UNIVERSIDADE FUMEC
FACULDADE DE CIÊNCIAS EMPRESARIAIS – FACE
Programa de Doutorado e Mestrado em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

EUSTAQUIO LAGES DUARTE

SEGURANÇA DA INFORMAÇÃO EM *SMART CITIES* USANDO *BLOCKCHAIN*

Belo Horizonte
2021

Eustáquio Lages Duarte

SEGURANÇA DA INFORMAÇÃO EM *SMART CITIES* USANDO *BLOCKCHAIN*

Dissertação apresentada ao Programa de Doutorado e Mestrado em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC como requisito parcial para obtenção do título de Mestre.

Área de Concentração: Sistemas de Informação e Gestão do Conhecimento.

Linha de Pesquisa: Tecnologia e Sistemas de Informação.

Orientador: Prof. Dr. Luiz Cláudio Gomes Maia.

Belo Horizonte

2021

Dados Internacionais de Catalogação na Publicação (CIP)

D812s Duarte, Eustáquio Lages, 1957-

Segurança da informação em *smart cities* usando *blockchain* / Eustáquio Lages Duarte. - Belo Horizonte, 2021.

121 f. : il.

Orientador: Luiz Cláudio Gomes Maia

Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento), Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2021.

1. Smart Cities. 2. Blockchains (Databases). 3. Tecnologia da informação. 4. Internet. I. Título. II. Maia, Luiz Cláudio Gomes. III. Universidade FUMEC, Faculdade de Ciências Empresariais.

CDU: 681.3.12.004.4

Ficha catalográfica elaborada pela Biblioteca Universitária-FUMEC

Dissertação intitulada "**SEGURANÇA DA INFORMAÇÃO EM SMART CITIES USANDO BLOCKCHAIN**" de autoria de Eustaquio Lages Duarte, aprovada pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Luiz Cláudio Gomes Maia – Universidade FUMEC
(Orientador)

Profa. Dra. Cristiana Fernandes De Müylder – Universidade FUMEC
(Examinador Interno)

Prof. Dr. Rodrigo Moreno Marques – UFMG
(Examinador Externo)

Prof. Dr. Fernando Silva Parreiras
Coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

Belo Horizonte, 26 de fevereiro de 2021.

Luiz Maia.

Cristiana De Muijlder

Rodrigo Moreno Marques

ABARIS

REQUESTED

TITLE	**Assinatura de ata e contra-capas Universidade**
FILE NAME	**8b5248cc-22c6-4ec2-8cde-26b83e416bc3.pdf**
RESQUEST ID	**signature_request_d5b9530d-fdb3-4fc7-a294-da47f**
RESQUESTED BY	**Júlio César Teixeira e Silva**
STATUS	**Completed**

Professor (luiz.maia@fumec.br)

SENDED	02/03/2021 19:42:23UTC±0	SIGNED	09/03/2021 19:49:57UTC±0 191.185.140.62

Professor (cristiana.muylder@fumec.br)

SENDED	09/03/2021 19:49:57UTC±0	SIGNED	10/03/2021 11:40:20UTC±0 189.59.181.9

Professor (rodrigomorenomarques@yahoo.com.br)

SENDED	10/03/2021 11:40:21UTC±0	SIGNED	10/03/2021 12:38:24UTC±0 168.195.101.145

COMPLETED

10/03/2021
12:38:24 UTC±0
The document has been completed.

Assinado Por:
EVELYN FERNANDA DE LELIS MOREIRA DE FREITAS:03475835630
Validade: 15/06/2022
Emissor: AC LINK RFB v2
Data: 10/03/2021 16:29

Agradecimentos

Gostaria de agradecer à coordenadora de área onde trabalho na ANATEL em São Paulo, Maria Aparecida Lourenço que foi a primeira a dar o sinal verde para que eu pudesse realizar esse projeto, e que também me deu o suporte durante essa longa jornada de 26 meses. (mais metade desse tempo passando pela pandemia do Covid-19).

Agradeço a Deus e aos meus familiares pelas vigílias durante esse período.

Agradeço ao orientador, o Professor Doutor Luiz Cláudio Gomes Maia, pela maestria na condução dos trabalhos.

Aos professores do curso que “asfaltaram” minha estrada.

E colegas de percurso durante a temporada, pelo sofrimento em comum, pela união de forças e pelos momentos de descontração e brincadeiras, pois tudo isso faz parte da vida acadêmica e deixa saudades.

Agradeço ao Professor Doutor Rodrigo Moreno Marques pelo início de tudo.

Agradeço a amiga Doutora Maria Ângela de Souza Fernandes pela inspiração.

E em especial, a professora Doutora Cristiana Fernandes De Müylder pelos ensinamentos e pela amizade.

“A Idade da Pedra chegou ao fim, não por falta de pedras”.

Sheikh Ahmed Zaki Yamani (1973).

Resumo

Uma das abordagens que lidam com os desafios atuais no campo do planejamento urbano e tecnológico é o desenvolvimento de *smart cities*. Mas, com a chegada de novos modelos para *smart cities* (cidades inteligentes) em ambiente de internet com "coisas" conectadas, vieram também as ameaças de ataques, fraudes e golpes. Portanto, urge desenvolver e adotar novas tecnologias para prover a segurança da informação frente a agentes maliciosos. Nessa visão, a presente investigação traz respostas à seguinte indagação: quais seriam as técnicas de *blockchain* que podem contribuir para aumentar o nível de segurança da informação em *smart cities*? Para se obter essas respostas, traçou-se uma metodologia para fazer a revisão sistemática de literatura em *sites* de pesquisa científica na internet. A revisão foi baseada nos ensinamentos registrados na literatura. A fundamentação teórica passou por internet das coisas (IoT), *blockchain* e *smart cities,* aplicada à tecnologia de informação e comunicação. A pesquisa responde aos objetivos com variada gama de opções e aplicações. Dada a natureza descentralizada da *blockchain,* já se pode dizer que muitos problemas/ameaças são evitados/minimizados. Baseados nesse atributo, somos levados a concluir que o mais importante é que a *blockchain*, uma vez implementada, sempre vai melhorar as condições de segurança da informação no sistema. Entende-se que não foi objetivo da pesquisa esgotar o assunto, mas deve-se ressaltar que instiga trabalhos futuros como o aprimoramento do uso de *blockchain* usando inteligência artificial.

Palavras-chave: *Smart Cities*. Cidades Inteligentes. Internet das Coisas (IoT). *Blockchain*. Segurança da Informação.

Abstract

One of the approaches that deals with the current challenges in the field of urban and technological planning is the development of smart cities. But, with the arrival of new models for smart cities in an Internet environment with "things" connected, threats of attacks, frauds and scams also came. Therefore, there is an urgent need to develop and adopt new technologies to provide information security against malicious agents. Within this view, the present investigation provides answers to the following question: what are the blockchain techniques that can contribute to increasing the level of Information Security in smart cities? To obtain these answers, a methodology was drawn up to systematically review the literature on scientific research sites on the internet. The review was based on literatures' teachings. The theoretical foundation went through the internet of things (IoT), blockchain and smart cities, always applied to information and communication technology. The research responds to objectives with a wide range of options and applications. Given the decentralized nature of the blockchain it can already be said that many problems / threats are avoided / minimized based on this attribute. Therefore, we are led to conclude that the most important thing is that the blockchain, once implemented, will always improve the information security conditions in the system. It’s understandable that it was not the objective of the research to exhaust the subject, it should be emphasized that the present study instigates future works such as improving the use of blockchain using artificial intelligence.

Keywords: Smart Cities. Internet of Things (IoT). Blockchain. Information Security.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

2FA	*Two-factor authentication*
ABI	Interface binária de aplicativo
ACM	*Association for Computing Machinery*
Add-on	*Software acessório ou extensão*
APIs	*Application Programming Interface*
AWS	*Amazon Web Services*
BaaS	*Blockchain-as-a-service*
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CA	Autoridade certificada
CCTV	Circuito fechado de televisão
CIA	*Confidentiality Integrity and Availability*
CISO	Diretor de Segurança da Informação
CNJ	Conselho Nacional de Justiça
DAG	Gráfico acíclico direcionado
DApps	Plataforma para desenvolver aplicações descentralizada
DDoS	*Denial of service*
DL	*Distributed ledger*
DLT	*Distributed ledger technology*
DoS	A ataque de negação de serviço
DPoS	Prova de aposta delegada
ECC	Criptografia de curva elíptica
EEA	*Ethereum Enterprise Alliance*
ERP	*Enterprise Resource Planning*
FedEx	*Federal Express*
GHZ	Greenberger-Horne-Zeilinger
Hash	Algoritmo matemático para a criptografia
HVAC	*Heating, ventilation, and air conditioning*
IA	Inteligência artificial
IaaS	*Infrastructure-as-a-service*
IBM	*International Business Machines*
ID	Identificação digital
IoT	Internet *of things*

IoV	Internet *of Vehicles*
IP	Internet *protocol*
IPv6	Internet *Protocol version* 6
ISO	*International Organization for Standardization*
ITS	Sistemas de transporte inteligentes
ITU	*International Telecommunication Union*
ITU-T	*International Telecommunication Union Standardization Sector*
LGPD	Lei geral de proteção de dados
LNSC	Modelo de negociação baseado em *blockchain*
M2M	*Machine to machine*
MB	Mercado Bitcoin
Medline	*Medical Literature Analysis and Retrieval System On-line*
MoU	Memorando de entendimento
MQTT	*Message Queue Telemetry Transport*
MVP	Produto de valor mínimo
MySQL	*Structured query language*
NE	Elemento de rede
ONU	Organização das Nações Unidas
OSI	*Open Systems Interconnection*
P2P	Par a par
PaaS	*Platform-as-a-Service*
PETCON	Sistema de comércio de eletricidade P2P baseado em *blockchain*
PHEVs	Veículos elétricos híbridos *plug-in*
PICOS	*Population, Intervention, Comparison, Outcome, Study type*
PIN	*Personal identification number*
PoA	Prova de autoridade
POC	Prova de conceito
PoET	Prova do tempo decorrido
PoS	Prova de aposta
PoW	Prova de trabalho
PQB	*Post quantum blockchain*
PubMed	Publicações Médicas
QDK	*Quantum distributed key*
qTESLA	Esquemas de assinatura pós-quântica

RSA	Rivest, Shamir e Adleman
Saas	*Software-as-a-Service*
SBAB	SBAB *Stockholm Bank*
SCADA	Controle de supervisão e dados aquisição
SciElo	*Scientific Electronic Library Online*
SCM	*Supply Chain Management*
SHA 256	*Secure hash algorithm*
SSI	Identidade autossoberana
Tbps	*Terabits* por segundo
TCP	*Transmission Control Protocol*
TCU	Tribunal de contas da união
TI	Tecnologia da Informação
TIC	Tecnologia de informação e comunicação
UDP	*User datagram protocol*
UNECE	*United Nations Economic Commission for Europe*

Sumário[1]

[1] Este trabalho foi revisado de acordo com as novas regras ortográficas aprovadas pelo Acordo Ortográfico assinado entre os países que integram a Comunidade de Países de Língua Portuguesa (CPLP), em vigor no Brasil desde 2009. E foi formatado de acordo com as Instruções para Formatação de Trabalhos Acadêmicos – Norma APA, 2019.

1 Introdução

O conceito de *smart cities* é oriundo das primeiras iniciativas de implantação de serviços de tecnologia de informação e comunicação (TIC) nas cidades que então se passaram a ser denominadas de cidades digitais, plugadas ou conectadas. *Smart cities* transcendem esse conceito, por irem além: elas devem integrar todas as soluções tecnológicas disponíveis a ela, incluindo nesse processo, principalmente, em tese, o cidadão, oferecendo-lhe condições para que ele atue como protagonista das soluções e serviços (INATEL, 2019).

Smart city, cidade inteligente, é aquela que supera os desafios do passado e conquista o futuro, sendo importante ressaltar que a tecnologia tem que estar presente para desempenhar esse papel (Cunha, Przeybilovicz, Macaya & Burgos, 2016).

Elas representam o assunto de interesse, com características de multidisciplinaridade, constantemente moldado com pensamento no desenvolvimento urbano, crescimento econômico e desenvolvimento da tecnologia urbana (Angelidou, 2017).

A complexidade envolvida na realização de *smart cities* com variadas redes de atores demanda um entendimento diferente do desenvolvimento de políticas urbanas, processos de direção e gestão operacional, até então percebidos. É necessário ter o entendimento de que o próprio governo urbano é uma das partes interessadas, e entre outras atuações deve priorizar a segurança da informação.

Entretanto, segurança e privacidade não vinham tendo ênfase em bases de sistemas de *smart cities* e não eram abordados prioritariamente, até quando chegaram os inesperados ataques *Denial of Service* (DDos) *Conducting Distributed Denial of Service* e ameaças de *ransomware* como *cryptolocker* (Liao et al., 2016), *cryptowall* (Cabaj & Mazurczyk, 2016) e *wannacry* (Mohurle & Patil, 2017). Os reflexos foram em escalas mundiais, fatos que geraram sentimento de desconfiança contra a internet das coisas (IoT), um dos três pilares das *smart cities* além de pessoas e processos. Alguns criticaram a IoT por ter se tornado a “internet das vulnerabilidades” (Angrishi, 2017).

A partir desse evento, pesquisadores envolvidos com IoT e comunidades de *smart cities* reagiram focando também em uma nova onda de pesquisas voltadas para a investigação da segurança cibernética e da privacidade de dados naquele âmbito. As empresas começaram a anunciar produtos seguros para *smart cities*. No entanto, as considerações aqui mencionadas sobre a segurança cibernética de *smart cities* transformaram muitos desses produtos seguros em vulneráveis a ataques cibernéticos não convencionais (Arias, Wurm, Hoang & Jin, 2015). O projeto de serviços robustos e seguros depende da compreensão de vários aspectos da pesquisa de segurança cibernética.

Com a chegada da tecnologia de *blockchain,* vieram as oportunidades de vencer tais desafios (Dai, Zheng & Zhang, 2019). Nesse contexto são explorados temas sobre a segurança da informação nessas cidades, bem como mostrar qual a melhor maneira de fazê-la eficazmente.

Já o conceito de *blockchain* surgiu há quase 12 anos, com o aparecimento da criptomoeda, a Bitcoin, introduzida por Satoshi Nakamoto (2008). A ideia original da *blockchain* foi proposta como segurança em criptomoeda. Ao investigar o potencial da *blockchain*, tem-se que ela foi reconhecida como a espinha dorsal das áreas onde o termo "inteligente" está associado. Ela oferece abordagem não centralizada, em que nenhum ente apenas detém o controle, e que os dados nunca são apagados, proporcionando a imutabilidade. Houve grande ênfase no uso de *blockchain* em uma variedade de aplicações, como em soluções que atendem à privacidade de identidade e proteção de transações usando uma estrutura não centralizada por meio de diversos métodos de contrato (inteligente). Exatamente em espaços progressivamente digitalizadas, como em *smart cities* (Aggarwal, Chaudhary, Aujla, Kumar, Choo & Zomaya, 2019).

Outros autores, como Sharma & Park (2018), reforçam que *blockchain* opera na vida real prometendo trabalhar para criar ambiente confiável, transparente, robusto e não centralizado. Fornece assistência segura, na qual *smart cities* podem ampliar o valor da vida, garantir processos administrativos e sustentabilidade ambiental. Oferece serviços não centralizados, segurança, preservação da privacidade, imutabilidade e

autenticidade e rastreabilidade. O conceito e a necessidade de s*mart cities* atraíram muita atenção devido ao seu contexto prático e realista. O reconhecimento de *smart cities* está intimamente ligado ao mesmo ponto de vista da IoT.

Este trabalho aborda os conceitos de internet das coisas (IoT), *smart cities* e *blockchain*, e o modo como eles se integram para prover a segurança da informação em *smart cities.*

1.1 O problema de pesquisa

A seguir, conforme explicam Georgescu & Popescul (2016), será visto que as vulnerabilidades na IoT são resultantes de sua natureza especial dos objetos interconectados e da grande variedade e sensibilidade dos dados coletados. Essas vulnerabilidades da IoT enfraquecem a segurança da informação em *smarts cities*, pois estas se baseiam naquela. Esse é um dos motivos de se falar em melhorar o nível de segurança.

