio de segurança: Como garantir a segurança dos dados na IoT em um ambiente cada vez mais digital e conectado?

O foco deste estudo é a união entre blockchain e Internet das Coisas (IoT) como uma estratégia inovadora para a segurança cibernética. A IoT, uma tecnologia em ascensão, possibilita a conexão de dispositivos e objetos do dia a dia à internet, viabilizando a coleta e o compartilhamento de dados em tempo real. Contudo, essa conectividade também acarreta desafios significativos no que diz respeito à segurança e privacidade dos dados. Nesse cenário, a blockchain se destaca como uma solução promissora para assegurar a segurança e privacidade dos dados na IoT. Este estudo oferece uma visão geral sobre segurança e privacidade na IoT, discute os principais desafios e explora como algumas soluções, como o uso de blockchain, buscam superar esses obstáculos (Sakamoto, 2020).

2. OBJETIVO

Este estudo tem como objetivo realizar uma análise da integração entre a Internet das Coisas (IoT) e a tecnologia Blockchain. O intuito é aprimorar a segurança dos dados e abordar desafios de escalabilidade nas organizações.

Os objetivos específicos deste estudo são identificar as aplicações práticas da IoT e analisar os desafios de segurança da IoT. Além disso, busca-se explorar o papel do Blockchain na segurança da IoT e investigar a integração da IoT com o Blockchain. Por fim, o estudo visa avaliar o impacto do Blockchain na imutabilidade dos dados.

Esses objetivos estão interligados e visam aprofundar a compreensão da relação entre a IoT e o Blockchain, bem como suas implicações para a segurança e a escalabilidade dos dados nas organizações.

3. DESENVOLVIMENTO

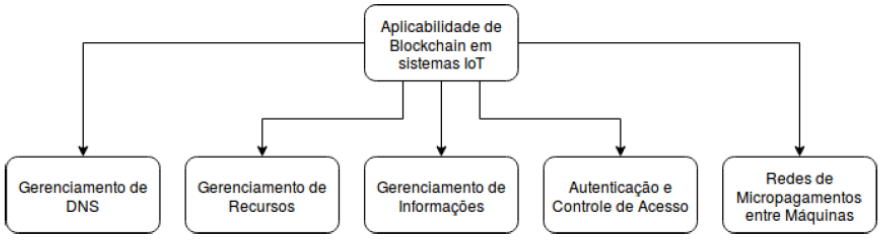
3.1. APLICAÇÃO PRÁTICA DA IOT

A Internet das Coisas (IoT) é vista como uma extensão da internet atual, permitindo que objetos do cotidiano com capacidade de comunicação e processamento se conectem à rede. Isso abre uma série de novas possibilidades para aplicações em vários setores. Por exemplo, na fabricação inteligente, essa tecnologia está sendo usada para conectar ativos e implementar manutenção preventiva e preditiva (Santos et al., 2016).

As redes de energia inteligentes estão utilizando a mesma para otimizar a distribuição e o uso de energia. As cidades inteligentes estão adotando essa abordagem para melhorar a eficiência dos serviços públicos e a qualidade de vida dos cidadãos. Além disso, a logística conectada e as cadeias de suprimentos digitais inteligentes estão aproveitando essa inovação para rastrear e otimizar o transporte de mercadorias. Essas são apenas algumas das muitas maneiras pelas quais a IoT está sendo aplicada atualmente e está transformando diferentes setores (Santos et al., 2016).

A IoT tem revolucionado o mundo corporativo, otimizando processos e melhorando a segurança através da coleta de dados. Empresas como Google e Apple estão desenvolvendo seus próprios ecossistemas com tecnologias distintas. Contudo, a falta de padronização pode ser um obstáculo. Assim, é essencial que academia e indústria trabalhem juntas para criar um ecossistema padronizado e próspero (FRACTTAL, 2020).

Figura 1 - Áreas de aplicabilidade de redes Blockchain em sistemas IoT.



Fonte: Machado (2018)

A Figura 1 de Machado (2018, pg.34) ilustra diversas aplicações da tecnologia Blockchain em sistemas IoT, exemplificando a versatilidade de sua adoção em diferentes contextos.

