UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES
CAMPUS PATOS DE MINAS

LUANA CAIXETA DUARTE

BLOCKCHAIN E O IOT:
Uma revisão bibliográfica sob a perspectiva de aplicações em segurança.

PATOS DE MINAS - MG
2025

LUANA CAIXETA DUARTE

BLOCKCHAIN E O IOT:
Uma revisão bibliográfica sob a perspectiva de aplicações em segurança.

Monografia apresentada à banca examinadora como parte das exigências para a aprovação na disciplina de Projeto Final de Curso 2 da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Orientador: Prof. Dr. Daniel Costa Ramos.

PATOS DE MINAS - MG

2025

LUANA CAIXETA DUARTE

BLOCKCHAIN E O IOT:
Uma revisão bibliográfica sob a perspectiva de aplicações em segurança.

Monografia apresentada à Universidade Federal de Uberlândia como requisito para conclusão do Projeto Final de Curso 2 de graduação em Engenharia Eletrônica e de Telecomunicações da Faculdade de Engenharia Elétrica.

Patos de Minas, 7 de maio de 2025.

Banca Examinadora

_____

Prof. Dr. Daniel Costa Ramos – FEELT/UFU (Orientador)

_____

Prof. Dr. André Antônio dos Anjos - FEELT/UFU (Membro 1)

_____

Prof. Dr. Renan Alves dos Santos – FEELT/UFU (Membro 2)

Dedico aos que sempre estiveram ao meu lado, em especial aos meus pais.

AGRADECIMENTOS

Agradeço a minha família, minha mãe Eunice, meu pai José Roberto, minha irmã Luma e meu irmão Leonardo por todo o apoio, paciência e principalmente incentivo em minha longa jornada.

Agradeço ao meu orientador, que com seus conselhos e suas piadas, soube deixar todo o caminho até este final leve, sempre ao meu lado com o suporte necessário, obrigada *Dr. Daniel Costa Ramos* por nunca desistir de mim, muito obrigada.

Agradeço à Universidade Federal de Uberlândia, Campus Patos de Minas, e a todos os docentes de quem fui aluna e onde tive a oportunidade de absorver o máximo que esteve ao meu alcance. Aos professores, *Dr. Renan Alves dos Santos*, *Dr. Davi Sabbag Roveri*, *Dra. Elise Saraiva*, *Dra. Karine Barbosa Carbonaro, Dr. André Antônio dos Anjos* e *Dr. Pedro Luiz Lima Bertarini,* o meu mais sincero e profundo agradecimento em especial por estarem muito presente e pela paciência, compreensão, muito também pela qualidade do ensino oferecido, disposição e competência.

Agradeço a todos que fizeram, de alguma forma, parte desta jornada, aos amigos *Kaoann Martins Carvalho, Caio Andrade Castro Cruz* e aos que não citei, mas que são muito importantes para este momento.

RESUMO

Sem dúvida a Internet das Coisas (IoT) tem mudado, e pode mudar, vários aspectos em nossas vidas. Seja na indústria, nas cidades, no campo e até mesmo nos lares, onde o conjunto dos objetos ou "coisas" conectadas à internet, identificadas de forma única e que trabalhem em cooperação, com um certo grau de inteligência. A IoT desde que foi criada até a plena maturidade, vem se estabelecendo como parte da futura Internet. Um dos desafios técnicos de ter milhares de dispositivos implantados em todo o mundo é a capacidade de gerenciá-los. Pensado por este motivo que o estudo sobre as falhas, principalmente em termos de segurança e privacidade, surge como pré-requisito. Este trabalho tem como seu principal objetivo levantar uma análise teórica e revisional, cujo enfoque se faz na junção das tecnologias do IoT e do *Blockchain*, onde é feito a crítica do atual cenário, propostas de arquiteturas que foram desenvolvidas sobre o tema e soluções. Visto que os recursos do *Blockchain* vão ao encontro dos problemas enfrentados pelo IoT nos quesitos já citados. Para isso foi utilizada a Teoria de Enfoque Meta Analítico Consolidado, que visa aproveitar de forma qualitativa das grandes bases de dados, tais quais o Google Scholar, IEEE, entre outros.

Sendo assim, uma coletânea de diversos trabalhos relacionados à IoT baseada em *Blockchain*, e este trabalho visa fornecer em detalhes trabalhos sobre IoT baseada em *Blockchain* ou BIoT. Buscou-se destacar a necessidade de garantir a segurança de um sistema IoT e apresentar uma comparação entre o *Blockchain* e outras técnicas de segurança em termos de robustez, custo de configuração, risco de falha, etc., além de propor uma técnica de segurança ideal que possa ser adotada para aplicações IoT.

Palavras-chave: Blockchain; Internet das Coisas; BIoT; Cyber segurança; Segurança de Redes IoT.

ABSTRACT

Undoubtedly, the Internet of Things (IoT) has several aspects, and can change, our lives. Whether in industry, in cities, in farms and even at our homes, where the set of objects or “things” connected to the internet, identified in a way, and working in accordance, with an intelligence. IoT has been establishing itself as part of the future Internet. One of the technical challenges of having thousands of devices installed worldwide is manageability. For this reason, the study of failures, especially in terms of security and privacy, appears as a prerequisite. This work is to raise an analysis, whose focus is reviewing works, as its theoretical objective, proposed for the IoT, and the criticism of the current scenario of the proposed architectures and solutions. Since Blockchain resources meet the problems already mentioned by IoT. For this, the Consolidated Meta-Analytical Focus Theory was used, which aims at qualitatively data from large databases, such as Google Scholar, IEEE, among others. Therefore, a collection of several works related to Blockchain-based IoT, and this work aims to provide in detail works on Blockchain-based IoT or BIoT. The aim was to highlight the need to ensure the security of an IoT system and present a comparison between Blockchain and other security techniques in terms of robustness, configuration cost, risk of failure, etc., in addition to proposing an ideal security technique that can be adopted for IoT applications.

Keywords: Blockchain; Internet of Things; BIoT; Cyber Security; IoT Network Security;

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

6LoWPAN	*Low-Power Wireless Personal Area Networks Working Group*
ABAC	*Attribute Based Access Control*
BC	*Blockchain*
BIoT	*Blockchain-based IoT*
BLE	*Bluetooth Low Energy*
BFT	*Byzantine Fault Tolerance*
CAGR	Taxa de Crescimento Anual Composta
CID	Confidencialidade, Integridade e Disponibilidade
CoAP	Protocolo de Aplicação Restrita
CRUD	*Create, Read, Update and Delete*
CTIF-IoT	*Collaborative Threat Intelligence Framework for IoT Security*
DDOS	*Distributed Denial Of Service*
DDS	Serviço de Distribuição de Dados
DNS	*Domain Name Server*
IoBT	*Internet of Battlefield Things*
IIoT	*Industrial Internet of Things*
IoMT	*Internet of Medical Things*
IoO	*Internet of Objects*
IoT	*Internet of Things*
IoV	*Internet of Vehicles*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
IEEE	*The Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
Ledger	Livro Razão
LoRa	*Long Range*
LGPD	Lei Geral de Proteção de Dados
LTE	*Long Term Evolution*
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
M2M	*Machine-to-Machine*
NFC	*Near Field Communication*

Nonce	*N = Número e Once = uma vez*
TEMAC	Teoria do Enfoque Meta Analítico Consolidado
P2P	*Peer-to-Peer*
REST	*Representational State Transfer*
RFID	*Radio Frequency Identification*
RPL	IPv6 *Routing Protocol for Low Power and Lossy Networks*
RSSF	Rede de Sensores Sem Fio
SHA	*Secure Hash Algorithm*
TCP	Protocolo de Controle de Transmissão
UDP	*User Datagram Protocol*
WSNs	*Wireless Sensor Networks*

SUMÁRIO

1 INTRODUÇÃO

O tema fundamental deste trabalho é o uso do *Blockchain* – (BC) em aplicações *Internet of Things* (IoT), especificamente em relação à segurança de redes dentro desse universo, tratando diretamente sobre segurança da informação e criptografia. Quão importante seria a sua utilização e quais os trabalhos já existentes em uma análise comparativa, de acordo com a metodologia escolhida.

A premissa do IoT está permeada em procurar satisfazer a ideia de que seria possível ter a conexão de inúmeros tipos de dispositivos à Internet. Assim cada, *"coisa"* (*Thing*), tem o seu motivo diferente dentro da rede. Alguns podem, por exemplo: serem sensores de temperatura, umidade, e várias outras grandezas físicas. Estes, porém, não se limitam a sensores, e são aplicados em TVs, casas, iluminação pública, carros e outros.

Assim como irá ser tratado em capítulos a frente, viu-se despontar uma gama significativa de conceitos do que é, onde atua, bem como definições para as ramificações, tais quais: *Smart Home, Smart Cities, Smart Warehouse* e muitos mais, assim sendo, vários mecanismos para os usuários com automação e obtenção e/ou distribuição de informações.

A conexão dos dispositivos é feita por exemplo de forma física com uso de cabos de rede ou fibra ótica, e por Wi-Fi, LTE (*Long Term Evolution*), 4G, 5G, Bluetooth, RFID (*Radio Frequency Identification*), etc. Uma vez conectados à Internet, sabe-se que estes dispositivos possuem mutabilidade no que diz respeito ao programa que o rege, assim fica possível coletar informações sobre uma "coisa" por meio do seu identificador único e então realizar alterações no seu estado a partir de qualquer lugar, a qualquer hora, por um outro dispositivo qualquer.

Parte dos dados de comunicação podem se perder durante a transmissão ou sofrer interceptação indesejada de terceiros. Essa vulnerabilidade sugere novos estudos, novas formas de visualizar este problema e procurar soluções que visem considerar as pautas citadas, propondo uma solução com robustez capaz de sanar de forma eficaz as mesmas.

O BC possui sua história atrelada ao do Bitcoin, onde fora idealizado um sistema que funcionava com blocos encadeados totalmente criptografados e seguros, com capacidade de tornar possível a criação de algo imutável e único, uma moeda. É praticamente impossível mexer com os dados dentro do bloco sem mudar os *checksums* ou *hash* (será mais elucidado no capítulo 4) e quebrar a corrente.

A tecnologia envolta ao BC e responsável por todo esse sucesso em termos de critérios de fidelidade "semi incorruptível", ou de difícil quebra, está sendo apontada como algo que

pode revolucionar o uso da internet como é percebido hoje e deve mudar o nosso modo de viver, trabalhar e negociar. Alguns entusiastas comparam o seu surgimento como quando: *"...um dia alguém disse que daria para transferir arquivos por uma grande rede mundial onde o mundo estaria absolutamente absorvido..."*, como mostra (ARATA; NASCIMENTO; DE NOVAIS, 2020).

Dentro do tema aqui tratado, pode-se dizer que "*usando o IoT com Blockchain melhora-se a conectividade da rede e dará mais facilidade de comunicação entre os usuários de forma direta, de um para outro (P2P – peer-to-peer), sem uma terceira parte*", tradução livre de (URIEN, 2018). Promovendo principalmente a descentralização com técnicas de segurança e privacidade para evitar *cyber-ataques*.

1.1 MOTIVAÇÃO

Com seu uso difundido por possuir extrema utilidade, o IoT traz problemas relacionados à segurança e privacidade de seus usuários, dito isso e sabendo o amplo compartilhamento de informações trocadas, seja pessoal ou algo importante para uma tomada de decisões pelos dispositivos na rede, tornou-se pertinente a busca por cessar os golpes sofridos neste âmbito quando foi dito desta referência. (SAKAMOTO, 2020; MOREIRA, 2019).

As características inerentes do IoT, prevê que este venha a ter uma heterogeneidade de dispositivos, restrições em termos computacionais e de energia, uma ausência de centralização, a maioria projetado em uma escala grande, e assim, uma maior superfície de ataques, tornando complicado e desafiador a segurança nestas redes.

Conforme dito por (SAKAMOTO, 2021), em 2016, houve relatos de ataques massivos de serviço contra diversas instituições a partir de uma *Botnet* chamada Mirai, foi estimado que sua estrutura contia 233 mil dispositivos IoT e com isso as perdas foram de milhares de dólares com problemas em disponibilidade de serviços e outros.

Além disso, acaba-se tendo também outro desafio com relação a tecnologia. Como, os limites relacionados à protocolos de comunicação sem fio, escalabilidade, consumo de energia e natureza distribuída da rede. E com relação à segurança ainda se tem que verificar a garantia da autenticação dos dispositivos, a confidencialidade quando estão em comunicação e a integridade das informações que são trocadas e muito mais.

Com isso, o BC acabou se tornando uma tecnologia atrativa e poderia resolver problemas de confiança e segurança de plataformas IoT. Em (FUKUDA, 2019; MOREIRA, 2019), pode-se ver que o uso do mesmo para este tipo de plataforma poderia ser útil para troca e compartilhamento de dados. Funções como registro, validação e serviço de segurança, e

para isso muitas pesquisas devem ser feitas no setor com tema de *cyber-segurança* utilizando o BC em ambientes físicos do IoT.

O BC possui estudos enaltecendo a *"sua capacidade de interromper extensivamente processos de negócios estabelecidos e gerar confiança e integridade, oferecendo ao mesmo tempo desintermediação e imutabilidade*" (CROSBY; PATTANAYAK; VERMA, 2016). Um paradigma que vem sendo discutido veementemente é justamente a aplicabilidade do BC em situações em que se voltem para o mundo além dá parte financeira, onde este já se encontra mais bem estabelecido. (ASARE; QUIST–APHETSI; NANA, 2019; DA MATA; RODRIGUES,2019; SAKAMOTO, 2020)

Como pode ser encontrado no artigo da Forbes (PACETE, 2022) até 2025, o número será de mais de 27 bilhões de dispositivos conectados. Ressalta-se que há previsões do aumento de comunicações entre máquinas, sem depender de um humano, de 780 milhões em 2016 para 3.3 bilhões até o ano, 2021, como cita (URIEN, 2018).

Um dos problemas mais comuns de segurança no IoT é o "*Distributed Denid Of Service (DDoS) que torna os usuários incapazes de acessar o servidor porque o invasor executou um grande número de solicitações ao servidor*" (AL-MADANI; GAIKWAD, 2020), traduzido livremente, e pensando nisso, as considerações levam ao fato de que o BC fornece um modelo descentralizado que torna a rede flexível, segura, e confiável capaz de oferecer suporte a serviços em tempo real (CROSBY; PATTANAYAK; VERMA, 2016; QUIST–APHETSI; FUKUDA, 2019; MOREIRA, 2019; SAKAMOTO, 2020).

Características intrínsecas desta rede já discutidas, como por exemplo a heterogeneidade de dispositivos, ausência de centralização, entre outros, permitem levar em consideração os estudos que serão apresentados como parte da solução (SAKAMOTO, 2020; FUKUDA 2019). Logo, é plausível analisar que as propostas fornecidas no protocolo de redes BC e encarar que este apresenta um grande potencial de usabilidade na indústria de IoT, "*haja vista a necessidade de comunicação entre nós descentralizados de maneira segura e a manutenção da privacidade desta comunicação*" (SAKAMOTO, 2020).

Por que estudar o uso combinado das duas plataformas e assim uma ser capaz de solucionar os problemas com segurança de redes da outra? É possível utilizar mesmo? Como será esta utilização? Quais estudos já foram realizados na tentativa de aplicações e se é possível repetir na prática? Este trabalho se propõe verificar estas questões, dentre outras que porventura venham a surgir no decorrer ou quem sabe em outros futuros. Deve-se atentar aos objetivos e problemas aqui levantados, o que de fato busca-se com o estudo desta tecnologia e sua aplicação no conceito de redes IoT.

1.2 OBJETIVOS

Nesta seção são apresentados o objetivo geral e os específicos do trabalho, relativos ao problema anteriormente apresentado.

1.2.1 **Objetivo Geral**

O objetivo principal deste trabalho é investigar, por meio de revisão bibliográfica, pesquisa e análise sistemática da literatura, os benefícios da implementação e aplicabilidade do BC, com o intuito de compreender como essa tecnologia pode contribuir para o aumento da segurança em redes IoT.

1.2.2 **Objetivos Específicos**

Foi feita uma análise dentro da literatura levantada de algumas soluções já apresentadas em outros estudos prévios, em que a busca é mostrar as diversas formas de usabilidade da tecnologia dentro do universo IoT. Podendo então serem descritos os objetivos específicos como:

- Fazer o levantamento de quais os pontos fracos de segurança do IoT e justificáveis do uso de redes BC para solucionar;
- Analisar as propostas de soluções de otimização de redes BC para solucionar os desafios de IoT;
- Verificar as falhas da tecnologia de BC nas bibliografias;
- Montar tabelas com propostas mais citadas entre os autores, verificando qual seria uma solução mais adequada e a qual tipo de aplicação está sujeita;
- Fazer um estudo sobre os temas correlacionados aos assuntos gerais de forma a entender desde o surgimento ao porquê de uma aplicação em áreas diversas, buscando exemplos de outras aplicações já em prática.

1.3 JUSTIFICATIVAS

O BC possui estudos descrevendo sua tecnologia como capaz de *"rastrear, coordenar, realizar transações e armazenar informações de uma grande quantidade de dispositivos, possibilitando a criação de aplicativos que não requerem nuvem centralizada."* (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018).

O autor (AL-MADANI; GAIKWAD, 2020) propõe em seu estudo uma rede para segurança de dados baseada em *service name* ao invés de usar o endereçamento. Portanto, os dados precisam de um refinamento quando se trata de técnicas de segurança. O BC oferece este modelo, que possa tornar a rede flexível, segura e confiável capaz de oferecer suporte a serviços em tempo real, conforme foi levantando em seus trabalhos em (GIANNOUTAKIS; SPATHOULAS; FILELIS-PAPADOPOULOS; COLLEN; ANAGNOSTOPOULOS; VOTIS; NIJDAM, 2020; SINGH; SANWAR HOSEN; YOON, 2021; AL-MADANI; GAIKWAD, 2020).

Assim como ressalta (SINGH; SANWAR HOSEN; YOON, 2021) a tecnologia do BC pode ser uma das mais atraentes para próxima geração, pois se encaixou muito bem a era da informação, sendo extremamente aplicável ao IoT; este autor por exemplo, discute os principais fatores que fornecem como seria os ataques de segurança e as soluções que podem ser apresentadas e as já existentes que estão sendo propostas para implementação como contramedida.

É importante salientar, que como em (DEDEOGLU, 2019), nas redes IoT os nós não necessariamente confiam uns nos outros e para estabelecer uma confiança, *hash* criptográficos e mecanismos de consenso distribuídos podem auxiliar. Assim o Iot em conjunto com o BC pode possibilitar uma arquitetura em camadas para melhorar a confiança de ponta a ponta podendo ser aplicada a uma gama diversificada de aplicativos IoT.

Conforme o texto apresentado em sua monografia (SAKAMOTO, 2020) elenca que justamente o fato de que o IoT transformou a indústria das telecomunicações, agregando novos conceitos e tecnologias a preceitos já existentes. O conjunto de “coisas” conectados à internet, com certa capacidade de raciocínio, traz desafios quanto a implementação e provimento de recursos de infraestrutura. No âmbito da segurança, privacidade e domínio do recurso mais robusto neste quesito, surgem desafios a serem superados. Como proposta do trabalho a autora propôs o BC como alternativa para completar estes itens levantados.

No caso do tema trazido por (MOREIRA, 2019), observa-se uma análise propondo uma otimização do BC para o IoT, principalmente levantando a usabilidade e o grande potencial na indústria, haja visto a necessidade de comunicação entre nós de maneira descentralizada e segura; mantendo em suma a privacidade durante esta. O autor faz o levantamento de como a atual situação se encontra, trazendo questões como: os benefícios da implantação do BC, as definições dos sistemas das duas tecnologias citadas, a otimização como um todo que as redes BC poderiam trazer ao IoT e o futro para as aplicações.

O autor (MACHADO, 2018) traz o desenvolvimento de bloco dentro da plataforma Ethereum, visto que este tipo de plataforma possibilita criações de Contratos Inteligentes e não somente moedas, o que poderia ser aplicável caso, este trabalho se propusesse a realização de testes em rede e a criação de bloco para teste e para trabalhos futuros. O texto do autor, também é valido, pois, descreve toda a história e relata o que á tecnologia do BC.

Baseando nos casos dos artigos citados e muitos outros levantados assim como nas monografias (MACHADO, 2018; MOREIRA, 2019; SAKAMOTO, 2020), em que foi possível verificar a aplicabilidade no contexto. Este trabalho então propõe o estudo sobre as duas tecnologias chaves, esmiuçando o conceito por trás de cada uma, e como visto nos autores, também buscará detalhar os estudos com o cenário do possível futuro para as aplicações BIoT (*Blockchain-based IoT*) e as oportunidades de pesquisas relacionadas através da implementação.

1.4 CONSIDERAÇÕES FINAIS

Todo o interesse pelo assunto surgiu de um documentário sobre o que é utopia ou não dentro da tecnologia do BC, visto em (CRYPTOPIA, 2020), em conjunto com o conhecimento dos problemas do IoT as perguntas surgiram naturalmente e a busca começava de forma natural.

O assunto é de fato instigante e muitas vezes considera-se usar literalmente o termo *Cryptopia*. Em termos gerais estaria-se vivendo uma utopia-diatópica onde tem-se os dois lados, onde se por vezes serão capazes de usar esta tecnologia descentralizada como uma nova camada de protocolos para a internet na qual poderá criar uma nova internet; destronar as gigantes de tecnologias, como Facebook, Google, Amazon; recuperar a liberdade de expressão; nos dar identidades invioláveis; facilitar o comercio livre em uma economia digital sem fronteiras; reconstruir a confiança na sociedade e talvez salvar o planeta; o outro lado não muito favorável é que facilitaram-se também as atividades criminais com o uso de algo de difícil rastreio. Serão os usuários que deverão escolher a melhor forma e como adaptar-se a ela. Logo, foi avaliado que o BIoT é um tema a ser explorado e pode trazer novas conquistas para todos de uma maneira geral, sendo de grande importância seu estudo.

Para chegar neste fim, o trabalho contará com quatro capítulos onde há a possibilidade do desenvolvimento do tema nos capítulos de referencial teórico, nos próximos serão apresentados os métodos, resultados e as conclusões, por último as referências.

2 REFERENCIAL TEÓRICO

Neste capítulo serão apresentados os conceitos de maior pertinência para o desenvolvimento deste trabalho, tais quais: um resumo a respeito da tecnologia do IoT, definição, arquitetura, focando em segurança da informação, mas abarcando temas como conceito, surgimento, utilização e outros; assim como a o que seria o BC, funcionamento, aplicações, exemplos onde já possui uso, arquitetura P2P e outros. Este levantamento foi feito com o intuito de fomentar fundamentos para o presente trabalho.

2.1 INTERNET DAS COISAS

A história do IoT é oriunda antes mesmo da internet, teve seu fundamento construído em conjunto com a tecnologia do RFID, utilizada hoje em lojas, caixas, roupas para identificação (etiquetas em geral, vista até nas fazendas no gado). Segundo (MARTINS, 2018), a criação do que viria ser o RFID, remonta a Segunda Guerra Mundial como forma de identificar quando os aviões captados pelo radar eram aliados ou inimigos. Funcionava quando o sinal captado pelo radar sinalizava o avião, então este deveria refletir essa informação recebida, baseada a partir da característica (como modelo da aeronave), e então o sistema de forma ativa ou passiva decidia através dos dados coletados compreender a que grupo o avião fazia parte. Como era de se esperar no pós-guerra, a tecnologia de radiofrequência se desenvolveu e foi se aderindo as áreas não militar.

Ao longo do tempo, novas gerações de tecnologias computacionais foram surgindo, acompanhadas pelo desenvolvimento da internet e dos telefones celulares. Nesse contexto, em 1991, Weiser publicou o artigo *The Computer for the 21st Century*, no qual explorava um futuro em que dispositivos estariam conectados de forma transparente e acessível, integrando-se naturalmente ao cotidiano humano. Porém, foi em 1999 que o Kevin Ashton usou o termo *Internet of Things* pela primeira vez, e assim é conhecido até hoje, enquanto apresentava uma ideia de um novo sistema de RFID para produtos na cadeia de suprimentos. Vale lembrar também, que John Romkey em 1990 criou o primeiro dispositivo conectado à internet, uma torradeira que podia ser ligada e desligada de forma remota (MANCINI, 2017).

Além do termo IoT, outras designações como mostra Banerjee, Lee e Choo (apud, SAKAMOTO, 2020) também se pautam a esse conceito, de maneira a surgirem como estudos específicos, como: Internet de todas as coisas (*Internet of Everything*), Internet das coisas médicas (IoMT - *Internet of Medical Things*), Internet das coisas militares (IoBT - *Internet of*

Battlefield Things), Internet dos veículos (IoV - *Internet of Vehicles*), Internet dos objetos (IoO - *Internet of Objects*), Internet das coisas Robóticas (IoRT – *Internet of Robotic Things*) e Internet Industrial das Coisas (IIoT – *Industrial Internet of Things*). Entretanto, alguns destes termos ainda possuem caráter recente, os conceitos correlatos que foram se aglomerando por trás do IoT já atravessam décadas (RIBEIRO, 2020).

Agora, visualize um cenário em que sua máquina de lavar seja capaz de identificar quando o nível de detergente está baixo, estabelecer automaticamente uma comunicação com o mercado, negociar as melhores condições de preço e realizar o pedido do produto necessário de forma autônoma. O mesmo acontece com os itens na geladeira: leite, ovos e assim por diante. Esses dispositivos inteligentes conhecerão seu calendário, adiando e organizando-se caso você estiver de férias ou fora de casa por um tempo.

Há uma certeza de que haverá alguns problemas iniciais com as primeiras iterações desses dispositivos e os contratos inteligentes associados a eles. Como os primeiros a adotar essa tecnologia, pode-se imaginar chegar em casa e encontrar uma pilha de grandes caixas de amaciante de roupas, o suficiente para durar uma vida inteira. Mas esses dispositivos e sua inteligência associada irão interagir e acertar para o mercado de massa.

2.1.1 Cenário do IoT

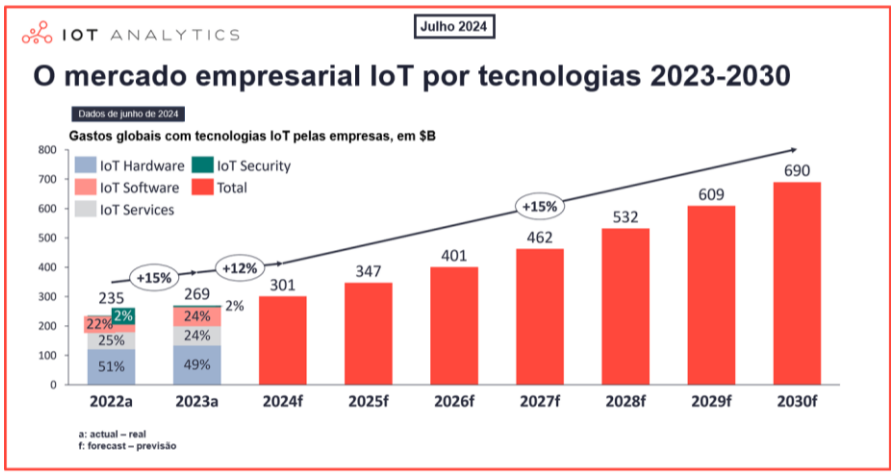
É com o cenário da digitalização da sociedade em uma velocidade exponencial, que existe o crescente ímpeto por inovar cada dia mais. O IoT acabou se infiltrando em todos os âmbitos, e a elevada exigência por dispositivos deste gênero é uma realidade. A tecnologia está inserida hoje em várias atividades, aumentando os benefícios, trazendo eficiência e ganho de tempo nos mais variados setores.