A urbanização sem planejamento adequado levou as cidades à degradação e criou condições que não apenas levaram ao colapso certas cidades, como também deteriorou a qualidade de vida dos cidadãos. Ficou impossível, com os métodos atuais de administração e desenvolvimento urbano, reverter tal nível de degradação. Uma das abordagens que lidam com os desafios atuais no campo do planejamento urbano e tecnológico é o desenvolvimento de *smart cities*. Com a chegada de seus novos modelos em ambiente de internet com "coisas" conectadas, vieram também as ameaças de ataques, fraudes e golpes. Portanto, urge desenvolver e adotar novas tecnologias para prover a segurança da informação frente a novos agentes maliciosos.

Esta pesquisa visa ampliar o leque de possibilidades de se usar outras técnicas mais aprimoradas para a segurança da informação. Aqui será enfocada a *blockchain* e, portanto, serão pesquisadas quais técnicas de *blockchain* podem ser adotadas para contribuir com o aumento do nível de segurança da informação em *smart cities*.

1.3 Lacuna a ser explorada

Este trabalho pretende buscar o conhecimento necessário para entender e analisar o assunto segurança da informação e, a partir disso, recomendar a aplicação e o uso de tecnologia de *blockchain* como um fator a mais para aumentar segurança da informação em *smart cities,* bem como internalizar esse conhecimento no Brasil para órgãos de governo, estatais e autarquias.

1.4 Justificativa/Importância do tema

Pode-se argumentar a relevância do tema frente a duas posições. A primeira, em relação ao cenário brasileiro. O Brasil é o segundo no mundo em perdas econômicas por ataques cibernéticos, conforme revelou audiência realizada no Senado em 05/09/2019. Essa foi a posição no índice de segurança cibernética da União Internacional de Telecomunicações (ITU, 2014), na sigla em inglês, órgão da Organização das Nações Unidas (ONU) que coordena, regulamenta e obtém as estatísticas em TIC.

Ainda segundo esse organismo internacional (ITU), naquela data, a partir de estudo realizado por 12 meses nos anos de 2017 e 2018, os prejuízos advindos dos ataques cibernéticos no Brasil ultrapassaram US$ 20 bilhões (mais de R$ 80 bilhões). Ainda em 5 de fevereiro de 2020, o Decreto nº 10.222 (Brasil, 2020a) exarou diversas iniciativas com a publicidade da estratégia de segurança da informação e comunicações e de segurança cibernética (*E-Ciber*). Um dos objetivos é elevar o estágio de maturidade e atender às necessidades do país em segurança cibernética, considerando os aspectos relativos ao ecossistema digital, nos âmbitos nacional e internacional. Desse modo, objetivos estratégicos visam nortear as ações estratégicas do país em segurança cibernética e representam macrodiretrizes basilares para que o setor público, o setor produtivo e a sociedade possam usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro.

A segunda frente refere-se aos esforços do governo federal para tornar o país moderno, ágil, com burocracia mínima, transparente e seguro, levando o Brasil a

estágio de maturidade tecnológica, e atender às necessidades do país em segurança cibernética, considerando aspectos relativos ao ecossistema digital, nacional e internacionalmente.

1.5 Objetivos

O objetivo principal é indicar aplicações e usos da tecnologia de *blockchain* que podem ser implementadas como alternativa de segurança da informação em *smart cities.*

Como objetivos específicos, são pesquisas que vão pavimentar a estrada até se atingir os objetivos específicos, quais sejam:

a) Analisar, qualificar e listar aplicações e usos de *blockchain* que podem ser implementadas em *smart cities,* para aumentar seu nível de segurança.
b) Mostrar suas implicações e impactos.
c) Identificar e caracterizar como as tecnologias de *blockchain* se relacionam aos sistemas de informação de *smart cities*, evidenciando suas características, parâmetros, aplicações e usos, que também farão parte essencial deste estudo.

2 Fundamentação Teórica

Neste capítulo apresentam-se conceitos e ensinamentos de obras consolidadas na literatura sobre *smart cities*, internet das coisas (IoT) e *blockchain*. São mostradas também as integrações entre essas três tecnologias e o modo como elas se interpenetram, preparando o ambiente para o entendimento da segurança da informação nesse particular.

2.1 *Smart cities*

Inicialmente, faz-se necessário entender como a comunidade envolvida define, conceitua ou aborda *smart cities* em suas diversas dimensões e perspectivas:

Tabela 1

Exemplos de definição de *smart cities*

Fonte	Referência	Definição/conceito
Acadêmica	Meijer & Rodríguez Bolívar, 2013	"Acreditamos que uma cidade é inteligente quando investimentos em capital humano, social e infraestrutura de comunicação tradicional (transporte) e moderna (TIC – [Tecnologia da Informação e Comunicação]) impulsionam o crescimento econômico sustentável e a alta qualidade de vida, com uma gestão inteligente dos recursos naturais, por meio de governança participativa".
Corporativa	Hitachi, 2014	A visão da Hitachi para a cidade inteligente busca alcançar a preocupação com o meio ambiente global, a segurança e conveniência do estilo de vida por meio da coordenação da infraestrutura. As cidades inteligentes sustentáveis realizadas por meio da coordenação de infraestruturas, consistem em duas camadas de infraestrutura que oferecem suporte ao estilo de vida dos consumidores, juntamente com a infraestrutura de gestão urbana que as conecta usando TIC.
Órgãos de governo	Giffinger, Fertner, Meijers & Kramar, 2007	"Uma cidade com bom desempenho de maneira voltada para o futuro em economia, pessoas, governança, mobilidade, meio ambiente e vida, construída sobre a combinação inteligente de dotações e atividades de cidadãos autodecididos, independentes e conscientes".
Agência Internacional	ITU *Focus Group*	É uma cidade com grande, eficiente e difundida rede tecnológica que fomenta o diálogo entre os cidadãos e os objetos do cotidiano. Integra a grande quantidade de informação disponível para gerar inteligência e melhorar o dia a dia num estilo de vida cada vez mais "inteligente". Combina inovação com meio ambiente, mobilidade e qualidade de vida. É um fenômeno novo, complexo e em rápida mudança. A inovação tecnológica avança em várias direções (edifícios verdes, mobilidade inteligente, e-saúde, e-governo).
Organização p padronização	ITU/UNECE, 2017	"Uma cidade inteligente e sustentável é uma cidade inovadora que usa tecnologias de informação e comunicação (TICs) e outros meios para melhorar a qualidade de vida, a eficiência da operação, serviços urbanos e a competitividade, garantindo que atenda às necessidades do presente e do futuro das gerações no que diz respeito aos aspectos econômicos, sociais e ambientais".

Unece: *United Nations Economic Commission for Europe*.
Traduções nossas.

Conforme descrito pela União Internacional de Telecomunicações (ITU, 2012), a sustentabilidade está melhorando a qualidade da vida humana enquanto se vive dentro da capacidade de suporte dos ecossistemas. Entre outras definições, atualmente “sustentabilidade” é usada como um termo genérico para toda atividade humana projetada para atender às necessidades atuais, sem prejudicar a capacidade de atender às necessidades das gerações futuras em termos de desafios econômicos, ambientais e sociais.

A *International Telecommunication Union* (ITU) é a agência especializada das Nações Unidas na área de telecomunicações, informações e tecnologias de comunicação (TICs). A *International Telecommunication Union Standardization Sector* (ITU-T) é um órgão permanente da ITU. A ITU-T é responsável pelo estudo das questões técnicas, operacionais e tarifárias e por emitir recomendações sobre estas, com o objetivo de padronizar as telecomunicações em nível mundial (ITU-T, 2014).

Acredita-se que não faz sentido estabelecer *smart city* que não seja sustentável. Portanto, quando se mencionar no texto *smart cities*, está-se referindo a s*ustainable smart cities* sustentáveis.

Novas pesquisas e relatórios de políticas revelam sinergias e benefícios na interseção de desenvolvimento urbano inteligente com sustentabilidade, conforme pode ser visto no referenciado estudo da série *World Urbanization Prospects* das Nações Unidas (*United Nations*, 2014), que não apenas documenta consistente tendência à urbanização global, mas também assevera que essa tendência evoluirá até pelo menos 2050. E, mais importante, demanda políticas integradas para melhorar as condições de vida urbana e rural e destaca o papel da tecnologia na mitigação dos crescentes desafios da sustentabilidade. De acordo com esse relatório, as implicações políticas decorrentes desse estudo incluem, entre outras, a necessidade de ter dados precisos, consistentes e atualizados para municiar a elaboração de políticas relacionadas à cidade, bem como o uso de tecnologias de informação e comunicação (TICs) para facilitar um modo sustentável de urbanização que aprimore e ofereça serviços de maneira mais eficiente às partes interessadas.

As Nações Unidas começaram a pesquisa orientada a ações nessa direção, explorando o papel das tecnologias para o desenvolvimento sustentável e, segundo esse conceito, *smart city* é baseada em três elementos principais: pessoas, tecnologia e processos.

Smart cities basicamente se apoiam em TIC (tecnologia), no seu tripé citado. A TIC permeia todas as dimensões de *smart city.* Portanto, sistemas de informação e a segurança da informação estão presentes ubiquamente em todos os seus processos.

Desse tripé, nesta pesquisa a abordagem é feita apenas no elemento tecnológico, e dentro deste a segurança da informação, que é o nosso objeto de estudo, e também seus reflexos que abarcam toda a estrutura de *smart cities.*

2.1.1 Os seis âmbitos de smart cities

Essa proposição foi posta em "*Smart cities*: *ranking of European medium sized cities*", *Centre of Regional Science*, *Vienna University of Technology*, outubro de 2007. Esse estudo apresenta múltiplos ângulos e focos de atenção, razão pela qual o conceito *smart city* foi decomposto em diferentes âmbitos.

A União Europeia, por exemplo, decompõe tal conceito da mesma maneira: esse conceito geral tem influenciado empresas e instituições em todo o mundo e foi adotado pelo Parlamento Europeu (European Comission, 2014).

a) *Smart economy*; (Economia): refere-se à competitividade de uma cidade com base em sua abordagem inovadora de negócios, pesquisa e desenvolvimento, empreendedorismo oportunidades, produtividade, flexibilidade dos mercados de trabalho e o papel econômico da cidade nos mercados nacional e internacional.
b) *Smart people*; (Educação): refere-se a fornecer alto nível de educação consistente aos cidadãos, bem como descrever a qualidade das interações sociais, a consciência cultural, a transparência e o nível de participação do cidadão na vida social.

c) *Smart mobility* (logística e infraestrutura): a mobilidade inteligente dá suporte a sistemas de transporte mais eficientes (por exemplo, opções não motorizadas) e impulsiona novas atitudes sociais em relação ao uso de veículos, o que garante o acesso dos cidadãos ao transporte público. A TIC aumenta a produtividade integrada. As *smart cities* buscam promover o movimento de pesso*as,* mercadorias e veículos em um ambiente urbano.

d) *Smart environment* (meio ambiente, sustentabilidade): o ambiente inteligente enfatiza a necessidade de uma gestão responsável de recursos e do planejamento de cidades sustentáveis. A beleza natural da cidade pode ser aumentada reduzindo as emissões de gases de efeito estufa e os esforços para proteger o meio ambiente. As *smart cities* promovem a eficiência energética, e a integração da inovação tecnológica leva a ganhos de produtividade.

e) *Smart living*;(segurança, saúde e qualidade de vida): vida inteligente, busca melhorar a qualidade de vida dos cidadãos por meio da oferta de condições de vida seguras e saudáveis. Cidadãos em cidades inteligentes têm fácil acesso a serviços e cuidados de saúde, gerenciamento eletrônico de saúde e serviços sociais.

f) *Smart governance* (gestão pública de *smart cities*): governança inteligente, aborda especificamente a participação dos cidadãos no nível municipal. O sistema de governo é transparente e permite que os cidadãos participem na tomada de decisão. As TICs facilitam a participação dos cidadãos e o acesso às informações e dados relacionados à gestão de sua cidade. Ao criar um sistema de governança estável e eficaz, as barreiras à comunicação e colaboração podem ser eliminadas. Os comentários a respeito de cada uma dessas dimensões da *smart city* são de autoria de Pourahmad, Ziari, Hataminejad & Parsa (2018).

2.1.2 Conexão de dispositivos em smart cities

As cidades usam dispositivos em soluções especializadas, como monitoramento de tráfego, medições de qualidade do ar e contaminação da água, entre outros. Soluções de IoT são compradas por linhas de negócios com um problema específico para ser resolvido, como mostrar o progresso de limpadores de neve no inverno. Isso se torna uma prioridade política e deve ser feito com rapidez e eficiência. Consequentemente, o projeto é conceituado e adquirido fora dos processos usuais de aquisição e implementação de tecnologia que está em vigor.

Por isso, muitas implementações de *smart cities* hoje são coleções desordenadas, com dispositivos que têm pouca ou nenhuma interoperabilidade e são difíceis de gerenciar. Eles foram adquiridos por alguém com necessidade tática em um domínio específico, mas não de acordo com qualquer iniciativa de tecnologia central geral ou visão estratégica. É importante considerar isso ao trabalhar com tecnologia de *smart cities*, pois elas apresentam uma série de desafios arquitetônicos que podem ser muito difíceis e caros de se trabalhar (Lisdorf, 2020). Ou seja, as compras de soluções técnicas devem ser planejadas e as tecnologias devem ser compatíveis entre si.

2.1.3 Gerenciando dispositivos em smart cities

Apesar da utilidade dos dispositivos conectados, eles também podem se tornar um grande desafio. Sistemas de tecnologia da informação (TI) em um contexto de *smart cities* têm uma janela de serviço, existem sistemas para implantar novas versões do código e é fácil reverter se algo der errado. Por exemplo, um sistema de contabilidade. Ninguém estaria usando esse sistema no domingo à noite, então, ele pode ser completamente fechado e atualizado. Ao inicializar, os funcionários testam e, se não funcionar, a cidade pode simplesmente voltar para a versão antiga e corrigir a atualização (Lisdorf, 2020).

Lisdorf continua, e afirma que para dispositivos conectados as coisas não funcionam assim. Mesmo para os dispositivos menos críticos, como medidores de água, é difícil encontrar um mecanismo para implantar um novo código. Lembre-se de que os

sistemas embarcados geralmente vêm pré-codificados de fábrica e normalmente não são feitos para serem atualizados constantemente.

Uma sistemática são as atualizações, mas outra coisa é a conectividade básica. Normalmente, é desejável ter algum tipo de conexão a um dispositivo e obter leituras dele se for um sensor ou controlá-lo se for um atuador. Uma das preocupações deve ser a segurança. Quando um dispositivo estava em uma rede fechada em casa, isso não era um grande problema, já que a segurança baseada no perímetro da rede garantia que ninguém pudesse obter acesso ao dispositivo se o usuário protegesse sua rede pessoal doméstica. Câmeras de segurança eram originalmente em circuito fechado ou pelo menos em uma rede interna cabeada conectada a um computador, onde se podiam assistir as imagens/vídeos das câmeras (Lisdorf, 2020).

Segundo o mesmo autor, há pouco tempo, as câmeras de segurança tornaram-se câmeras internet *protocol* (IP) baseadas na internet. A parte boa é que não se precisa preocupar tanto em construir a rede, como adicionar novas câmeras. Todas as câmeras ficaram fáceis de alcançar a partir de qualquer computador com ligação à internet, em qualquer lugar do mundo.

Nesse aspecto, fica claro que a segurança da rede pessoal acabou, pois a conectividade com o dispositivo na internet não pode ser considerada confiável. Para garantir a proteção da confidencialidade do dispositivo é necessário dispor de mecanismos. A autenticação torna-se importante para dispositivos quando eles estão na Internet e não mais atrás de um *firewall* em uma rede interna. Existem soluções boas e comprovadas para isso, como usar certificados para autenticar e estabelecer uma conexão confiável. Todas as principais plataformas em nuvem do mercado possuem algum tipo de segurança para gerenciar dispositivos conectados. A *Amazon Web Services* (AWS) tem a plataforma AWS IoT, Azure, o Hub IoT (Lisdorf, 2020), que serão vistas a seguir em *blockchain-as-a-Service* (BaaS).

Quando se deseja gerenciar dispositivos em uma cidade inteligente, a escalabilidade rapidamente se torna um grande problema. Quando se vai além da prova de conceito

(POC) e das implementações maiores, com grande quantidade de dispositivos, o jogo muda radicalmente.

Uma cidade como Nova York tem mais de 30.000 veículos em sua frota. Cada veículo possui um dispositivo para rastrear sua localização. Ela também tem centenas de milhares de medidores de água. Ou seja, a geração de informações é enorme (Lisdorf, 2020). Naquela cidade foi necessário desenvolver mecanismos diferentes, mas eficientes, que foram empregados para dimensionar as implementações de *smart cities* envolvendo dispositivos conectados. Os grandes fornecedores de tecnologia que vendem plataformas de IoT não têm, ainda em 2020, grandes soluções prontas para fazer isso em escala, o que é uma limitação importante ao se considerar o uso de suas plataformas como base para iniciativas de *smart cities* (Lisdorf, 2020).