Um exemplo concreto dessa aplicação é a gestão de tráfego em grandes cidades, onde dispositivos móveis atuam como sensores, coletando e compartilhando dados de trânsito através de aplicativos como Waze ou Google Maps (FRACTTAL, 2020).

3.2. OS DESAFIOS DE SEGURANÇA DA IOT

Na gestão de dados na Internet das Coisas (IoT), Santos et al. (2016) destacam três pilares essenciais de segurança: confidencialidade, integridade e disponibilidade. A confidencialidade assegura que os dados transmitidos sejam acessíveis apenas aos participantes autorizados na comunicação.

A integridade, por outro lado, busca garantir que os dados não sejam alterados por entidades não autorizadas na rede. A disponibilidade tem como objetivo assegurar que o sistema esteja sempre acessível e protegido contra ataques maliciosos (Santos et al., 2016).

Contudo, a ausência de padronização pode resultar em um ecossistema que pode não se desenvolver adequadamente, tornando-se uma das principais preocupações na gestão da segurança dos dados na IoT. Assim, é fundamental que a comunidade acadêmica e empresarial se dedique às padronizações e à construção de um ecossistema propício para a IoT (Santos et al., 2016).

Ademais, é relevante ressaltar que os requisitos de segurança para a IoT variam conforme a aplicação e, portanto, devem considerar um ou mais dos objetivos de segurança mencionados anteriormente ao implementar uma aplicação (Santos et al., 2016).

Os desafios da segurança de dispositivos IoT são multifacetados, abrangendo problemas de baixo nível (hardware e camadas físicas), intermediário (comunicação, roteamento e gerenciamento de sessão) e alto nível (aplicações e middleware) (Sakamoto, 2020).

Além disso, desafios gerais como segurança e privacidade dos dados, falta de padrões comuns, questões técnicas, segurança ponta-a-ponta, gerenciamento de acesso e identidade, controle de acesso e compliance são igualmente importantes. Esses desafios levam aos quatro principais requisitos de segurança em IoT: autorização, autenticação, integridade e confidencialidade. Portanto, é crucial desenvolver e implementar medidas de segurança robustas para proteger esses dados e garantir a confidencialidade, integridade e disponibilidade das informações (Sakamoto, 2020).

A privacidade é outro aspecto crucial na IoT. Como os usuários do Bitcoin usam um pseudônimo (endereço) para realizar suas transações, isso pode levantar preocupações sobre a

possibilidade dessas transações revelarem informações além de uma simples identificação (Silva, 2021).

3.3. O PAPEL DO BLOCKCHAIN NA SEGURANÇA DA IOT

O artigo “Como o blockchain pode ajudar na segurança da IoT” do site Tecflow discute o potencial da tecnologia blockchain para melhorar a segurança na Internet das Coisas (IoT). Ele destaca que a adoção de blockchain e IoT pode gerar economias significativas, evitando fraudes relacionadas aos alimentos em toda a cadeia de abastecimento. A tecnologia blockchain, através do uso de criptografia elíptica, fornece uma plataforma imutável e compartilhada para rastrear e rastrear ativos, economizando tempo e recursos. Isso resulta em maior segurança não só no consumo de alimentos, mas também na perenidade e auditoria automática de processos e operações.

O blockchain pode desempenhar um papel significativo na melhoria da segurança da Internet das Coisas (IoT). Ele pode ser usado para autenticação e controle de acesso, proporcionar segurança e privacidade através de sua natureza descentralizada, e oferecer transparência para aumentar a confiança do usuário. Além disso, técnicas de anonimização de dados podem ser aplicadas para preservar a privacidade do usuário. No entanto, existem desafios a serem superados, como o conflito entre a natureza imutável do blockchain e as diretrizes de proteção de dados, bem como os requisitos de alto processamento e armazenamento do blockchain. Portanto, embora o blockchain tenha um grande potencial para melhorar a segurança da IoT, ainda há muito trabalho a ser feito nesta área (Sakamoto,2020).