O site https://iot-analytics.com em 9 de julho de 2024 publicou uma análise em que foi avaliado o atual tamanho do mercado do IoT empresarial e as previsões até 2030, com dados coletados do ano de 2023 que já haviam fechado seus ciclos de quartenários dentro do mercado internacional, veja na Figura 1. Deve-se observar que no ano passado essa faixa atingiu US$ 269 bilhões com leve desaceleração em 2024 de acordo com (FERNANDEZ, 2024), muito influenciado por um mercado muito incerto em geral, e ainda sofrendo muito economicamente com guerras e instabilidades políticas dos países com industrialização alta, chamados mercados regionais (países como: EUA, China, Índia e Coréia do Sul) e verticais (tais como indústrias automobilísticas, chips e outros).

O crescimento de acordo com (FERNANDEZ, 2024) em 2022 havia sido 3% maior, mas espera-se que os gastos empresariais com IoT possam mostrar mais sinais de recuperação

com taxa de crescimento a partir de 2025, a partir de uma CAGR (*Compound Annual Growth Rate*) de 15% projetada até 2030, visto na Figura 1.

Figura 1: O mercado IoT empresarial por tecnologia 2023-2030.



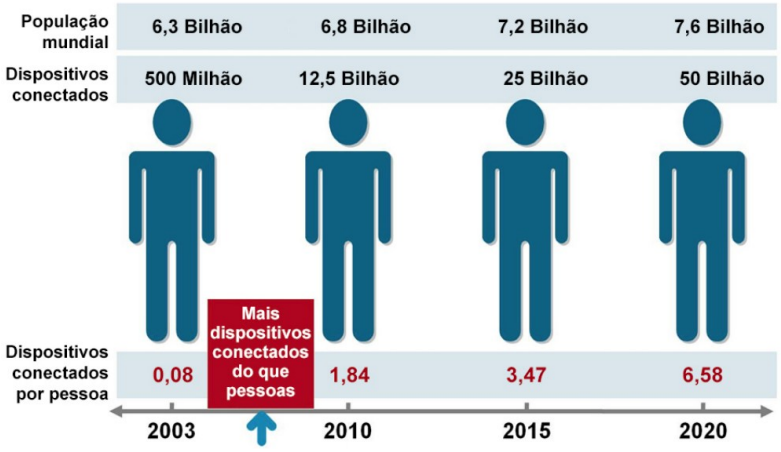
Fonte: (FERNANDEZ, 2024)

Sakamoto (2020) faz uma outra projeção:

> Segundo estudo apoiado pelo BNDES em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) divulgado em 2018, a Internet das Coisas terá um impacto econômico de 4 a 11 trilhões de dólares no mundo até 2025. No Brasil, a estimativa é de 50 a 200 bilhões de dólares por ano. (SAKAMOTO, 2020).,

Ainda como forma de revalidar a quantidade cada dia maior de dispositivos, o autor (NOVO, 2018) em seu artigo, revela que a previsão para 2022, no ano em que foi escrito sua obra, seria de 18 bilhões de dispositivos. O que segundo ele, tornou a tecnologia uma grande influência nos mercados verticais. Assim como (MAGRINI, 2018) em seu livro destaca que os estudos da Cisco, garantiam por volta de 50 bilhões de dispositivos conectados em 2020. Conforme a relação trazida por (FUKUDA, 2020) mostrada na Figura 2.

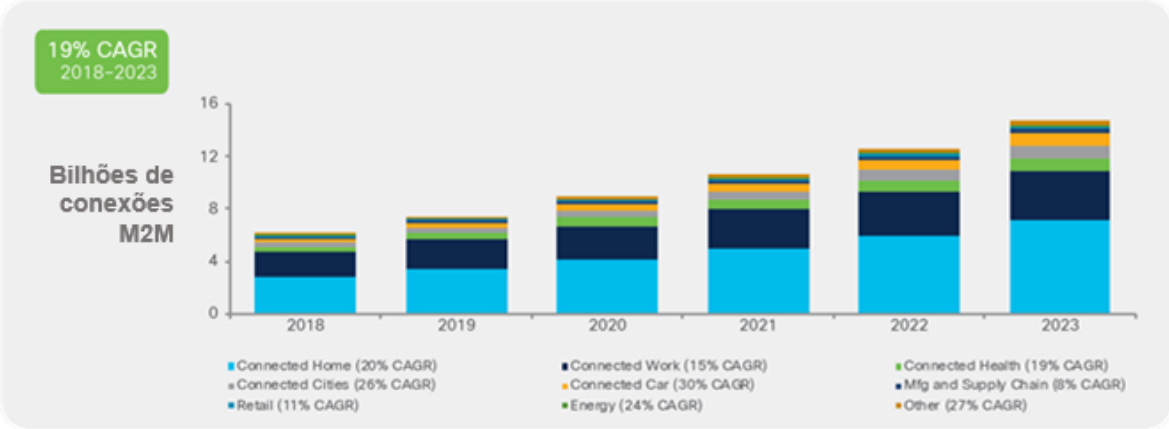
Figura 2: Dispositivos/Pessoas.



Fonte: (FUKUDA, 2020)

Em 2020 a Cisco em seu "Relatório Anual da Internet da Cisco (2018–2023) White Paper" previa para o ano de 2023 que as conexões de aparelhos seriam de 14,7 bilhões do total das interações M2M (*Machine-to-Machine)* conforme observa-se na Figura 2. A previsão da empresa foi de 1,8 aparelhos para cada pessoa. Diferente um pouco da otimista previsão feita há alguns anos mostrada na Figura 3, mas ainda muito elevada.

Figura 3: Crescimento global da conexão M2M por setores.



Fonte: (CISCO, 2020)

2.1.2 Conceitos do IoT

A IoT em resumo pode ser apresentada como "*um ecossistema cyber físico de sensores e recursos interconectados, que permitem a tomada de decisões inteligentes*" (ALVES, PEIXOTO, ROSA, 2021). Uma ideia de que a internet estaria presente em todas as coisas. O conceito de IoT então permeia a ideia de fusão do mundo real com o mundo digital, "*fazendo com que os indivíduos estejam em constante comunicação e interação com outras pessoas e objetos"*, sendo uma evolução da computação com seus respectivos desafios, conforme apontou (MORAIS, GONÇALVES, LEDUR, 2018).

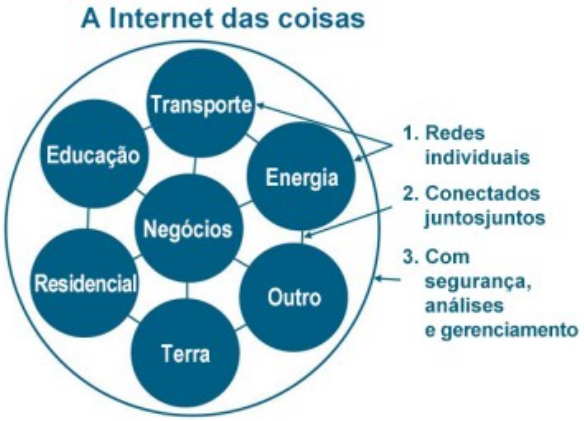
Conforme Olga Cavalli (apud MAGRINI, 2018, p. 20) "*O que hoje é chamado de internet das coisas (internet of things) é um conjunto de tecnologias e protocolos associados que permitem que objetos se conectem a uma rede de comunicações e são identificados e controlados através desta conexão de rede*.". Ou como o próprio autor (MAGRINI, 2018) delibera, seria basicamente que todas as definições de IoT acabam se assemelhando em alguns pontos como: concentram-se em "*como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade.*" Ao iniciar seu livro (SERPANOS; WOLF, 2017) descreve com simplicidade, mas de forma muito sagaz

o termo como "*a Internet das Coisas é o passo evolutivo da Internet que cria um mundo infraestrutura interligando máquinas e humanos*.".

De acordo com a estrutura conceitual de 2020, a IoT é expressa como uma fórmula simples (WANG; ZHU; NI.; GU; ZHU, 2020): "*IoT = Serviços + Dados + Redes + Sensores. Assim, IoT é uma combinação de dados de sensores e redes que fornecem diferentes serviços inteligentes"*, levando em conta todos os conceitos e resumo ilustrado por (ARATA; NASCIMENTO; DE NOVAIS, 2020).

A configuração da rede de objetos interconectados, como mostra na Figura 4, cada um sendo identificado de forma única, comunicando entre si e com outros sistemas, acabam oferecendo vários serviços. Esse conjunto de "coisas" está conectado à Internet, possuindo assim a capacidade de capturar e compartilhar dados, podendo ser usado para realização de tarefas complexas com um alto grau de inteligência (FUKUDA, 2019; SAKAMOTO, 2020).

Figura 4: Modelo estruturado de uma rede IoT.

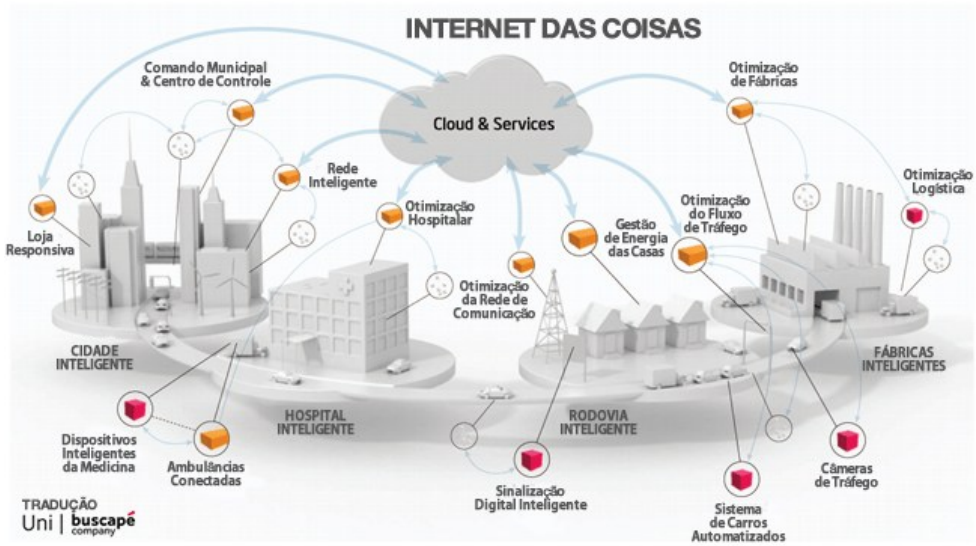


Fonte: (EVANS, 2011).

Assim como descritos pelos autores aos conceitos anteriores para o IoT ele é como uma rede de dispositivos com endereço IP, com capacidades de sensorização, recolha e envio de dados usando sensores embutidos, hardware de comunicação e processadores, como indicado na Figura 5, onde é possível verificar várias redes se comunicando e conectando a uma nuvem comum a todas. Logo com tais características, algumas áreas são especialmente beneficiadas por medidas arquitetadas nesses cenários onde ocorrem problemas recorrentes.

Quando se verifica cada um dos conceitos elencados a premissa é sempre a mesma, e o resumo pode ser exatamente o que mostra a Figura 6, verifica-se que se pode conectar uma coisa em qualquer lugar mesmo se estando em movimento, em ambiente fechado ou aberto e a qualquer hora do dia. Que resume o que foi trazido por (SERPANOS; WOLF, 2017) e (MORAIS, GONÇALVES, LEDUR, 2018).

Figura 5: Arquitetura das redes se conectando.

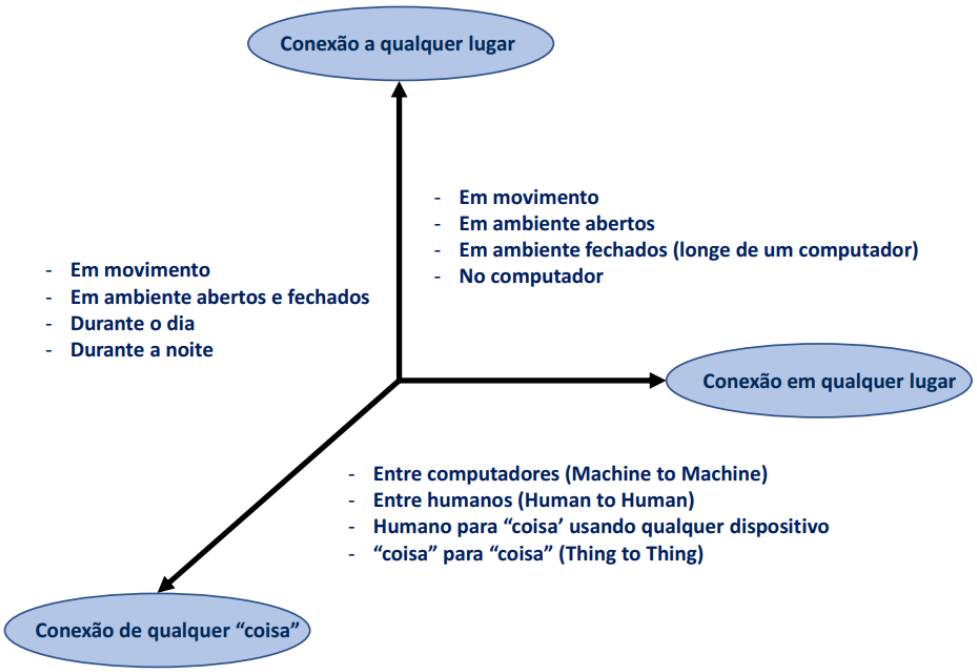


Fonte: (SATIZTPM, 2022).

Existe o agrupamento de três tipos de interações quando se trata de aplicações no campo de pesquisa, como relembra (SAKAMOTO, 2020) e é visto em um dos eixos do gráfico apresentado na Figura 6:

- entre pessoas (*people-to-people*);
- entre máquinas (*machine-to-machine*);
- entre pessoas e objetos;
- entre objetos (*things-to-things*).

Figura 6: Eixos de uso do IoT.



Fonte: adaptado de (ARATA; NASCIMENTO; DE NOVAIS, 2020)

2.1.3 Aplicações

Sob esse ponto de vista de quais lugares pode-se encontrar o IoT, há aplicações não somente ligadas ao ambiente doméstico em que o conceito pode ter se difundido rapidamente principalmente pelo ganho de produtividade, os sistemas IoT são úteis em uma ampla gama de aplicações, como por exemplo:

- Os sistemas industriais utilizam sensores para monitorar os próprios processos industriais – a qualidade do produto – e o estado do equipamento. Hoje já existem motores elétricos, por exemplo, que incluem sensores que coletam dados usados para prever falhas iminentes sugerindo trocas de determinadas peças ou oléos ou manutenções, assim garantindo uma maior vida útil;
- Edifícios inteligentes usam sensores para identificar a localização das pessoas e também do estado do edifício. Esses dados podem ser usados para controlar aquecimento/ventilação/sistema de ar condicionado e de iluminação para reduzir custos operacionais. As estruturas também usam sensores para monitorar a saúde estrutural;
- As cidades inteligentes utilizam sensores para monitorar o tráfego de pedestres e veículos e podem integrar dados de edifícios inteligentes;
- Transporte público: usuários podem saber, pelo smartphone ou em telas instaladas nos pontos de embarque, qual a localização de determinado ônibus. Os sensores também podem ajudar a empresa a descobrir que um veículo apresenta defeitos mecânicos, assim como saber como está o cumprimento de horários;
- Os sistemas médicos conectam uma ampla gama de sensores de monitoramento de pacientes que podem ser localizados em casa, em veículos de emergência, no consultório médico ou no hospital; pacientes podem utilizar dispositivos conectados que medem batimentos cardíacos ou pressão sanguínea, por exemplo, e os dados coleta dos serem enviados em tempo real para o sistema que controla os exames;
- Agropecuária: sensores espalhados em plantações podem dar informações bastante precisas sobre temperatura, umidade do solo, probabilidade de chuvas, velocidade do vento e outras informações essenciais para o bom rendimento do plantio. De igual forma, sensores conectados aos animais conseguem ajudar no controle do gado: um chip colocado na orelha do boi pode fazer o rastreamento do animal, informar seu histórico de vacinas e assim por diante;

2.1.4 Questões de segurança

A comunicação do tipo M2M é inimaginável estar sem nos dias atuais, contudo essa interação e suas tecnologias merecem cuidado e atenção, devido aos impactos que promovem em todas as áreas. Como dito anteriormente a premissa do IoT é ter tudo conectado entre si o tempo todo e com isso riscos associados são trazidos. E estes riscos não são apenas individuais eles ocorrem de forma coletiva nas redes.

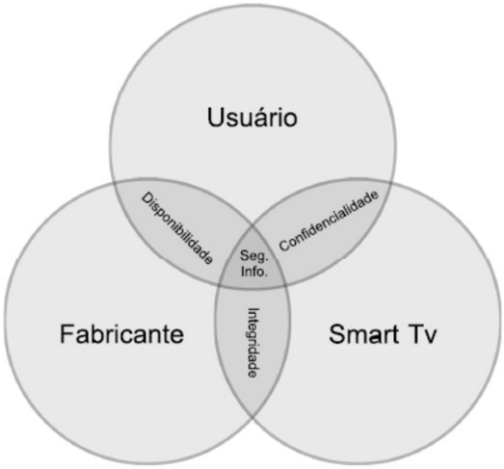
Quando se leva em consideração que existem relações entre pessoas e "coisas", é importante avaliar fatores éticos e legais, e com relação a isso se fez importante a criação de leis que protegessem dados e privacidade dos usuários, a Lei Geral de Proteção de Dados, a LGPD. No Brasil em 14 de agosto de 2018 a lei 13.709, traria as condições do tratamento dos dados pessoais, inclusive nos meios digitais, "*por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*" (BRASIL, 2018)

Assim devem estar de acordo com os seis grandes pilares de segurança e privacidade: confidencialidade (é garantir que o acesso aos dados sejam restritos apenas ao público-alvo); integridade (refere-se a manutenção da acuidade e integridade dos dados, em resumo protege-los de serem alterados por ações de partes não autorizadas); disponibilidade (as informações devem ser de fácil acesso quando solicitadas); autenticidade (garantido pela busca de que a informação sejam oriundas de fonte confiável); irretratabilidade (ou não repúdio, impedimento que outro usuário negue a autoria de uma informação, garantindo a sua autenticidade); e por fim legalidade (caráter de informação é real juridicamente, em acordo com as legislações regentes) (ALVES, PEIXOTO, ROSA, 2021).

Então como indicado na Figura 7, presente no livro dos autores (ALVES, PEIXOTO, ROSA, 2021) é que cabe tanto ao usuário final, quanto aos fabricantes e finalmente a "coisa" as responsabilidades de uso das informações, que por exemplo uma Smart TV irá utilizar os dados coletados durante o tráfego e uso dos seus aplicativos.

Fundamentando sua comunicação principalmente na "tríade CID" ou "*CIA Triad*", que são: (a) confidencialidade, (b) integridade e (c) disponibilidade; o IoT busca ampliar seus horizontes sem perder o principal dentro dos parâmetros exigidos hoje pela segurança da informação, mas vem esbarrando em vários problemas (FUKUDA, 2019; SAKAMOTO, 2020; GIANNOUTAKIS; SPATHOULA; FILELIS-PAPADOPOULOS; COLLEN; ANAGNOSTOPOULOS; VOTIS.; NIJDAM, 2020).

Figura 7: Como deve funcionar a Segurança da Informação.



Fonte: (ALVES, PEIXOTO, ROSA, 2021)

Segurança para o IoT é algo crítico, a grande disponibilidade de objetos interligados, trocando informações a todo momento, soluções de segurança é um desafio para a Internet das Coisas. E como elencado acima hoje a preocupação com os dados dos usuários e as leis estão em pauta e precisam ser cada dia mais ampliadas.

Com a ampla possibilidade de ter conexão em qualquer ambiente, aumenta consideravelmente as possibilidades de comunicação, interação, serviços e recursos provindos da Web, porém por outro lado, também existe o aumento da área de risco a um ataque, o próprio Departamento Federal de Investigação, o *FBI*, em nota oficial, fez um alerta a população orientando sobre as possibilidades de ataque de hackers em ambientes IoT, conforme lembra (FUKUDA, 2019).

Como foi dito por Balaguer (apud FUKUDA, 2019):

> Com a rápida expansão da utilização da Internet das Coisas em todo o mundo, além da crescente disseminação de *malwares* para todo tipo de *hardware* e *software* (sejam sistemas operacionais ou aplicativos), a preocupação com a Segurança da Informação (dados pessoais e corporativos) também deve seguir entre as principais prioridades da indústria de Tecnologia da Informação. (apud FUKUDA, 2019)

Analisando os inúmeros riscos e as vulnerabilidades em dispositivos *IoT*, torna-se cada vez mais comum, e ameaçador principalmente porque erros cometidos por fabricantes de dispositivos que ainda não estão familiarizados com as práticas de segurança, conforme relata (ZANI, 2016 in FUKUDA, 2019):

> Os dispositivos de Internet das Coisas muitas vezes não são projetados para a segurança. A maioria dos dispositivos não tem uma abordagem coordenada de segurança de rede, não exigem senha ou não se preocupam com complexidade das mesmas, armazenam informações pessoais e contém diversas vulnerabilidades. A proliferação de novos dispositivos, a baixíssima preocupação com segurança e alto valor dos dados contidos nesses objetos farão com que os ataques cibernéticos visando esses dispositivos cresçam de forma abundante (ZANI, 2016 in FUKUDA, 2019).

Tratando desses dispositivos, é possível cauterizá-los em três agrupamentos conforme as funções exercidas, como informa (FUKUDA, 2019):

1º) Dispositivos para coleta de informações, via sensores, transmitindo essas informações constantemente.

2º) Dispositivos para receber informações coletadas, pelo primeiro grupo via internet.

3º) Dispositivos específicos, que representa a junção dos demais grupos, coleta e recebe informações.

Os dispositivos IoT são suscetíveis a diversos tipos de malware, cada um com o seu propósito:

- Botnets DDoS: programas maliciosos assumem o controle de dispositivos IoT para lançar ataques distribuídos de negação de serviço (DDoS);
- Ransomware: direcionado a dispositivos IoT, especialmente aqueles que contêm dados de usuários, o ransomware criptografa arquivos e exige resgates para descriptografia;
- Mineradores: apesar do seu poder de processamento limitado, alguns cibercriminosos tentam usar dispositivos IoT para mineração de criptomoedas;
- Alteradores de DNS (*Domain Name Server)*: ou também DNS *hijacking,* onde certos malwares alteram as configurações de DNS em roteadores Wi-Fi, redirecionando os usuários para sites maliciosos;
- Proxy Bots: Os dispositivos IoT infectados são empregados como servidores proxy para redirecionar o tráfego malicioso, dificultando o rastreamento e a mitigação de tais ataques.

Em 2013, *hackers* invadiram a rede da Target e roubaram as informações de cartões de crédito de milhões de transações. O ataque aconteceu através do roube de credenciais do login de um fornecedor de HVAC (em inglês: *Heating, Ventilating and Air Conditioning*, ou AVAC – Aquecimento, Ventilação e Ar-Condicionado), que usava sensores IoT para monitorar a Target em termos de consumo de energia e tornar os sistemas mais eficiente. (CAMPOS, 2023)

Um par de especialista em 2015 em segurança cibernética, testou os níveis de robustez do novo Jeep Grand Cherokee usando seu sistema de multimidia como porta de entrada, assim comprovaram que eram capazes de não só se conectar a outros componentes do veículo, como também reprogramá-lo, controlar volante, motor, freios e muito mais. (CAMPOS, 2023)

O órgão que controla as liberações médicas e alimentícias nos EUA, o FDA (*Food and Drug Administration*), anunciou em 2017 que mais de 465.000 dispositivos de marca-passos implantáveis estavam passíveis a ações hackers. Embora até aquele ano, não houvesse registro de ataques, foram feitas correções dos aparelhos, porém foi o bastante para alarmar uma perturbadora preocupação acerca de algo tão importante a vida e vulnerável. (CAMPOS, 2023)

Um dos ataques mais famosos oriundos de botnet DDoS citado por (FUKUDA, 2019), ocorreu no final do ano de 2017, onde a Spotify, Netflix, Twitter, Tumblr, CNN e Reddit, tiveram suas atividades temporariamente interrompidas, devido ao "Dyn", um provedor de internet, ter sido invadido por hackers, através de uma variável da botnet Mirai. Após o estudo do problema, foi possivel verificar que os invasores utilizaram os sistemas de câmeras de segurança, conectados à internet, forçando o acesso ao site do Dyn, o ataque DDoS, congestionou o sistema e o serviço saiu fora do ar.

Outro exemplo muito conhecido é o da *Amazon Web Service* (AWS), em 2020 quando o serviço de computação em nuvem da AWS foi atingido por um gigantesco ataque DDoS em fevereiro daquele ano. Onde o Protocolo de Acesso a Diretório Leve Sem Conexão (CLDAP, *Connectionless Lightweight Directory Access Protocol*, sigla em inglês) que recebeu dados de terceiros vulneráveis e amplificou a quantidade dos dados enviados ao IP da vítima de até 70 vezes. Ao final dos 3 dias de ataque o pico atingiu 2,3 terabytes por segundos. (RIGUES, 2020)

Com isso, verifica-se que a segurança é a maior pauta de fato em termos do próximo passo para o que será ajustado e assim o IoT cresça conforme projeções ou mesmo ultrapasse-as. Como parte de curiosidade hoje os códigos fontes dos botnets e de algumas das ameaças descritas estão disponíveis em portais na internet, superfície e *dark web*, o que aumenta a proliferação de ataques e as inovações nos mesmos.

2.1.5 Funcionamento e arquitetura

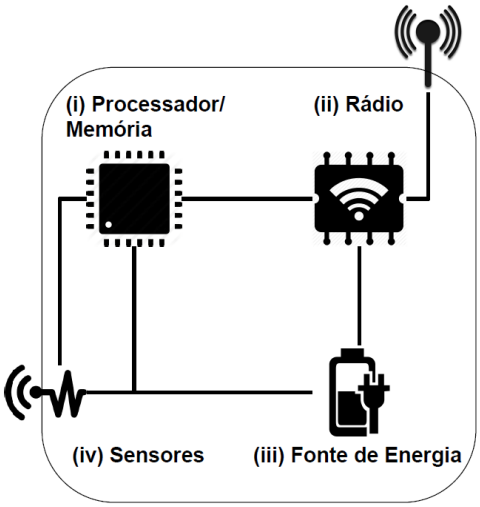
Não existe uma arquitetura universalizada para IoT, em particular, devido seu uso diversificado e as aplicações funcionarem em uma arquitetura de rede orientada a elas. Relembrando o que já foi dito, basicamente todas as "coisas" precisam se conectar o tempo todo, e então seguindo essa premissa, mesmo seguindo caminhos diferentes elas precisam basicamente possuir o mesmo objetivo. Surge então, como descreve (MORAIS, GONÇALVES, LEDUR, 2018) uma base comum, uma arquitetura master, que origina as

subarquiteturas com suas especificidades, porém essa foi a forma de garantir a interoperabilidade em todos os níveis.

É visto na Figura 8, uma ideia que essa arquitetura básica teria que trazer os requisitos já descrito acima por (SANTOS, 2016) e assim em congruência com o que cita (MORAIS, GONÇALVES, LEDUR, 2018) garantir as funcionalidades para que um objeto seja considerado IoT. Lembrando que a arquitetura básica M2M deve possuir três tipos de camadas: camada de aplicação; camada de serviços comuns; camada de serviços de rede.

A camada de aplicação fica responsável pela ponta, onde encontra se os sensores, GPS (*Global Positioning System*), *smarthphones*, entidades de aplicação. Onde essa implementa uma ou mais requisições de serviços, que são reconhecidos por uma identificação. Na camada de serviço comuns uma outra entidade utiliza funções comuns a arquitetura funcional e em conjunto com a camada de aplicação, por meios de bibliotecas de desenvolvimentos conhecidas por elas (API - *Application Programming Interface*) fazem uma interação de interpretação. E assim a camada de serviços de redes pode através de protocolos, comunicar-se com dispositivos e nuvem. (MORAIS, GONÇALVES, LEDUR, 2018)

Figura 8: Arquitetura dos dispositivos.