2.1.4 Comunicação com dispositivos

Quando um dispositivo estiver conectado a uma plataforma ou solução central, geralmente opera-se com uma representação central desse dispositivo. Isso é chamado de gêmeo digital ou sombra digital, dependendo do fornecedor. A ideia é que o sistema centralizado monitore o estado atual do dispositivo. Assim, pode-se gerenciar esse dispositivo conectado (Lisdorf, 2020).

O mesmo autor sugere considerar um semáforo que pode assumir os valores de vermelho, amarelo e verde. A sombra digital pode relatar que atualmente está verde. A central deverá ler esse *status* verde e poderá enviar um comando para mudar o *status* de verde para vermelho. Ou seja, a central tem que trocar dados com os dispositivos para que isso aconteça. Os dados/informações recebidos do dispositivo são chamados de dados de telemetria. Essa medição pode ter muitos formatos diferentes e frequentemente é codificada em algum protocolo proprietário que é ininteligível. Às vezes, as leituras estão em um formato de máquina que precisa de interpretação para fazer sentido; às vezes, é criptografado. É difícil trabalhar com dados de dispositivos em seu formato bruto.

O padrão emergente para comunicação com dispositivos é o protocolo *Message Queue Telemetry Transport* (MQTT). Esse padrão foi inicialmente criado pela *International Business Machines* (IBM). É um protocolo leve que usa um padrão publicar-assinar. Isso significa que certas informações, como leituras de dispositivos, são publicadas em um tópico. Os clientes podem se inscrever nesse tópico e receber informações. O protocolo MQTT é construído sobre o protocolo *Transmission Control Protocol /* internet *protocol* (TCP/IP). Ressalta-se que o TCP era o protocolo usado na camada de transporte. A vantagem do sistema TCP/IP é que ele é seguro e confiável e garante que todos os pacotes de dados sejam recebidos e contabilizados. É a base da internet e, portanto, muito difundido (Soni & Makwana, 2017).

Santos, Silva, Celes, Borges Neto, Peres, Augusto, Vieira, Vieira, Goussevskaia e Loureiro (2016) reforçam que o MQTT é um protocolo projetado para dispositivos limitados, tal e qual dispositivos de tecnologia IoT, e utiliza a estratégia de *publish/ subscribe* para transferir mensagens. Seu principal objetivo é minimizar o uso de largura de banda da rede e economizar recursos dos dispositivos. Além disso, provê mecanismos para a garantia de entrega de mensagens. O MQTT utiliza os protocolos das camada de transporte e rede da arquitetura TCP/IP.

Muitos dispositivos usam *User datagram protocol* (UDP). Este tem um modelo de conexão muito mais simples e não fornece o *handshake* que o TCP oferece. Isso significa que o UDP é considerado menos seguro e mais sujeito a erros, pois não há reenvio de pacotes em caso de perdas ou erros, como no TCP. A vantagem é que ele tem muito menos sobrecarga e é mais rápido. Aplicativos sensíveis ao tempo que não precisam ter a ordem correta dos pacotes e que podem lidar com um pouco de ruído, portanto, muitas vezes empregam UDP. Por exemplo, se se estiver transmitindo continuamente localizações ou um *feed* de vídeo, pode não ser um grande problema se algumas coordenadas de localização ou alguns quadros forem perdidos. Pode-se facilmente reconstruir a rota do veículo e seguir a imagem/vídeo gerado e transmitido (Lisdorf, 2020).

2.2 Internet das coisas – IoT (*internet of things*)

Khan (2019) entende que a IoT é um sistema distribuído de TIC que integra sensores, dispositivos de computação, algoritmos e objetos físicos conhecidos como coisas que são identificáveis de forma única. As coisas têm a capacidade de coletar e transferir dados a sistemas conectados sem qualquer intervenção humana, oferecendo, assim, capacidade de processamento de dados autônomos. Uma rede de comunicação é um dos elementos-chave de um sistema IoT que permite o fluxo de informações entre uma variada gama de tipos de sensores, atuadores, dispositivos, controladores e armazenamentos de dados, etc.

Animada por tecnologias, Khrais (2020) explica que a Quarta Revolução Industrial está em curso, crescendo exponencialmente à medida que o mundo se transforma em uma conexão *web*. Novos mercados surgem, como *smart cities* que utilizam tecnologias como pagamento *online*, conectividade com a internet e *blockchain*, entre outras, para realizar transações de forma rápida e segura. Para Khrais (2020), a Quarta Revolução Industrial é movida a dados e, portanto, qualquer tecnologia que faça uso intensivo de dados como a internet das coisas, computação em nuvem, aprendizado de máquina e inteligência artificial agrega valor e tende a ser amplamente utilizada.

Xia, Yang, Wang & Vinel (2012) entendem que o objetivo da IoT é permitir que as coisas sejam conectadas. Os objetos tornam-se reconhecíveis e obtêm inteligência ao tomar ou possibilitar decisões relacionadas ao cenário, regidas pelos *smart contratcs*, e pelo fato de que podem trocar informações sobre si mesmos, obtendo informações de outros. Eles podem acessar informações que foram agregadas por outras coisas ou podem ser componentes de serviços complexos. Essa transformação foi possível graças ao surgimento de capacidades de computação em nuvem, à transição da internet para Internet *Protocol version* 6 (IPv6) com capacidade de endereçamento quase ilimitada, *Big Data*, entre outros.

Internet das coisas (IoT) é um conceito e um paradigma que considera a presença generalizada no ambiente de uma variedade de coisas/ objetos que, por meio de conexões sem fio e com fio e esquemas de endereçamento exclusivos, são capazes

de interagir entre si e cooperar com outras coisas/ objetos para criar aplicativos/ serviços e atingir objetivos comuns. Dessa forma, os desafios de pesquisa e desenvolvimento para criar um mundo inteligente são significativos. Um mundo onde o real, o digital e o virtual estão convergindo para criar ambientes inteligentes que tornam a energia, os transportes, as cidades e muitas outras áreas mais inteligentes (Xia *et al*., 2012).

O número de dispositivos presentes na IoT é alto e variado. Questões relacionadas a representação de informações, armazenamento de informações, interconexões, busca e organização das informações produzidas pela IoT tornaram-se muito complexas. Diferentes abordagens categorizadas como abordagens estruturais, abordagens metodológicas e abordagens de *design* têm sido discutidas. Na internet atual, os domínios de aplicativos são separados. São necessárias técnicas de padronização para unir, logicamente, todos os domínios de aplicativos separados de maneira inteligente (Haroon, Ali, Asim, Naeem, Kamran & Javaid, 2016).

A diversidade dos dispositivos é uma característica peculiar da IoT, o que levou ao problema principal, que é interoperabilidade. Considera-se que a normalização das tecnologias conduz a melhor interoperabilidade, já que a interoperabilidade depende de padrões para funções e interfaces. O desafio é resolver as falhas de interoperabilidade técnica entre diversos dispositivos. Destaca-se que, no cenário de comunicação máquina a máquina (M2M), as técnicas de padronização fornecem um *middleware* para lidar com os mecanismos de comunicação, gerenciamento de dispositivos e acessibilidade entre terminais. Além disso, é necessário seguir padrões para que os dispositivos funcionem juntos na mesma plataforma da IoT (Haroon *et al*., 2016).

2.2.1 Aplicações típicas de IoT

O IoT facilita o desenvolvimento de uma quantidade de aplicações orientadas para a indústria, comércio, governo, além de aplicações específicas do usuário. Enquanto os dispositivos e as redes fornecem conectividade física, os aplicativos IoT permitem interações entre dispositivos e entre pessoas. Os aplicativos IoT precisam garantir que

os dados/mensagens foram transmitidos, recebidos e tratados de maneira correta e em tempo hábil. Por exemplo, os aplicativos de transporte e logística monitoram o estado dos bens transportados, como frutas, produtos minimamente processados, carnes e laticínios. Durante o transporte, o estado de conservação (temperatura, umidade, etc.) é monitorado constantemente e as ações apropriadas são tomadas para evitar problemas nos alimentos quando a conexão está fora de área de cobertura (Lee & Lee, 2015).

Por exemplo, a *Federal Express* (FedEx) usa o *software SenseAware* para controlar a temperatura, a localização e outros sinais vitais de um pacote, incluindo quando ele é aberto e se foi adulterado ao longo do caminho. Cada vez mais os aplicativos IoT centrados no ser humano fornecem visualização para apresentar informações aos usuários finais. e permitir a interação com o ambiente.

Com base nas tendências de tecnologia, Lee & Lee (2015) identificam três categorias de IoT para aplicativos corporativos:

a) Monitoramento e controle;
b) *big data* e análise de negócios;
c) compartilhamento e colaboração de informações.

Compreender como essas três categorias de IoT podem aumentar o valor para o cliente de uma organização é um pré-requisito para a adoção de IoT com sucesso (Lee & Lee, 2015).

A seguir, além dessas três categorias de IoT, tem-se uma ilustração de diversas ideias de aplicativos de IoT do mundo real.

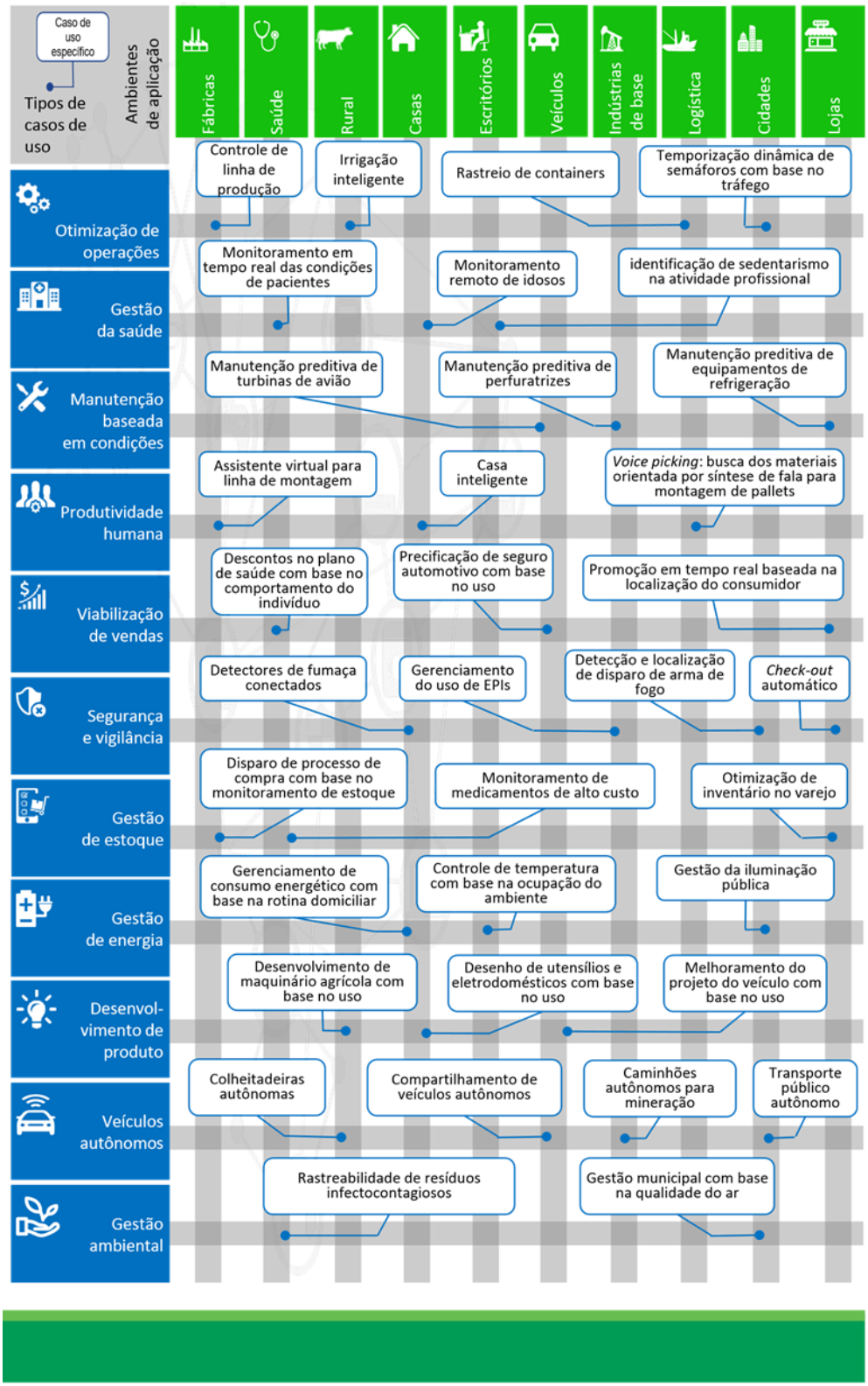

Figura 1
Casos de uso nos principais ambientes de aplicação de IoT.
Fonte: Banco Nacional de Desenvolvimento Econômico e Social (BNDES, 2017)..

2.2.2 *Os requisitos da IoT*

A Figura 2 mostra as seis dimensões principais necessárias para implantar a IoT orientada a serviços. Cinco fatores-chave para implantar a internet do futuro: dispositivos inteligentes, redes avançadas, computação em nuvem e *big data analytics,* que neste trabalho não terão ênfase. Já o fator mais crítico, a segurança, receberá mais atenção, pois é nele que a chave desta pesquisa se encontra (Haroon *et al*., 2016).

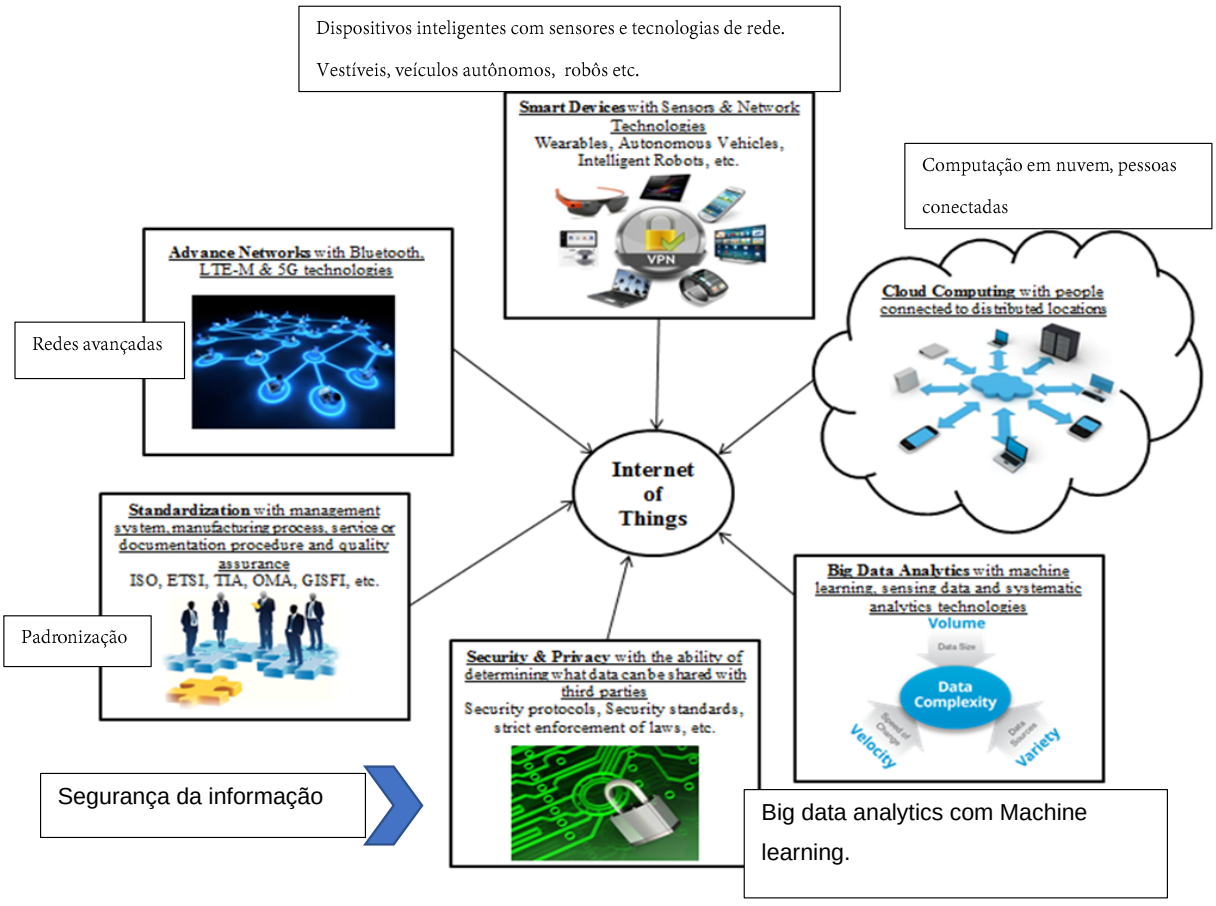

Figura 2
As seis dimensões principais necessárias para internet das coisas.
Fonte: Haroon *et al*. (2016). Tradução nossa.