Essa tecnologia pode melhorar a segurança da informação em sistemas IoT através de autenticação e controle de acesso, garantindo que apenas dispositivos autorizados possam acessar a rede. A integridade dos dados é assegurada através do uso de hashes, enquanto a transparência e rastreabilidade são proporcionadas pelo livro-razão público e distribuído. A natureza descentralizada do blockchain aumenta a robustez do sistema e dificulta ataques, enquanto o uso de chaves criptográficas permite o anonimato e a privacidade (Sakamoto,2020).

No entanto, existem desafios significativos na aplicação da tecnologia blockchain à IoT, incluindo o alto processamento e armazenamento exigidos pelo blockchain, bem como questões relacionadas à conformidade com as leis de proteção de dados. Portanto, embora o blockchain tenha um grande potencial para melhorar a segurança da IoT, ainda há muito trabalho a ser feito nesta área (Sakamoto,2020).

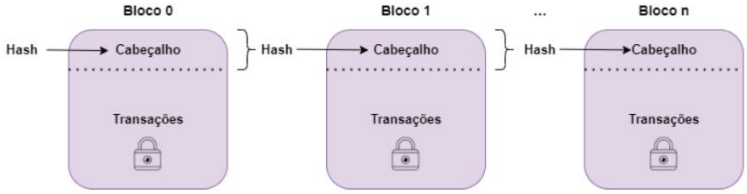
3.4. A INTEGRAÇÃO DA IOT COM O BLOCKCHAIN

A tecnologia Blockchain, conforme descrito por Lins e Morais (2021), é uma base de dados distribuída que registra transações em uma rede peer-to-peer (P2P). As operações, que podem variar de transferências financeiras a registros de dados, são agrupadas em estruturas denominadas blocos. Cada bloco contém um cabeçalho com dados de identificação e um conteúdo onde as transações são armazenadas. Além disso, cada bloco possui um código de identificação único, conhecido como hash, que permite o encadeamento dos blocos na Blockchain.

No contexto dessa tecnologia, a identificação dos usuários é feita por meio de um par de chaves criptográficas. A chave privada é usada para assinar as transações e a chave pública representa o usuário na rede. As transações são registradas em blocos que, após serem validados, são adicionados à cadeia. Este processo de validação é realizado por mineradores que resolvem problemas matemáticos complexos. O conjunto de blocos validados forma o livro-razão, onde todas as transações são registradas (Sakamoto, 2020).

Antes de serem adicionados à cadeia, os blocos passam por um processo de validação através de protocolos de consenso. Existem diferentes tipos de Blockchains, como públicas, privadas e consórcio, cada uma com suas próprias características e usos. A imutabilidade e transparência da Blockchain são garantidas pela natureza inalterável das informações uma vez adicionadas à cadeia (Sakamoto, 2020).

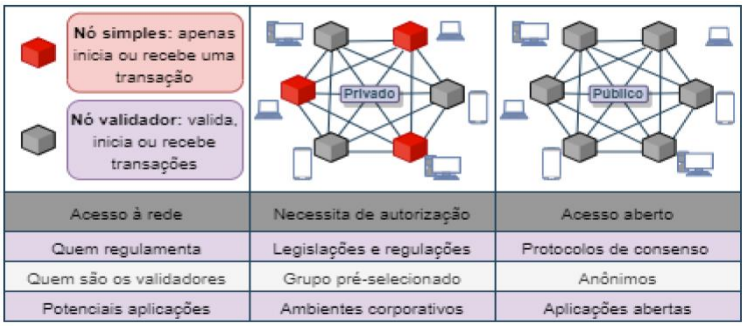
Figura 2 – Estrutura da *Blockchain*



Fonte: Lins e Morais (2021).

A Figura 2 (Lins e Morais, 2021) oferecem uma representação visual das estruturas dos blocos e seu encadeamento.

Figura 3 – *Blockchain* Privada x *Blockchain* Pública.



Fonte: Lins e Morais (2021).

A Figura 3 (Lins e Morais, 2021) ilustram a estrutura de funcionamento dos dois principais tipos de Blockchain, pública e privada.