Fonte: (SANTOS, 2016)

Hoje, as tecnologias de comunicação/identificação são além dos dois principais RSSF (Rede de Sensores Sem Fio) e o RFID, vistos por exemplo de acordo com (FUKUDA, 2019; SANTOS et al, 2016), WiFi, Bluetooth, *Bluetooth Low Energy* (BLE), IEEE 802.15.4 (ZigBee), 3G/4G/5G, NFC (*Near Field Communication*), LoRa (*Long Range*) e Sigfox. Os dispositivos estão cada vez menores e possuem mais recursos. Pode-se esperar ainda que essa evolução continue e, no futuro, possivelmente observados em outras tecnologias de hardware empregadas na IoT.

Como a forma de identificar os dispositivos na rede é usando os endereços de IP como diz (MARTINS, 2018), assim os endereços são gerenciados por um protocolo chamado IPv4 (*Internet Protocol Version* 4), que possui um limite máximo de 4,3 bilhões de endereços. Este número findou em 2015, fazendo com que a IETF (*Internet Engineering Task Force*), reformulasse e propusesse outro protocolo de identificação, o qual recebeu o nome de IPv6 (*Internet Protocol Version* 6). Este novo protocolo possui endereços formados por oito pacotes de 16 bits cada, totalizando 128 bits escritos em dígitos hexadecimais, muito mais que seu antecessor que somava apenas 32 bits. Isso permite cerca de 34 x 10^{38} endereços IP, que é um número relativamente grande e o IoT tem feito proveito dessa ordem de grandeza para aumentar sua expansão. (SANTOS et al, 2016).

Entretanto, o IPv6 possui um tamanho de pacote maior que o quadro dos protocolos usados pelos dispositivos de IoT (o pacote IPv6 é transmitido dentro da área de dados do quadro do protocolo de acesso ao meio). Seria mais ou menos a ideia da pilha criada na Tabela 1 em que o protocolo anteriormente difundido e utilizado principalmente por seu tamanho era o IPV4.

Tabela 1: Exemplo de pilha de protocolos.

Aplicação/Serviço	HTTP
Transporte	TCP/UDP
Rede	IPV4
Enlace e Física	WiFi, Bluetooth, BLE, IEEE 802.15.4 (ZigBee), 3G/4G/5G, NFC, RSSF, RFID, LoRa e Sigfox

Fonte: Elaboração própria.

Assim a IETF com o objetivo de gerenciar, padronizar e levantar os requisitos para as redes de baixa potência, LLN (*Low-Power and Lossy Networks*) criou o IPv6 em *Low-Power Wireless Personal Area Networks Working Group* ou conhecido como 6LoWPAN para redes que seguiam comunicação no padrão IEEE 802.15.4, quem limita os pacotes a 128 bytes. (SANTOS et al, 2016). O 6LoWPAN é uma camada de adaptação desenvolvida para o padrão

IEEE 802.15.4, de forma inicial. A principal ideia seria comprimir os pacotes IPv6, desta maneira, mesmo com baixo poder computacional o IoT em alguns objetos, ele então use o IPv6 sem problemas. Veja Tabela 2 como ficaram as camadas após as adaptações para o novo protocolo na camada de redes, e é possível ver que também houve mudanças na camada de aplicação.

Tabela 2: Pilha de protocolos após as adaptações com várias aplicações de exemplo.

<table>
<tr><td>Aplicação/Serviços</td><td>CoAP</td><td>AMQP</td><td>DDS</td><td>MQTT</td></tr>
<tr><td>Transporte</td><td colspan="2">UDP</td><td colspan="2">TCP</td></tr>
<tr><td>Redes</td><td>ICMPv6</td><td colspan="2">IPv6</td><td>RPL</td></tr>
<tr><td>Adaptação</td><td colspan="4">6LoWPAN e LoRaWAN</td></tr>
<tr><td rowspan="2">Enlace e Físca</td><td colspan="4">IPSP</td></tr>
<tr><td colspan="4">WiFi, Bluetooth, BLE, IEEE 802.15.4 (ZigBee), 3G/4G/5G, NFC, RFID, LoRa e Sigfox</td></tr>
</table>

Fonte: Elaboração própria.

Elementos da Tabela 2 que são importantes:

Camada de aplicação:

- CoAP ou protocolo de aplicação restrita, é um protocolo de rede e largura de banda restrita para dispositivos limitados que permite que o cliente envie uma solicitação ao servidor e este o retorne em HTTP, pois atualmente diversos serviços web operam utilizando o modelo de arquitetura REST (*Representational State Transfer*) para desenvolver cabeçalhos de transferência de pacotes dentro da web; e é empregado de forma binária (ARATA, NASCIMENTO, DE NOVAIS, 2020).
- AMQP ou protocolo avançado de enfileiramento de mensagens oferece roteamento e enfileiramento para ambiente de *middleware* orientado à mensagem. Usado para conexão ponto-a-ponto, tem suporte para troca de dados entre dispositivos e nuvem. Definido em três componentes básicos, *Exchange, Massage Queue e Binding*, que juntos garante trocas satisfatórias.
- DDS ou serviço de distribuição de dados é um protocolo ponto-a-ponto flexível, conseguindo fazer praticamente tudo, até a execução de pequenos dispositivos até a conexão de redes de alto desempenho.

- MQTT ou Transporte de Telemetria da Fila de Mensagens é um protocolo também conhecido como assinatura/publicação, responsável por mensagens leves e tem sido escolhido para os dispositivos de IoT por suas características. Ele é capaz de coletar dados de diversos nós e supervisioná-los remotamente, oferece suporte a troca de mensagens orientada a eventos e por meio de redes sem fio. Geralmente, seus dispositivos exigem menos memória e seu protocolo de transporte preferencialmente é o TCP.

Camada de transporte: UDP (*User Datagram Protocol*) é rápido, pois não estabelece uma conexão formal antes de transferir os dados. O TCP (Protocolo de Controle de Transmissão), ao contrário do UDP, é um protocolo que provê maior confiabilidade justamente por sequenciar e verificar erros dos pacotes transmitidos entre os nós durante as comunicações.

Camada de redes: RPL ou IPv6 *Routing Protocol for Low Power and Lossy Networks*, é um protocolo de roteamento também de baixo custo energético que se baseia em vetor de distância, otimizado para comunicação multi-hop e muitos para um, porém suporta mensagens de um para um. ICMPv6 ou Internet *Control Message Protocol Version* 6 que faz parte da arquitetura do IPv6 e é usado para acusar erros, performar diagnósticos e enviar mensagens sobre algo que ocorra ou característica especificas da rede.

Camada de adaptação: LoRaWAN protocolo de rede que define como os dispositivos conectados usam a tecnologia LoRa.

Camada de enlace e física: IPSP refere-se ao um perfil de suporte do protocolo de internet e a um *gatway* IPSP presentes em nós de baixo custo que se conecta em redes WiFi. WiFi funciona com base em ondas de rádio nas frequências de 2,4 GHz, 5 GHz e 6 GHz e permite a conexão de dispositivos à internet sem o uso de cabos; Bluetooth transmissões de rádio na faixa de frequência de 2,4 GHz, é uma tecnologia de conexão sem fio de curto alcance que permite a comunicação entre dispositivos; BLE Bluetooth Low Energy, também chamado de Bluetooth LE ou Bluetooth Smart, é uma tecnologia que permite que dispositivos como fones de ouvido e *smartwatches* façam conexões com menor custo de energia, BLE trabalha com apenas 40 canais em espaços de 2 MHz entre eles na referida faixa de frequência, enquanto o Bluetooth clássico o faz com 79 canais e espaço de 1 MHz; IEEE 802.15.4 (ZigBee) podem usar uma das três bandas de frequência disponíveis para a operação: 868.0–868.6 MHz: Europa, 902–928 MHz: América do Norte, 2400–2483.5 MHz resto do mundo; 3G/4G/5G - as aplicações de IoT são bem suportados por LTE-M e NB-IoT baseados em redes celulares 4G e o 5G trouxe maior rapidez e maior capacidade de banda; NFC

tecnologia de comunicação sem fio que permite a troca de informações entre dispositivos próximos, como celulares, relógios inteligentes, cartões de crédito e débito, em distancias de até 10 cm; LoRa tecnologia de baixo consumo de energia e de longo alcance, que permite a comunicação entre dispositivos em distâncias de até 10 km em áreas urbanas e até 15 km em áreas rurais; e Sigfox no Brasil, há duas configurações de Rádio nas quais os dispositivos podem operar: frequência de 902,2 MHz e 920,8 MHz. (SANTOS, 2016)

Tendo essa perspectiva em mente, o cenário divergente entre os vários equipamentos conectados quanto as restrições de energia e largura de banda incentivaram a computação a caminhar por outro rumo. Hoje, processadores relativamente pequenos têm realizado um volume de processamento de dados altíssimo. Reconhecer eventos interessantes usando processamento de borda reduz a quantidade de largura de banda de rede consumida; também reduz o consumo de energia, uma vez que a comunicação sem fio requer grandes quantidades de energia. Computação em nuvem (servidores centralizados) ou *fog computing* (servidores mais próximos da borda) podem ser usados para executar processamento adicional, surgindo a ideia do que hoje se conhece como *Big Data*. (SERPANOS; WOLF, 2017)

2.1.6 Big Data

Quando, “coisas” se conectam à internet capazes de compartilhar, processar, armazenar e analisar um volume exagerado de dados entre si, ocorre um acúmulo de informação. Essa prática é o que une os conceitos de IoT e *big data*. *Big data* é um termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados onde sempre há o potencial de ser explorado ou extraído graus de informações. Como propriedade primordial envolvendo o *Big Data* pode-se destacar o volume crescente de dados.

2.1.7 Cloud

A computação em nuvem depende do compartilhamento de recursos, o que é um fundamental requisito para a plataforma IoT. O *Cloud Computing*, como também é chamado, não é apenas a capacidade de interação, mas também a de maximizar os recursos. Isto ocorre independentemente da localização, visto que os usuários acessam os serviços em nuvem de qualquer local e de inúmeros dispositivo precisando apenas de conexão à internet. Quando se fala de plataforma IoT, é possível verificar que se deve levar em conta a virtualização de

dispositivos físicos como ponto crucial, pois permite que os usuários compartilhem facilmente informações dentro das redes.

Além disso, a nuvem oferece elasticidade e é escalável, o serviço e os recursos são facilmente acessíveis. Portanto, a convergência de *Cloud* e IoT oferece grandes oportunidades para ambas as tecnologias.

2.2 BLOCKCHAIN

Pode-se compreender melhor o porquê em 2008 sob o pseudônimo Satoshi Nakamoto um *white paper* (documento de apresentação, ou artigo introdutório) intitulado "*Bitcoin: A Peer-To-Peer Electronic Cash System*" (NAKAMOTO, 2008) buscou-se a necessidade de criar um sistema econômico mais eficiente, confiável e seguro para conduzir e registrar transações financeiras. Para contextualizar, o mundo estava passando por uma das piores crises financeiras, conhecida como "bolha imobiliária".

Basicamente, isso ocorreu quando diversos bancos passaram a oferecer mais créditos, expandindo o crédito imobiliário e atraindo os consumidores, o que causou a valorização dos imóveis. Até que com a alta procura, a taxa de juros subiu, derrubando os preços dos imóveis. Como muitos destes empréstimos foram de alto risco, muita gente não teve como pagá-los e diversos bancos ficaram descapitalizados.

Combinado com fato que ao longo da história a sociedade buscou instrumentos de aumentar a confiança quando o assunto é criação de suas moedas/dinheiro, desde quais elementos são usadas na fabricação para tal (como por exemplo uso de metais e a carga que estes têm nas especulações financeiras das moedas locais, como as reservas de ouro de um país), quanto seus sistemas bancários, e até sistemas de transações.

Então Satoshi Nakamoto, sugeriu uma solução para lidar com os níveis de complexidades, vulnerabilidade e ineficiência dos custos dos sistemas vigentes. Ele desenvolveu o sistema do Bitcoin, uma moeda digital que foi lançada em 2009, baseando-se no que havia sido publicado nas nove páginas do artigo do autor (ou como muitos pensam, autores, já que se especula que podem ser vários autores sob este pseudônimo).

A ideia se tratava de uma estrutura de dados inicialmente proposta por Haber e Stometta em 1990 segundo (VIANNA; DA SILVA; PEINADO, 2020), que já naquela década levantaram a ideia em que um grupo de indivíduos, trabalhando de forma descentralizada, poderia contribuir para o compartilhamento seguro de informações. Porém, foi Nakamoto quem descreveu uma versão P2P de um caixa eletrônico, de forma que o usuário poderia fazer pagamentos para os demais usuários sem a necessidade de instituições, intermediários (ou o

que é chamado no artigo de terceira parte); e sugeriu a utilização de um sistema de blocos de informações financeiras (tecnologia BC), que não poderiam ser corrompidas. Assim como o Bitcoin, nascia a primeira aplicação direta ao conceito por trás da BC e sua popularidade aumentou o interesse para demais aplicações.

A primeira transação por Bitcoins ocorreu alguns dias depois de sua criação, quando um programador e usuário, o Hal Finney, usando um intermediador que aceitou trocar os Bitcoins por dólares, compraram duas pizzas custando U$ 25,00, onde a transação ocorreu no bloco 170 do Bitcoin correspondendo ao uso de 10.000 Bitcoins (BTC). Ou seja, observa-se que nessa primeira transação, cada Bitcoin valia 0,0025 centavos de dólar americano (USD). Esse bloco havia sido presenteado a Hal Finney por Satoshi Nakamoto em agradecimento à sua contribuição na criação do código (MORAES, 2021). Hoje o atual valor de um bitcoin, consultado no dia quatro de dezembro de 2024, está em U$ 98.782,80, se houvesse guardado o valor hoje seria o equivalente U$ 987.828.000,00.

Entretanto, o Bitcoin é apenas uma parcela do BC e é muito importante deixar claro que são coisas distintas. Porém, está ao alcance pensar de forma metafórica no BC como um sistema operacional, como Microsoft Windows ou Linux, e Bitcoin seria apenas um dos muitos aplicativos que podem ser executados nesse sistema, como simplifica (GUPTA, 2017).

E não se pode deixar de fora ainda que após o Bitcoin crescer, houve uma expansão das criptomoedas, dos NFTs (*non fungible tokens*), aplicações das moedas no Metaverso, *smart contracts* (entre bancos, imobiliárias e empresas), que vieram contribuir para acelerar a evolução desse futuro, que será cada vez mais digital. A digitalização de processos é irreversível.

Com a adoção por parte dos países de legislações cada vez mais voltadas à proteção de dados, com uma busca efetiva de que cada indivíduo tenha gestão mais ativa e um controle maior sobre seus dados, exemplos da já citada LGPD, mas também permite-se verificar GDPR (*General Data Protection Regulation*) na União Europeia (MORAES, 2021). A tecnologia BC vem sendo apontada como representante para uma possível evolução no assunto.

Diferentemente dos sistemas tradicionais, que exigem uma vasta e rigorosa gama de regulações e controles centralizados, para assegurar a confiança e a segurança das operações, essa tecnologia viabiliza um sistema sem a necessidade de se confiar a uma entidade específica a manutenção e a validação das transações e base de dados (*trustless system*). Baseando e garantindo seu funcionamento por meio de um registro distribuído aos usuários da

rede, ela confere maior transparência no trato da informação, ao mesmo tempo em que cria uma rede mais livre, democrática e igualitária. (MARCHSIN, 2022)

Seria em resumo uma coleção de dados ou um banco de dados que sustenta uma cadeia de registros em crescimento contínuo. A rede é feita em nós, distribuída de ponto a ponto, de maneira que pode ser aproveitada para armazenar dados nela como um todo. Cada nó contém a mesma cópia dos mesmos dados, assim a confiabilidade e a disponibilidade dos dados são alcançadas de maneira única. Cada vez que um novo registro é anexado a cadeia, cada nó ou os que estão participando desta, receberão a cópia atualizada da cadeia. Isso cria a abordagem descentralizada no armazenamento, erradica e reduz a probabilidade de o ponto único falhar e cria um ambiente muito mais flexível, como trás os autores (URMILA; HARIHARAN; PRABHA, 2019).

2.2.1 Conceitos do *Blockchain*

Uma definição para a tecnologia foi feita por Swan (2015 apud MARCHSIN, 2022, p.11):

> Devemos pensar na *Blockchain* como uma outra categoria de coisas como a Internet – uma ampla tecnologia de informação com níveis técnicos em camadas e múltiplas classes de aplicação para qualquer forma de registro de ativos, inventários e trocas, incluindo todas as áreas de finanças, economia e dinheiro; ativos tangíveis (propriedade física, imóveis, carros); ativos intangíveis (votos, ideias, reputação, intenção, registros médicos, informação etc.). Mas o conceito de *Blockchain* é ainda maior, é uma nova organização de paradigmas para a descoberta, valoração e transferência de toda quanta (áreas específicas) de qualquer coisa, e potencialmente para a coordenação de toda atividade humana em uma escala muito maior do que tem sido possível até então. (2015 apud MARCHSIN, 2022, p.11)

O termo BC era somente para descrever dentro da informática a estruturação e compartilhamento de dados, onde armazena dados de transações em blocos que estão ligados entre si para formar uma cadeia, à medida que as transações crescem o mesmo acontece com a cadeia de blocos. Os blocos conseguem registrar e gerar relatório de confirmação de hora, assim como a sequência das transações que foram logadas na rede. (LAURENCE, 2019; MARCHSIN, 2022; GUPTA, 2017) Criptograficamente seguros, dispensam o uso de validações por entidades confiáveis e centralizadas. Com isso (NAKAMOTO, 2008) descreve que as transações, com alto recurso computacional, seriam impraticáveis quando se trata de reverter, e esse caráter traria a proteção aos usuários contra fraudes, criando um sistema “caução” de rotina, onde ele protegeria os vendedores e compradores igualmente. As transações criariam um carimbo ou prova computacional, bem como uma ordem cronológica das transações. O sistema se torna seguro desde que os nós honestos controlem de forma

coletiva as informações, assim como o poder computacional, inviabilizando que os grupos cooperantes de nós invasores consigam resolver o *hash* em tempo hábil.

Originalmente a ideia proposta por (NAKAMOTO, 2008) para a BC, seria uma forma de resolver o problema do "gasto duplo", pois nas transações online usuais sempre se faz necessário um terceiro para intermediá-las, mas para sua criptomoeda virtual, o Bitcoin, ele propusera então remover a necessidade do intermediário. Sem falar que muitas transações comerciais permanecem ineficientes, caras, e vulneráveis, sofrendo das seguintes limitações:

- O dinheiro é utilizável somente no local da transação e em pequenas quantias;
- O tempo entre uma transação e o acordo é relativamente longo;
- A validação por parte de um terceiro gera o gasto duplo citado por Nakamoto, exigindo a presença de um intermediário;
- Fraudes, cyber-ataques, e até mesmo erro humano, o que gera custos e prolonga a complexidade durante a negociação, além de expor todos os participantes ativos na rede centralizada a riscos, tais quais o próprio banco;
- Envolve-se muita burocracia durante o processo o que consome esforço humano e computacional, em acréscimo o consumo de tempo para o preenchimento;
- Metade das pessoas do mundo não possuem acessos a contas bancárias e tem desenvolvido sistemas paralelos de conduzir transações. [traduzido livremente de (GUPTA,2017)]

Hoje considerada por alguns a "quinta evolução" da computação, tal feito veio por ser capaz de incrementar uma camada de confiança hoje ausente para internet. Considera-se uma abordagem de base de dados distribuída, onde grupos de pessoa podem controlar o que se armazena e compartilha. (LAURENCE, 2019; MARCHSIN, 2022) Ainda neste ano, os relatórios apontam a importância de se investir na busca de adaptação a tecnologia BC e assim "*drasticamente reduzir os custos de transações e, se adotada de forma ampla, remodelar toda a economia*", traduzido livremente de (IANSITI; LAKHANI; MOHAMED, 2017). É uma tecnologia que se popularizou e tem ganhado uma maior fluidez de investimentos, mesmo com o alto nível tecnológico de adaptação.

(CROSBY; PATTANAYAK; VERMA, 2016) observaram duas vantagens da tecnologia BC que poderiam ser utilizadas por organizações: o aumento da agilidade, da eficiência na emissão e negociação de títulos corporativos e a possibilidade de desenvolvimento de negócios diretos entre duas partes interessadas. Além de trazer inúmeros exemplos como aplicação na indústria da música, criando selos e aumentando a segurança por

trás dos royalties; a descentralização do IoT; dentro de questões envolvendo logística e o atraso de entregas; aplicações na internet, usando por exemplo uma versão descentralizada do DNS. Os autores (YING; JIA; DU, 2018) afirmam que estas vantagens se devem às características de segurança criadas, sua transparência e impossibilidade de alteração dos dados, quando estes são registrados nos blocos.

Outro exemplo é mostrado pelo autor (GUPTA,2017), BC permite que os títulos sejam liquidados em minutos em vez de dias. Isto também pode ser usado para ajudar as empresas a gerenciar o fluxo de mercadorias e pagamentos relacionados, ou permitir que os fabricantes compartilhem a produção logs com fabricantes de equipamentos originais (OEMs) e reguladores para reduzir o recall de produtos.

2.2.2 Os Tipos de *Blockchain*

Tanto o setor público quanto o setor privado têm grandes expectativas em relação a tecnologia BC porque fornecem a base para o desenvolvimento de plataformas P2P para troca de informações, ativos e bens digitalizados sem intermediários, como o observado em (MOREIRA, 2019). Isso porque é possível verificar as vantagens entre sistemas centralizados e descentralizados conforme Tabela 3, como diz (MARCHSIN, 2022):

> Em um sistema centralizado, confiamos em um terceiro (bancos, provedores de serviços e pagamentos, operadoras de cartões de crédito etc.) para atuar como intermediário que garante a integridade e a validade das transações. Em um sistema descentralizado, a confiança é distribuída e garantida por meio de criptografia que nos permitem determinar a validade e a integridade das transações. Não há ponto central de controle. Ao invés, as decisões são tomadas via consenso em uma rede distribuída de computadores. (MARCHSIN, 2022, p.12

Tabela 3: Diferenças entre sistemas.

Sistemas Centralizados	**Sistemas Descentralizados**
Têm um controle central detentor de toda a autoridade. Esses sistemas são fáceis de se projetar, manter, governar ou impor confiança, mas sofrem limitações: • são menos estáveis, uma vez que têm um ponto central de falha; • são mais vulneráveis a ataques e menos seguros; • a centralização de poder cria condições para a corrupção em diferentes atividades de governo; • a escalabilidade é mais difícil.	Não têm controle central da autoridade e cada nó tem um poder igual. Tais sistemas são difíceis de se projetar, manter, governar ou impor confiança. No entanto, não sofrem as limitações convencionais dos sistemas centralizados. Suas vantagens são as seguintes: • são mais estáveis, pois não têm um ponto central único suscetível a falhas; • são mais seguros e mais resistentes a ataques; • Por conferir autoridade igual a todos, o sistema é mais simétrico, democrático e tem sido visto como uma ferramenta capaz de combater a corrupção.

Fonte: adaptado de (MARCHSIN, 2022)

Remover essa autoridade pontual, que fica no centro das operações, dos modelos centralizados é uma ideia que pode ter levado alguns a interpretação equivocada de total ausência de tipos de controle. É preciso ter em mente que mesmo com a tecnologia envolta com o conceito de descentralização, a graus de controle e permissões dentro das redes, como na Figura 9 onde o os registros são fechados em seus centros de acessos e à medida que se observa a retirada da autoridade em um nó, o que se altera é a forma como é disponibilizada a permissão, o caráter (público ou privado) do que é compartilhado, do nível tradicional totalmente centralizado ao descentralizado usado hoje no modelo aplicado pelo Bitcoin.

Figura 9: Tipos de registro com relação a centralização nestes.

Fonte: (MARCHSIN, 2022)

As redes privadas se modificam das redes públicas e como exemplo o uso modificado de um tipo da rede, logo tem-se a divisão, entre o uso particular por empresas de uma BC (o que ocorre hoje nos casos da Volvo, Mercedes Benz, que usam a tecnologia dentro e fora do chão de fábrica), chamada de privada. Os sistemas públicos são transparentes, uma vez que todas as alterações e operações feitas pelos usuários são visíveis.

O BC, conforme já dito, tem um histórico completo com todas as transações e fornece uma confiança global distribuída, afinal cada transação é compartilhada no *ledger* (Livro-razão), público ou privada, o que altera é a maneira que esta informação é verificada pelos nós, que estão ativamente envolvidos na verificação e validação de transações de forma que exista um consenso. Uma vez que as transações passam por essas etapas por consenso, os dados dos blocos serão imutáveis, não podendo serem apagados ou modificados.

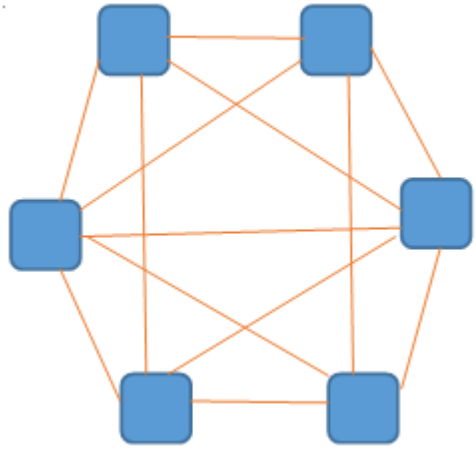
Assim para melhor entender as diferenças entre os tipos:

- Públicas: qualquer um pode acessar a rede para ler ou escrever como mostra a Figura 10, onde os nós estão livres sem barreiras e os nós abertos a consultas sem necessidade de chaves entre as operações, é possível customizar a rede

para dar autorização de leitura, escrita ou ambos. O BC é protegido por verificação criptográfica apoiada por incentivos para os mineradores. Qualquer um pode ser um minerador para agregar e publicar essas transações. Os conceitos de verificação são *proof-of-work (PoW)* ou *proof-of-stake (PoS)*. Possui código aberto central geralmente mantido e incrementado por uma comunidade ativa, um exemplo é o Bitcoin. (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018; NOVO, 2018; TSENG, 2020)

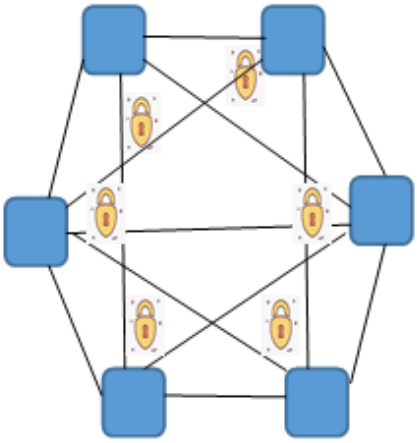
- Consórcio ou Permissionados: o *ledger* é distribuído onde o processo de consenso é controlado por um conjunto pré-selecionado de nós, por exemplo, um consórcio de nove instituições financeiras, cada uma das quais opera um nó e das quais cinco (como a Suprema Corte dos EUA) devem assinar cada bloco para que o bloco seja válido. O direito de ler o BC pode ser público ou restrito aos participantes, existem rotas híbridas, como os *hashes* raiz dos blocos sendo públicos juntamente com uma API que permite que membros do público façam um número limitado de consultas e obtenham provas criptográficas de algumas partes do estado da cadeia. Podem ser considerados "parcialmente descentralizados". Tem-se o exemplo do Ripple que controla funções que pessoas podem desempenhar dentro de redes, seu código central não é aberto em sua maioria das vezes. (BAMBARA; ALLEN, 2018; LAURENCE, 2019)
- Privados: usado geralmente por grandes empresas de caráter homogênea como mostra a Figura 11, onde cada nó tem seu controle ativo por assinatura e *hash* de validação, mais rápida que a publica como possui menores custos e tempos de validação mais curtos (devido ao menor número de nós, o problema matemático pode ser simplificado), menor risco de ataques (visto que os nós que validam transações são conhecidos) e maior privacidade sendo que as permissões podem ser concedidas apenas a nós selecionados). As permissões de gravação são mantidas centralizadas em uma organização. As permissões de leitura podem ser públicas ou restritas de forma arbitrária. Os aplicativos prováveis incluem gerenciamento de banco de dados e auditoria interna de uma única empresa, portanto, a legibilidade pública pode não ser necessária em muitos casos, embora em outros casos a auditoria pública seja desejada. (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018; BAMBARA; ALLEN, 2018)

Figura 10:Rede pública para aplicação em IoT.