2.2.3 *Quantidade de dispositivos conectados*

Para facilitar a vida dos cidadãos, como tornar a casa inteligente ou chamada de casa inteligente, controlando o interruptor elétrico da casa, controle do interruptor do ar-condicionado, otimizando a temperatura da casa, detectando fumaça em caso de

incêndio na casa, etc. Atualmente, os dispositivos de IoT se aplicam a muitos grupos para sustentar a vida. Existem casas inteligentes, rede inteligente, cidade inteligente, saúde inteligente, vestíveis inteligentes, agricultura inteligente, transporte/ mobilidades inteligentes, indústrias/ manufatura inteligentes e cadeia de suprimentos inteligente, entre outros (Pukkasenung, 2020).

O mesmo autor afirma que, de acordo com estatísticas relatadas pelo Departamento de Pesquisa Statista, no final de 2018 havia aproximadamente 22 bilhões de dispositivos IoT conectados em todo o mundo. E é provável que continue a aumentar. As previsões sugerem que até 2030 aproximadamente 50 bilhões de dispositivos IoT sejam usados em todo o mundo (Figura 3).

É importante enfatizar que esses dispositivos poderão estar conectados em uma *smart city* e que as tentativas de intrusão serão maiores, pois cada dispositivo desse atuará como pelo menos uma porta de entrada para as *smart cities*. Portanto, é necessário estar atento à segurança da informação, lembrando que dispositivos IoT estão dentro das salas de cirurgias. Segundo Costa, Sola e Garcia (2020), a telemedicina já é uma realidade, fazendo a segurança de grandes instituições financeiras ou até conduzindo veículos autônomos.

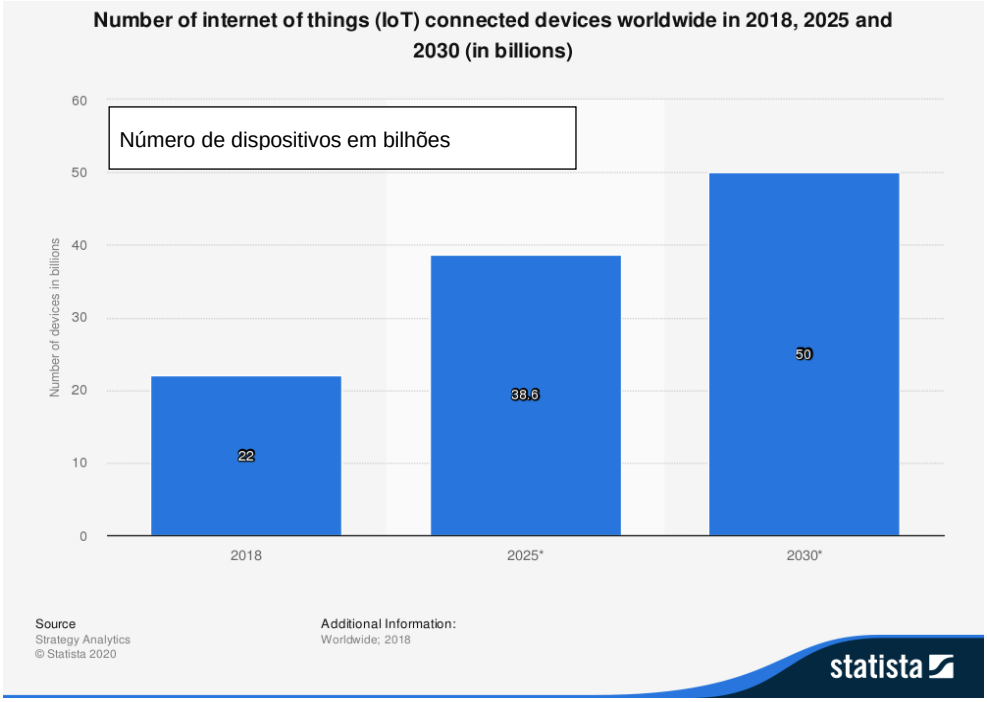

Figura 3
Número de dispositivos conectados de internet das coisas no mundo.
Fonte: Statista (2020).

2.2.4 Vulnerabilidades de segurança IoT

As vulnerabilidades na IoT são resultantes de sua natureza especial dos objetos interconectados e da grande variedade e sensibilidade dos dados coletados.

Os objetos interconectados na IoT e usados em *smart cities* são caracterizados pela ubiquidade, miniaturização, autonomia, comportamento imprevisível e difícil identificação. Sua grande heterogeneidade varia de objetos minúsculos/ invisíveis a sistemas embarcados muito sofisticados (Georgescu & Popescul, 2016).

Numa cidade, podem-se identificar facilmente os sensores usados para monitorar a poluição e a qualidade do ar, o tráfego e a maior infraestrutura viária, segurança pública e privada, consumo de energia e água, gestão de resíduos, etc.: sensores vestíveis colocados na roupa ou sob a pele; coisas usuais como chaves, relógios, filtros de café, geladeiras, controladores de aquecimento doméstico, livros, portas, etc.; e dispositivos com muita potência computacional, como *smartphones*, *tablets*, impressoras, TVs, dispositivos médicos, controle de supervisão e dados aquisição

sistemas (SCADA), carros, etc. Seu número aumenta diariamente, assim como as conexões entre eles.

Tais dispositivos podem ser muito *"smarts"* no desempenho operacional, mas não em termos de segurança de dados. Hossain, Fotouhi & Hasan (2015) afirmam que as limitações de *software*, *hardware* e rede restringem a inclusão de mecanismos de segurança adequados (por exemplo, criptografia) diretamente em objetos inteligentes. Por esse motivo, as medidas de segurança geralmente são deixadas de lado e a exposição a ataques é alta. Estudo da Hewlett-Packard (2016) mostra que 80% das coisas na IoT falham ao exigir senhas de complexidade e comprimento suficientes, 70% permitem que um invasor identifique contas de usuário válidas por meio da enumeração de contas, 70% usam rede não criptografada de serviços e 60% levantam questões de segurança com suas interfaces de usuário. Fica óbvio que é necessário o desenvolvimento de segurança da informação suplementarmente (Georgescu & Popescul, 2016).

Outro autor, Lisdorf (2020), enumera algumas razões dos dispositivos serem tão ingerenciáveis:

a) Difícil de interagir - precisam ser acessados por meio de algum console ou outro equipamento. Quando eles vêm com *Application Programming Interface* (API) geralmente são APIs que oferecem dados em um formato proprietário e apenas as ferramentas do fornecedor podem fazer interface com eles.
b) Produção de baixo custo - a maioria dos dispositivos é produzida em um mercado em que o baixo custo é a propriedade mais importante. As medidas de segurança sempre aumentam os custos, e a configuração de sistemas e processos exige tempo e esforço. Além disso, a segurança geralmente torna a implantação e a usabilidade mais difíceis.
c) Falta de foco na segurança - para fornecedores de dispositivos, é raro que a empresa tenha um diretor de segurança da informação (CISO). Se comparar essa situação com os dos grandes fornecedores de nuvem, há muita diferença. Esses fornecedores estão lidando com uma equipe de TI experiente que conhece todos os fundamentos de segurança de seus aplicativos corporativos, e essa segurança é o principal motivador na adoção de soluções em nuvem.

d) Inércia de desenvolvimento - tradicionalmente, os dispositivos são implantados em uma rede fechada que não pode ser acessada facilmente sem controle físico. Isso não exige medidas de alta segurança. Os desenvolvedores continuam desenvolvendo dispositivos como se estivessem em um circuito fechado, porque foram condicionados a fazê-lo na época das soluções de vigilância circuito fechado de televisão (CCTV).
e) Escala - cada dispositivo é como um pequeno computador e precisa ser gerenciado como tal. Quando se têm milhares, isso se torna um problema agravado pelos fatores anteriores. Torna-se necessário construir sistemas elaborados para controlar cada dispositivo individualmente, para que ele possa ser acessado com segurança.
f) Todos esses fatores podem e devem ser melhorados. As cidades estão em uma posição única para impulsionar isso. Uma iniciativa-chave seria, portanto, desenvolver e adotar um conjunto robusto de práticas para melhorar as deficiências do mercado de dispositivos atual. Lisdorf (2020) alerta que isso faz parte do desafio que enfrentam na cidade de Nova York. A estratégia foi iniciar um esforço interagências para desenvolver e adaptar os padrões existentes para o novo mundo da IoT.

2.3 *Blockchain*

Para conceituação inicial, é importante conhecer as três definições de *blockchain* sugeridas por Holbrook (2020):

Essa tecnologia foi claramente transformadora nos setores financeiro, logístico e governamental. As seguintes definições estão alinhadas aos públicos específicos de técnicos, comerciais e jurídicos. Como um profissional de relacionamento com o cliente, é necessário definir o jargão de *blockchain* certo para o público certo. Nem todos serão técnicos, nem todos estão apenas preocupados com os aspectos do negócio. Quando se discute *blockchain* com clientes, tem-se que verificar a função que eles desempenham, para trabalhar com a definição para cada contexto.

a) Definição técnica - uma estrutura de dados protegida e compartilhada globalmente que mantém um banco de dados de *back-end* (servidor computacional interno à rede), transacional que é imutável.
b) Definição de negócios - uma rede de negócios que é usada entre pares para trocar valor. O valor pode ser moedas, informações de rastreamento ou qualquer coisa que as partes interessadas requeiram para ser mantida no livro razão da *blockchain*.
c) Definição legal - uma *string* (cadeia de caracteres) resistente à corrupção de entradas do razão (livro) compartilhada em uma rede por várias partes que não requerem um intermediário centralizado para apresentar e validar transações.

Por que a *blockchain* é considerada revolucionária? Durante o curso dos últimos 100 anos ou mais, o avanço das tecnologias de mudança de vida foi dramático. A tecnologia muitas vezes pode ser revolucionária e a tecnologia *blockchain* parece que será uma delas (Holbrook, 2020).

A tecnologia *blockchain* é revolucionária de várias maneiras, conforme se segue:

a) A tecnologia *blockchain* é uma sincronização de tecnologias que agora faz sentido implementar estrategicamente.
b) A confiança está no centro da tecnologia de *blockchain* e, por meio do uso de consenso, remove intermediários da rede e, assim, cria novas eficiências das quais as empresas podem realmente se beneficiar, como fornecer transparência, uma raiz de confiança, uma redução em custos de mão de obra e vários outros benefícios.
c) A tecnologia *blockchain* em seu verdadeiro sentido, conforme especificado por Nakamoto, é um livro-razão público de valor à prova de violação. A plataforma Bitcoin permitiu aos cidadãos do mundo fazer transações sem a necessidade de intermediários.

A tecnologia *blockchain* é perturbadora para o *status quo*, uma vez que os processos anteriores, como os processos de negócios, são eliminados com a introdução da tecnologia, uma plataforma com vários casos de uso para empresas. O número e a qualidade das organizações que investem em testes de *blockchain*, implementação e especificações de produção são impressionantes (Holbrook, 2020).

De acordo com estudo do Tribunal de Contas da União - TCU (Brasil, 2020b, p. 7) foram feitas as seguintes considerações:

A blockchain também pode ser enquadrada como uma tecnologia de propósito geral, ou seja, uma tecnologia com características únicas e capazes de impactar drasticamente as relações econômicas e sociais preexistentes, bem como prover significativas melhorias e facilitar a criação de inovações em diversos setores da economia. Destaca-se que a transformação tecnológica vai além da inovação trazida pelas *blockchains* do Bitcoin e da *Ethereum*. Segundo a empresa de consultoria Gartner, até 2023 a tecnologia *blockchain* suportará o movimento global e rastreamento de dois trilhões de dólares de bens e serviços anualmente. A empresa de consultoria também afirma que a *blockchain* tem, no mínimo, o potencial de otimizar e, possivelmente, transformar, de forma disruptiva, os serviços públicos. A tecnologia *blockchain* é indicada quando há necessidade de aumentar a confiabilidade de informações e processos em situações que envolvem muitas partes interessadas e heterogêneas. Por meio de trilhas de auditoria confiáveis é possível rastrear todas as operações sobre os dados que são armazenados em um livro-razão digitalizado na internet, aumentando a transparência e aperfeiçoando o processo de prestação de contas.

2.3.1 Conceitos importantes

2.3.1.1 *Ledgers*

Esse conceito remete ao antigo livro de Contabilidade: O livro-razão em versão *on-line*.

The word "ledger" originates from the 15th century Dutch word, "leggen," meaning "a book that lies permanently in some specified place."

A palavra "razão" origina-se da palavra holandesa do século 15, "leggen", que significa "um livro que está permanentemente em algum lugar especificado".

Figura 4
Definição e origem da palavra *ledger*.
Fonte: Moore, Rainwater & Stahl (2018). Tradução nossa.

Lewis (2018) enfatiza que, para entendimento do tema, é preciso diferenciar entre tecnologias de *blockchain* e livros-razão de *blockchain* específicos:

> As tecnologias de *blockchain* são as regras ou padrões de como um razão (livro) é criado e mantido. Diferentes tecnologias têm diferentes regras de participação, diferentes regras de rede, diferentes especificações sobre como criar transações, diferentes métodos de armazenamento de dados e diferentes mecanismos de consenso (Lewis, 2018, p. 326).

Quando uma rede é criada, a *blockchain* ou livro de registro fica inicialmente vazio de transações, assim como um novo livro de capa de couro físico está vazio. Alguns exemplos de tecnologias de *blockchain* são: Bitcoin, *Ethereum,* NXT*,* Corda*, Fabric e Quorum,* que serão vistas à frente (Lewis, 2018).

Existem várias instâncias do mesmo tipo de banco de dados: uma corporação pode usar mais de um banco de dados. O mesmo acontece com *blockchains*. Algumas tecnologias de *blockchain* operam de uma maneira, outras de outro modo (Lewis, 2018).

2.3.1.2 Categorização de tipos de *blockchain*

Blockchains públicas (não necessita de permissão): as *blockchains* mais populares, como *Ethereum* ou Bitcoin, não precisam ter permissão para entrar e são públicas. Em princípio, são acessíveis a todos, desde que haja infraestrutura adequada. Os participantes são geralmente anônimos e se representam apenas por uma identificação digital (ID) aleatória como endereço pessoal. Em primeira instância, não há um provedor central para supervisionar o tráfego em andamento. As *blockchains* públicas têm duas vantagens principais sobre as *blockchains* privadas ou consorciadas: em primeiro lugar, permitem a participação de dispositivos aleatórios (máquinas, telefones celulares, *tablets,* etc.), que são desconhecidos uns dos outros e não precisam ser confiáveis. Em segundo lugar, não há necessidade de um consórcio ou provedor privado admitir novos aplicativos baseados em *blockchain*. Em um cenário futuro de IoT, com dispositivos aleatórios se comunicando quase em tempo real, essas duas características são fundamentais para o sucesso dessas tecnologias (Treiblmaier & Beck, 2018a).

Blockchains privadas (necessitam de permissão): , o acesso é concedido apenas a participantes conhecidos, mediante autorização/permissão que podem ler e/ou gravar dados. O provedor tem controle total sobre ela e conhece todos os participantes *a priori*. De modo geral, as *blockchains* privadas não possuem as propriedades de anonimato e irreversibilidade. Com *blockchains* privadas é possível desenvolver e implantar novos aplicativos rapidamente. Os campos de aplicação mais promissores podem ser processos de negócios internos, voltados para alto rendimento de dados. É possível cortar e arquivar a *blockchain* em intervalos frequentes, por exemplo, anualmente, o que pode reduzir o tamanho do volume de armazenamento significativamente. As *blockchains* privadas não precisam necessariamente de uma moeda digital subjacente, já que nenhum incentivo financeiro precisa ser definido para os mineradores (Treiblmaier & Beck, 2018a).