3.5. O IMPACTO DO BLOCKCHAIN NA IMUTABILIDADE DOS DADOS

A tecnologia Blockchain exerce um impacto significativo na imutabilidade dos dados, uma vez que, após a adição de um bloco à cadeia, ele não pode ser alterado ou removido sem que isso seja percebido pelos demais nós em toda a rede. Isso é viabilizado pelo uso de hashes, códigos de identificação únicos para cada bloco, que permitem percorrer toda a cadeia até atingir o bloco inicial, conhecido como bloco gênesis (Lins e Morais, 2021).

Os protocolos de consenso, como o Proof-of-Work (PoW) ou o Proof-of-Stake (PoS), são fundamentais para a manutenção da imutabilidade dos dados na Blockchain. Eles garantem que todos os nós na rede concordem com o estado atual da Blockchain antes da adição de um novo bloco. Isso torna extremamente difícil para um ator mal-intencionado alterar os dados em um bloco, pois ele precisaria controlar a maioria dos nós na rede para fazer isso, o que é praticamente impossível em redes grandes e descentralizadas (Lins e Morais, 2021).

A imutabilidade dos dados é uma das principais vantagens da tecnologia Blockchain, tornando-a ideal para aplicações onde a integridade dos dados é de extrema importância, como em sistemas financeiros, registros médicos, cadeias de suprimentos e, claro, na Internet das Coisas (IoT). A imutabilidade dos dados na Blockchain pode ajudar a garantir que os dados gerados pelos dispositivos IoT sejam autênticos, confiáveis e não possam ser alterados após serem registrados.

Isso pode melhorar significativamente a segurança e a confiabilidade dos sistemas IoT (Lins e Morais, 2021).

A interseção entre a tecnologia Blockchain, a Internet das Coisas (IoT) e a Lei Geral de Proteção de Dados Pessoais (LGPD) apresenta tanto oportunidades quanto desafios. A Blockchain, sendo uma estrutura de rede ponto a ponto (P2P) e um livro-razão de registros imutáveis, pode resolver questões relacionadas às características intrínsecas da IoT. No entanto, também surgem desafios, principalmente em relação à compatibilidade da tecnologia com aspectos específicos da LGPD, como a exclusão de dados e o papel do controlador de dados (Sakamoto, 2020).

Isso sugere que a imutabilidade inerente à Blockchain, uma vez que uma informação seja adicionada à cadeia de blocos, ela não pode ser modificada ou alterada. Isso pode entrar em conflito com a LGPD no que diz respeito à exclusão de dados (Sakamoto, 2020).

Além disso, o conceito de “envenenamento por privacidade” ou “blockchain privacy poisoning”, que ocorre quando informações pessoais são inseridas na cadeia de blocos, também pode gerar conflitos com a LGPD (Sakamoto, 2020).

Por fim, a LGPD atribui responsabilidades aos controladores de dados. No entanto, em uma rede blockchain pública, devido à descentralização, esse papel não existe (Sakamoto, 2020).

4. METODOLOGIA

A metodologia desta pesquisa envolveu uma revisão bibliográfica abrangente e análise de conteúdos corporativos sobre a integração da tecnologia blockchain e a Internet das Coisas (IoT). As principais fontes de literatura foram artigos de empresas que discutem a utilização de dispositivos IoT, e diversos artigos científicos e trabalhos acadêmicos relevantes (Cernev & Moraes, 2021; Lins & Morais, 2021; Messias & Santos, 2020; Sakamoto, 2020; Silva, 2021; Santos et al., 2016).

Para facilitar a pesquisa, foram utilizadas ferramentas como o Research Rabbit e o Mendeley Cite. O Research Rabbit auxiliou na busca e seleção de artigos relevantes, enquanto o Mendeley Cite foi utilizado para gerenciar as referências bibliográficas e garantir a correta citação dos trabalhos consultados.

Os critérios de inclusão para os artigos foram: (1) artigos que discutem a integração da tecnologia blockchain; (2) artigos publicados em revistas científicas revisadas por pares. Para análises corporativas, foram incluídas aquelas que discutem a utilização de dispositivos IoT em suas empresas. Os critérios de exclusão foram: (1) artigos que não são diretamente relevantes para o tópico de pesquisa; e (2) artigos que não estão disponíveis em texto completo.