Fonte: (MACHADO, 2018)

Figura 11: Rede privada para aplicação em IoT.



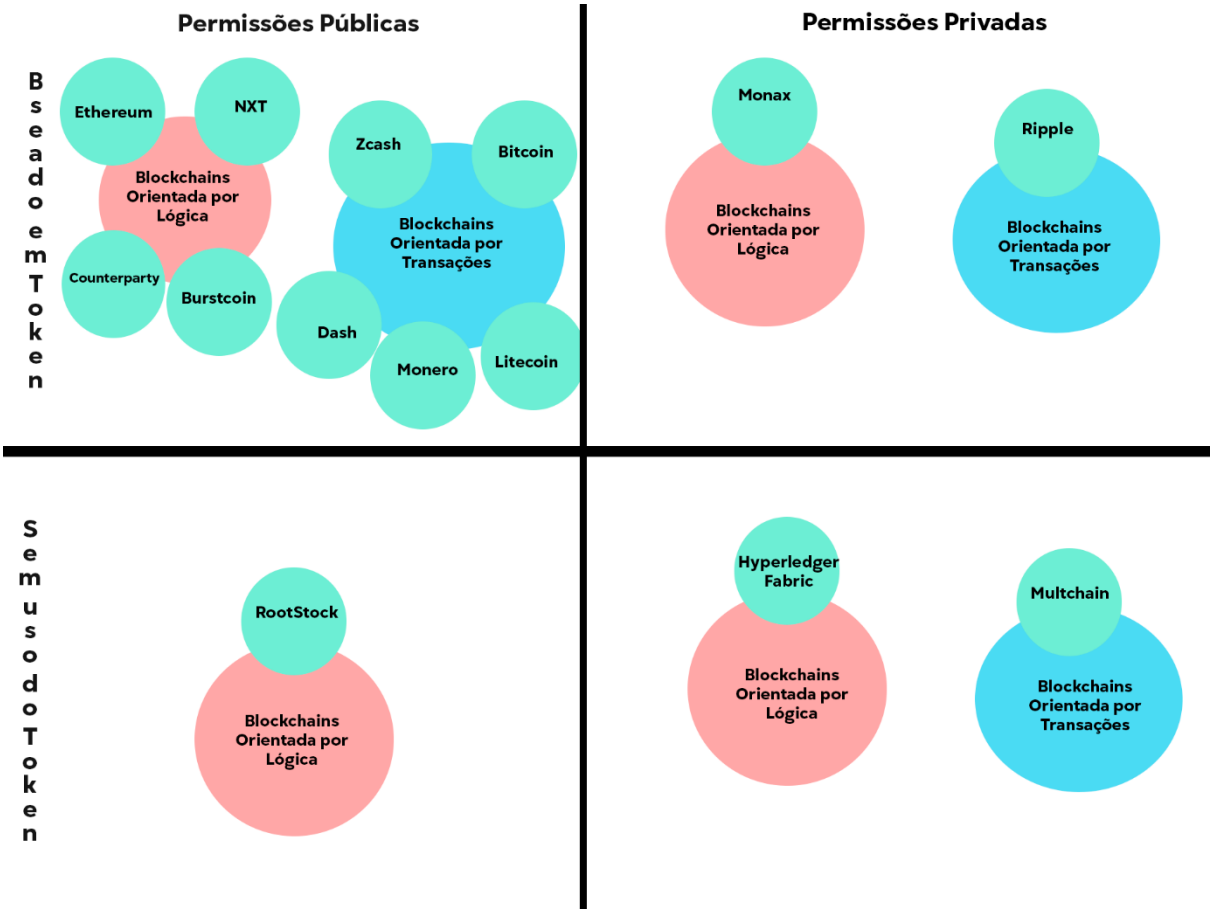
Fonte: (MACHADO, 2018)

Deve-se levar em conta o uso ou não do token nas transações, a principal função da criação deste recurso em uma rede BC é que eles são utilizados para mantê-la funcionando e fazem checagem de manutenções nos códigos aos quais foram inseridos. Como é o caso da maior parte das criptomoedas, isso porque estas são complexas de serem desenvolvidas, enquanto os tokens são relativamente simples, sobretudo para aqueles que já possuem algum conhecimento em programação, um exemplo disso é o Ethereum que criou o token ETH.

As redes privadas como dito acima por serem menores e de maior facilidade quanto a correções de erros geralmente trabalham sem token introduzido em seus códigos fontes, como é o caso do *Hyperledger Fabric* que é uma plataforma de *ledger* distribuída aberta e de nível corporativo. Ele tem controles de privacidade avançados, para que você só compartilhe os dados que deseja entre os participantes da rede com permissão ou conhecidos.

Em resumo, é possível de forma a ilustrar os diferentes tipos de BC*s* onde estão representados na Figura 12, juntamente com vários exemplos de implementações além dos dois citados acima que seguem a mesma linha de pensamento, todas as empresas citadas ainda estão ativas. Para elucidar melhor BC*s* orientadas por lógica fazem seus registros por operações matemáticas e lógica de programação, enquanto o orientada por transação segue as transações dentro dos nós e registra como um identificador cada uma.

Figura 12:Taxonomia para BC e exemplos práticos.



Fonte: adaptado de (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018)

2.2.3 Funcionamento e Arquitetura

Um conceito muito importante para entender o funcionamento do BC é o *ledger*, ele se comporta como o pessoal da contabilidade das empresas, pois é nele que ficam gravadas as operações. Então usando *consenso* que é o processo de ambas as partes em negociação para compartilhamento da informação estarem em acordo. Esses são os *full nodes* na rede, que são transações de validação que participam da rede para serem registradas como parte do *ledger*. (LAURENCE, 2019; MORAES, 2021)

Para que o usuário inicia então sua transação dentro da BC ele necessita da sua assinatura digital. Fazendo uso de criptografia de chaves públicas (criptografia assimétrica, uma chave é utilizada para encriptação, outra é usada para decriptação) e privadas (criptografia simétrica, baseado no conhecimento entre as partes de uma chave secreta, geralmente utilizada quando existe uma grande quantidade de dados a ser criptografada, fazendo uso de um algoritmo seguro de troca de chaves, como o Diffie Hellman), as

validações são certificadas a cada transação. (MARCHSIN, 2022) Assim, a assinatura digital é implementada, e a autenticação pode ser melhorada com o uso de certificados digitais.

Como é definido pelo próprio (SAKAMATO, 2008), quando idealizou os princípios do BC, quando cada proprietário estivesse em uma cadeia de assinaturas digitais, poderia transferir a informação, assinando digitalmente um *hash* da transação anterior e a chave pública do próximo proprietário estariam todas contidas no bloco, assegurando os lastros da troca. Caso futuramente houvesse transações dentro desse bloco, o beneficiário iria poder verificar as assinaturas e verificar a cadeia de propriedade daquela informação gravada naquele *ledger*.

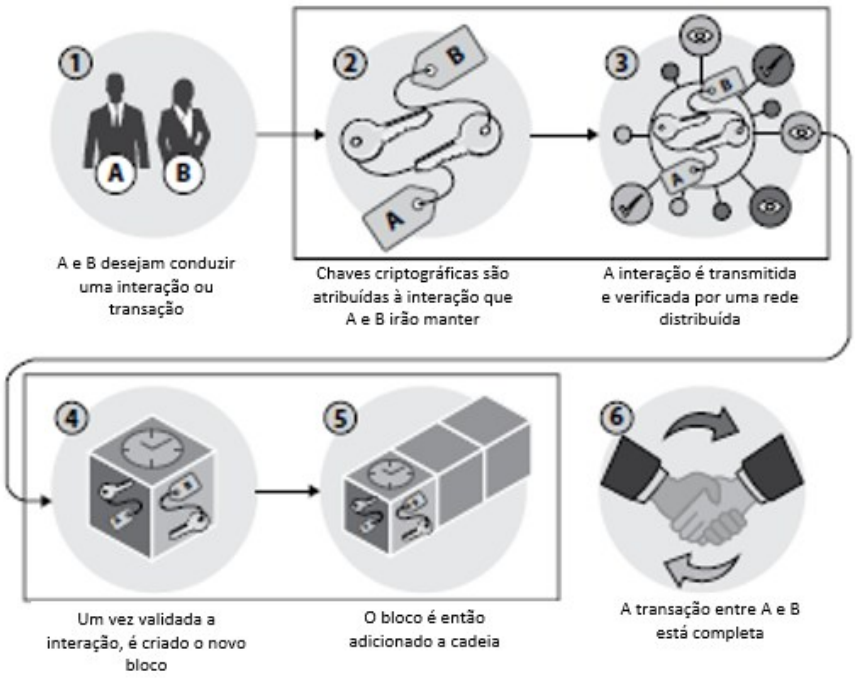
O *hash* no BC é criada a partir dos dados que estavam no bloco anterior. Sendo definido como a impressão digital desses dados, e sempre ordena e data o bloco que for inserido. Embora BC*s* seja recente, *hashing* não é. Este foi inventado há cerca de três décadas e está sendo usada hoje dentro da cadeia de blocos porque cria uma função unilateral que não pode ser decodificada. Uma função *hash* cria um algoritmo matemático que projeta dados de qualquer tamanho em uma cadeia de bits de tamanho fixo. Uma cadeia de bits geralmente tem 32 caracteres, *Secure Hash Algorithm* (Algoritmo de Dispersão Seguro — SHA) é uma das funções *hash* criptografadas usadas em BC*s*. SHA-256 é um algoritmo comum que gera uma *hash* quase única, exemplos de algoritmos de *hashing* são SHA256 256 bits (32 bytes), MD4 & MD5 (128 bits), SHA1 (160 bits)

Conforme visto em (KUROSE, ROSS, 2006, p. 533) "[...] *uma função de hash pega uma entrada de dados, m, e processa uma cadeia de tamanho fixo conhecida como hash*", ou seja, essa função singular gera uma cadeia de tamanho fixo que é improvável de retornar ao valor de entrada. O BC utiliza a função *hash* com o intuito de impossibilitar modificações dos arquivos digitais armazenados dentro deles, além de cada novo bloco utilizar a saída da função do bloco anterior para gerar um novo bloco, interligando todos os blocos, de maneira que qualquer modificação afetaria todos os blocos depois dele, sendo assim facilmente identificado por todos na rede.

Como trás (GUPTA, 2017) e (BAMBARA; ALLEN, 2018) um BC é um banco de dados que abrange uma cadeia física de blocos de comprimento fixo que incluem 1 a N transações, onde cada transação é adicionada a um novo bloco, verificada, validada e inserida no mesmo. Quando o bloco é concluído, ele é adicionado ao final da cadeia de blocos já existente. Existem duas operações, ao contrário do CRUD (*Create, Read, Update and Delete*) clássico, de adicionar e visualizar a transação. Portanto, o processamento básico do BC consiste nas etapas a seguir:

- Adicione transações novas e não excluíveis e organize-as em blocos. Visto na Figura 13 em 1, 2 e 3.
- Verifique criptograficamente cada transação no bloco. Visto na Figura 13 em 4.
- Anexe o novo bloco ao final do BC imutável existente. Visto na Figura 13 em 5.

Figura 13: Fluxo de transação pública do BC.



Fonte: adaptado de (BAMBARA; ALLEN, 2018)

Também, se pode resumidamente observar pelo fluxograma que segue, as transações abaixo na Figura 14, trazida por (LAURENCE, 2019), quando descreve os passos para que uma operação seja concluída dentro da rede usando BC.

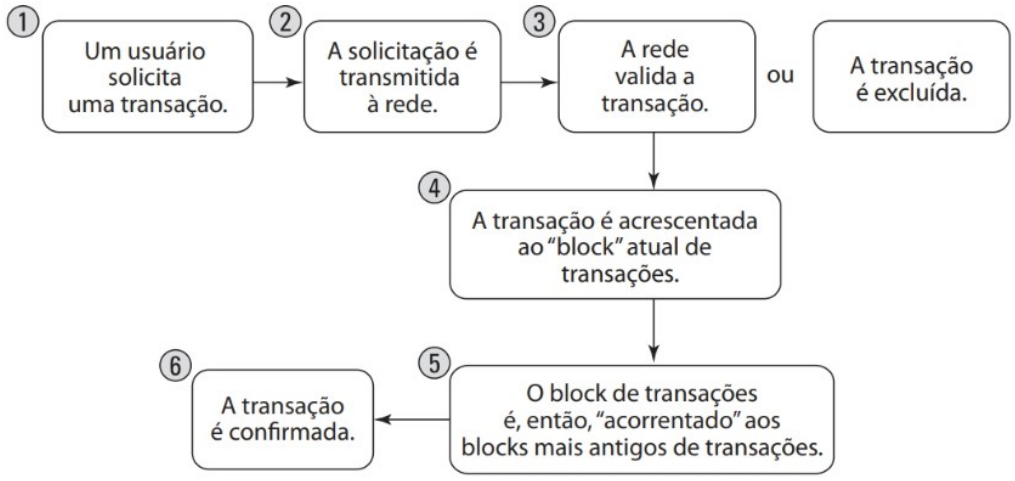
Resumindo, como foi dito por (IANSITI; LAKHANI; MOHAMED, 2017), em cinco princípios primordiais de como o BC funciona:

1. BANCO DE DADOS DISTRIBUÍDO: Cada parte em um BC possui acesso de todo o banco de dados e sua completa história. Nenhuma parte controla os dados ou informações. Cada frente pode verificar os registros de seus parceiros de transação diretamente, sem intermediário.
2. TRANSMISSÃO P2P: A comunicação ocorre diretamente entre pares, ao invés de um nó central. Cada nó armazena e encaminha informações para todos os outros nós.
3. TRANSPARÊNCIA COM PSEUDONIMIDADE: Cada transação e seus valores associados são visíveis para qualquer pessoa com acesso ao sistema. Cada nó, ou

usuário, em um BC tem um único endereço alfanumérico de mais de 30 caracteres que o identifica. Os usuários podem optar por permanecer anônimo ou fornecer prova de sua identidade para os outros. Transações ocorrem entre endereços dentro da rede.

4. IREVERSIBILIDADE DE REGISTROS: Uma vez que uma transação é inserida o banco de dados e as contas são atualizados, os registros não podem ser alterados, pois estão vinculadas a todos os registros de transação que vieram antes (portanto o termo "cadeia"). Vários algoritmos e abordagens computacionais são implantados para garantir que a gravação na base de dados seja permanente, cronologicamente separada e disponível para todos os outros dentro da rede.
5. LÓGICA COMPUTACIONAL: A natureza digital do *ledger* significa que as transações BC podem ser ligadas à lógica computacional e em essência programada. Assim, os usuários podem definir criar algoritmos e regras que automaticamente acionem transações entre nós.

Figura 14: Fluxograma de transação do BC.



Fonte: (LAURENCE, 2019)

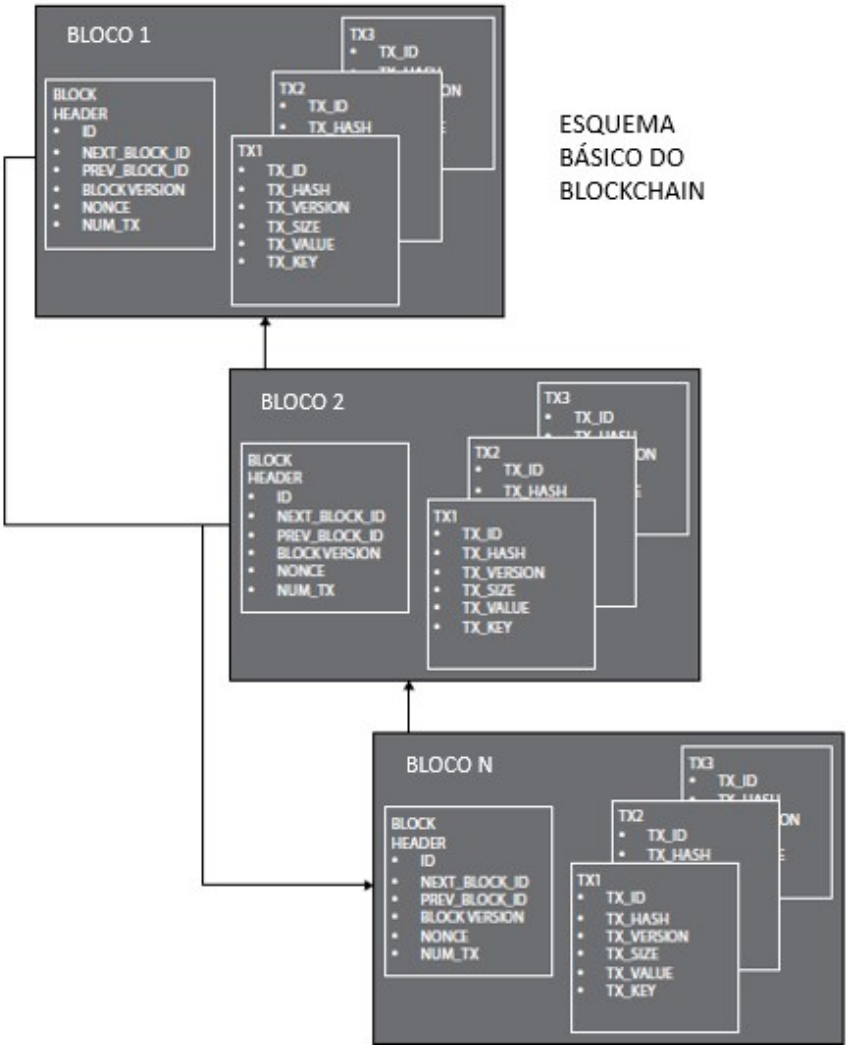
O *timestamp* tem como finalidade dificultar e impossibilitar fraudes no BC. (NAKAMOTO, 2008) elucida que "*o timestamp prova que os dados devem ter existido no momento, obviamente, para entrar no hash*", logo, comprovam a existência na hora do registro no BC. Assim o objetivo de acrescentar mais um elemento de segurança ao BC é atingido, pois é possível agora identificar o proprietário ou portador das chaves pública e privada garantindo que somente ele realize modificações. Para (KUROSE, ROSS, 2006, p.

530) "*a assinatura digital é uma técnica criptográfica usada para cumprir essa finalidade no mundo digital*", uma forma de garantir a propriedade de um arquivo ou dado.

Como visto anteriormente, cada bloco contém um *hash* (uma impressão digital ou identificador único), através do uso de uma rede P2P e uma rede com servidor distribui o carimbo de lotes com data/hora que determinam a validade das transações, e são capazes de mostrar quais são mais recentes, buscando o *hash* do bloco anterior. Este vincula os blocos juntos e impede que qualquer bloco seja alterado ou um bloco seja inserido entre dois blocos existentes. Nesse caminho, cada bloco subsequente reforça a verificação do bloco anterior e, portanto, todo a BC. O método renderiza toda a cadeia, o que o torna quase inviolável, concedendo-lhes o atributo chave de imutabilidade, um banco de dados BC*s* público é gerenciado de forma autônoma, por exemplo. Considerado assim um *ledger* aberto e distribuído, pode registrar transações entre duas partes de forma eficiente, verificável e permanente, conforme elenca (GUPTA, 2017).

O próprio *ledger* também pode ser programado para acionar transações automaticamente. BC*s* são seguros por design e um exemplo de um sistema de computação distribuído com alta tolerância a falhas bizantinas. O esquema primordial dos blocos e como vão se agrupando, formando a cadeia é exemplificado na Figura 15 a seguir, quando o Bloco 1 com as informações de texto contidas em TX1, 2 e 3 é identificado com o cabeçalho contendo o seu ID, o próximo bloco ID, e o bloco ID anterior, assim sendo possível todas as operações anteriores conterem criptografia e *hashing*. Uma vez em operação dentro da rede ele se conecta ao Bloco 2 e novamente tudo ocorre, em N vezes determinadas pelo tamanho da N da rede BC*,* pois todos os cabeçalhos dos blocos da cadeia se comportaram desta maneira*.*

Figura 15: Layout de dados e blocos para uma cadeia.

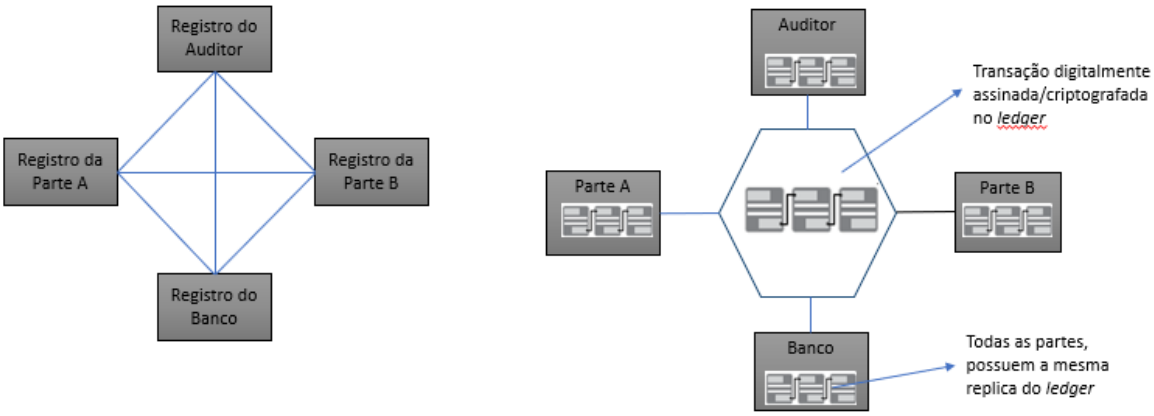


Fonte: adaptado de (BAMBARA; ALLEN, 2018)

A arquitetura então proposta pelo BC como é mostrado na Figura 17, usando o exemplo da Figura 16 de uma rede de negócios na esquerda representa a forma padrão utilizada hoje e na direita, a rede utilizando a tecnologia descentralizada que oferece esta tecnologia. Verifica-se que a rede da direita oferece aos participantes a capacidade de compartilhar um *Ledger* que é atualizado, por meio de replicação P2P, sempre que é adicionado alguma informação na rede, ou ocorre uma transação ela se replica. Isto ocorre em pares, assim cada nó na rede atua como um editor e um assinante, desse modo cada um pode receber ou enviar transações para os demais nós da rede. Todos os dados, portanto, estarão sincronizados à medida que são transferidos (ou inseridos). Os participantes em ambos os sistemas de transação são os mesmos. O que mudou é que o registro da transação agora é compartilhado e disponível para

todas as partes e não mais centralizado em parte caso necessário. E nas duas situações é possível perceber o registo auditável das ações.

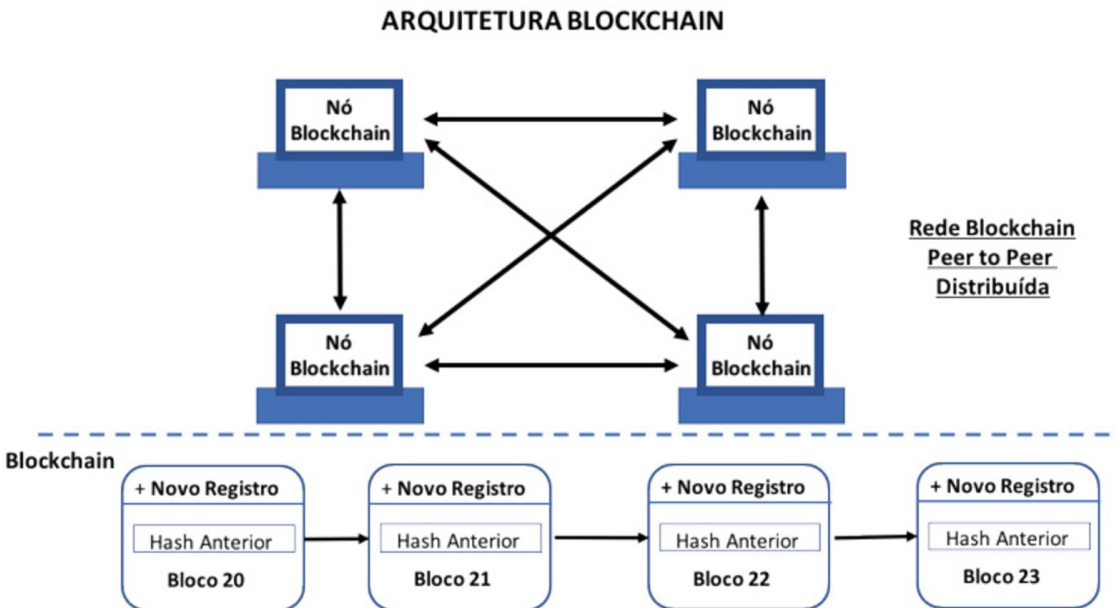
Figura 16: Sistema Sem e Com BC.



Fonte: adaptado de (GUPTA, 2017)

Pode-se observar a arquitetura do BC, realizando a comunicação dos nós usando uma rede P2P. Os blocos com os registros das transações são encadeados, criando-se assim uma cadeia, veja na Figura 17:

Figura 17: Arquitetura BC.



Fonte: (MORAES, 2021)

2.2.4 Minerar informação

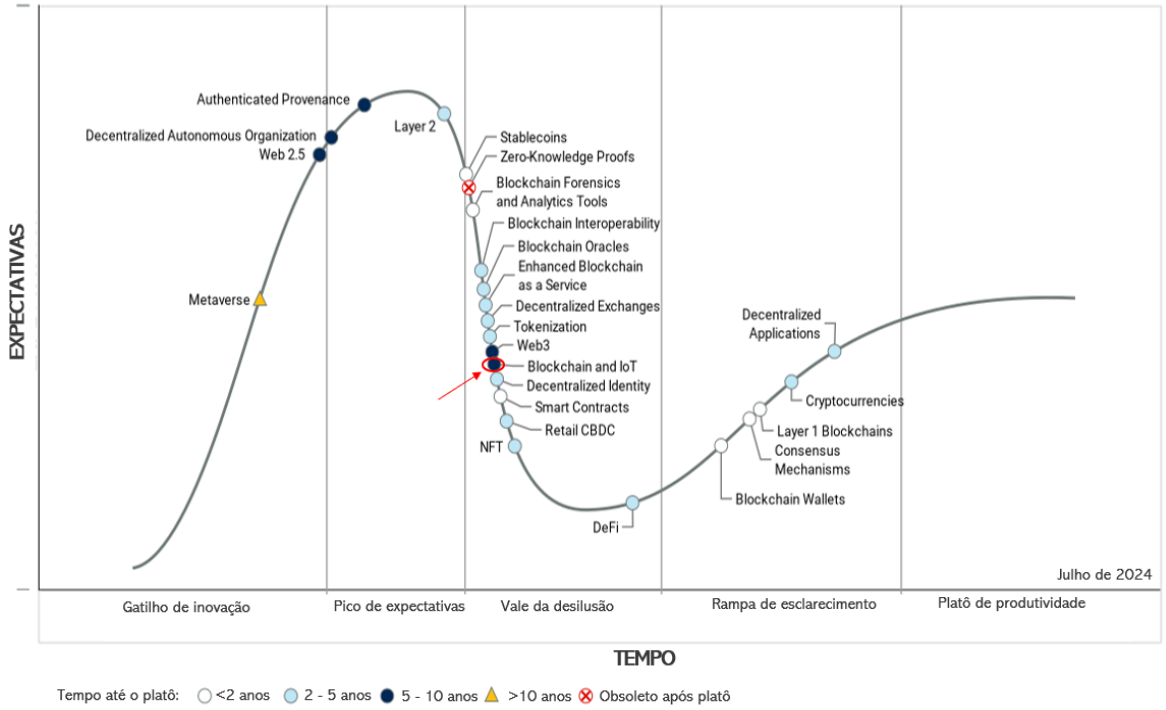
O processo de mineração consiste em utilizar capacidade de processamento (CPU) e memória para resolver um problema matemático necessário para a criação de blocos do Bitcoin e outras criptomoedas. Normalmente, o algoritmo de mineração envolve as seguintes tarefas: aguarda a verificação das assinaturas digitais, ou seja, recalcula o *hash* e compara com aquele encriptado e compara os dois; pergunta aos demais nós sobre o histórico, aguarda novos blocos e valida a transação *nonce* (é um número gerado aleatoriamente que é usado apenas uma vez em uma transação criptográfica); caso receba dados começa a minerar e criar um novo bloco, agrupando as transações que vieram do último bloco, validando cada operação; ao terminar, deve-se estar validado pelos outros nós, pois assim entra em consenso e seu bloco será aceito na rede; a partir do momento que o bloco minerado é aceito, o minerador recebe um prêmio normalmente conhecido como tarifa de transação (*transaction fee*), que é pagamento pelo custo energético desprendido, por volta de 1% ao mês de lucro dependendo do nível da dificuldade da rede encontrada.