Blockchains em consórcio: ou de propósito especial, como *blockchains* semiprivadas (com permissão compartilhada), podem ser vistas como um meio termo entre *blockchains* públicas e privados. Aqui, apenas participantes verificados têm permissão

para validar blocos. Algoritmos de consenso otimizados permitem transações significativamente mais rápidas do que *blockchains* públicas. Geralmente, as *blockchains* em consórcio oferecem a possibilidade de serem ajustadas às necessidades específicas do mercado de energia, por exemplo, renunciando ao anonimato ou aumentando o volume de transações dependendo da aplicação. Nesse sentido, a questão da interoperabilidade entre tipos de *blockchain* pública, privada e consórcio com indústrias é considerada um dos principais fatores de sucesso dessa tecnologia (Treiblmaier & Beck, 2018a).

2.3.1.3 Mecanismo/algoritmo de consenso

De acordo com Restuccia, Kanhere, Melodia & Das (2019)*, o* objetivo da *blockchain* é permitir transações parte a parte, que são validadas, organizadas em blocos e armazenadas em um razão (livro) distribuído.

Numa *blockchain*, algoritmos especializados de consenso, descentralizados determinam como e quando um grupo de transações pode ser incluído no razão.

Cada novo bloco só pode ser incorporado à *blockchain* se a maioria dos nós da rede concordar com sua inclusão, ou seja, somente se houver consenso entre os usuários da cadeia (Restuccia *et al.*, 2019*).*

Cada nó na rede mantém uma cópia local da *blockchain*. Quando um novo bloco chega a consenso, ele é transmitido pela rede. Assim, cada nó anexa o novo bloco à sua cópia local da *blockchain*. Portanto, muitas cópias consistentes são criadas na *blockchain*, de forma que assim que a maioria dos nós possuir a mesma cópia da *blockchain*, a rede pode ser considerada confiável e segura.
As primeiras implementações da *blockchain* adotaram o mecanismo de consenso de prova de trabalho (PoW), que fornece um mecanismo distribuído para manter e validar a *blockchain*. A ideia por trás do PoW é obter consenso entre os nós da rede por meio de quebra-cabeças computacionais difíceis de computar, mas fáceis de verificar. Por exemplo, uma *blockchain* pode pedir a seus usuários (também chamados de mineradores) para encontrar um número aleatório de 4 *bytes*, ou seja, o *nonce*, de

modo que o valor de *hash secure hash algorithm* (SHA256) de um novo bloco seja igual ou menor que determinado limite (Restuccia *et al.*, 2019).

Embora o cálculo do *nonce* seja difícil e exigente em termos computacionais, verificá-lo é tarefa simples. Consequentemente, o primeiro nó que encontra um possível *nonce* notifica à rede *blockchain* e transmite o novo bloco. O *nonce* obtido, que representa o PoW do minerador, é testado por outros nós que determinam se o *nonce* é ou não uma solução real do quebra-cabeça de *hashing.* Quando a validação do *nonce* é bem-sucedida, os nós adicionam o novo bloco à *blockchain* (Restuccia *et al.*, 2019).

Proof of work, *proof of stake*, *delegated and proof of stake* (prova de trabalho, prova de participação e delegado prova de aposta).

Com a evolução da *blockchain* criaram-se muitas políticas de mecanismos de consenso. O primeiro foi criado pela Bitcoin e muitos outros foram construídos para resolver problemas que existem em mecanismos. Os mais usados são:

a) Prova de trabalho (PoW);
b) prova de aposta (PoS);
c) prova de aposta delegada (DPoS).

Além desses três, existem outros consensos, como prova de importância, prova do tempo decorrido (PoET), prova de autoridade (PoA), prova de queima, prova de capacidade, prova de atividade,etc. (Restuccia *et al.*, 2019).

PoW foi o primeiro e mais popular mecanismo; é usado por Bitcoin e *Ethereum*, que são as criptomoedas mais populares até então. A PoW é alcançada tendo uma rede de mineradores para os quais é apresentando um problema matemático. Quando os mineradores resolvem o problema, eles são recompensados com uma criptomoeda. A recompensa é a prova do “trabalho” realizado, e é daí que vem o nome. PoW determina qual par faz o trabalho pela quantidade de potência do computador (taxa de *hash*) e aloca o trabalho como uma porcentagem para que seja pago e pelo preço justo. A PoW não confia em par algum na rede individualmente, mas a rede confia em

todos eles como uma rede coletiva. Um minerador precisa encontrar uma solução para um problema matemático complexo para se tornar o líder e ser capaz de criar o próximo bloco a ser adicionado à *blockchain*. Quanto mais mineradores existirem na rede, mais complexa e mais difícil será a questão matemática que precisa ser resolvida para validar a transação (Restuccia *et al*., 2019).

2.3.1 4 Contratos inteligentes

Esse conceito é muito importante e se constitui em um dos pilares da tecnologia. Internet das coisas (IoT), conforme o entendimento de Restuccia *et al.* (2019), tem como características a capacidade de permitir comunicações autônomas e a auto-organização máquina a máquina (M2M). É importante projetar mecanismos de forma que as interações sejam iniciadas automaticamente; e que não haja a necessidade de controlar e verificar individualmente a confiabilidade de cada comunicação. Contratos inteligentes demonstraram ser eficazes para resolver os problemas citados.

Contratos inteligentes são programas de *software* que especificam e impõem contratos entre duas ou mais partes. Para entender como eles funcionam, vamos considerar: Alice aluga uma casa para Bob. Bob é obrigado a enviar um pagamento mensal para Alice. O contrato pode ser facilmente codificado em um contrato inteligente. Na verdade, é suficiente escrever algumas linhas de código para gerar e vincular o contrato a Bob, de modo que o pagamento mensal possa ser acionado automaticamente por um programa de *software*. Ou seja, é semelhante ao débito automático.

Os contratos inteligentes têm sido amplamente usados na *Ethereum*, onde cada contrato é representado por uma série de operações computacionais que são expressas por meio de uma linguagem de programação especificada por uma interface binária de aplicativo (ABI).

Contratos inteligentes podem implementar operações muito complexas e podem ser ligados um ao outro, gerando assim uma estrutura aninhada (por exemplo, sublocação). As vantagens dos contratos inteligentes são inúmeras, e seu impacto nas redes IoT é considerável. Como os contratos são armazenados dentro da

blockchain, seu conteúdo é confiável entre as partes, pois não pode ser modificado ou corrompido após sua inclusão na *blockchain*. E, ainda, cada contrato recebe um endereço inequívoco na *blockchain* e pode ser acessado diretamente da internet, tornando, assim, os contratos inteligentes adequados para serem acessados por dispositivos IoT, conectados remotamente. Esses contratos consistem em poucas linhas de código que os dispositivos podem entender e executar facilmente (Restuccia *et al*., 2019).

A aplicação de contratos inteligentes à IoT ainda está em evolução. Resultados mostram que várias aplicações IoT se beneficiam de tecnologias de *blockchain,* por exemplo, controles de acesso que dependem de contratos inteligentes para regular o acesso à rede IoT. Atividades desse tipo aproveitam a imutabilidade da *blockchain* para gerar uma lista de controle de acesso em tempo real que também regula e descreve as políticas de acesso aos recursos do dispositivo. Pode-se conseguir o monitoramento inteligente da cadeia de suprimentos por meio de contratos inteligentes. Não apenas os contratos inteligentes podem ser usados para regular transações e taxas relacionadas aos processos de produção e remessa de mercadorias, mas também para controlar sua posição, como normalmente o é (Restuccia *et al*., 2019).

2.3.1.5 Criptografia

a) Criptografia clássica

Existem várias técnicas criptográficas que foram usadas em cifras históricas. Essas cifras *ad hoc* não são mais seguras o suficiente para serem usadas em aplicativos atuais, mais por causa de sua simplicidade, mas ainda assim elas ajudam a entender o conceito envolvido. Explorar os pontos fracos da criptografia clássica também ensina mais sobre alguns dos princípios da criptografia (Raj, 2019).

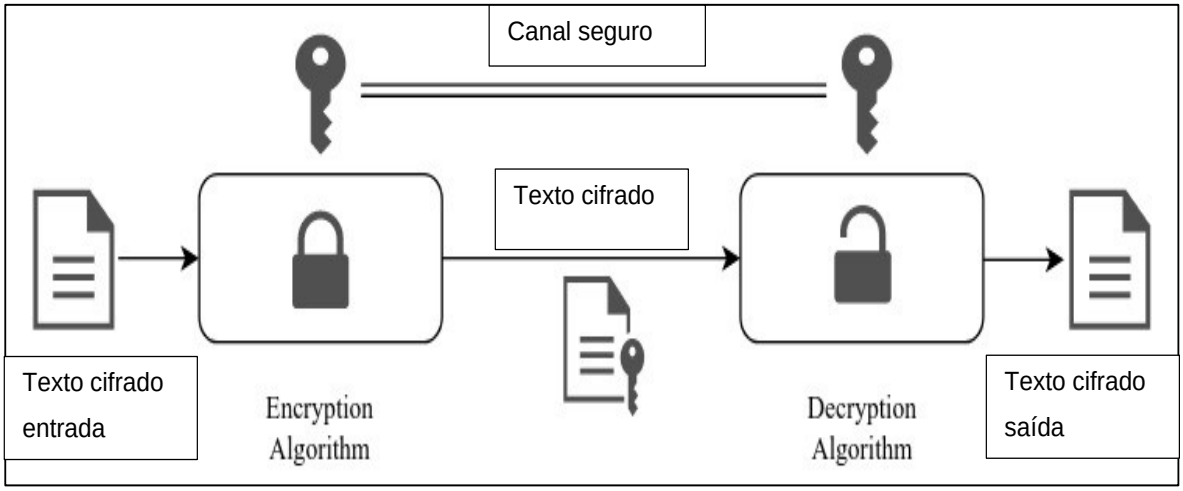

Figura 5
Modelo de criptografia convencional.
Fonte: Raj (2019). Tradução nossa.

A Figura 5 mostra o modelo de criptografia convencional usado para criptografar um texto simples usando uma chave secreta que é compartilhada com o outro usuário por um canal seguro. O usuário que deseja ler o texto terá que descriptografar o texto cifrado usando a chave secreta, que retornará o texto ao original. A chave é privada e os algoritmos de criptografia e descriptografia tornam-se públicos porque é impossível descriptografar o texto cifrado sem a chave (Raj, 2019).

Dois tipos de operação são usados para transformar texto simples em texto cifrado: substituição e transposição. Ambas as técnicas garantem que a operação seja reversível e, portanto, podem ser usadas em algoritmos de criptografia. Uma cifra de substituição é um método de criptografia no qual os caracteres do texto simples são substituídos por outros caracteres de maneira fixa. O problema óbvio com essa cifra é que o método é fixo e não há chave envolvida. A cifra polialfabética foi o estágio seguinte na evolução das cifras. Essa cifra introduziu várias substituições em diferentes posições na mensagem. Uma cifra de transposição é um método de criptografia em que as posições das letras do texto simples são alteradas de acordo com um sistema conhecido. Apenas a ordem do texto simples é alterada. Todas as letras do texto simples permanecem as mesmas. Esse tipo de técnica de cifra pode ser descriptografado encontrando os padrões de transposição usando anagramas (Raj, 2019).

Conforme Gaur, Desrosiers, Novotny, Ramakrishna, O'Dowd & Baset (2018), a criptografia é um dos principais blocos de construção de uma solução de *blockchain*. A segurança fundamental da cadeia de blocos de Bitcoin é a elegante ligação criptográfica de todos os principais componentes do livro-razão. Transações são vinculadas umas às outras, principalmente por meio da árvore Merkle. Uma árvore Merkle é baseada no conceito de uma estrutura de dados em árvore onde cada nó folha tem um *hash* calculado de seus dados e onde o nó não folha tem um *hash* de todos os seus filhos subjacentes. Esse método fornece uma maneira de garantir a integridade dos dados, mas também propicia privacidade, permitindo remover uma folha que é considerada privada, mas deixa o *hash*, preservando, assim, a integridade da árvore. A árvore Merkle tem suas raízes incorporadas ao cabeçalho do bloco, que inclui uma referência aos cabeçalhos do bloco que o precedem.

As transações também são criptografadas e conectadas ao resto da estrutura da cadeia de blocos por meio da árvore Merkle (Gaur *et al*., 2018).

2.3.1.6 Árvore *Merkle*

Merkle tree é um *add-on* (acessório), de acordo com Hassija, Chamola, Saxena, Jain, Goyal & Sikdar (2019), que pode ser adicionado à estrutura de dados da *blockchain* para aumentar a segurança dos dispositivos conectados. Essa técnica também ajuda a reduzir o número geral de blocos que estão sendo adicionados à cadeia. Uma árvore Merkle é como uma árvore binária onde cada nó contém dois nós filhos, exceto os nós folha. Os nós da folha contêm os dados ou transações, e as raízes são os valores *hash* dos dados nos nós folha. Com base no tamanho da árvore, várias transações podem ser combinadas para gerar um único *hash* de raiz. Em vez de tratar cada transação como um bloco, cada *hash* raiz pode ser considerado um bloco na cadeia. Isso pode ajudar a reduzir o número de blocos. Além disso, devido a vários níveis de *hashing*, em cada nível da árvore a segurança dos dados é aprimorada. Os dispositivos IoT envolvem muitas pequenas comunicações entre si e, portanto, usar a árvore Merkle junto com a *blockchain* pode ser uma solução promissora, como preleciona Muñoz (2014, como citado em Hassija *et al*., 2019).

2.3.2 Funcionamento básico da tecnologia

Kim & Deka (2020) demonstram que o substrato da *blockchain* não é um conceito novo. Foi inspirado no algoritmo de ordenação de carimbo de data/hora dos anos 90, que era usado para evitar adulteração de documentos. Essa marcação/registro de tempo foi estendida para o uso de livros e transações, a fim de facilitar mecanismos de pagamento seguros.

Desde 2008, porém, após artigo de Nakamoto (2008), vários programadores, criptógrafos e cientistas trabalharam nesse conceito de *blockchain* para produzir uma rede de criptomoeda chamada Bitcoin. O principal objetivo do projeto e a introdução à *blockchain* e à IoT seria resolver dois problemas principais. Um era o gasto duplo (significa gastar o mesmo dinheiro duas vezes); e o segundo, eliminar a necessidade de uma terceira parte, central, confiável nas transações. *Blockchain* é considerada a segunda revolução digital após o advento da internet. Tem-se observado o crescente uso de *blockchain* em segurança de *smart cities*. S*mart city* abarca uma gama de variedade de dimensões, como educação, mobilidade, casa, energia, saúde, indústria, segurança, privacidade, etc. Como muitas estruturas inteligentes ainda estão sendo atualizadas, os problemas de segurança e proteção se converteram em um temor, o que requer contramedidas eficazes. Metodologias habituais de garantia de segurança digital não podem ser aplicadas eficazmente a essas aplicações, considerando as qualidades dinâmicas, a heterogeneidade e a adaptabilidade das *smart cities* (Cui, Xie, Qu, Gao & Yang, 2018).

Em uma abordagem centralizada, diferentes domínios da *smart city* têm, portanto, diferentes desafios. A internet das coisas depende de padrões com capacidade e processamento, ainda limitados. É mais dispendiosa, pois está sujeita a despesas causadas pela instalação e manutenção de servidores. Por essa razão a *blockchain* se torna possivelmente o fator mais preponderante desse sistema. A utilização de uma abordagem não centralizada, distribuída, padrão não apenas reduzirá os custos relacionados à manutenção e implementação de grupos de servidores, mas também compartilhará as necessidades de planejamento e espaço de muitos dispositivos na arquitetura da IoT, sem outros recursos adicionais. Ficou claro que a *blockchain*

oferece uma resposta que se adapta à necessidade de cada etapa do processo (Ahmed, Shah & Wakil, 2020).

É bom ressaltar que há divergências entre Quiniou (2019) e a maioria dos outros autores em relação ao termo “descentralizado”, amplamente usado para se referir à *blockchain* ou seus aplicativos, que não se parece totalmente apropriado para se referir à arquitetura *blockchain*. De fato, a descentralização conceitualmente é um movimento do centro para as bordas ou extremidades. A arquitetura da *blockchain* não é descentralizada; faz parte de modelos paralelos centralizados ou parcialmente descentralizados, portanto, os termos “distribuído” ou “não centralizado” parecem mais apropriados. Doravante, devido a esse detalhe e para ser mais rigoroso, o termo “não centralizado” será adotado neste trabalho.