Os artigos selecionados foram lidos e analisados em profundidade. As informações relevantes foram extraídas e sintetizadas para atender aos objetivos da pesquisa. Durante a análise, foi dada especial atenção aos benefícios e desafios da integração da tecnologia blockchain com a IoT, bem como às possíveis soluções para esses desafios.

5. RESULTADOS E DISCUSSÕES

Este estudo apresenta contribuições significativas para a aplicação da tecnologia blockchain na Internet das Coisas (IoT). De acordo com Oliveira (2022), a implementação de tecnologias blockchain na “Energy Cloud” pode melhorar a gestão de energia em sistemas interconectados, onde dispositivos IoT desempenham papéis cruciais.

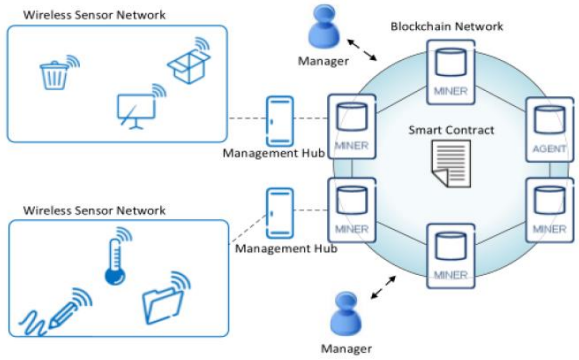
Oliveira (2022) também realizou uma análise detalhada das aplicações e serviços em que as tecnologias blockchain podem ser utilizadas no contexto de IoT e sistemas de energia. Isso inclui a análise de políticas de rede, aplicações centradas no usuário final e o potencial para inovação em áreas como comércio de energia, resposta à demanda e gerenciamento de dispositivos inteligentes.

Contudo, a aplicação da tecnologia blockchain à IoT pode enfrentar desafios devido à sua natureza descentralizada e à necessidade de consenso entre os nós da rede, o que pode resultar em

tempos de confirmação mais longos em comparação com sistemas centralizados (Machado, 2018).

A abordagem descrita por Machado (2018) propõe uma arquitetura onde dispositivos IoT, devido à sua limitação de poder computacional, interagem com uma rede Blockchain através de hubs de gerenciamento. Esses hubs atuam como intermediários, transferindo informações entre os dispositivos e a Blockchain. O controle de acesso às informações é centralizado em um Smart Contract específico na rede Blockchain. Os usuários podem alterar ou consultar informações dos dispositivos que possuem, realizando transações quando necessário. A manutenção de uma criptomoeda na rede incentiva os nós validadores a continuarem verificando as transações.

Figura 4 - Modelo de arquitetura de redes de sensores sem fio.



Fonte: Modelo proposto por Oscar Novo (apud MACHADO, 2018)

A figura 4 ilustra essa arquitetura, mostrando o fluxo de informações entre redes de sensores sem fio, hubs de gerenciamento, managers e a rede Blockchain.

Para superar obstáculos como esses, estão sendo desenvolvidas soluções como redes blockchain otimizadas para transações de IoT. Um exemplo é o Tangle da IOTA, projetado para lidar com um grande volume de microtransações de maneira mais eficiente e rápida (Machado, 2018). Outras estratégias incluem a implementação de algoritmos de consenso mais eficientes e o uso de canais de pagamento off-chain para acelerar as transações (Sousa, 2023).

Silva (2023) avaliou o desempenho da rede Ethereum em termos de latência, vazão e consumo de recursos computacionais quando modificada para funcionar com dispositivos IoT. Os testes revelaram desafios significativos relacionados ao alto custo computacional e energético inerente ao protocolo de consenso Ethash (proof-of-work), que é inviável para dispositivos com recursos limitados como o Raspberry Pi.

Para realizar benchmarks sistemáticos em redes Ethereum privadas, Silva (2023) empregou uma versão modificada do Blockbench. Isso incluiu a integração de um Raspberry Pi como nó participante, avaliando seu desempenho na rede.