Por exemplo, a cada 10 minutos, um minerador de Bitcoin recebe um prêmio, mas o prêmio está cada dia menor a cada valorização da moeda, que está alta. A mineração é o único mecanismo para criação de novos blocos para as moedas digitais. (MORAES, 2021)

2.3 O BIOT – BLOCKCHAIN-INTERNET OF THINGS

Anualmente o grupo Gartner fornece dados sobre o ciclo das tecnologias quanto a maturidade e adoção, e as previsões para o futuro destas, conhecido como *Hype Cycle*, onde a versão exclusiva para o uso da BC e Web3, realizado em 29 de julho de 2024, pode ser observado na Figura 18. Verifica-se uma curva de expectativa por mais que esteja presente no vale da desilusão, onde o mercado cria uma desesperança parcial com a inovação, pois começa-se os primeiros estudos e desenvolvimentos de propostas, a junção das duas tecnologias permanecem junto à Web3 como as únicas com uma expectativa maior, e caminha para o ideal platô de produtividade, que é quando as soluções evoluem no nível e audiência aceita para ser totalmente praticável. Nota-se que a previsão ainda garante de 5 a 10 anos de expectativas sobre inovações constantes no assunto.

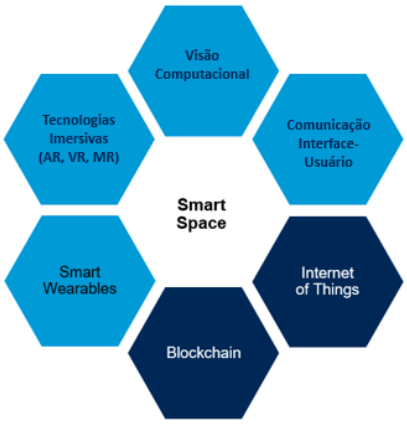
Figura 18: Gartner Hype Cycle para BC e Web3, 2024.



Fonte: adaptado de (DIGITALASSET, 2024)

Assim como (LITAN, 2022) lembra que quase sempre são associadas quando se trata de lugares inteligentes, ou "*Smart Spaces*", nesse caso é observado que as duas se colocam lado a lado para trazer benefícios aos ambientes e proporcionar maior segurança e automatização, conforme Figura 19, logo, é possível notar que elas são células ativas que possuem o intuito maior de moldar os *Smart Spaces*.

Figura 19: As seis tecnologias dos Smart Spaces.



Fonte: adaptado de (LITAN, 2022)

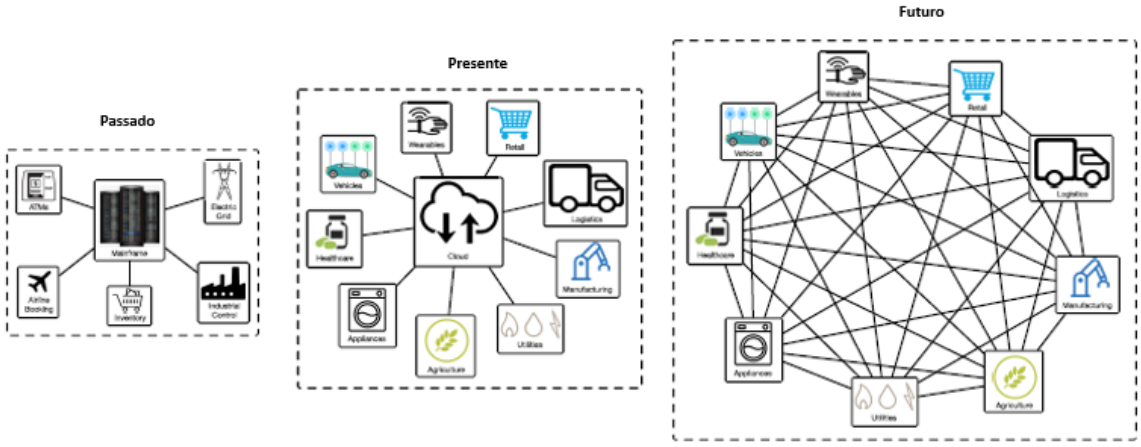
Existem trabalhos que já buscam o caminho a ser traçado para as arquiteturas emergentes que fundem esses dois campos de estudos, que de forma eficiente possam retirar os pontos positivos e assim criar um ambiente desejado com segurança, confiabilidade e robustez. Conforme dito por (TSENG, 2020), mesmo diante do plural mundo novo

vislumbrado por todos, ainda existe a viabilidade de citar duas categorias que sofreram com desafios para o BIoT:

- Integração: onde os desafios podem ser a forma heterogênea dos sistemas de IoT; a integração em si entre os dois, já que IoT e o BC foram desenvolvidos por comunidades diferentes, com objetivos dispares; isso pode acarretar dificuldades no suporte e compatibilidade.
- Administração/Implementação: problemas com recuperação em caso de falhas; monitoramentos e sua capacidade de ser auditável; e a capacidade de ser extenso e flexível.

As tecnologias da BC como são capazes de rastrear, coordenar, realizar transações e armazenar informações de uma grande quantidade de dispositivos, possibilitando a criação de aplicativos que não passariam mais requerer uma nuvem centralizada. O que pode ser visto na Figura 20, proposta por (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018), onde a atual circunstância poderá futuramente conter uma rede descentralizada baseada em cadeias de redes se conectando sem precisar passar por *cloud.*

Figura 20: Passado, presente e futuro das arquiteturas IoT.



Fonte: adaptado de (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2018)

Neste trabalho o foco principal consta em se aprofundar em uma apresentação das propostas feitas pelos autores, em suas as arquiteturas que fundem a matriz de como cada um vislumbra o BIoT, hoje e futuramente. Como modo de inclusive ilustrar o ícone representado na Figura 21, ele descreve como seria a interação das duas tecnologias e se tornou por estudiosos a figura que melhor ilustra a fusão feita.

Figura 21: Imagem ilustrativa do BIoT.

Fonte: (BAMBARA; ALLEN, 2018)

O papel do BC na segurança no IoT então é trazer as vantagens discutidas anteriormente, com a parte de criptografia e a imutabilidade, sua forma de compartilhar e rastrear ativos dentro de uma rede economizando perdas de tempo e recurso.

2.4 CONSIDERAÇÕES FINAIS

É importante saber sobre os dois assuntos de maior relevância ao trabalho para que se possa seguir com as discussões acerca de quais contribuições significativas já foram aplicadas ao BIoT no geral e quais ainda podem levar tempo considerável para serem praticáveis. Em particular atenção aos dois conceitos em separados, pois somente ao se elucidar cada um particularmente pode-se criar uma solução em conjunto para uma nova arquitetura que inove o já difundido uso do IoT. Para superar obstáculos como os citados, as soluções como a redes BC poderão ser o futuro.

3 MATERIAIS E MÉTODOS

Será apresentado neste capítulo a metodologia empregada e de pertinência valorizada ao desempenho deste trabalho e de sua continuidade.

3.1 METODOLOGIA

Uma evidente quantidade de informação hoje está disponível e de acesso quase livre, tornando cada vez maior a dificuldade de garantir uma amostra que contenha representatividade e relevância sobre o tema com uma voz totalmente inovadora. Produz-se, por sorte, cada vez mais e paradoxalmente enfrenta-se o caos da sobrecarga de publicações, então cabe ao pesquisador buscar qual de fato seria aplicável e relevante ao seu trabalho, mesmo que essa tenha se tornado uma tarefa intricada e de grande valor.

É de fundamental importância ao pesquisador encontrar métodos de pesquisas que o tornem capaz de distinguir dentro dessa grande quantidade de literatura disponível e assim consolidar de forma adequada seu tema. Sempre com o intento de uma boa performance, que este método possa auxiliar de forma positiva para atingir os resultados sólidos ao qual se propôs, visando que o esforço empregado seja equânime aos resultados encontrados, valendo o tempo deslocado para realizá-lo.

Neste viés este trabalho utilizou uma base de dados para o embasamento teórico. Onde para isso, fora explorado um levantamento de dados necessários para responder à pergunta principal do tema inicial proposto. Entretanto, como já é de conhecimento, a maioria das vezes já existem inúmeros outros trabalhos sobre o mesmo assunto, cabe então ao investigador levantar o que irá ser de maior interesse utilizando-se de metodologias como a apresentada aqui.

3.2 TEORIA DE ENFOQUE META ANALÍTICO CONSOLIDADO

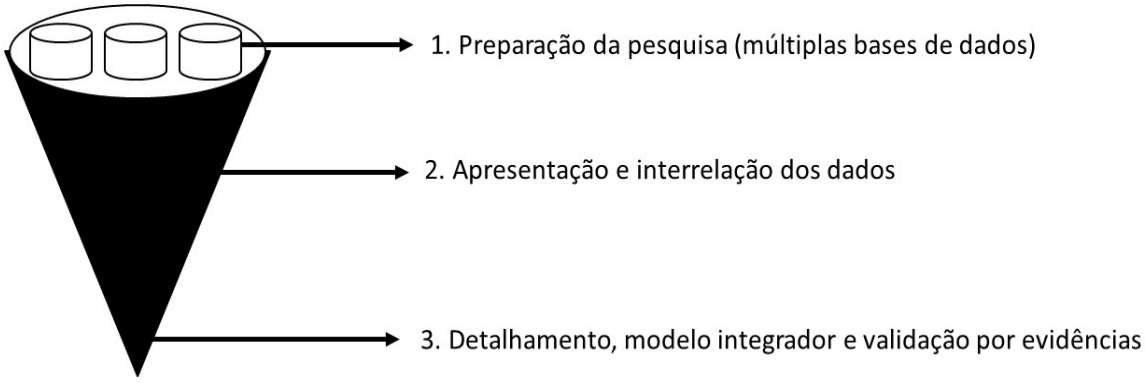
Como o trabalho consiste em uma revisão de literatura, cabe então escolher qual melhor revisão pode ser adotada para atingir os objetivos propostos neste projeto. Um tipo lembrado e visto em (MARIANO; SANTOS, 2017) é o de Teoria de Enfoque Meta Analítico Consolidado – TEMAC.

O enfoque meta analítico, é o que deu origem ao TEMAC, e diz que a amostra deve conter uma pesquisa qualitativa e quantitativa, tratando-se de um método feito em etapas, que segue critérios como impacto dos locais onde foram publicados, dos autores e a frequência de

palavras-chaves com o intuito de obter um conjunto de material a ser utilizado confiável, dando respaldo ao trabalho a ser realizado. E assim, em (MARIANO; SANTOS, 2017), o principal a ser avaliado no documento científico será então, precisão, robustez, validade, funcionalidade, tempo e custos.

Assim o TEMAC, veio a aumentar o raio de atuação, considerando que possa ser usada quantas bases de dados julgar necessária. É sempre importante, imaginar as etapas de forma clara e possuir todo o respaldo criado das teorias bibliométricas. "*O TEMAC está divido em 3 etapas: a. preparação da pesquisa; b. apresentação e interrelação dos dados; c. detalhamento, modelo integrador e validação por evidências*" (MARIANO; SANTOS, 2017) conforme Figura 22:

Figura 22: Cone de afunilamento proposto para o TEMAC.



Fonte: (MARIANO; SANTOS, 2017)

Vale ressaltar que a internet trouxe algumas mudanças, como a possibilidade de hoje se ter bancos de dados não mais vinculados a instituições, ganhando novos formatos sendo acessados em qualquer lugar a qualquer hora, em uma versão global. Um destes exemplos e que é utilizado para buscas de artigos, monografias e livros, pode ser trazido aqui com o Google Scholar (http://scholar.google.com), que foi muito utilizado neste trabalho; outro utilizado com muita recorrência nesse trabalho foi o IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp); assim como para complementar fora utilizado Scopus (https://www.scopus.com/home.uri).

A partir dos conceitos apresentados, o trabalho está dividido nas seguintes etapas:

1) Levantamento Bibliográfico Inicial

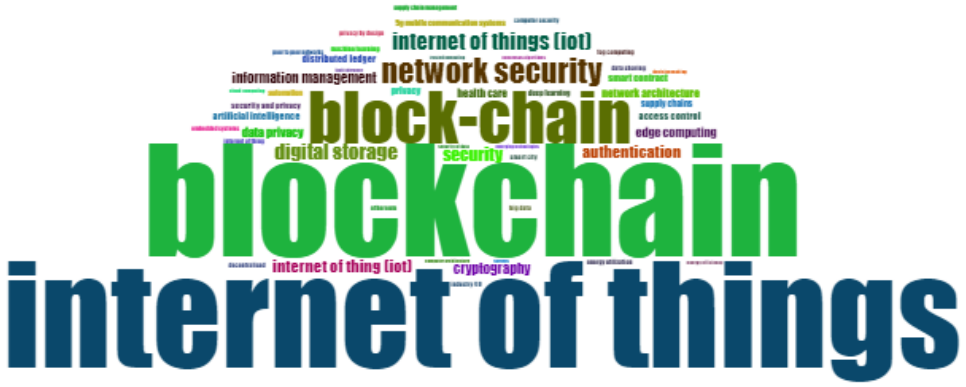
Foi utilizado o método TEMAC como referência para levantamento e organização das referências. Para isso, foram eleitas as palavras-chaves que melhor representaram as buscas como: *Blockchain and* IoT, *Blockchain security* IoT, *Blockchain cybersecurity* IoT,

Blockchain network IoT *solutions*, *Blockchain* segurança IoT, Redes IoT usando BC, Redes IoT, Uso do BC. Um outro campo muito relevante é o de espaço-tempo, que é crucial, geralmente é buscado de 5 a 10 anos, de 2016 início da pesquisa a 2024, em especial pelo caráter recente da tecnologia. Assim, após feitas as buscas, foram utilizados filtros criados pelo autor de acordo com o tema e escolhidos os mais relevantes (*BIoT, Security of IoT, Blockchain to IoT*), lei do 80/20, *"ampliação e redução de acervos de acordo com uso de 20% da informação por 80% dos usuários"* (MARIANO, A. M.; SANTOS, M. R., 2017).

A partir do programa integrado ao Google Sheets e Docs via extensão para o Google Chrome foi feita uma nuvem de palavras presente nos títulos dos vários artigos, livros e monografias escolhidos para ilustrar e a partir dela fazer um levantamento inicial da tratativa vista na etapa dois abaixo, onde foi visto a importância do autor e se atendia ao tema e aos objetivos escolhidos, sendo que as palavras chaves dos seus artigos foram inseridas no banco de dados usado no programa citado, visto na Figura 24.

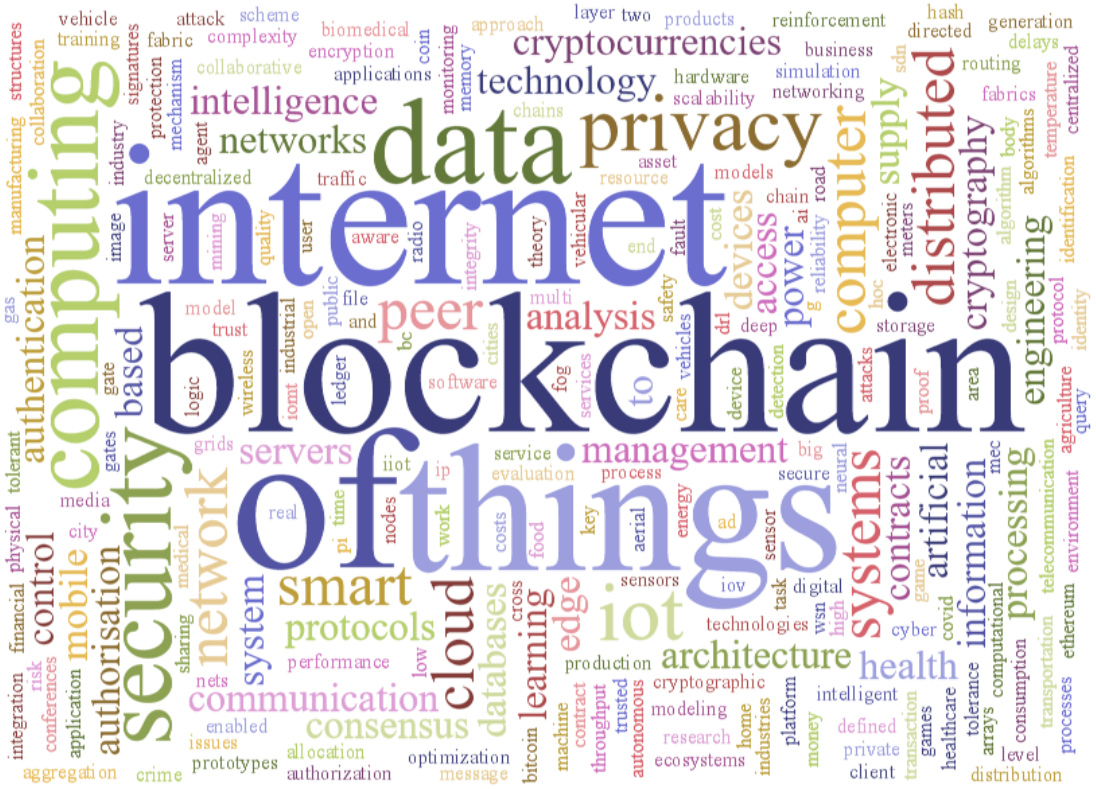
Foi usado também RStudio na versão 2022.12.0+353, que através da biblioteca "bibliometrix" foi possível reduzir ainda mais a nuvem com o mesmo banco de dados de informação sobre os artigos, agora já utilizando a regra aplicada pelo TEMAC, visto na Figura 23.

Figura 23: Nuvem de palavras utilizando o RStudio.



Fonte: Elaboração própria.

Figura 24: Nuvem de palavras utilizando Google Sheets.



Fonte: Elaboração própria.

2) Organização das Bibliografias

O uso do Excel aqui fora importante para separar em planilha: nome do autor, nome do trabalho, quantidade de citações, ano de publicação, tipo de estudo, ano de publicação e possível aproximação entre trabalhos e estudos. O Apêndice A apresenta a estrutura do mesmo e como estão organizadas em uma das colunas a lista de priorização para composição de relevância de uso neste trabalho. A coluna mãe que determina a busca dos artigos e monografias com maior relevância é a coluna F, porém a coluna C também é de suma importância para parametrizar a importância do autor dentro da comunidade acadêmica.

3) Estudo / Leitura dos artigos

O estudo e leitura teve início assim que foi definido o tema. Sempre seguindo os critérios adotados e descritos previamente nos tópicos anteriores, tendo sempre como prioridade aqueles que cruzem o nível de interesse a este trabalho de acordo com o proposto.

4) Filtro / Verificação / Eliminação

Conforme visto no item 2, o uso da planilha, visto no Apêndice A foi primordial para que fosse criado um filtro de validação, verificação e eliminação dos textos que iriam ser

utilizados. A eliminação ocorria quando não atingia os critérios conforme descrito acima, ou fugia relativamente do tema principal proposto, ou não se inseria dentro das nuvens de palavras obrigatória eliminatória feita após os primeiros passos. Atendendo os padrões estipulados, logo foi possível a verificação e inclusão, dada a relevância em termos de contribuição. Assim sendo, sempre que incluso uma nova obra, foi feita toda a análise e alimentado a planilha para que se tenha uma visão geral, caso não tivessem dentro dos padrões a eliminação ocorria.

5) Escrita e Conclusão

Quando feito a leitura, estudo e crítica dos textos escolhidos, também foram feitos resumos para que a escrita e a interpretação de relevância de cada um fossem parametrizadas. Por fim, a escrita e transcrição de forma analítica do que fora extraído para que o trabalho pudesse conter o que fora levantado e levado em consideração. A partir do tema principal e dando enfoque naquilo que fosse mais importante acerca do assunto, tratando cada passo textual, atentando-se aos textos de maneira singular e interpretativa.

3.3 TEXTOS ESCOLHIDOS

Conforme visto nos passos anteriores, o trabalho seguiu priorizando após ressalvas do TEMAC e escolhas conforme elucidado a seguir. Foram considerando todas as premissas estabelecidas na metodologia, seguindo o processo descrito no item 4 de filtragem, verificação e eliminação. Além disso, foi avaliada a relevância dos autores na comunidade acadêmica, como mencionado no item 2, onde se demonstrou, no Apêndice A, a organização das referências bibliográficas de acordo com o número de citações; o que assegura em partes a importância daquele trabalho e daquele autor, pois há uma validação dentro desta comunidade.

Com base nisso pode-se validar que os artigos precisavam ter nota 5 na coluna F do Apêndice A, e em concomitância com a coluna C em que apresenta o número de Citações atualizadas, mas também tiveram que ser feitos considerações sobre o assunto e a forma que as arquiteturas e soluções eram apresentadas, pois em alguns casos foi visto que alguns trabalhos tinham qualidade para serem abordados de forma a corroborar, mesmo tendo um número menor de citações por exemplo.

Exemplos de artigos considerados como cruciais e de muita importância dentro dos paramentos principais discutidos anteriormente: "*An agri-food supply chain traceability system for China based on RFID & Blockchain technology* (TIAN, Feng., 2016. p. 1-6.)" que

possui 2006 citações e foi considerado para o trabalho com 5 de nota de importância, assim como "*Blockchain meets IoT: An architecture for scalable access management in IoT* (NOVO, Oscar, 2018)" com 1550 citações e com a mesma qualificação. Em contrapartida os artigos "*A Permissioned Blockchain based Access Control system in iot* (ISLAM, A.; MADRIA, S. K., 2020)", "*A Blockchain Proxy for Lightweight IoT Devices* (DITTMANN G.; JELITTO, J., 2019)", "*Blockchain IoT (BIoT) A New Direction for Solving IOT security and trust issues* (URIEN, P, 2018)" e "*Collaborative threat intelligence: Enhancing IoT security through Blockchain and machine learning integration* (NAZIR, A; et. all, 2024)", os quais apresentam um número de citações abaixo de cem, porém são tão importantes para estruturação de como foram sendo propostas as arquiteturas nos últimos anos, sendo classificados com 5 para analise deste trabalho.

Os temas principais discutidos entre os artigos foram: Segurança e Confiança em IoT são Desafios Significativos; BC como Ledger Distribuído para Dados de IoT; Uso de *Smart Contracts* para Lógica de Negócios e Controle de Acesso; Autenticação e Integridade de Dados; Gerenciamento de Confiança e Reputação; Controle de Acesso Baseado em Atributos (ABAC); Uso do Hyperledger Fabric; Integração com Aprendizado de Máquina (ML – *Machine Learning*); Desafios de Desempenho e Escalabilidade; e por fim Aplicações Práticas. A partir daqui foi possível escolher os que seriam trabalhados e quais foram eliminados, pois, como o TEMAC salienta é importante usar a lei do 80/20 de acordo com o público sob a perspectiva do trabalho proposto.

Esses pontos em comum demonstram um reconhecimento geral do potencial da tecnologia BC para resolver os desafios de segurança e confiança no ecossistema do IoT, oferecendo soluções para autenticação, integridade de dados, controle de acesso e gerenciamento de confiança. A combinação da BC com outras tecnologias, como ML, é vista como uma direção promissora para aprimorar ainda mais a segurança da IoT. Estes trabalhos serão apresentados no próximo capítulo de Resultados individualmente.

Assim, com os artigos escolhidos, foi possível mostrar em tabelas e quadros os pontos congruentes, abordar as perspectivas de cada solução, verificar as aplicações atuais praticadas e soluções que estão em desenvolvimento a partir de conceitos que cada autor projetou.

3.4 RECURSOS

Foram utilizados basicamente a Internet e buscadores de artigos e monografias conforme descritos em 3.1, da Metodologia, além da leitura de livros sobre o assunto. Uso de ferramentas da Microsoft Office, como Word e Excel, do Google, Docs e Sheets, além da

versão gratuita do Adobe Reader. Os livros e demais referenciais bibliográficos foram escolhidos os com disponibilidade gratuita em formato PDF. Foi utilizado o Power BI sob a licença de uso em desktop, sem permissão de publicação pública para acessos de terceiros.

3.5 CONSIDERAÇÕES FINAIS

É sempre importante escolher o melhor método a ser seguido para que se tenha um bom resultado científico no final do trabalho e foi buscando este proposito que foi feito a escolha apresentada para que se consiga atingir o objetivo final quando este trabalho for concluído.

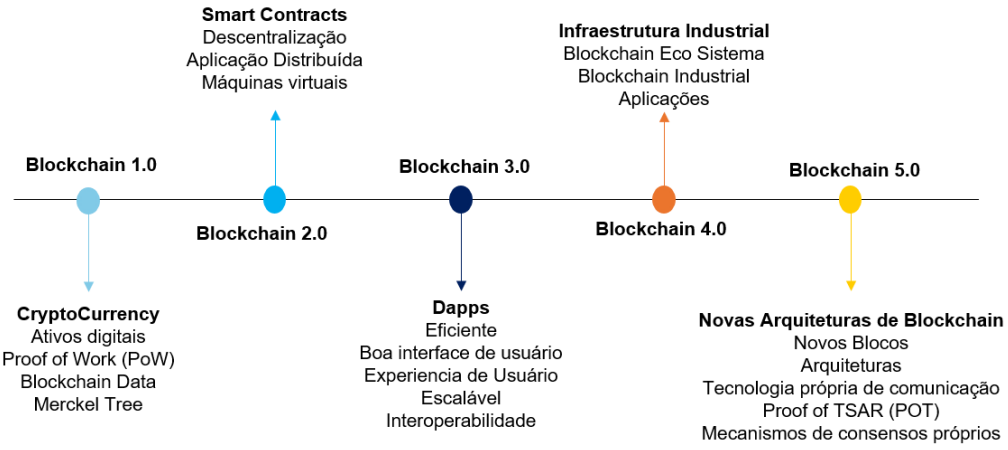
4 RESULTADOS

Neste capítulo será apresentado os artigos de projetos em desenvolvimento para as soluções BIoT, com análises de quais tem sido citado e correlacionado em outros trabalhos, mostrando aplicações nas mais diversas áreas. Ainda ter-se-á o cuidado de aprofundar no futuro daquelas propostas que estão em desenvolvimento.