A internet revolucionou e mudou a vida das pessoas, da sociedade e dos negócios. Paradoxalmente, o processo em que as pessoas e as corporações executam transações entre si não mudou muito. A grande expectativa é de que a *blockchain* seja o fator de mudança para tornar a internet tecnicamente mais segura. Para entender como ela funciona, é necessário compreendê-la sob a perspectiva dos negócios quanto a perspectiva técnica.

Panda, Dhameja & Singhal (2018) ensinam que a *blockchain* é um sistema de registros para transacionar ativos, não apenas dinheiro, moeda. A transação é realizada de maneira ponto a ponto, somente entre as duas partes envolvidas. Significa que não há necessidade de um intermediário confiável, como bancos, corretores ou outros serviços de custódia, para atuar como um terceiro confiável. Por exemplo, se Alice paga a Bob R$ 10, por que esse valor deveria passar por um banco? Isso representa perda de tempo, despesas e burocracias. Ao passo que se essa transação fosse realizada de uma pessoa para outra diretamente, não haveria tais inconvenientes (Figura 6).

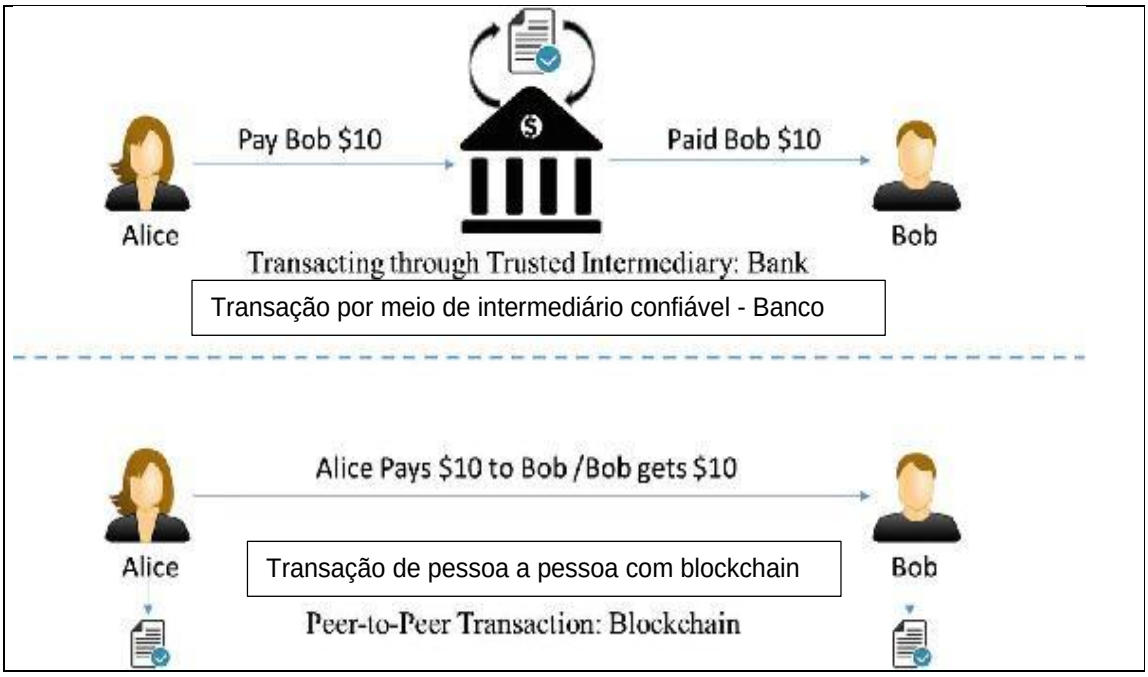

Figura 6
Transação por meio de intermediário *vs* transação direta parte a parte.
Fonte: Singhal, Dhameja & Panda (2018). Tradução nossa.

A seguir, tem-se outro exemplo. Uma transação envolvendo ações tipicamente acontece em segundos, mas sua liquidação pode levar muitos dias. A Figura 7 ilustra essa situação.

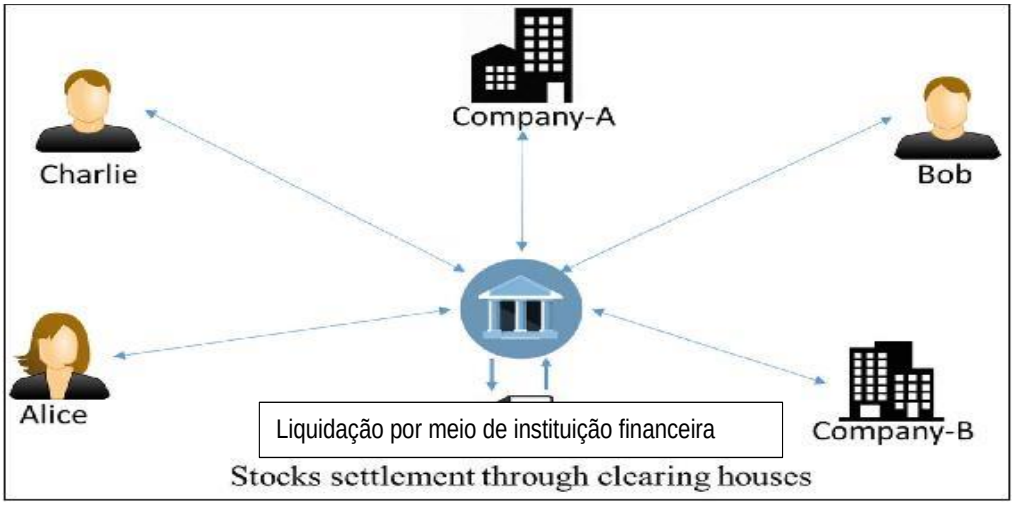

Figura 7
Negociação de ações por meio de uma instituição ou câmara intermediária.
Fonte: Singhal *et al*. (2018). Tradução nossa.

Noutro caso, se alguém deseja comprar algumas ações de uma empresa ou pessoa, pode simplesmente comprá-las diretamente com liquidação instantânea, sem a

necessidade de corretores, câmaras de compensação ou outras instituições financeiras entre elas. Uma solução descentralizada e ponto a ponto para essa situação está representada na Figura 8.

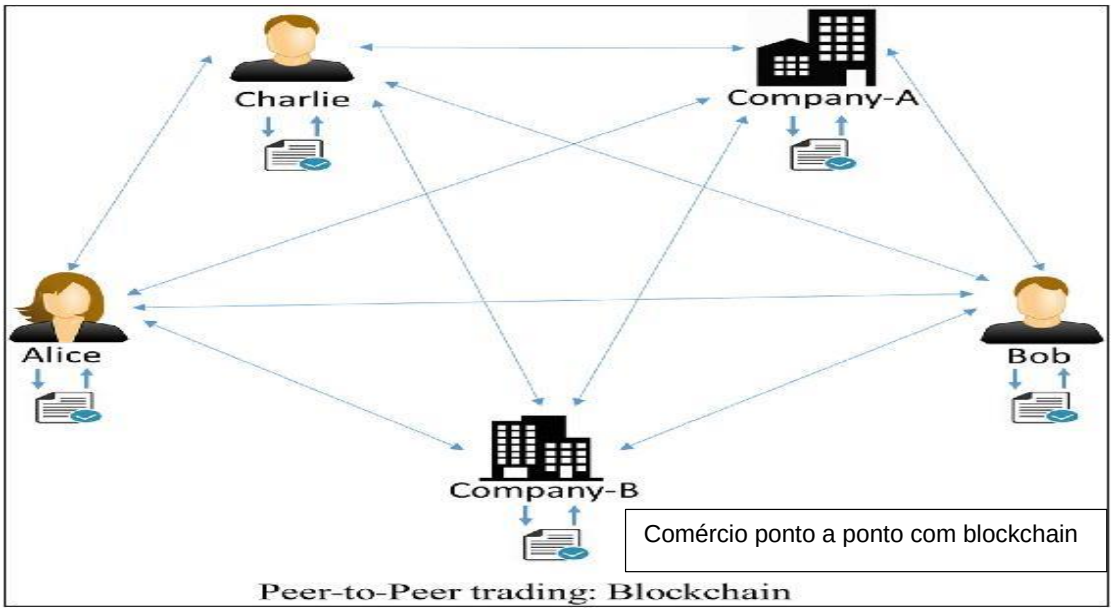

Figura 8
Transação de ações parte a parte.
Fonte: Singhal *et al*. (2018). Tradução nossa.

Atentem que essa transação e mais a liquidação não são tratadas como duas entidades diferentes em uma configuração da tecnologia *blockchain*. Essa é a grande diferença. As transações são análogas a transações em moeda fiduciária, nas quais se alguém paga outra pessoa com o valor monetário de R$ 10, este alguém não o possuirá mais, e esse valor de US$ 10 é fisicamente transferido para o novo proprietário (Panda *et al*., 2018).

2.3.3 Plataformas blockchain

Perwej, Dhameja & Singhal (2013) consideram algumas das organizações que estão desenvolvendo novas tecnologias para *blockchain*. O número de empresas desenvolvendo novas ferramentas e soluções está em constante expansão, e aqui mostram-se três exemplos de diferentes tipos de *blockchain*:

a) Ripple: é uma *blockchain* com foco no setor de serviços financeiros. Perwej, Dhameja & Singhal (2013) afirmam que não estão usando a *blockchain*, mas

outra, a *distributed ledger* (DLT). Eles desenvolveram uma tecnologia de razão distribuída para permitir que bancos em todo o mundo enviem pagamentos internacionais em tempo real, sem a necessidade de uma autoridade centralizada. Na realidade, é uma rede de pagamento para transferir instantaneamente qualquer tipo de moeda em todo o mundo. Eles desenvolveram uma rede global distribuída que hospeda nós de pagamento para transferir valor em todo o mundo.

b) IOTA: é uma criptomoeda completamente diferente porque não usa uma *blockchain*, mas sim um gráfico acíclico direcionado (DAG) chamado *tangle*. Ele foi desenvolvido especialmente para a Indústria 4.0, onde os dispositivos conectados devem ser capazes de realizar micro ou nanotransações entre si.
c) *Ethereum*: o britânico Wood (2014) codesenvolveu a *blockchain Ethereum* como uma plataforma para servir como base primária para o uso de aplicativos de “contrato inteligente” do livro-razão da *blockchain*. Fornecer esse tipo de plataforma permitiu que os desenvolvedores começassem a implementação de contratos autoexecutáveis ou “inteligentes”.

Os aplicativos da *Ethereum* são executados em uma *blockchain* personalizada, uma infraestrutura global compartilhada que pode movimentar valores e representar o registro da propriedade. É uma plataforma descentralizada para desenvolver aplicações descentralizadas (DApps) que funcionam por meio de contratos inteligentes. Esses contratos inteligentes são pequenos programas de *software* que executam uma tarefa, uma espécie de declaração *If, This, Then, That* (se, então, senão...). Eles são executados em uma *blockchain* personalizada e, como tal, não há chance de fraude, censura ou interferência de terceiros (Perwej *et al*., 2013).

Wood (2014) afirma que se pode dizer que *Ethereum* é uma versão muito especializada de uma máquina de estado baseada em transações criptograficamente segura. Sistemas de acompanhamento, como o Namecoin, adaptaram essa aplicação “moeda original” para outras aplicações.

Ethereum é um projeto que tenta construir a tecnologia generalizada, na qual todos os conceitos de máquina de estado baseados em transações podem ser construídos.

Além disso, visa fornecer ao desenvolvedor final um sistema totalmente integrado de ponta a ponta para a construção de *software* em um paradigma de computação até então inexplorado no *mainstream*: uma estrutura de computação de mensagem de objeto confiável.

As estratégias nesse sistema proposto têm vários atributos, nem sempre encontrados no mundo real. A incorruptibilidade do julgamento, muitas vezes difícil de encontrar, vem naturalmente de um intérprete algorítmico desinteressado. Transparência ou ser capaz de ver exatamente como um estado ou julgamento ocorreu por meio do log de transações e regras ou códigos de instrução, coisa que nunca acontece perfeitamente em sistemas baseados em humanos, uma vez que a linguagem natural é necessariamente vaga, muitas vezes faltam informações e eivadas de preconceitos antigos, difíceis de mudar (Wood, 2014).

Na Tabela 2 veem-se as principais plataformas de *blockchain* e suas especificações técnicas.

Esses parâmetros são importantes, pois são eles que decidem qual a plataforma a ser implantada de acordo com as aplicações e com o grau de segurança a ser adotado em *smart cities*, órgãos de governo, empresas estatais, cartórios notariais, autarquias ou quaisquer outras entidades. Também, importante é ter acesso ao *site* do desenvolvedor da plataforma.

Tabela 2

Plataformas de *blockchain* e especificações

	Blockchain Platform	***Hash Function***	***Memory Data Structure***	***Secondary Storage***	***Consensus Protocol***	***Project Website***
1	**Bitcoin**	SHA-256	*Merkle Tree*	*Level* DB	*Proof of Work*	https://bitcoincore.org https://bitcoin.org
2	***Ethereum***	Keccak256	*Trie*	*Level* DB, *Rocks* DB	*Proof of Work (Ethash)*	https://ethereum.org/
3	***Hyperledger Fabric***	SHA3 SHAKE 256	*Bucket-tree, Merkle Tree*	*Rocks* DB	*Supports pluggable consensus like Practical Byzantine Fault Tolerance* (PBFT), Raft, PoW, PoS	https://www.hyperledger.org/
4	**Corda R3**	SHA-256	*Merkle tree*	H2 *database*	*Validity consensus, Uniqueness consensus, pluggable consensus*	https://www.corda.net/

5	***Quorum***	Keccak256	*Trie*	*Level* DB	*QuorumChain pluggable consensus (*PoS*,* Raft*, Istanbul* – BFT*)*	https://www.jpmorgan.com/global/Quorum
6	**IOTA**	Winternitz hash	*Acyclic Directed Graph*	*Trytes, Balanced Trinary System*	PoW	https://www.iota.org/
7	***Ripple***	SHA2-512	*Merkle Tree, Knowledge Grap*	*Rocks* DB*, NuDB*	XRP *Ledger Consensus Protocol*	https://ripple.com/
8	***Kadena***	BLAKE2	*Merkle*	*Oracle*	BFT *Raft, Scalable*BFT	https://kadena.io
9	***Tezos***	SHA-256, BLAKE2	*Merkle*	*Distributed Database*	*Proof-of-Stake*	https://tzscan.io
10	***Sawlooth***	SHA-512,SHA256	*BlockCache, Radix Merkle Tree*	*BlockStore*	*Pluggable consensus algorithms Proof of Elapsed Time (*PoET*),* PoW, PBFT	https://www.hyperledger.org/projects/sawtooth
11	**NEM**	SHA-256d	*Web, Portable or Network database*	*Web Database, Access database*	*Proof of Importance*	https://nem.io/
12	***Multi Chain***	SHA3-256	*Merkle Tree*	*Level* DB	PoW	https://www.multichain.com
13	***Hydra Chain***	SHA3-256	*Merkle tree*	*Level* DB	PBFT	https://github.com/HydraChain
14	***Big ChainDB***	SHA3-256	*Associative Array*	*Mongo* DB	BFT	https://www.bigchaindb.com
15	***Open Chain***	SHA-256	*Associative Array*	*SQLite, SqlServer, Mongo DB*	*Proof of Work*	https://www.openchain.org/

Fonte: Shrivas (2019).

2.3.4 Combinando IoT com blockchain

No entendimento de Reyna, Martín, Chen, Soler & Díaz (2018) (2018), a integração de tecnologias promissoras como IoT e computação em nuvem provou ser inestimável. Da mesma forma, reconhecem o enorme potencial da *blockchain* em revolucionar a IoT. A *blockchain* pode enriquecer a IoT, fornecendo um serviço de compartilhamento confiável, cujas informações são confiáveis e podem ser rastreadas. As fontes de dados podem ser identificadas a qualquer momento e os dados permanecem imutáveis ao longo do tempo, aumentando sua segurança. Nos casos em que as informações de IoT devem ser compartilhadas com segurança entre muitos participantes, essa integração representa uma revolução fundamental. Por exemplo, uma rastreabilidade exaustiva em vários produtos alimentares é um aspecto fundamental para garantir a segurança alimentar. A rastreabilidade dos alimentos

pode exigir o envolvimento de muitos participantes: fabricação, alimentação, tratamento, distribuição, e assim por diante. Um vazamento de dados em qualquer parte da cadeia pode levar à fraude ou retardar os processos de busca de evidências de doenças, o que poderia afetar seriamente a vida dos cidadãos.