A dissertação de Silva (2023) compara a eficácia dos protocolos de consenso Ethash (proof-of-work) e Clique (proof-of-authority). Os resultados indicam que o protocolo Clique

proporciona melhor desempenho em termos de latência, vazão e consumo de recursos, sendo mais adequado para redes IoT.

Foi constatado que o Raspberry Pi não pode funcionar como minerador em uma rede que utiliza Ethash devido à intensidade computacional requerida. No entanto, ele pode operar como um nó leve, indicando que ajustes na blockchain são necessários para acomodar dispositivos com capacidades computacionais limitadas.

Val (2024) discute a importância da segurança da informação na integração das tecnologias Blockchain e IoT. Ele enfatiza a gestão da segurança da informação como essencial para a proteção dos investimentos e a mitigação dos riscos de segurança. Val (2024) também destaca várias funções de segurança essenciais proporcionadas pelo Ethereum, que são particularmente benéficas para usuários e desenvolvedores.

O documento de Silva (2023) fornece dados concretos sobre a performance da blockchain em diferentes configurações, destacando as potenciais melhorias na integração entre Ethereum e IoT. Esta pesquisa contribui para um entendimento mais profundo de como a blockchain pode ser ajustada para melhor servir aplicações IoT em termos de eficiência e custo-benefício.

Esses pontos sublinham a importância da seleção de um protocolo de consenso adequado e das modificações necessárias na tecnologia blockchain para garantir sua viabilidade em ambientes IoT com dispositivos de recursos limitados. Os resultados desses estudos enfatizam a necessidade de inovações que possam reduzir o consumo de energia e aumentar a eficiência dos sistemas de blockchain para torná-los mais adequados para IoT, especialmente em aplicações de IoT.

Figura 5 - Análise comparativa entre sistemas centralizados e aplicações Blockchain.

ANÁLISE COMPARATIVA ENTRE PLATAFORMAS CENTRALIZADAS E BLOCKCHAIN		
ASPECTOS	**PLATAFORMA CENTRALIZADA TRADICIONAL**	**PLATAFORMA DISTRIBUÍDA Blockchain**
Manipulação de dados	Suporte para as quatro operações: **Criar, Ler, Atualizar e Excluir**.	Disponível nas operações de **Leitura e Gravação.**
Autoridade	**Centralizada**: controlada por uma entidade administradora.	**Descentralizada**.
Integridade	Permitem **alteração e exclusão**.	**Dados imutáveis.**
Privacidade	**Maior vulnerabilidade de ataques** mal-intencionados.	Dados criptografados que possibilitam **mais proteção**.
Transparência	**Possibilidade de dados não transparentes.**	Por estarem em uma rede distribuída, **permitem maior transparência.**
Garantia de Qualidade	Necessidade de **autenticação por uma entidade administradora.**	Dados rastreáveis desde sua origem **garantem imutabilidade protegidos** por criptografias com Hash de dados.
Tolerância a falhas	**Alto risco** de pena em ponto único.	**Tolerância a falhas** em sua arquitetura de projeto.
Custos	**Fácil de implementar e manter.**	Por não ser de grande domínio, **maior custo de desenvolvimento e manutenção.**
Desempenho	**Maior rapidez em transações** processadas e maior escalabilidade.	**Menor desempenho** pela menor quantidade de aplicações desenvolvidas, possibilidade de melhoria ao longo de novos projetos.
Força de trabalho	**Elevado número de Profissionais** em diversas plataformas de sistemas tradicionais centralizados.	**Escassez de mão de obra qualificada** para desenvolvimento e suporte a aplicações Blockchain.
Escalabilidade	**De fácil atualização**, permite adoção da escalabilidade sem grandes modificações, como tamanho dos registros e aumento no número de transações.	**Um desafio à Blockchain** visto que por sua natureza de registros fixos imutáveis e maior tempo de processamento nas transações.
Legislação	Regulamentado pelo RGPD.	Controvérsias quanto à aplicação do **RGPD**.