4.1 AMBIENTAÇÃO PARA O BIOT

A tecnologia BC pode ser aplicada em muitas áreas de uso, a sua aplicabilidade e evolução começou com Bitcoin (BC 1.0), então evoluiu para contratos inteligentes (BC 2.0) e posteriormente mudou-se para aplicativos de justiça, eficiência e coordenação (BC 3.0), como lembra (FERNÁNDEZ-CARAMÉS, 2018). Como observa-se na Figura 25, o BC já está na etapa de Nova Arquitetura com novos blocos e uma tecnologia de comunicação de prova e contraprova, novos mecanismos de consenso.

Figura 25: Desenvolvimento do *Blockchain.*



Fonte: adaptado de (OBAIDAT, M.; RAWSHDH, M.; ALJA´AFREH, M.; ABOUALI, M.; THAKUR, K.; KARIME, A., 2024)

Vitalik Buterin ao desenvolver a rede Ethereum em 2013, expandiu o potencial da tecnologia. Ela é indiscutivelmente a plataforma mais popular baseado em BC para execução de contratos inteligentes, embora possa realmente executar outros aplicativos distribuídos e interagir com mais de um BC. Na verdade, a Ethereum é caracterizada como sendo um Turing completo, que é um conceito matemático que indica que a linguagem de programação da Ethereum pode ser usada para simular qualquer outro idioma (FERNÁNDEZ-CARAMÉS, 2018). Esses contratos podem ser aplicados em diferentes áreas, inclusive onde os aplicativos

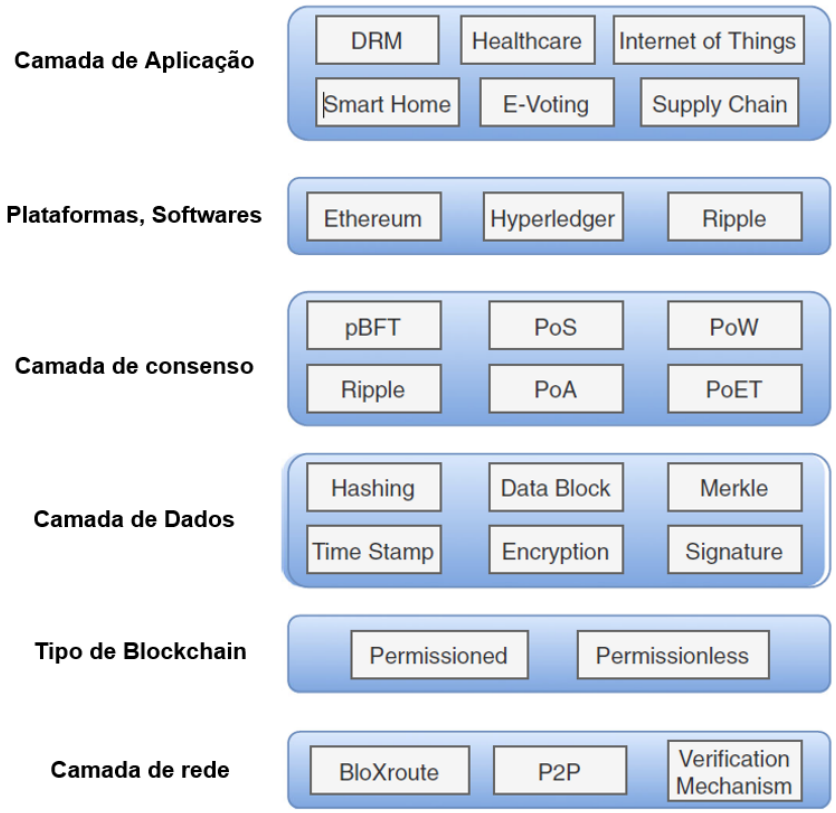
IoT estão envolvidos. Permitindo a criação de aplicações descentralizadas (dApps) e contratos inteligentes. (OBAIDAT, M.; RAWSHDH, M.; ALJA´AFREH, M.; ABOUALI, M.; THAKUR, K.; KARIME, A., 2024)

Em relação aos contratos inteligentes, eles são definidos como peças de código descentralizado autossuficiente que são executados autonomamente quando certas condições são satisfeitas. Contratos inteligente podem ser aplicados em muitos casos práticos, incluindo transferências internacionais, hipotecas ou *crowdfunding*.

Após 2021, a tecnologia vem abrangendo o metaverso, a infraestrutura industrial e um ecossistema robusto, que levou a BC 5.0, que se concentra em avanços no controle de identidade e acesso, confia em mechanismos, e tecnologia de comunicação, incluindo a antecipação e adaptação à segurança e preocupações com a privacidade de eras futuras.

Uma maneira de apresentar as camadas do BIoT de forma geral, com os vários tipos de protocolos e aplicações pode ser a vista na Figura 26, em que resumo uma maneira visual de como a maior parte dos trabalhos aplicados pelo tema tem seguido:

Figura 26: Arquitetura atualizada para BC.



Fonte: adaptado de (DWIVEDI, A.; SINGH, R.; KAUSHIK, K.; MUKKAMALA, R.R.; ALNUMAY, W. S., 2021)

4.2 AUTORES E TRABALHOS

Conforme apresentados as considerações no item 3.3, os trabalhos escolhidos são apresentados na Tabela 4 para a análise revisional conforme metodologia descrita no capítulo anterior, visando a verificação da aplicabilidade e dificuldades que o BIoT tem encontrado nos estudos para desenvolvimento de sua implementação.

Tabela 4: Comparação da literatura principal sobre integração de IoT e BC.

Autores	**Título**	**Contribuição principal**	**Soluções propostas**	**Palavras chaves**
URIEN, P.	*Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues.*	Utilizando o BIoT, testou protocolos comuns as tecnologias, para comunicações com firewall via WiFi, na ideia de usar na camada de transporte, o protocolo TLS/DTLS.	Uma nova arquitetura de transação entre objeto e rede BC, baseado em Ethereum, de acordo com cálculos de gastos computacionais.	*Blockchain; Internet of Things*; segurança
NAZIR, et al.	*Collaborative threat intelligence: Enhancing IoT security through Blockchain and machine learning integration*	Através da combinação de adaptações nas camadas para aumentar a segurança do IoT, com relação aos usuários de ecossistema iOS.	A central de controle de dispositivos dos aparelhos comandados por iOS, utilizariam Machine Learning em conjunto com a rede BC e assim lidaria mais eficiente contra as ameaças.	*Internet of Things Machine learning Ensemble learning* IoT Segurança *Blockchain* iOS
TIAN, Feng.	*An agri-food supply chain traceability system for China based on RFID & Blockchain technology*	Explora a aplicação combinada de RFID (Radio-Frequency Identification) e tecnologia BC para aprimorar a rastreabilidade e segurança na cadeia de suprimentos	Detalha o processo de implementação do sistema de rastreamento em cada etapa da cadeia de suprimentos, desde a produção até a venda ao consumidor, visando garantir a autenticidade das informações.	*Suply chain* Sistema de rastreamento RFID *Blockchain* Controle alimentar
ISLAM, A.; MADRIA, S. K. A	*A Permissioned Blockchain based Access Control System for IOT*	Fazendo uso de contratos inteligentes, implementam controle de acesso (ABAC - attribute based access control), para o controle de acessos dos nós.	Visibiliza uma nova arquitetura permissionada com a utilização da rede Hyperledger Fabric	IoT, *BC*, Controle de Acesso
DITTMANN G.; JELITTO, J.	*A **Blockchain** Proxy for Lightweight IoT Devices*	Usando uma abordagem em que a rede BC com identidade baseada em PKI faz o gerenciamento dos dispositivos IoT.	Através do Hyperledger Fabric, verifica a criação de uma transação em que os *peers* façam o consenso e criem assinaturas.	***Blockchain***, IoT, certificado de autoridade

Fonte: Elaboração própria.

Tabela 4: Comparação da literatura principal sobre integração de IoT e BC.

Autores	Título	Contribuição principal	Soluções propostas	Palavras chaves
MALIK, Sidra et al.	*TrustChain: Trust Management in Blockchain and IoT supported Supply Chains*	Propõe uma estrutura de gestão de confiança de três camadas baseada em BC para cadeias de suprimentos.	A novidade do *TrustChain* seria um modelo de reputação, com o uso de contratos inteligentes Sobrecarga mínima em termos de latência e *throughput* em comparação com um modelo simples de cadeia de suprimentos baseado em *BC*. Camadas de dados, *BC* e aplicação bem definidas.	*Suply chain* *Blockchain* permissionado *Trust Management Systems* Baseado em reputação Arquitetura em Camadas
NOVO, O.	*Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT*	Baseando-se em uso de redes Ethereum, e a partir do uso da implementação de PoC para um sistema de controle de acessos via *smart contracts*.	Uma das diferenças das propostas anteriores é o uso da biblioteca CoAP para as aplicações IoT na tentativa de abranger o *benchmark* de uso.	Controle de Acesso, *Blockchain*, *Internet of Things* (IoT), *smart contracts*
DEDEOGLU, Volkan et al.	*A trust architecture for Blockchain in IoT*	Propõe uma arquitetura em camadas para melhorar a confiança de ponta a ponta em aplicações de IoT baseadas em BC, onde os nós da rede podem não confiar uns nos outros.	A arquitetura proposta visa avaliar a confiabilidade das observações dos sensores na camada de dados e adaptar a verificação de blocos na camada. Arquitetura em Camadas	*Blockchain* IoT *data trust* Baseado em reputação *Distributed Consensus* Arquitetura em Camadas
WAZID, Mohammad et al.	*Security in 5G-Enabled Internet of Things comunication: issues, challenges, and future research roadmap*	Oferece uma visão geral abrangente sobre a segurança em ambientes de comunicação IoT habilitados por 5G.	Um dos focos principais do artigo é a categorização e análise dos protocolos de segurança propostos para o ambiente 5G-IoT.	5G IoT Privacidade e segurança Chave de segurança Autenticação Controle de Acesso Detecção de intruso

Fonte: Elaboração própria.

Como modo de comparar a maneira que cada autor foi pensando suas arquiteturas, tem-se a Tabela 5, que demonstra que mesmo nesta pequena amostra de artigos uma preferência por uma abordagem de uso de algumas tecnologias em particular, que é por exemplo o uso em quase todos os trabalhos de *smart contract* diferenciando a maneira como subdivide sua aplicação.

Tabela 5: Comparativo por autor por tecnologias utilizadas nas arquiteturas.

Autores	Ano	*Smart Contract*	Hyperledger Fabric	Controle de Acesso	*Machine Learning*	Reputação / Consenso	Arquitetura de Camadas
URIEN, P.	2018	✓				✓	
NAZIR, et al.	2024	✓			✓		
TIAN, Feng.	2016	✓				✓	
ISLAM, A. et al.	2019	✓	✓	✓			
DITTMANN G et al.	2019	✓	✓			✓	
NOVO, O.	2018	✓		✓			
MALIK, Sidra et al.	2019	✓		✓		✓	✓
DEDEOGLU, Volkan et al.	2019	✓		✓		✓	✓
WAZID, Mohammad et al.	2020	✓		✓		✓	

Fonte: Elaboração própria.

Considerando então os autores citados, foi feito um levantamento de cada arquitetura destacadas abaixo, explicitando a forma que os autores trabalharam as suas propostas diante do assunto.

4.3 ARQUITETURAS E PROPOSTAS REVISIONADAS DOS AUTORES:

De acordo com (URIEN, P. 2018) a ideia central do BIoT é inserir dados de sensores em transações BC, conforme traz o autor. O artigo destaca que os objetos IoT não estão logicamente conectados às plataformas BC, necessitando de entidades controladoras para encaminhar as informações necessárias para a criação de transações. Os objetos precisam de recursos de computação confiáveis, como os elementos seguros integrados na Arquitetura de Quatro Quartos proposta em trabalhos anteriores ao dele, como ele salienta. Esta arquitetura inclui uma GPU, um SoC de rádio, sensores/atuadores e elementos seguros com *stacks* TLS/DTLS, onde os microcontroladores seguros também gerenciam as bibliotecas criptográficas (URIEN, P. 2018).

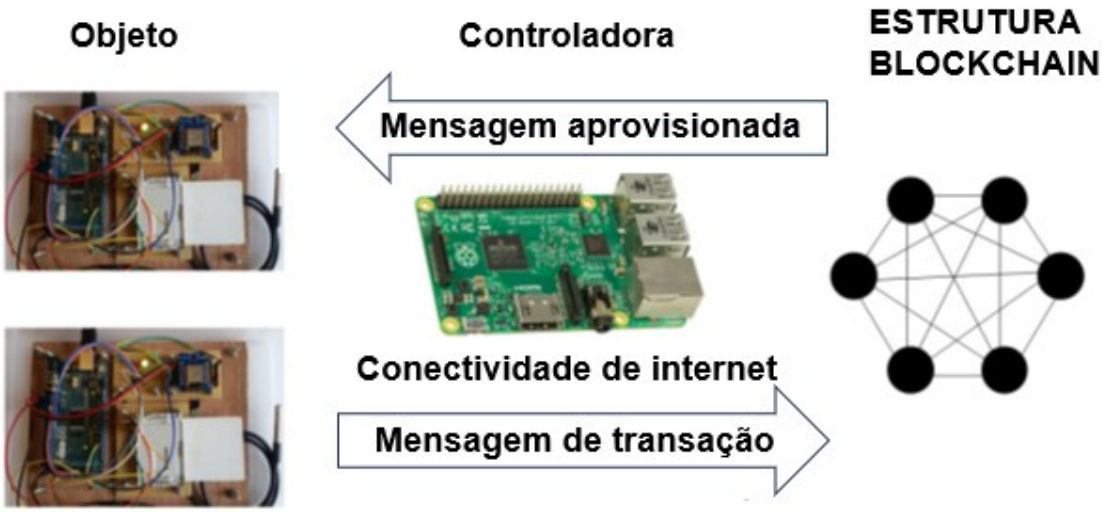
Com essa premissa ele propõe uma arquitetura que faz o encontro das estruturas do IoT com o BC, utilizando algoritmo de consenso aplicado para ordenação de criação de blocos (principal ideia utilizada a de mineração), e se valendo da certificação de blocos com os algoritmos de PoW e PoS. Teve seu experimento baseado em uma rede a partir da Ethereum, com tarifa de transação inclusive pautada nesta, definido por: "*gasPrice* = 21000 + tamanho_dado_bytes x preço_por_byte" (URIEN, P. 2018). Ideia inicial apresentada é a de encapsular os dados de um sensor dentro de transações BC, que seriam gravadas usando o formato RLP (*Recursive Length Prefix*). O autor cita que para os testes foram gastos 68

SATOSHIs por byte para dados não nulos, 4 para nulos e uma taxa de transferência igual a 15.

Toda aplicação com conexão pela internet será protegida pela camada de gravação com o TLS. Assim quando o os dados forem ser gravados no *ledger*, teriam outra camada de proteção. Após guardados por chaves privadas e identificadas por seus endereços e administradores com acesso à internet. Esses, teriam controle do banco de dados composto no *ledger* e de lá poderiam resgatar informações.

Assim, ilustra-se com a Figura 27, o fato de que como objeto não faz parte de cadeia de contexto de dados usuais para o BC, é necessário um controlador (Arduino por exemplo), na visão do autor, para fazer o papel intermediário como aprovisionador da mensagem (URIEN, P. 2018).

Figura 27: Exemplo de uma transação usando Ethereum com proposito IoT.



Fonte: adaptado de (URIEN, 2018).

Em acordo com (NAZIR et al., 2024), um dos mais recentes artigos utilizados neste trabalho, os autores abordam uma nova forma para melhorar a segurança do IoT através da inteligência colaborativa contra ameaças, integrando a tecnologia BC com modelos de ML e um aplicativo iOS atuando como um centro de controle. Conceitualmente os autores apresentam a forma que pensaram com que o aumento de credibilidade e segurança, em que essa central faria validações e transações completas, validadas pela rede, mas ao mesmo tempo as três pontas do sistema estariam conectados em ML para que erros já corrigidos não

retornem, incrementando uma maior classificação de tentativas de ataques e suporte a expertises em segurança dado pela ferramenta, diminuindo os falsos positivos/negativos.

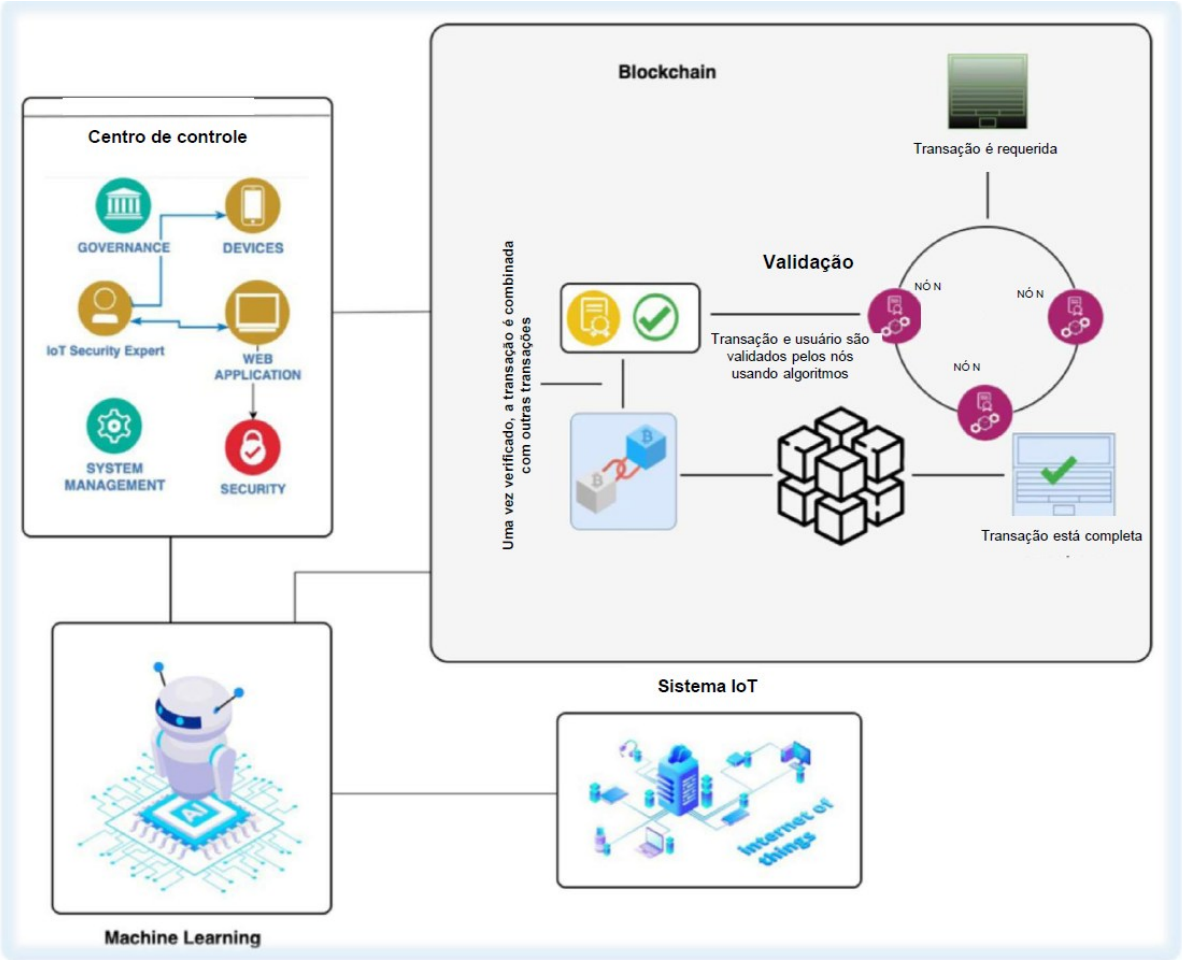
Para enfrentar os desafios de ameaças e a crescente de dispositivos interconectados, os autores propõem um *framework* inovador, o CTIF-IoT (*Collaborative Threat Intelligence Framework for IoT Security*), que combina o poder dos algoritmos de ML, um aplicativo iOS como centro de controle e a tecnologia BC (NAZIR et al., 2024). E para isso conseguiu-se listar que os principais componentes e funcionamento deste *framework* está nas particularidades como:

- Ecossistema do IoT fácil de integrar ao intermediador;
- Camada de aprendizado com ML, que é capaz de monitorar o tráfego initerruptamente, criando os padrões de anomalias caso ocorram;
- Os modelos de ML citados pelos autores utilizados *Random Forest, Decision Tree, Ensemble, LSTM e CNN*, treinados com o *dataset* IoT23;
- Centro de Controle iOS: Atua como um hub de comunicação entre a Camada de ML e o homem. Alertas de potenciais ameaças detectadas pela ML são enviados como notificações *push* da Apple para especialistas em segurança. O aplicativo também permite o relato de ameaças e interação com os modelos de ML;
- **BC:** Funciona aqui para registrar incidentes de segurança validados. Quando uma ameaça é confirmada, os dados relevantes são transmitidos de forma segura para a BC usando contratos inteligentes. A BC garante a integridade e a transparência dos dados de ameaças;
- Com o ciclo de *Feedback* alimentado por especialistas que fiscalizam a cadeia, junto ao aprendizado da máquina, os algoritmos de ML analisam o *feedback* armazenado na BC para melhorar sua precisão na identificação de ameaças e minimizar alarmes falsos. (NAZIR et al., 2024)

O fluxo de informação sempre tem início dentro do *framework* quando os dados são gerados em algum dispositivo IoT como ilustra a Figura 28, deixando o aplicativo iOS com o papel de atuar como uma interface intuitiva para usuários monitorarem e gerenciarem a segurança IoT, recebendo alertas em tempo real e permitindo a validação de ameaças. É após a conexão com o dispositivo que a rede vai aprender de forma interconectada como mostra a figura, quais padrões, e classificar os incidentes em tempo real. A partir, do uso *smart contracts* os autores (NAZIR et al., 2024) utilizaram-se de uma rede no modelo Ethereum

onde os dispositivos eram registrados a partir de suas características, funções. O *framework* seria altamente colaborativo quando o assunto é inteligência contra ameaças.

Figura 28: Conceito do *framework* proposto pelos autores.



Fonte: adaptado de (NAZIR et al., 2024).

Segundo a análise dos autores, o resultado foi de um aumento de assertividade da ML para o modelo proposto, quando se treina, simbolizando uma validação excelente para identificar atividade criminosas de alto risco na internet.

A partir do artigo de (TIAN, Feng, 2016), o autor traz a discussão a preocupação com a segurança alimentar na China devido a problemas persistentes e à inadequação do sistema logístico tradicional. Propõe um sistema de rastreabilidade da cadeia de suprimentos de produtos agrícolas baseado em tecnologias RFID combinado com BC para aumentar a segurança reduzir as perdas logísticas. Segundo o autor o RFID é uma boa escolha por algumas razões, como a de se poder etiquetar, salvar e gerenciar informações de objetos através de sinais de radiofrequência e possui vantagens como conveniência, resistência à poluição, grande capacidade de informação e ser passível de reciclagem. Este tipo de

tecnologia já é utilizado na logística para rastreamento, gerenciamento de armazéns e combate à falsificação e furto.

O sistema proposto pelo autor para aumentar a rastreabilidade utiliza a RFID para a aquisição, circulação e compartilhamento de dados nas diversas etapas da cadeia de suprimentos dos produtos, desde a etapa inicial até a venda. A tecnologia BC entraria para garantir que as informações compartilhadas no sistema sejam confiáveis e autênticas. O sistema abrange empresas em toda a cadeia de suprimentos, bem como centros de supervisão de segurança alimentar, como órgãos governamentais e reguladores terceirizados. Isso permite o rastreamento e o monitoramento em toda a cadeia, facilitando a identificação da origem de problemas de segurança alimentar e a tomada de medidas emergenciais.

O sistema proposto apresenta várias vantagens:

• Para o gerenciamento de rastreabilidade, criando uma cadeia de informações transparente para todos os membros da cadeia de suprimentos, desde o produtor até o consumidor;

• No aumento da credibilidade das informações de segurança alimentar, eliminando a necessidade de uma organização centralizada confiável e fornecendo uma plataforma aberta, transparente, neutra, confiável e segura;

• Benefícios no combate a produtos falsificados, protegendo os produtos com IDs únicos de *tags* RFID e tornando as informações imutáveis graças à BC (TIAN, Feng, 2016).

No entanto, o sistema também apresenta desvantagens:

• O alto custo das *tags* RFID em comparação com os códigos de barras e o investimento necessário em equipamentos e atualização de sistemas. Para reduzir custos, a RFID pode ser aplicada principalmente em paletes e embalagens em vez de em cada produto individual;

• A imaturidade da tecnologia BC, com limitações na capacidade de transação e desafios no gerenciamento do crescimento contínuo do tamanho do BC (TIAN, Feng, 2016).

Basicamente o autor em 2016 procurava mostrar uma aplicabilidade para que outras futuras arquiteturas pudessem surgir.

De acordo com (ISLAM, A.; MADRIA, S. K. A, 2019) os sistemas tradicionais de controle de acesso para IoT são centralizados e não incluem todos os stakeholders no processo de tomada de decisão. Para resolver essa lacuna, os autores desenvolveram um sistema onde a criação de políticas de acesso e a tomada de decisões de controle de acesso ocorrem com o consenso de todos os stakeholders. Assim eles projetaram e implementaram o ABAC em uma BC permissionada chamada *Hyperledger Fabric*, aproveitando seus *smart contracts* e consenso distribuído para habilitar um controle de acesso distribuído para IoT.

As BC*s* públicas ou sem permissão, como Bitcoin e Ethereum, sofrem de problemas de escalabilidade. Já as privadas ou permissionadas oferecem transações mais rápidas, utilizando protocolos de consenso mais rápidos, como o *Byzantine Fault Tolerance* (BFT), e são mais adequadas para controle de acesso em IoT segundo (ISLAM, A.; MADRIA, S. K. A, 2019).

O sistema proposto utiliza uma BC permissionada e implementa o ABAC através de *smart contracts*, que é considerado mais adequado para o ambiente diversificado de IoT do que outros mecanismos de controle de acesso. A arquitetura do sistema consiste em redes IoT locais e a BC permissionada. Os principais atores são o provedor/proprietário do recurso e o solicitante. O modelo ABAC define atributos com nome, tipo e valor. Quatro tipos de atributos são considerados: sujeito, recurso, ambiente e ação. As políticas são expressas como expressões booleanas de atributos e seus valores. A avaliação da política envolve a verificação da satisfação das expressões de valor dos atributos e das expressões dos atributos em si. **(**ISLAM, A.; MADRIA, S. K. A**, 2019)**

A implementação ABAC em *Hyperledger Fabric* envolve a formação da rede BC com múltiplas organizações gerenciadas por MSPs (***Managed Service Provider*)**, o gerenciamento de atributos envolve criação e atribuição, com o *AttributeMgr smart contract* garantindo a unicidade dos atributos.

Em uma arquitetura proposta discutem um sistema por setor, onde é descrito que existem atores que atuam e para funcionar dispõe-se de uma rede IoT e recursos de acesso e requisição, que podem ser externos ou não. Isso então seria definido por Requisição de Acesso, onde após fazer a requisição, uma autorização é solicitada para a transação x, entre a requisição a rede e o gateway é avaliada os *smart contract* e as políticas marcando a transação como aprovada/rejeitada através de protocolos de consenso. A rede de blocos, envia uma transmissão de Tx e quando o gateway verifica Tx e recupera uma chave k de Tx, ela responde com x, o nó então conhece Tx e entrega ao dispositivo IoT. Isso é também conhecido como *Resource Access Process by the Requester*. **(**ISLAM, A.; MADRIA, S. K. A**, 2019)**

Utilizando implementação em *Hyperledger Fabric*, os autores afirmam que como é também uma BC baseada em *smart contract* ela seria capaz de validar e não validar os *peers* e tudo depende da maneira que será apresentado o uso da ferramenta desenvolvida. Por exemplo empresas como Google, Amazon e outras que provem serviços baseados em IoT podem ser elas mesmas as figuras autoritativas nas redes de BC dos serviços que disponibilizarem. Ou mesmo casos de *smart, homes, cities, farms* e outros.