Portanto, uma agência de saúde de nível municipal, estadual ou federal tem valiosa e precisa ferramenta de avaliação. Tem melhor controle nessas áreas, aumenta a segurança alimentar, melhorando o compartilhamento de dados entre os participantes e reduzindo o tempo de busca em caso de surto alimentar, que pode salvar vidas humanas. Além disso, em outras áreas, como *smart cities* e carros autônomos, o compartilhamento de dados confiáveis pode favorecer a inclusão de novos participantes nos ecossistemas e contribuir para melhorar seus serviços e sua adoção. Portanto, o uso de *blockchain* pode complementar a IoT com informações confiáveis e seguras. Isso já bem reconhecido e mencionado. A tecnologia *blockchain* é identificada como a chave para resolver problemas de escalabilidade, privacidade e confiabilidade relacionadas ao paradigma IoT (Reyna *et al*., 2018).

Já Cao, Li, Zhang, Zhang, Mumtaz, Zhou & Peng, (2019) referem em outra análise que a implementação de IoT e *blockchain* está em pauta na indústria e outras áreas onde já existem soluções promissoras em diversas áreas. Na indústria da cadeia de suprimentos existem modelos de cadeia de suprimentos habilitados para *blockchain*. Nesse modelo, as informações armazenadas na *blockchain* podem servir como um log de entrega para embarques de contêineres. Todo o movimento de contêineres, da origem ao destino, pode ser rastreado por qualquer entidade da cadeia de suprimentos, para que o atraso na remessa possa ser minimizado e o ativo ausente possa ser rastreado com precisão. Na dimensão da saúde existem modelos centrados no usuário para o processamento de dados pessoais de saúde usando a rede *blockchain*, garantindo a propriedade dos dados dos indivíduos, bem como a integridade dos dados (também mostrado por Minoli & Occhiogrosso, 2018). Ao aplicar políticas de controle de acesso, o sistema garante que os usuários possam lidar com seus dados pessoais sem se preocupar com questões de privacidade. Além disso, a *blockchain* também está disponível em outras aplicações IoT, como atualizações remotas de *software* e seguro para veículos (Cao *et al.*, 2019).

Os autores referenciados reconhecem que, particularmente, a *blockchain* desempenha importante papel no comércio de energia para aplicações de IoT na internet de energia. Existem algumas tecnologias de *blockchain* que investigaram como promover o compartilhamento de energia entre dispositivos IoT para aumentar a eficiência de utilização de energia. Tomando a internet de veículos (IoV) como exemplo, os veículos elétricos têm a capacidade de absorver energia excessiva durante a área fora de pico e fornecer energia como geradores distribuídos durante o período de pico. Para melhorar a eficiência da negociação, foi proposto um esquema de pagamento baseado em crédito, que arca com a negociação rápida e frequente entre nós de energia a partir do estabelecimento de bancos de crédito virtuais. Além disso, algumas moedas digitais foram apresentadas para o comércio de energias renováveis com base em *blockchain*.

Cao *et al*. (2019) mostram, na Figura 9, que para operar um sistema IoT habilitado para *blockchain* desenvolvem-se as seguintes etapas:

a) Todos os dispositivos IoT operam na mesma rede *blockchain*;
b) um dispositivo IoT gera uma transação para pagamento (ou registra informações significativas) e a transmite para a rede;
c) os dispositivos IoT recebem as informações e transações na rede e as valida;
d) todos os dispositivos IoT executam um algoritmo *hash* para eleger um vencedor cujo bloco candidato será transmitido e validado como um novo bloco;
e) todos os dispositivos IoT inserem a cópia idêntica do novo bloco em seus livros-razão locais;
f) a transação armazenada no livro-razão da *blockchain* aciona o contrato inteligente no dispositivo IoT;
g) o dispositivo IoT realiza uma tarefa específica, ou seja, a movimentação do contêiner no cenário da cadeia de abastecimento, fornecimento de energia no cenário de energia inteligente.

Obs: Um contrato inteligente é apenas uma opção nesse círculo, que é um aplicativo no topo da *blockchain*. Os dispositivos IoT podem usar *blockchain* para muitos outros aplicativos sem depender de um contrato inteligente.

Na Figura 9, Cao *et al*. (2019) mostram que o mecanismo de consenso é a base em um sistema IoT habilitado para *blockchain*, que constrói uma ponte entre os dados brutos da infraestrutura e as informações confirmadas para a execução de várias aplicações.

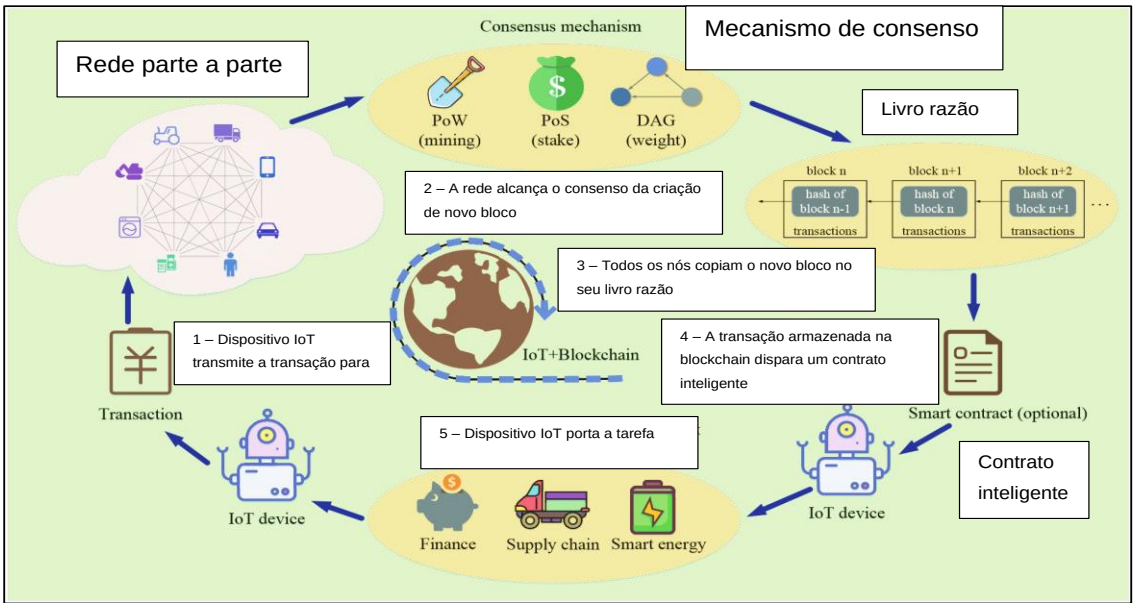

Figura 9
Exemplo de implementação de *blockchain* IoT.
Fonte: Caio *et al*. (2019). Tradução nossa.

Na fase V, o autor dessa dissertação enfatiza que as atividades de finanças, cadeia de suprimentos e energia inteligente podem estar ligados a empresas privadas, órgão de governo, *smart cities*, fazendas, etc., como já visto no corpo da pesquisa.

2.3.5 Blockchain e hyperledger

Santos & Moura (2019) explicam que existem muitos *frameworks* ou tecnologias em torno da *blockchain*: R3 (corda), *Ethereum*, Neo e Nem, cada uma com um *design* e arquitetura específicos.

Santos & Moura (2019, p. 61) acrescentam:

> A *hyperledger* faz parte da *Linux Foundation*, que foi lançada em 2016 com uma estrutura de governança técnica e organizacional e 30 membros corporativos fundadores. Mais de 230 membros já fazem parte dessa iniciativa. Isso inclui empresas como Cisco, Hitachi, IBM, ABN AMRO, ANZ *Bank*, *Red Hat*, VM*ware* e JP *Morgan*. Hoje, a *hyperledger* trabalha com muitos projetos

> sob o mesmo guarda-chuva e foca nas diferenças dos casos de uso da *blockchain*, bem como na cobertura de *frameworks* e ferramentas. Uma boa descrição dos projetos da *hyperledger* pode ser encontrada em https://www.hyperledger.org. Aqui, afirma-se que a *hyperledger* incuba e promove uma variedade de tecnologias de *blockchain* de negócios, incluindo estruturas de livro-razão distribuídas, motores de contrato inteligentes, bibliotecas de clientes, interfaces gráficas, bibliotecas de utilitários e aplicativos de amostra. A estratégia de guarda-chuva da *hyperledger* incentiva a reutilização de blocos de construção comuns e permite a inovação rápida de componentes *distributed ledger technology* (DLT), tecnologia de livro-razão distribuída (*blockchain* e *hyperledger*).

Continuando, esses autores esclarecem, explorando os projetos da *hyperledger*, têm-se cinco *frameworks* e cinco ferramentas. As estruturas são *Sawtooth*, *Iroha*, *Burrow*, *Indy* e *Fabric*. As ferramentas são *Caliper*, *Composer*, *Cello*, *Explorer* e *Quilt*.

Como exemplo, os autores citam que *hyperledger sawtooth* segue a mesma arquitetura e características de outros *frameworks hyperledger*. É uma plataforma *blockchain* corporativa para a construção de redes e aplicativos distribuídos.

A característica mais marcante do *sawtooth* é a facilidade de usar as APIs, assim como muitas linguagens como *Python*, C ++, Go, Java, *JavaScript* e *Rust*. Isso auxilia no desenvolvimento de aplicativos que rodam na plataforma *Sawtooth*. Além disso, podem-se escrever contratos inteligentes no *Solidity* para uso com a família de transações *Seth*. Outro bom recurso é a execução de transações paralelas. A maioria dos *blockchains* requer execução de transação serial para garantir ordenação consistente em cada nó da rede. A compatibilidade de contrato *Ethereum* também pode ser usada com *seth*; o projeto de integração *Sawtooth*/*Ethereum* estende a interoperabilidade da plataforma *Sawtooth para Ethereum* (Santos & Moura, 2019).

Para exemplificar o uso de ferramentas, esses autores recomendam que, se precisar testar uma ideia, criar uma prova de conceito (POC) ou um produto de valor mínimo (MVP) ou mesmo iniciar um projeto, a *hyperledger composer* pode ajudar a fazer isso de forma rápida e fácil. Pode-se testar uma rede de negócios com um aplicativo da *web* chamado *composer playground*. Com alguns cliques e um bom caso, pode-se criar uma rede corporativa integrada aos seus sistemas. Outra opção é criar um aplicativo de *front-end* para usar seu contrato inteligente.

A Figura 10 representa uma visão geral oficial da arquitetura no *site* da ferramenta *hyperledger composer.*

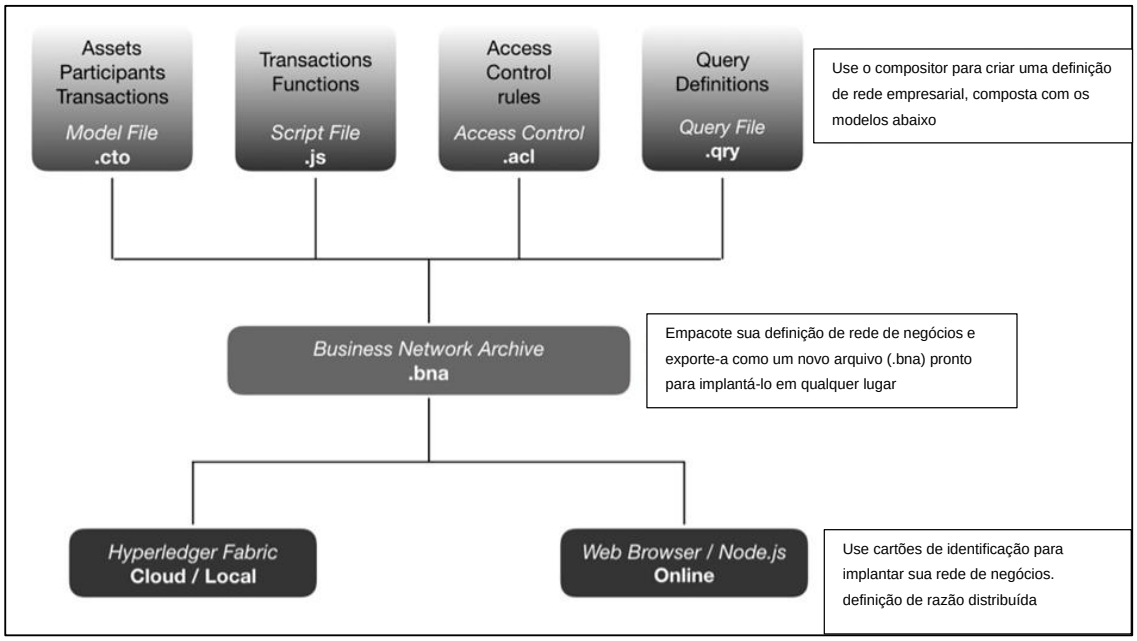

Figura 10
Hyperledger composer: visão geral.
Fonte: Santos & Moura (2019). Tradução nossa.

2.3.6 Blockchain as service (BaaS): blockchain como serviço

Singh & Michels (2018) atestam que em relação a plataformas subjacentes aos dois provedores BaaS mais estabelecidos, o BaaS da IBM (IBM *Cloud*) é baseado nos resultados da *hyperledger consortium* (visto anteriormente).

A visão da *Microsoft* (Azure) é oferecer suporte a vários protocolos. Inicialmente mostrou algum alinhamento com a plataforma *Ethereum*, sendo membro fundador e membro do conselho rotativo da *Ethereum Enterprise Alliance* (EEA). Os consórcios *Hyperledger* e EEA têm muitas empresas como membros, em uma variedade de setores. A *hyperledger* concentra-se em cadeias autorizadas sem uma base de criptomoeda (*tokens*), enquanto a EEA visa construir e adaptar *Ethereum* (que inclui *Ether,* um *token*/ ativo de suporte) para atender às necessidades de negócios, como gerenciamento de permissões. Observa-se também que a base de código da *hyperledger* é administrada por seu consórcio, enquanto a EEA baseia-se na

Ethereum, que é administrado pela *Ethereum Foundation*, uma organização separada (Singh & Michels, 2018).

Um dos recursos de computação em nuvem da nova geração é a *blockchain-as-a-service* (BaaS), uma fusão da tecnologia *blockchain* e o modelo de computação em nuvem. A BaaS permite o *offshoring* (fora do escritório) da implementação de *blockchain* de qualquer empresa para o ambiente de nuvem, sem a necessidade de algum conhecimento de TI. Assim, as empresas podem se beneficiar da BaaS como um serviço utilitário e atender às suas necessidades. BaaS é relativamente uma nova adição às tecnologias de *blockchain* com tecnologias de nuvem (Onik & Miraz, 2019).

Blockchain-as-a-service (BaaS) significa criar, gerenciar, hospedar e usar vários aspectos das tecnologias de *blockchain*, como nós de aplicativos, contratos inteligentes e livro-razão distribuído, na nuvem. Esses serviços baseados em nuvem facilitam a configuração de *blockchain*, plataforma, segurança e outros recursos associados. Assim, a BaaS apresenta a plataforma de serviço *blockchain*, dando suporte a recursos centrais da *blockchain*, com base na infraestrutura de computação em nuvem com o ambiente de desenvolvimento integrado para desenvolvedores e consumidores (Onik & Miraz, 2019).

Na verdade, o conceito-chave de BaaS é quase semelhante ao do *software-as-a-service* (SaaS). De acordo com a arquitetura (Figura 11 seguinte) da computação em nuvem, a BaaS pode funcionar explicitamente utilizando *platform-as-a-service* (PaaS) ou implicitamente por meio de *software-as-a-service* (SaaS) (Onik & Miraz, 2019).