Autor: Val (2024)

Essa abordagem é reforçada pela análise comparativa entre plataformas centralizadas tradicionais e plataformas distribuídas blockchain, como mostrado na figura 4 do estudo de Val (2024), que se destaca como uma contribuição visual significativa para este texto. A imagem destaca a segurança reforçada, a transparência aumentada e a melhor garantia de qualidade fornecida pela blockchain, todos fundamentais para a implementação efetiva de soluções IoT. A comparação clara entre os dois modelos de plataforma ressalta os benefícios da blockchain, como dados imutáveis e a capacidade de tolerar falhas sem comprometer o desempenho do sistema, uma preocupação central no contexto da IoT.

6. CONCLUSÃO

A integração entre a tecnologia blockchain e a Internet das Coisas (IoT) possui o potencial de transformar significativamente a segurança cibernética. Este estudo demonstrou que o blockchain pode oferecer uma robusta camada de segurança aos dispositivos IoT, garantindo a integridade e autenticidade dos dados. Além disso, a descentralização inerente ao blockchain proporciona uma maior resiliência contra ataques cibernéticos, permitindo um controle mais efetivo sobre os dados pelos usuários finais.

No entanto, apesar dos benefícios claros, a implementação prática dessas tecnologias enfrenta desafios consideráveis, incluindo a complexidade técnica e os custos associados à implementação de sistemas blockchain em ambientes IoT. Além disso, a conformidade com regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD) requer uma abordagem cuidadosa, dado o conflito potencial entre a imutabilidade do blockchain e a necessidade de exclusão de dados.

Para empresas que buscam explorar essas tecnologias, é crucial uma abordagem estratégica e bem planejada, que considere não apenas os benefícios de segurança, mas também a viabilidade econômica e técnica da integração. Além disso, a colaboração contínua com especialistas em blockchain e IoT e a realização de testes rigorosos são essenciais para adaptar-se às rápidas mudanças tecnológicas e regulatórias.

Concluindo, enquanto a combinação de IoT e blockchain oferece promessas significativas para a melhoria da segurança cibernética, os stakeholders devem navegar cuidadosamente pelos desafios técnicos e regulatórios para capitalizar plenamente as vantagens dessas tecnologias disruptivas.

7. REFERÊNCIAS

CERNEV, A. K.; MORAES, T. K. L. No rastro do blockchain. GV-EXECUTIVO, v. 20, n. 1, p. 18-21, 2021.

FRACTTAL. As 9 aplicações mais importantes da Internet das Coisas (IoT). Fracttal Blog. Disponível em: https://www.fracttal.com/pt-br/blog/as-9-aplicacoes-mais-importantes-da-internet-das-coisas-iot. Acesso em: 21 out. 2023.

LINS, V. C.; DE MORAIS, A. M. Simulação e avaliação de desempenho de uma Blockchain para aplicações IoT. GESTÃO. Org, v. 19, n. 2, p. 169-183, 2021.

MACHADO, R. N. Análise sobre otimização de Blockchain para Internet das Coisas. 2018.
MESSIAS, F. A.; SANTOS, L. M. F. Os benefícios da combinação de blockchain e Iot em termos de segurança, confiança e validação de dados. 2020.

OLIVEIRA, Henrique Luís Sauer et al. O impacto de tecnologias blockchain na energy cloud. 2022.

SAKAMOTO, S. G. Segurança, Privacidade e Blockchain no Contexto de Internet das Coisas. Monografia de Especialização em Internet das Coisas, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

SANTOS, B. P. et al. Internet das coisas: da teoria à prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 31, 16, 2016.

SILVA, Maykon Valério da et al. Avaliação de Desempenho e Custo Computacional na Utilização da Blockchain Ethereum em Dispositivos de Internet das Coisas. 2023.

SOUSA, F. E. et al. Sistema de verificação de integridade de dados baseado em oráculo de blockchain para internet das coisas (IoT). 2023.

TECFLOW. Como o blockchain pode ajudar na segurança da IoT. Disponível em: https://tecflow.com.br/2021/07/06/como-o-blockchain-pode-ajudar-na-seguranca-da-iot/. Acesso em: 22 out. 2023.

VAL, Ronaldo Borges do. Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT. 2024.