No caso deste artigo, os autores citam o uso do *Policy Evaluation* uma lógica implementada para *smart contract* chamada de *Access Control Decision Maker* (ACDecMaker*)* que endossa a responsabilidade aos *peers* de transação de solicitação de acesso a recursos Tx. **(**ISLAM, A.; MADRIA, S. K. A**, 2019)**

Durante os experimentos dos autores e analisando os graficos por eles apresentados é visto que a latencia do tempo de resposta entre as requisições é melhorada significativamente e a criação de novos blocos também foi satisfatória. Porém, estão limitados a transações com altas taxas de latência, para altas taxas ficaria horas em requisição.

Já com (DITTMANN G.; JELITTO, J., 2019) a abordagem sugerida pelos autores assume que o uso do BC baseado em PKI para dispositivos IoT leves, seguindo a SDK (*Software Development Kit*) da rede que verifica que o certificado de autoridade (CA) é registrado na rede, estabelecendo então o provedor de identidade confiável através dos *peers* da BC. Então, para CA fica a cargo identificar uma chave privada e assinar a transação ao bloco. Por exemplo um sensor em uma cadeia de suprimentos que acompanhe a localização e gerencie o embarque em determinadas datas. Os sensores podem prover os dados e relatar o que ocorreu caso tenha algo errado.

O ativo criado a ser protegido são os dados coletados pelo dispositivo IoT, que devem ser invioláveis. A chave privada do dispositivo também é um ativo crítico. O sistema passa a confiar nos nós da BC para autenticar e confirmar transações válidas de forma imutável, e na CA para emitir credenciais apenas para dispositivos confiáveis. É visto também as ameaças físicas, troca de dispositivos, alterações que descaracterizem o dispositivo, manipulação de dados em trânsito, ataques DDoS, ataques *man-in-the-middle* e *replay attacks* (DITTMANN G.; JELITTO, J., 2019). A assinatura do dispositivo impede a adulteração dos dados em trânsito.

A implementação sugerida por eles, é a partir do *Fabric Proxy* desenvolvido para *Hyperledger Fabric*, uma BC permissionada que contêm pré-ordem de execução e separação entre os nós, *peers.* Partindo da ideia de a aplicação IoT envia de maneira fluida para os *peers* do Fabric por meio Fabric Proxy. Assim a aplicação mantém o Proxy SDK do Fabric em execução, assim é enviado um Tx, que é transmitido pela Proxy aos nós e é verificada a autenticidade, simulada a assinatura da proposta de resposta. É então retornada a resposta entre a Proxy e Proxy SKD. Todas as respostas têm assinaturas Tx gravadas e, portanto, rastreáveis. (DITTMANN G.; JELITTO, J., 2019)

O objetivo do Proxy é reduzir o poder de computação e largura de banda consumida por transações BC em um dispositivo IoT. Os resultados mostram economias significativas para o

dispositivo IoT em tempo de CPU (38%), dados enviados (21%) e dados recebidos (81%). Os testes foram realizados em um *laptop*, assumindo uma escala linear para processadores IoT mais fracos. (DITTMANN G.; JELITTO, J., 2019)

Neste artigo, os autores (MALIK, Sidra et al**,** 2019) propuseram o *TrustChain*, um *framework* de gestão de confiança idealizado em três camadas, baseado em BC de consórcio para rastrear interações entre participantes da cadeia de abastecimento e atribuir dinamicamente pontuações de confiança e reputação com base nessas interações. O artigo argumenta que, embora a tecnologia melhore a rastreabilidade e a imutabilidade nas cadeias de abastecimento, ela sozinha não resolve o problema da confiança nos dados.

O *TrustChain* visa abordar a falta de confiança nos dados registrados dentro dos blocos em cadeia dentro do BC em relação à qualidade das mercadorias e à confiabilidade das entidades em participação. Os sistemas de reputação existentes não são adequados para aplicações de gestão onde os participantes precisam gerenciar uma cadeia de abastecimento baseadas em BC devido a observações limitadas, falta de granularidade e automação, e questões de *overhead* não exploradas, conforme explora os autores.

O modelo proposto partiria do princípio onde a reputação seria avaliada e a qualidade das mercadorias e a confiabilidade das entidades com base em múltiplas observações de eventos. Seguido de um suporte para pontuações das reputações separadas entre um participante de cadeia de abastecimento e os produtos, conduzindo uma técnica onde geraria especificidades para diferentes tipos de ofertas do mesmo participante.

O uso do *smart contracts* para cálculos transparentes, eficientes, seguros e automatizados destas reputações acelera o processo de avaliação. Possuindo então uma sobrecarga mínima em termos de latência e *throughpout* em comparação com um modelo simples (MALIK, Sidra et al**,** 2019).

Quanto ao *framework TrustChain* as estruturas de três camadas podem ser vistas na Figura 29 abaixo em que se observa as seguintes divisões sugeridas pelos autores (MALIK, Sidra et al**,** 2019):

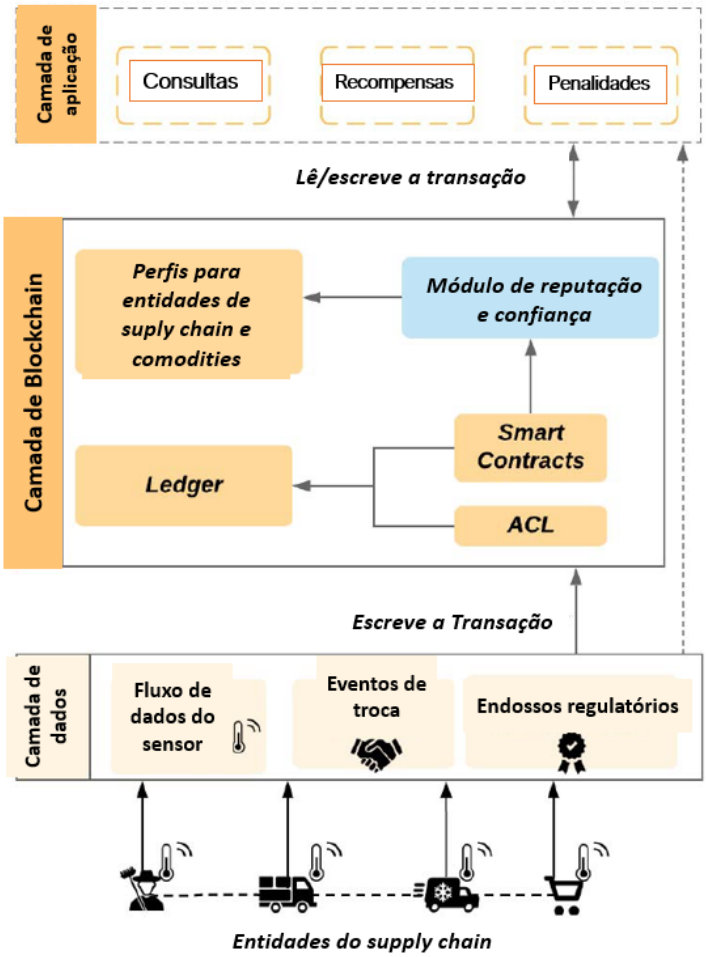
Camada de Dados: Envolve dados da cadeia de abastecimento produzidos por sensores IoT, eventos de negociação entre entidades e endossos regulatórios. Os dados brutos podem ser armazenados fora da cadeia, enquanto os resumos de mensagens dos dados são enviados para a camada BC como transações.

Camada BC: As transações são armazenadas no *ledger* e processadas seguindo regras de acesso definidas por uma Lista de Controle de Acesso (ACL). Os *smart contracts* são invocados pelas transações para gerar reputação e valores de confiança para entidades e

classificações de qualidade para mercadorias. Essas pontuações são armazenadas nos perfis digitais de entidades e mercadorias na BC.

Camada de Aplicação: Interage com a camada BC por meio de consultas. Administradores e reguladores consultam as pontuações de confiança e qualidade. Recompensas e penalidades são acionadas com base nessas pontuações.

Figura 29: Estrutura de três camadas do Framework TrustChain



Fonte: adaptado de (MALIK, Sidra et al, 2019)

Conforme dito anteriormente o *TrustChain* utiliza *smart contracts* para automatizar o cálculo das classificações para entidades e mercadorias. Existem dois tipos principais de *smart contracts* propostos para a aplicação neste artigo de acordo com (MALIK, Sidra et al**,** 2019):

Contrato de Qualidade: Instalado para cada mercadoria, define critérios de avaliação de qualidade (por exemplo, limites de temperatura) e gera notificações de aviso e pontuações de reputação da mercadoria (*Repsens*(t)) com base nos dados do sensor (TX*sens*). A pontuação final de qualidade da mercadoria (R*sens*) é gerada quando a mercadoria chega ao varejista (TX*rec*).

Contrato de Avaliação: Computa a reputação do vendedor (R*epseller*(t)) para um evento de negociação (TX*tr*) com base em três entradas: reputação da mercadoria (R*epsens*(t)), avaliação do regulador (R*epreg*(t)) e avaliação do comprador (R*eptrader*(t)). Essa reputação pode ser calculada como uma soma ponderada.

Um módulo de reputação e confiança agrega as pontuações de reputação calculadas pelos *smart contracts* e utiliza um modelo de confiança variável no tempo para calcular a pontuação de confiança geral de um *trader* (T*trader*(tn)). Eventos recentes têm maior peso nesse cálculo. A pontuação de confiança também pode levar em consideração outros recursos específicos da aplicação. O *TrustChain* foi implementado como uma prova de conceito usando o *Hyperledger Composer* (MALIK, Sidra et al**,** 2019).

Para o (NOVO, O., 2018), é possível baseando-se na ideia de centros de gerenciamento para as redes descentralizadas criadas a partir de *smart contracts,* sensores e dispositivos presentes em um sistema IoT poderiam se comunicar com a rede BC através de protocolos de comunicação como CoAP que suportam canais seguros através de DTLS. Os centros assinalados, seriam dispositivos entidade IoT que seriam identificados no sistema por suas chaves públicas. Assim sendo, os recursos conseguiriam identificar seus nomes, consentindo permissão ou prevenindo checagens, modificações ou execuções através de operações do *AddAccessControl.*

O como na arquitetura proposta em que agente M1 administra a rede, ele fixa no *smart contract* os registros de M1 registra S1 (adicionando um novo dispositivo S1 registrado como fonte R1) sob a solicitação do M1, as informações são inseridas no *smart contract*. Por mineração é encontrado o endereço e através da tradução de CoAP é enviada um RPC (*Remote Procedure Call)* com a mensagem a ser reproduzida é então solicitada a presença do M2, o novo centro de gerenciamento que irá participar da cadeia. M2 então pede acesso a S1, S2 e R1. Então quando um dispositivo IoT S2 recebe CoAP contendo informações de IP/R1, ele recebe a informação vinda da cadeia e de forma segura (NOVO, O., 2018).

Como neste caso os agentes que controlam vão estar sempre a frente dos nós e de certa maneira no poder destes e terá uma maior acuidade na resposta e melhor enfrentamento contra cenários de ataques.

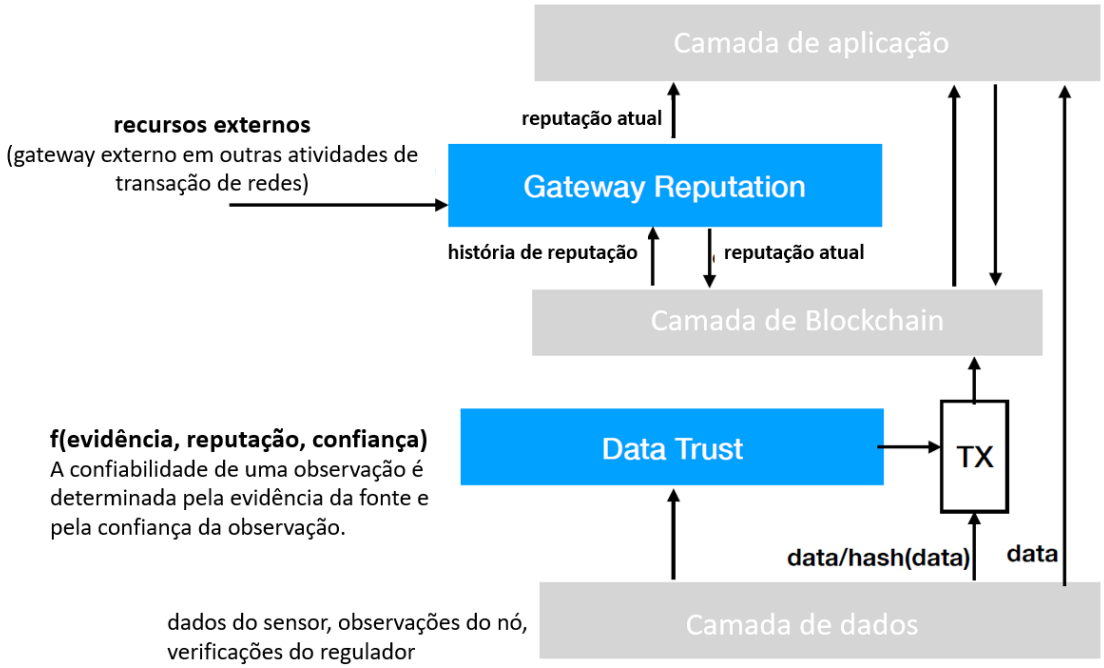
Neste artigo, (NOVO, O., 2018) aborda o problema de escalabilidade do gerenciamento do acesso a bilhões de dispositivos com restrições na IoT. Certamente, os sistemas de controle de acesso centralizados não conseguem lidar com o aumento de carga de forma eficiente. Como a maioria dos dispositivos de IoT é amplamente limitada a suportar diretamente a tecnologia BC, os autores propuseram que os dispositivos de IoT não pertencem à rede BC, o

que facilita a integração dos dispositivos de IoT atuais para se adaptarem ao nosso sistema. O objetivo deste artigo foi fornecer um sistema de controle de acesso genérico, escalável e fácil de gerenciar. Em geral, a solução é capaz de se adaptar a diversos cenários de IoT, confirmando que a tecnologia BC pode abraçar a tecnologia IoT em sua plenitude.

De acordo com os autores (DEDEOGLU, Volkan et al., 2019), a arquitetura se dividiria em três camadas como mostra a Figura 30 onde ilustra os seguintes: camada de dados, que envolve a coleta de dados observacionais de dispositivos IoT e outras fontes. Os dados são convertidos de sinais físicos para digitais e podem estar sujeitos a ruído ou manipulação; camada BC, que recebe transações da camada de dados e mantém o BC, interagindo bidireccionalmente com a camada de aplicação; e finalmente a camada de aplicação, que ficaria responsável pelo processamento de dados e fornecimento de serviços aos usuários finais.

O artigo discute uma arquitetura de confiança em camadas para aplicações IoT baseadas em BC, visando melhorar a confiança de ponta a ponta.

Figura 30: Arquitetura de confiança em camadas proposta



Fonte: adaptado de (DEDEOGLU, Volkan et al., 2019).

Na visão deles, seria imprescindível a construção de dois módulos principais para gestão de confiança dentro do modelo da arquitetura. Um destes seria o Módulo de Confiança de Dados, que quantificaria a confiança dos dados observacionais de sensores com base em:

- Evidências de outras fontes de dados próximas;
- A reputação da fonte de dados com base no comportamento a longo prazo;

- O nível de confiança da observação reportada pela fonte. O valor de confiança da observação (Trusti j) é calculado por uma função (f) que combina esses três fatores. A reputação de um nó é atualizada com base na confiança da observação e na evidência de outras observações (DEDEOGLU, Volkan et al., 2019).

O outro seria o Módulo de Reputação de *Gateway*, que rastreia a confiabilidade a longo prazo dos participantes da rede BC, (nós de *gateway*). A reputação de um *gateway* (Rep(Gi)) é atualizada com base na validade dos blocos gerados, considerando a validade das transações de sensores e a correção dos valores de confiança atribuídos. Fontes externas de reputação (Ext(Gi)) também podem ser consideradas. A reputação do *gateway* influencia o processo de validação de blocos (DEDEOGLU, Volkan et al., 2019).

Isso tornaria a arquitetura proposta leve e privada aplicável ao IoT, com mecanismo de geração de blocos rápidos e sem peso computacionais, onde os *gateways* em intervalos periódicos validariam e calculariam a confiança, gerando os novos blocos. As validações de blocos seriam adaptativas baseada em reputação. E o mecanismo de consenso distribuído, formando validadores que enviam mensagens indicando se um bloco é valido ou invalido, rejeitando rapidamente caso haja algo de errado.

A análise de desempenho apresentada pelos autores (DEDEOGLU, Volkan et al., 2019) demonstra a capacidade do módulo de confiança de dados de atribuir valores de confiança mais altos a nós honestos e mais baixos a nós maliciosos. A validação adaptativa de blocos visa reduzir o custo computacional da validação. A análise de segurança considera ataques por nós sensores maliciosos, *gateways* maliciosos e nós BC em conluio, bem como ataques de *impersonation*, e discute como a arquitetura proposta pode mitigar essas ameaças.

Neste artigo os autores (WAZID, Mohammad et al., 2020), oferecem uma visão geral da segurança na comunicação IoT habilitada por 5G, abordando questões, desafios e um roteiro para futuras pesquisas, tendo como premissa discutir e consolidar os vários tipos de protocolos de segurança no contexto do IoT habilitado por 5G. Segundo eles, o principal motivador é a camada de vulnerabilidade, podendo sofrer diversos tipos de ataques.

Apresentam modelos de sistemas, de rede e de ameaças, necessários para que o ambiente IoT habilitado por 5G se proteja, analisando os requisitos de segurança e dos ataques potenciais. Abordando as categorias de protocolos de segurança, como gerenciamento de chaves, autenticação de usuário/dispositivo, controle de acesso/controle de acesso de usuário e detecção de intrusão, no ambiente IoT habilitado por 5G.

E através das análises do atual cenário cita os vários protocolos baseados em nós de confiança utilizando BC, com operações descentralizadas, eficientes e transparentes para

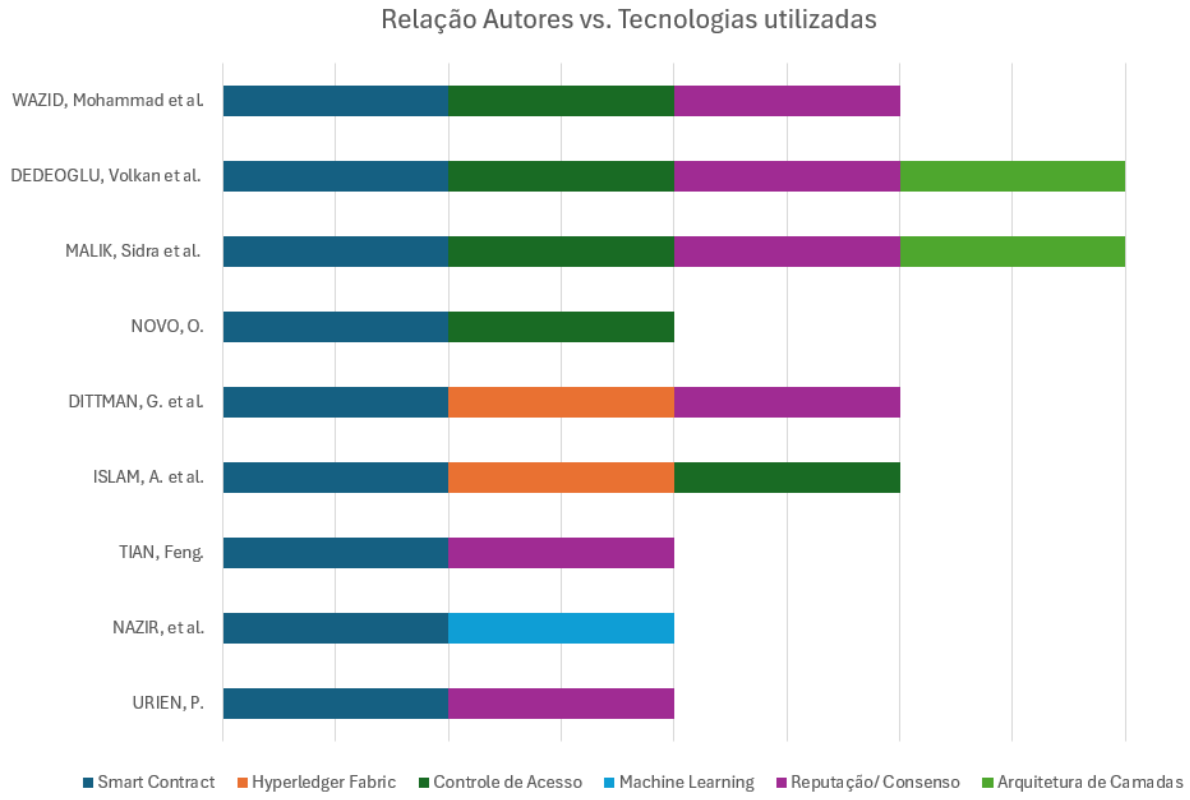
todas as entidades do ambiente de comunicação. Para elaborar protocolos de segurança em ambiente de IoT habilitado para 5G, os autores afirmam “operações de BC” são também aplicáveis.

Para executar a tarefa, um bloco seria os dados sobre a funcionalidade necessária, por exemplo, outro a mensagem de autenticação, assim o protocolo de dados pode ser criado e adicionado ao BC. Tendo vista todas as questões, os autores entendem que o BC é uma tecnologia que tem sido fornecido para entidades de rede legais, então elas podem acessar os dados usando os seus blocos de forma transparente. Esse trabalho pode ser realizado de forma eficaz usando a operações já conhecidas e comuns por exemplo em redes baseadas em *smart contracts*. Consequentemente, para ampliar a capacidade de proteger, (WAZID, Mohammad et al., 2020) visa que criar “protocolos de segurança baseados em BC” pode vir a ser uma solução a longo prazo tanto para o atual 5G quanto paras futuras gerações.

4.4 VERIFICAÇÃO DOS RESULTADOS

Trazendo conforme visto na Tabela 5 e observando o gráfico abaixo apresentado na Figura 31, anunciada acima, é percebido que todos os artigos eleitos para análise neste trabalho possuem um ponto em comum: o uso de *smart contract*, que hoje permite a permanência e a não corrupção, antes adotada somente por papel entre as partes. Ele é a forma que assegura que algo seja executado conforme descrito e acordado, sendo o BC o intermediário e executor. Assim o processo unanime entre todas as propostas passam pela etapa de criação de *smart contract* dentro das arquiteturas propostas, como forma de não quebrar as negociações para o aumento na condução por parte da solução.

Figura 31: Gráfico com relação entre autores vs. tecnologias utilizadas.



Fonte: Elaboração própria.

Quando criado o acordo entre as partes descrito nesses contratos é possível então estipular quais pontos serão seguidos pela solução posteriormente, como são os casos de a cada cinco em nove usarem controle de acesso, com uma margem de mais ou menos 55,56% dos casos apresentados; e seis em nove usarem a ideia reputação com ou sem checagem de reputação dos nós ou *gateways*, que correspondem 66,67%. Propostas por arquitetura de camadas e o uso do Hypledger Fabric que é uma plataforma assim como Ethereum, foram duas cada, num total neste trabalho de aproximadamente 22,22% cada solução.

O interesse comum na aplicação da tecnologia do BC para buscar resolver os problemas de segurança e confiança no contexto do IoT, podem ser apontados de forma comum em todos os nove artigos que trazem em seus textos introdutórios a preocupação de achar uma forma de garantir os requisitos necessários. Em resumo, os artigos convergem na visão de que a BC oferece um potencial significativo para fortalecer a segurança, a confiança e a integridade dos dados em sistemas IoT, embora reconhecendo os desafios relacionados às limitações de recursos dos dispositivos e à necessidade de integração com outras tecnologias e modelos de confiança.

Sempre em congruência com a premissa das limitações dos recursos dos dispositivos, como é o caso do artigo em que (DITTMANN G et al., 2019) aborda diretamente a questão de

como aplicar que como foi visto, propôs um proxy baseado em Hyperleder Fabric para comunicação *offload*, resultando em economia de largura de banda e CPU, alinhado com a proposta (URIEN, 2018) em que um intermediário interpretaria e controlaria as negociações entre o objeto e a estrutura do BC, diminuindo gastos conforme proposta anterior de uso de recursos. Nesse caso em especial o objetivo dos autores (DITTMANN G et al., 2019) é validado nos resultados apresentados conforme observado, e eles citam que o uso do modelo evitou contra-ataques DDoS. (ISLAM, A.; MADRIA, S. K. A, 2019) também segue o mesmo pensamento dos autores anteriormente citados utilizando-se de controle de acesso com uma otimização para Hyperledger Fabric, os autores diminuíram significantemente a latência das operações e detecções.

Os casos de duas soluções voltadas para *supply chain* vistas em (TIAN, Feng, 2016) e (MALIK, Sidra et al, 2019), conseguem vislumbrar maneiras diferentes do uso da tecnologia onde o primeiro comenta em 2016 uma ideia de todo o processo dentro da cadeia sendo totalmente rastreável utilizando RFID. Já em um segundo momento, anos mais tardes, os autores (MALIK, Sidra et al, 2019), entendem que aquela ideia poderia ser mais bem aproveitada se um *framework* fosse desenvolvido baseado em uma arquitetura de camadas, que teria capacidade de avaliar a reputação e a confiança das entidades participantes (sensores distribuídos em toda a cadeia produtiva), portanto muito mais completo e complexo com ganhos tanto em menor latência e melhor *throughput*, indo muito além de ser um sistema de rastreabilidade e passando a ser um modelo baseado em patamar de reputação e qualidade.

De acordo com (NOVO, O., 2018), projeta uma solução genérica que se aproveita da pilha de camadas do IoT, e buscando se valer dos seus protocolos para se adaptar ao BC e assim todas a heterogeneidade neste artigo é uma preocupação que o autor procura levar em consideração. Faz uma adaptação que procura gerar uma maior abordagem quanto ao número de dispositivos que podem utilizar-se de sua solução e nos cenários de testes foi possível atingir um pico de estabilidade e até de queda no *throughput* mesmo com o aumento de dispositivos. Fazendo uso do controle de acesso para tomada de decisões de operações. Algo muito similar ao visto em (WAZID, Mohammad et al., 2020) que para o 5G, visa o uso do BC justamente nas questões de tomada de decisões quanto a autenticação de usuário por dispositivo, controle de acesso e detecção de intrusão.

Para (DEDEOGLU, Volkan et al., 2019) o foco é na reputação dos nós ou *Gateway*, onde é possível controlar os nós maliciosos e validar como blocos inválidos, personificando estes como ataque externo a rede. Nos resultados os autores, conseguiram simular ataques com blocos inválidos e assim colocar em prova seus cálculos e modelo, e os mesmo

obtiveram uma resposta de acerto de 98%. De acordo com os gráficos de latência, os autores conseguiram manter a margem baixa mesmo durante o processo de validação dos blocos.

A solução mais recente é ofertada no artigo dos autores (NAZIR et al., 2024), aqui é visível as evoluções que foram atingidas. O uso da ML intensifica e torna a proposta mais robusta que as demais, pois primordialmente possibilitou que padrões de ataques pudessem ser aprendidos e não repetidos. Como os autores foram capazes de criar *Randon Forest* que é um classificador capaz de discriminar ameaças severas DDoS e *Comand and Control* (C&C), fazendo com que as métricas de avaliação do modelo tenham erros mínimos. Assim como o outro *Decision Tree* que também se mostrou eficaz na distinção de diferentes classes de ameaças. Visto também que o classificador *Ensemble* alcançou uma precisão perfeita de 1.00 para as ameaças *Attack*, DDoS, *FileDownload* e C&C-*FileDownload*. A central de controle aqui apontadas por eles seria um aplicativo inicialmente proposto para iOS, um facilitador, já que por ele o usuário seria capaz de conferir e atuar em casos de ameaças.

Consegue-se então perceber durante as análises e leituras que no transcorrer dos anos de 2016 até 2024 a evolução e a chegada de novas tecnologias que foram sendo intercaladas e as visões de melhoria, propostas, foram para outro patamar.

4.5 CONSIDERAÇÕES FINAIS

Como analisado as arquiteturas já estão avançadas e cada ano que se passou, é possível identificar que os autores desenvolveram métodos que o BIoT poderá e já está sendo aproveitado em nosso dia a dia, desde 2021 com o BC *5.0* o mundo tem sofrido uma alteração e cada vez mais a tecnologia se infiltrou nos usos do IoT por ser uma solução inteligente a ele.

Os autores escolhidos conseguiram bons resultados que demonstraram economias significativas no tempo de CPU, na largura de banda consumida por transações BC no dispositivo IoT, assim como avaliaram a latência para operações de criação, atribuição e criação de políticas de atributos, mostrando que esta aumenta com o aumento do tamanho dos blocos em determinadas soluções, mas mesmo assim conseguem uma rede capaz de permitir maior capacidade adaptativa de prevenção contra os ataques maliciosos. Em outros, os modelos apresentados mostram-se capazes de prever e serem eficientes em quase 90% e ou 100% dos casos de invasores ou no que eles chamam de detecção de intrusos.

Assim como os autores (ISLAM, A.; MADRIA, S. K. A, 2019) citam que as arquiteturas podem misturar conceitos já existentes e propor para equipamentos primeiro menores como os IoT de sistemas médicos ou alguns que é utilizado em residência, assim como faz os autores como é o caso de (DEDEOGLU, Volkan et al., 2019) ou (WAZID,

Mohammad et al., 2020). Ou como o uso de ML proposto pelos autores (NAZIR, et al., 2024) visando não só implementar a junção das duas tecnologias como aumentar a projeção de alcance contra ameaças.

5 CONCLUSÃO

O presente trabalho explorou como o BC pode contribuir para a segurança e privacidade no cenário atual do IoT. O objetivo geral neste trabalho foi analisar através de uma revisão sistemática da bibliografia, onde se realizou a compreensão de quais são os benefícios da implementação e aplicabilidade do BC ao IoT. Verificou-se a partir das tabelas e dos gráficos demonstrados que é possível incrementar a segurança nas redes IoT, sendo o BIoT uma realidade aplicável.

Além disso, foram elucidados os conceitos por trás de cada parte atuante durante a investigação do tema. Conforme havia sido estipulado, foi feita a apresentação da revisão da literatura dos artigos e assim como visto no item 4.3 e 4.4, onde se é observado a aplicabilidade e investigações no ramo que consideram a implementação de arquiteturas apresentadas nos artigos revisados. Notou-se uma tendência comum nas soluções, conforme apresentado neste como a unanime escolha nas soluções pelo uso de *smarts contracts.* Cumprindo os requisitos a qual foi proposto.

É singular a necessidade tanto de revisões teóricas, como está, assim tem-se a noção da maturidade da tecnologia por trás do assunto e de quanto ela poderá se desenvolver a cada ano que passar é imprescindível a realização de revisões teóricas contínuas que ajudem a mensurar a maturidade da tecnologia. Em um estudo futuro poder-se-á até mesmo, combinar técnicas vista de forma teórica, onde deste híbrido surgirá uma nova arquitetura melhorada, como visto em alguns dos trabalhos aqui apresentados**,** com o intuito de poder quem sabe seguir pesquisas dentre as escolhidas e aprofundar os estudos destas.

Por fim, a expectativa em relação ao BIoT é promissora. Este trabalho proporcionou uma análise crítica das vantagens e desvantagens identificadas, confirmando que o este apresenta promessas significativas para a melhoria da segurança cibernética.

6 REFERÊNCIAS

AL-MADANI A. M.; GAIKWAD, A. T**. IoT Data Security Via Blockchain Technology and Service-Centric Networking**. Fifth International Conference on Inventive Computation Technologies (ICICT-2020), Coimbatore, 2020, p.17-21.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. Internet das Coisas (IoT): Segurança e privacidade de dados pessoais. Rio de Janeiro: Editora Alta Books, 2021. E-book. ISBN 9786555202793. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555202793/. Acesso em: 02 jan. 2024.

ARATA, Estefânia A. Pianoski; NASCIMENTO, Maikol; DE NOVAIS, Caroline Batista Fantini. **Segurança da Informação para aplicações IOT – Internet Of Things**. South American Development Society Journal, [S.l.], v. 6, n. 18, p. 301, dez. 2020.

ASARE, B. T.; QUIST–APHETSI, K.; NANA L. **Nodal Authentication of IoT Data Using Blockchain.** International Conference on Computing, Computational Modelling and Applications (ICCMA), Costa do Cabo, 2019, p.125-129.

ATLAM, Hany F. et al. Blockchain with Internet of things: Benefits, challenges, and future directions. **International Journal of Intelligent Systems & Applications**, v. 10, n. 6, 2018.

BAMBARA, J. J.; ALLEN, P. R., **Blockchain: A practical guide to developing business, law, and technology solutions.** New York: McGraw Hill, 2018.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65..>. Acesso em: 02 jul. 2022.

BESSA, Emanuel Estrela; BARBOSA, Joberto Sérgio Martins**. Tecnologia Blockchain – Princípios e Aplicação.** Anais da 16ª Jornada UNIFACS de Iniciação Científica – JUIC, Salvador, nov. 2019.

BOVÉRIO, M. A.; SILVA, V. A. F. da**. Blockchain: uma tecnologia além da criptomoeda virtual.** Revista Interface Tecnológica, Taquaritinga, [S. l.], v. 15, n. 1, 2018, p. 109-121.

CAMPOS, C. **O que é Segurança em IoT? Riscos, Exemplos e Soluções**. Emnify, 2023. Disponível em: < https://www.emnify.com/pt-br/glossario-iot/seguranca-iot>. Acesso em: 02 jul. 2024.

CISCO. **Cisco Annual Internet Report, 2018–2023.** 9 de mar. 2020. Disponível em: < https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html?dtid=osscdc000283>. Acesso em: 02 jul. 2024

CROSBY, M.; PATTANAYAK, P.; VERMA, S. & Kalyanaraman, V. **Blockchain technology: Beyond bitcoin**. *Applied Innovation*, nº 2, Berkley, 2016, p. 6-19.

CRYPTOPIA - BITCOIN, **BLOCKCHAINS** AND THE FUTURE OF THE INTERNET. Direção: Torsten Hoffmann, Michael Watchulonis. Produção: Torsten Hoffmann. Australia, Estados Unidos e Alemanha: Norddeutscher Rundfunk and Studio Hamburg Enterprises, 2020. Amazon Prime.

DA MATA, Rafael Zerbini Alves; RODRIGUES, Carlo Kleber da Silva**. Uma Análise Competitiva entre as Tecnologias Blockchain e Tangle para o Projeto de Aplicações IoT.** Brazilian Journal of Development, Curitiba, v. 5, n. 7, p. 7961-7979, jul. 2019.

DEDEOGLU, Volkan et al. A trust architecture for Blockchain in IoT. In: **Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services.** 2019. p. 190-199.

DIGITALASSET. **Access the Gartner® Hype Cycle™ for Web3 and Blockchain.** 2024. Disponível em: < https://www.digitalasset.com/gartner-hype-cycle-for-web3-and-blockchain-2024> .Acesso em: 25 out. 2024.

DITTMANN G.; JELITTO, J. **A Blockchain Proxy for Lightweight IoT Devices.** Crypto Valley Conference on Blockchain Technology (CVCBT), Zurich, 2019, p. 82-85.

DWIVEDI, A.; SINGH, R.; KAUSHIK, K.; MUKKAMALA, R.R.; ALNUMAY, W. S., **Blockchain and artificial intelligence for 5G-enabled**
Internet of Things: Challenges, opportunities, and solutions. Emerging Telecomunications Technologies, Wiley, vol. 35. 2021

EVANS, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. CISCO, 2011. Disponível em: < https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: 25 jul. 2022.

FAKHRI, D.; MUTIJARSA, K. **Secure IoT Communication using Blockchain Technology**. International Symposium on Electronics and Smart Devices (ISESD), Bandungue, 2018.

FERNANDEZ, J. **IoT market update: Enterprise IoT market size reached $269 billion in 2023, with growth deceleration in 2024**. 9 de jul. 2024. Disponível em: <https://iot-analytics.com/iot-market-size/>. Acesso em: 23 de nov. 2024

FERNÁNDEZ-CARAMÉS, Tiago M.; FRAGA-LAMAS, Paula. A Review on the Use of Blockchain for the Internet of Things**. IEEE Access**, v. 6, p. 32979-33001, 2018.

FUKUDA, Leonardo Massami. **Segurança da informação em IOT**. 2019. Trabalho de Conclusão de Curso (Especialização em Gestão da Tecnologia da Informação e Comunicação) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/19442>. Acesso em: 30 jan. 2021.

GIANNOUTAKIS, K. M.; SPATHOULAS, G.; FILELIS-PAPADOPOULOS, C. K.; COLLEN, A.; ANAGNOSTOPOULOS, M.; VOTIS, K.; NIJDAM, N. A. **A Blockchain**

Solution for Enhancing Cybersecurity Defence of IoT. IEEE International Conference on **Blockchain** (BC), Rodes, 2020, p. 490- 495.

GUPTA, M. Blockchain**:** for dummies**.** IBM. New Jersey: John Wiley & Sons, 2017.

HARIS, Raseena M. AL-MAADEED, Somayya**. Integrating Blockchain Technology in 5G enabled IoT: A Review**. IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, p. 367-371, 2020.

HERNANDEZ, Raphael. **Governo da Estônia usa Blockchain para guardar registros de pacientes**. 15 de abr. de 2017. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/04/1875751-governo-da-estonia-usa-blockchain -para-guardar-registros-de-pacientes.shtml>. Acesso em: 12 jan. 2021.

IANSITI, M.; LAKHANI, K. R.; MOHAMED, H. It will take years to transform business, but the journey begins now. **Harvard Business Review**, v. 95, n. 1, p. 118-128, 2017.

ISLAM, A.; MADRIA, S. K. **A Permissioned Blockchain based Access Control System for IOT**. IEEE International Conference on Blockchain (BC), Atlanta, GA, 2019, p. 469-476.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. São Paulo: Person, v. 28, 2006.

LAURENCE, Tiana. Blockchain Para Leigos. Rio de Janeiro: Editora Alta Books, 2019. E-book. p.7. ISBN 9788550808024. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788550808024/>. Acesso em: 05 jul. 2024.

LITAN, A. Gartner Hype Cycle for Blockchain and Web3, 2022. **Gartner,** 22 jul. 2022**.** Disponível em: < https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/?_ga=2.157341882.1471034588.1659064498-487594063.1659064498> Acesso em: 25 jul. 2022.

MACHADO, Rafael Nunes. **Análise sobre otimização de Blockchain para Internet das Coisas.** Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Centro de Informática, Universidade Federal de Pernambuco, Recife, 2018. Disponível em: <https://www.cin.ufpe.br/~tg/2018-2/TG_CC/tg_rnm.pdf>. Acesso em: 13 dez. 2020.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: Editora FGV, 2018.

MANCINI, Mônica. **Internet das coisas: história, conceitos, aplicações e desafios**. São Paulo: Tudo Sobre IoT, 2017. Disponível em: < https://www.researchgate.net/publication/326065859_Internet_das_Coisas_Historia_Conceitos_Aplicacoes_e_Desafios> Acesso em: 13 dez. 2020.

MARCHSIN, Karina Bastos K. **BC e smart contracts: As inovações no âmbito do Direito**. Rio de Janeiro: Expressa, 2022. *E-book.* p.11. ISBN 9786555599398. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555599398/>. Acesso em: 05 mar. 2024.

MARIANO, A. M.; SANTOS, M. R. **Revisão da literatura: Apresentação de uma abordagem integradora.** XXVI Congreso Internacional AEDEM, International Conference - Economy, Business and Uncertainty: ideas for a European and Mediterranean industrial policy? Régio da Calábria, 2017. Disponível em: <https://www.researchgate.net/publication/319547360_Revisao_da_Literatura_Apresentacao_de_uma_Abordagem_Integradora>. Acesso em: 23 mar. 2021.

MARTINS, J. Dos S. **Exploração de vulnerabilidade em redes IOT.** Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Instituto Municipal de Ensino Superior de Assis – IMESA, Fundação Educacional do Município de Assis – FEMA. Assis, 2018. Disponível em: <https://cepein.femanet.com.br/BDigital/arqTccs/1511420616.pdf>. Acesso em: 25 fev. 2021.

MORAES, Alexandre Fernandes de. **Bitcoin e Blockchain: a revolução das moedas digitais**. Rio de Janeiro: Expressa, 2021. *E-book.* p.16. ISBN 9786558110293. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786558110293/>. Acesso em: 04 jan. 2024.

MORAIS, Izabelly Soares de; GONÇALVES, Priscila de F.; LEDUR, Cleverson L.; et al. Introdução a Big Data e Internet das Coisas (IoT). Porto Alegre: SAGAH, 2018. E-book. ISBN 9788595027640. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595027640/>. Acesso em: 04 jan. 2024.

MOREIRA, Kleber Brito. **Blockchain - Tecnologia, Arquitetura e Aplicações.** Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Software) - Universidade de Brasília, Brasília, 2019. Disponível em: <https://bdm.unb.br/handle/10483/26357>. Acesso em: 01 dez. 2020.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 01 abr. 2021

NAZIR, A; HE, J. ZHU, N.; WAJAHAT, A.; ULLAH, F.; QURESHI, S.; MA, X.; PATHAN, M. S. **Collaborative threat intelligence: Enhancing IoT security through Blockchain andmachine learning integration.** Journal of King Saud University - Computer and Information Sciences, 2024

NETO, Afonso B. S.; ORTIZ, Marcos Dantas; REGO, Paulo Antonio Leal. **Um mecanismo leve de consenso e confiança para controle de acesso em redes IoT baseadas em Blockchain**. *In*: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 37., 2019, Gramado. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019.

NOVO, Oscar. Blockchain meets IoT: An architecture for scalable access management in IoT. **IEEE internet of things journal**, v. 5, n. 2, p. 1184-1195, 2018.

OBAIDAT, M.; RAWSHDH, M.; ALJA´AFREH, M.; ABOUALI, M.; THAKUR, K.; KARIME, A. **Exploring IoT and Blockchain: A Comprehensive Survey on**

Security, Integration Strategies, Applications and Future Research Directions. Suíça**:** MDPI, Big Data Cogn. Comput., 2024

REBELLO, Gabriel Antonio Fontes; DUARTE, Otto Carlos Muniz Bandeira. **Correntes de Blocos em Redes Virtualizadas: Protocolos de Consenso e Fatiamento Seguro da Rede.** In: CONCURSO DE TESES E DISSERTAÇÕES - SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 38., 2020, Rio de Janeiro. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 89-96.

RIBEIRO, Arlindo Jorge de Jesus. **Problemas de Segurança na Internet das Coisas.** Monografia (Mestrado em Cibersegurança e Informática Forense) – Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, Leiria, 2020. Disponível em: <https://iconline.ipleiria.pt/handle/10400.8/5568>. Acesso em: 23 fev. 2021.

RIGUES, Rafael. **Serviço da Amazon consegue parar o maior ataque DDoS da história**. Olhar Digital, 18 jul. 2020. Disponível em: <https://olhardigital.com.br/2020/06/18/noticias/servico-da-amazon-consegue-parar-o-maior-ataque-ddos-da-historia/> Acesso em: 23 nov. 2024.

RODRIGUES, Carlo Kleber da Silva. **Uma análise simples de eficiência e segurança da Tecnologia Blockchain.** Revista de Sistemas e Computação, Salvador, v. 7, n. 2, p. 147-162, jul./dez. 2017.

SAKAMOTO, S. G. **Segurança, Privacidade e Blockchain no Contexto de Internet das Coisas.** Monografia, (Especialização em Internet das Coisas) - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2020. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/19677>. Acesso em: 21 jan. 2021.

SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>. Acesso em: 29 jun. 2022.

SATIZTPM. Internet of things – Redes conectadas. Disponível em: <https://www.satiztpm.it/internet-things/>. Acesso em: 20 jul. 2022.

SERPANOS, Dimitrios; WOLF, Marilyn. **Internet-of-things (IoT) systems:** architectures, algorithms, methodologies. Atlanta: Springer, 2017.

SINGH, M.; SINGH A.; KIM, Shiho. **Blockchain: A Game Changer for Securing IoT Data**. IEEE 4th World Forum on Internet of Things (WF-IoT), Singapura, 2018, p. 51- 55.

SINGH, S.; SANWAR HOSEN, A. S. M.; YOON, B. **Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network**. IEEE Access, Volume: 9, 2021. p. 13938-13959.

TIAN, Feng. **An agri-food supply chain traceability system for China based on RFID & Blockchain technology**. In: 2016 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016. p. 1-6.

TSENG, Lewis et al. Blockchain for managing heterogeneous internet of things: A perspective architecture. **IEEE network**, v. 34, n. 1, p. 16-23, 2020.

URIEN, P. **Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues**. 3rd Cloudification of the Internet of Things (CIoT), 2018.

URMILA, M. S. A.; HARIHARAN, B.; PRABHA, R. **Comparitive Study of Blockchain Applications for Enhancing Internet of Things Security.** 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kampur, 2019.

VIANNA F. R. P. M.; DA SILVA P. C. G.; PEINADO J. O Blockchain e suas aplicações para além das criptomoedas: Uma revisão sistemática de literatura.
REVISTA DE TECNOLOGIA APLICADA (RTA), Curitiba, v. 9, n. 1, 2020, p. 67-81.

WANG, Qin; ZHU, X.; NI, Y.; GU, L.; ZHU, H. Blockchain for the IoT and industrial IoT: A review. **Internet of Things**, v. 10, p. 100081, 2020.

XU, Jinliang et al. Edgence: A Blockchain -enabled edge-computing platform for intelligent IoT-based dApps. **China Communications**, v. 17, n. 4, p. 78-87, 2020.

YING, Wenchi; JIA, Suling; DU, Wenyu. Digital enablement of Blockchain: Evidence from HNA group. **International Journal of Information Management**, v. 39, p. 1-4, 2018.

ZHANG, Y., WEN, J. **The IoT electric business model: Using Blockchain technology for the internet of things**. *Peer-to-Peer Netw. Appl.* **10,** p. 983–994, 2017.

APÊNDICE A

Abaixo segue a tabela com a classificação das referências.

Tabela de Artigos, Monografias e Livros (1 menos importante, 5 mais importante)					
Nome do Artigo	Autor(es)	Nr de Citações	Publicado em	Local de Busca	Importância
Bitcoin A Peer-to-Peer Electronic Cash System	NAKAMOTO, Satoshi	38111	2008	Scholar Google	5
An overview of blockchain technology: Architecture, consensus, and future trends	Z Zheng, S Xie, H Dai, X Chen	6050	2017	Scopus	5
Blockchain challenges and opportunities: A survey	Z Zheng, S Xie, H Dai, X Chen	5206	2018	Scopus	5
BlockChain Technology: Beyond Bitcoin	Crosby, M., Pattanayak, P., Verma, S. & Kalyan	3798	2016	Scholar Google	5
It will take years to transform business, but the journey begins now	Iansiti e Lakhani	3236	2017	Scholar Google	4
An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 2016 13th international cont	TIAN, Feng.	2006	2016	IEEE	5
Blockchain meets IoT: An architecture for scalable access management in IoT	NOVO, Oscar	1550	2018	IEEE	5
A Review on the Use of Blockchain for the Internet of Things	FERNANDEZ-CARAMES, Tiago M.; FRAGA-	1315	2018	IEEE	5
Applications of blockchains in the Internet of Things: A comprehensive survey	MS Ali, M Vecchio, M Pincheira, K Dolui	998	2018	Scopus	3
Towards an optimized blockchain for IoT	A Dorri, SS Kanhere, R Jurdak	950	2017	Scopus	3
Redes de Computadores e a Internet. São Paulo: Person, v. 28, 2006.	KUROSE, James F.; ROSS, Keith W.	929	2006	Livro	4
The IoT electric business model: Using blockchain technology for the internet of things	ZHANG, Y., WEN, J.	789	2017	Scholar Google	5
Blockchain in internet of things: challenges and solutions	A Dorri, SS Kanhere, R Jurdak	669	2017	Scopus	3
Blockchain with Internet of things: Benefits, challenges, and future directions.	ATLAM, Hany F. et al.	523	2019	Scholar Google	5
Blockchain for the IoT and industrial IoT: A review.	WANG, Qin; ZHU, X.; NI, Y.; GU, L.; ZHU, H	453	2020	Scholar Google	5
Trustchain: Trust management in blockchain and iot supported supply chains	MALIK, Sidra et al.	399	2019	IEEE	5
Blockchain for dummies	GUPTA, Manav	362	2017	Livro	4
A Internet das Coisas	MAGRINI, Eduardo	347	2018	Livro	5
Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed iot network	SINGH, S.; SANWAR HOSEN, A. S. M.; YOO	343	2021	IEEE	4
Digital enablement of blockchain: Evidence from HNA group	YING, Wenchi; JIA, Suling; DU, Wenyu.	339	2018	Scholar Google	3
Internet das coisas: da teoria à prática	SANTOS, Bruno P. et al.	276	2016	Scholar Google	5
Revisão da literatura apresentação de uma abordagem integradora	MARIANO, A. M.; SANTOS, M. R	275	2017	Scholar Google	1
Internet-of-Things (IoT) Systems - Architectures, Algorithms, Methodologies	SERPANOS, Dimitrios; WOLF, Marilyn.	244	2018	Livro	4
Blockchain A Game Changer for Securing IoT Data	Singh, M.; Singh A.; Kim, Shiho	226	2018	Scholar Google	5
Blockchain for managing heterogeneous internet of things: A perspective architecture.	TSENG, Lewis et al	165	2020	IEEE	5
A trust architecture for blockchain in IoT	DEDEOGLU, Volkan et al.	145	2019	Scholar Google	5
Secure IoT Communication using Blockchain Technology	Fakhri, D.; Mutijarsa, K.	143	2018	IEEE	4
Blockchain_ A Practical Guide to Developing Business, Law, and Technology Solutions	BAMBARA, J. J.; ALLEN, P. R.	138	2018	Livro	5
Security in 5G-Enabled Internet of Things comunication: issues, challenges, and future research roadmap	WAZID, Mohammad et al.	101	2020	IEEE	5

Nome do Artigo	Autor(es)	Nr de Citações	Publicado em	Local de Busca	Importância
A Permissioned Blockchain based Access Control system in iot	Islam, A.; Madria, S. K.	90	2019	Scholar Google	5
Edgence: A Blockchain-Enabled Edge-Computing Platform for Intelligent IoT-Based dApps	XU, Jinliang et al. Edgence	64	2020	IEEE	4
A Blockchain Proxy for Lightweight IoT Devices	Dittmann G.; Jelitto, J.	62	2019	Scholar Google	5
Integrating Blockchain Technology in 5G enabled - IOT review	HARIS, Raseena M. Al-Maadeed, Somayya.	56	2020	IEEE	2
A Blockchain Solution for Enhancing Cybersecurity defense of iot	Giannoutakis, K. M.; Spathoulas, G.; Filelis-Pap	55	2020	IEEE	3
Blockchain IoT (BIoT) A New Direction for Solving IOT security and trust issues	URIEN, P	53	2018	IEEE	5
Redes de computadores	Behrouz A. Forouzan; Firouz Mosharraf	39	2013	Minha Bibliteca Digital (	5
Collaborative threat intelligence: Enhancing IoT security through blockchainandmachine learning integration	NAZIR, A.; HE, J.; ZHU, N.; WAJAHAT, A.; U	34	2024	Scopus	5
Introdução a Big Data e Internet das Coisas (IoT)	Izabelly Soares de Morais; Priscila de Fátima Go	31	2018	Minha Bibliteca Digital (	3
IoT Data Security Via Blockchain Technology and service centric network	Al-madani A. M.; Gaikwad, A. T.	25	2020	IEEE	5
A Comparitive Study of Blockchain Applications for Enhancing Internet of Things Security	Urmila, M. S. A.; Hariharan, B.; Prabha, R.	23	2019	IEEE	3
BLOCKCHAIN uma tecnologia além da criptomoeda virtual	BOVÉRIO, M. A.; SILVA, V. A. F. da	22	2018	Scholar Google	3
Blockchain Para Leigos	Tiana Laurence	22	2019	Minha Bibliteca Digital (	4
Nodal Authentication of IoT Data Using Blockchain	Asare, B. T.; Quist–Aphetsi, K.; Nana L.	14	2019	IEEE	5
Uma análise simples de eficiência e segurança da Tecnologia Blockchain	RODRIGUES, Carlo Kleber da Silva	14	2017	Scholar Google	5
Bitcoin e Blockchain: a revolução das moedas digitais	Alexandre Fernandes de Moraes	12	2021	Minha Bibliteca Digital (	4
Blockchain e smart contracts: As inovações no âmbito do Direito	Karina Bastos Kaehler Marchsin	12	2022	Minha Bibliteca Digital (	4
O Blockchain e suas aplicações para além das criptomoedas	Vianna F. R. P. M.; Da Silva P. C. G.; Peinado J	9	2020	Scholar Google	5
Internet das Coisas (IoT): Segurança e privacidade de dados pessoais	David Alves; Mario Peixoto; Thiago Rosa	4	2021	Minha Bibliteca Digital (	5
SEGURANÇA DA INFORMAÇÃO EM IOT	FUKUDA, Leonardo Massami.	3	2019	Scholar Google	3
SEGURANÇA, PRIVACIDADE E BLOCKCHAIN NO CONTEXTO DE INTERNET DAS COISAS	SAKAMOTO, S. G.	2	2020	Scholar Google	5
Análise sobre otimização de Blockchain para Internet das Coisas	MACHADO, Rafael Nunes	1	2018	Scholar Google	5
Um mecanismo leve de consenso e confiança para controle de acesso em redes IoT baseadas em Blockchain	NETO, Afonso B. S.; ORTIZ, Marcos Dantas; R	1	2019	Scholar Google	4
Problemas de Segurança na Internet das Coisas	RIBEIRO, Arlindo Jorge de Jesus	1	2020	Scholar Google	3
SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES IOT – INTERNET OF THINGS	ARATA, Estefânia A. Pianoski; NASCIMENTO	0	2020	Scholar Google	4
Tecnologia Blockchain – Princípios e Aplicação.	BESSA, Emanuel Estrela; BARBOSA, Joberto S	0	2019	Scholar Google	3
Protocolo para segurança da informação em Gateways IoT	CÂNDIDO, Aubani Júnio Teixeira.	0	2019	Scholar Google	2
Uma Análise Competitiva entre as Tecnologias Blockchain e Tanglepara o Projeto de Aplicações IoT	da Mata, Rafael Zerbini Alves; Rodrigues, Carlo	0	2019	Scholar Google	3
EXPLORAÇÃO DE VULNERABILIDADES EM REDES IOT	MARTINS, J. Dos S.	0	2018	Scholar Google	4
Blockchain: tecnologia, arquitetura e aplicações	MOREIRA, Kleber Brito	0	2019	Scholar Google	5
Correntes de Blocos em Redes Virtualizadas - Protocolos de Consenso e Fatiamento Seguro da Rede	REBELLO, Gabriel Antonio Fontes; DUARTE,	0	2020	Scholar Google	1