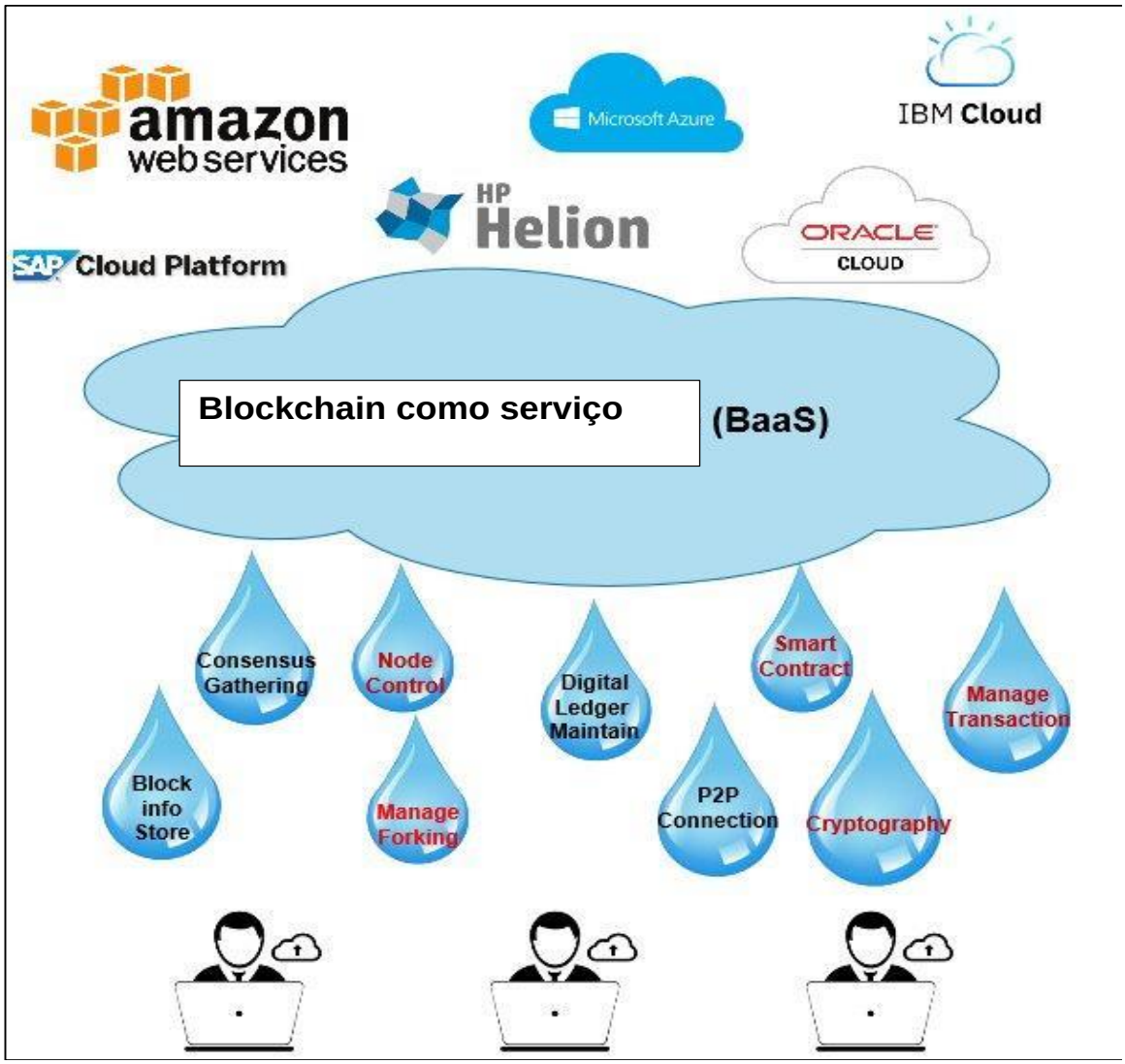

Figura 11
Arquitetura de *blockchain-as-a-service* (BaaS): exemplo.
Fonte: Onik & Miraz (2019).

Os mesmos autores citam os seguintes benefícios:

a) Com uma plataforma de nuvem já estabelecida, os usuários de *blockchain* podem receber perfeitamente serviço com custos muito menores do que a implementação real (no local).
b) Na arquitetura *blockchain* atual, vários regulamentos e normas, como verificação de nó, anexação de nó, exclusão de nó, bifurcação, devem ser cuidados. No entanto, a BaaS pode lidar com esses itens estratégicos sem qualquer intervenção do cliente.
c) A tecnologia *blockchain* está sendo usada além das criptomoedas. Portanto, a interação com outra plataforma, serviço, infraestrutura aumentou muito nos

últimos anos. Como a tecnologia de *blockchain* BaaS é construída utilizando a infraestrutura de nuvem existente, *infrastructure-as-a-service* (IaaS), PaaS, SaaS e outros aspectos semelhantes da nuvem permanecem nativos para BaaS - oferecendo mais interoperabilidade.

d) A implementação atual da *blockchain* requer moderado grau de conhecimento no domínio da criptografia e tecnologias distribuídas. Alternativamente, a BaaS, que é oferecida como um serviço completo pelos provedores, permite a implantação, gerenciamento e operação da tecnologia de *blockchain* sem qualquer conhecimento técnico específico.

Por fim, Singh & Michels (2018) alertam que muito do interesse em *distributed ledger* (DL) decorre de sua capacidade de descentralizar e desintermediar, removendo a necessidade de terceiros confiáveis. Em muitos casos, é a natureza descentralizada das DLs que traz considerações de segurança, resiliência e integridade de dados. A BaaS, no entanto, envolve a introdução de um provedor para fornecer e/ou gerenciar (aspectos da) infraestrutura DLT. Isso pode implicar a volta da centralização de aspectos da DL.

Conclui-se que a BaaS traz considerações sobre segurança e confiança. Na prática, se a BaaS suscita preocupações significativas depende das particularidades do serviço, do risco do aplicativo, do perfil de ameaça e do objetivo da DL.

- **Comparação das plataformas**

A Tabela 3 fornece a disponibilidade de várias plataformas de hospedagem de *blockchain* pelas principais plataformas BaaS:

Tabela 3

Plataformas de BaaS e recursos

Ethereum	*Quorum*	*Corda*	*Hyperledger Fabric*	*Multi chain*	*Digital As set*
AWS	√	√	√	√	
Azure	√	√	√	√	√
Google	√	√	√		
HPE	√				
IBM	√				
Oracle	√				
SAP	√				

Fonte: Onik & Miraz (2019).

Outros autores, como El Ioini & Pahl (2018), para comparar quatro tecnologias, utilizaram a Tabela 4. Como pode ser visto, cada tecnologia visa a um conjunto de propriedades para se diferenciar das demais. Ao olhar para seus documentos técnicos, as três tecnologias (*sidechain, tangle e hashgraph*) comparam muitos de seus pontos fortes com a *blockchain*. Embora esteja claro que todas as tecnologias visem a segurança e transparência, elas diferem em termos de desempenho e privacidade. Melhorar a economia da máquina e a comunicação máquina a máquina está entre as principais oportunidades para implementar as tecnologias discutidas.

Tabela 4

Comparação das DLTs: critérios de qualidade

	Blockchain	***Sidechain***	***Tangle***	***Hasgraph***
Data structure	*Linked list*	*Listo f linked lists*	DAG	DAG
Concensus	*PoW: SHA256-Hash*	*Pow: Ethash*	*PoW: hashcash*	*Virtual voting*
Translactions	*Grouped intro blocks*	*Two chains of blocks*	*Single transactions*	*Gossinp events contains transactions*
Fees	*Yes*	*Yes for the public chain*	*No fee*	*No fee*
Tps	*4 to 7*	*Limit by consortium chain*	*501 to 800* *500*	*>200,000*
Validation time	*Order of minutes*	*Order of minutes*	*Order of seconds*	*Order of seconds*
Privace	*Low*	*High*	*Low*	*Low*
Security	*High*	*High*	*High*	*High*
Maturity	*Many implementation*	*Experimental*	*Experimental*	*Experimental*
Platforms	*Biticoin, ethereum*	*Ethereum & monax*	*IOTA*	*Hedra*
Coyright	*Open source*	*Open source*	*Open source*	*Patented*
Typologies	*Public*	*Public and private*	*Private*	*Private*

Fonte: El Ioini & Pahl (2018).

Salienta-se que, observando-se a Tabela 4, em todas as DLTs os níveis de segurança são altos.

- **Critérios de qualidade e descrição (El Ioini & Pahl, 2018)**

a) Estrutura de dados: que tipo de estrutura de dados foi usada e com que finalidade, ou seja, quais informações são armazenadas nela.
b) Transações: como as transações são representadas.
c) Consenso: o mecanismo de consenso usado para aceitar transações na rede.
d) Taxa: qual é o custo do envio de transações.
e) Tps: quantas transações podem ser tratadas pela rede (transações por segundo).
f) Tipologia: como acessar a rede e os usuários tem funções diferentes.
g) *Copyright*: quais direitos autorais que a plataforma adota.
h) Privacidade: como a rede lida com privacidade.
i) A segurança: o nível de segurança garantido pela rede.
j) Tempo de validação: tempo necessário para validação de transações.
k) Maturidade: quão madura é a tecnologia.

Em abordagem recente, Nguyen, Pathirana, Ding & Seneviratne (2020), em artigo de setembro de 2020, mostra que em ecossistemas baseados em *blockchain* para IoT na nuvem, a *blockchain* pode ser considerada uma BaaS, que é integrada à computação em nuvem para oferecer serviços de TI completos a fim de ajudar pesquisadores e empresas a desenvolver, verificar e implantar a *blockchain* para aplicativos de IoT em nuvem. Os serviços BaaS são capazes de fornecer arquitetura básica e suporte técnico para garantir que os sistemas descritos anteriormente possam alcançar operações robustas e eficientes. Hoje em dia, há muitos provedores de BaaS nos mercados comerciais para permitir que os clientes adotem serviços sem se preocupar com a instalação de infraestrutura e investimento no sistema, o que pode acelerar as implantações dessas tecnologias de IoT em nuvem baseadas em *blockchain*.

Serão apresentadas as plataformas BaaS de última geração, líderes disponíveis no mercado, que estão prontas para uso. As principais características técnicas de cada plataforma são descritas resumidamente na Tabela 5 a seguir. O código-fonte para exemplos e modelos de BaaS também está disponível na plataforma de compartilhamento de código *Github*. Na verdade, muitos projetos de pesquisa empregaram tais plataformas BaaS para desenvolver seus aplicativos de IoT. Por exemplo, a nuvem IBM apresenta uma plataforma BaaS bem desenvolvida para usuários de IoT. A plataforma foi apresentada em uma rede veicular, em cujo projeto a plataforma IBM IoT em nuvem baseada em *blockchain* é integrada aos serviços IBM BaaS para gerenciar dados de sensores de veículos (mensagens de veículo a veículo e dados de monitoramento de veículo) e garantir a segurança durante o compartilhamento de dados na rede veicular. Enquanto isso, a plataforma BaaS da nuvem Oracle provou seu grande potencial por meio de ampla gama de projetos de IoT em nuvem baseada em *blockchain*, como bancos, gerenciamento de dados de saúde e gestão de pagamentos.

Recentemente, o provedor de nuvem *Hewlett Packard* colabora com a gigante da manufatura automotiva Continental para lançar uma plataforma baseada em *blockchain* para fabricantes de automóveis compartilharem e venderem dados de veículos. Esse projeto permite que clientes, incluindo motoristas de veículos, fabricantes de automóveis e prestadores de serviços, possam compartilhar dados de veículos com segurança em redes veiculares não confiáveis, tornando a mobilidade mais segura, ecológica e acessível. Embora as plataformas BaaS ainda estejam em desenvolvimento, o sucesso de tais projetos iniciais nessas plataformas deve garantir novas oportunidades para futuras implantações desse tipo (Nguyen *et al*., 2020).

Tabela 5

Plataformas BaaS para aplicativos IoT em nuvem

Serviços BaaS	Descrição	*Blockchain*	Ano de lança-mento
Microsoft Azure bkockchain	A *Blockchain* da *Microsoft* no *Azure* é uma plataforma BaaS hospedada na computação em nuvem do *Microsoft Blockchain Azure* para criar e configurar a infraestrutura de *blockchain* do consórcio rapidamente. Ele agora está disponível em duas camadas: básico para serviços com custo otimizado para testar aplicativos *blockchain* e padrão para executar aplicativos BCoT reais.	*Ethereum, Hyperledger Fabric or R3 Corda*	2016
IBM *Blockchain*	IBM *blockchain* é uma plataforma de desenvolvimento de aplicativos *blockchain* pronta para empresas. Ele permite que as empresas desenvolvam, governem e operem sistemas *blockchain* com *software* integrado e atualizações de rede na nuvem IBM. Alguns dos maiores setores bancários e comerciais usaram o *blockchain* da IBM.	*Hyperledger Fabric*	2017
Amazon	O serviço de *blockchain* da *Amazon* facilita a configuração, implantação e gerenciamento de redes *blockchain* escalonáveis. Pode ser útil em muitos casos de uso de IoT, como sistemas de manufatura, seguro, comércio, varejo e bancário.	*Ethereum and Hyperledger Fabric*	2018
Oracle	A BaaS na nuvem *Oracle* fornece uma plataforma de contabilidade distribuída de nível empresarial que pode ajudar as empresas a aumentar a confiança e fornecer agilidade nas transações em suas redes de negócios. O *Oracle* BaaS pode se conectar perfeitamente com uma série de soluções populares da *Oracle*, como *Oracle Supply Chain Management* (SCM) *Cloud* e *Oracle Enterpri*se *Resource Planning* (ERP) *Cloud*.	*Hyperledger Fabric*	2018
Hewlett-Packard (HP)	*Blockchain.* A HP lançou seu BaaS chamado HPE *Mission Critical Blockchain*, que permite aos clientes executar cargas de trabalho de razão distribuída em ambientes industriais com alta segurança. Ele também garante escalabilidade massiva de projetos de *blockchain* baseados em HP para apoiar negócios.	*Ethereum*	2017
Alibabá	O Alibabá BaaS é um PaaS (*Platform as a Service*) de nível empresarial que é construído em *blockchain* no Alibaba *Cloud Container Service* para *clusters Kubernetes*. Ele traz benefícios como alta segurança, facilidade de uso, alta estabilidade, abertura e serviços de compartilhamento eficientes para aplicativos baseados em *blockchain*	*Ethereum and Hyperledger Fabric*	2017
Baidu	*Baidu* BaaS é uma plataforma comercializada para simplificar o desenvolvimento de Dapp. Ele fornece aos desenvolvedores serviços como estruturas de várias cadeias e camadas intermediárias, bem como contratos inteligentes e modelos DApp na computação em nuvem do Baidu. Seus aplicativos consistem em IoT com BCoT, finanças e dados	*Ethereum, Hyperledger Fabric, and Baidu XuperChain*	2018
Huawei	*Huawei* BaaS é um serviço de nuvem que aproveita as vantagens do contêiner em nuvem da Huawei e das tecnologias de segurança. Ele oferece vantagens importantes, como recursos abertos, fáceis de usar, flexíveis e eficientes, bem como proteções robustas de segurança e privacidade.	*Hyperledger*	2018

Continua

Tabela 5

Plataformas BaaS para aplicativos IoT em nuve*m* - conclui

Google	O *Google* BaaS é baseado na plataforma *Ethereum* com recursos importantes, como integração de API, algoritmos de consenso configuráveis e a capacidade de usar um banco de dados SQL tradicional para consultar e relatar dados de *blockchain*.	*Ethereum*	2018
SAP	O SAP BaaS fornece a porta de entrada mais fácil e de menor risco para experimentar a tecnologia de razão distribuída. Está hospedado na plataforma de nuvem SAP, permitindo prototipar, testar e construir aplicativos *blockchain* (privados e consorciados) e contratos inteligentes.	*MultiChain and Hyperledger Fabric*	2018

Fonte: Nguyen *et al*., 2020. Tradução nossa.

2.3.7 Blockchain para 2FA

Conforme Gupta (2018), em sistemas *two-factor authentication* (2FA - autenticação em duas fases) convencionais acontecem vários incidentes de violação de dados, e é crescente o número de contas de *sites* sociais e profissionais sendo invadidos/ hackeados. Um erro humano pode de repente causar sérios transtornos para usuários nas cidades. Às vezes, é fácil prever a senha de um usuário com base em sua atividade diária, comportamento ou mesmo nome. Os usuários ainda tendem a usar palavras-passe de texto simples para proteger sua conta.

2FA é uma camada extra de segurança usada para garantir que apenas o proprietário legítimo possa acessar sua conta. Nesse método, o usuário irá primeiro inserir uma combinação de nome de usuário e senha e, em vez de acessar diretamente sua conta, o usuário tem que fornecer outras informações.

Blockchain é reconhecida como uma das tecnologias mais revolucionárias e inovadoras que existem. A *blockchain* tem satisfeito o princípio da tríade de segurança da *confidentiality, integrity, and availability* (CIA), *triad models* baseada em soluções de segurança cibernética. A 2FA tem sofrido críticas em medidas de segurança por vários anos, pois os invasores conseguem comprometer esses sistemas. Vejam como a *blockchain* pode transformar o sistema 2FA para obter um método de segurança melhorado/avançado (Gupta, 2018).

Dada a sua natureza, a *blockchain* é uma tecnologia descentralizada que permite transações de qualquer tipo de valor entre vários participantes sem o envolvimento de terceiros. Aproveitando-a, pode-se garantir que essas informações confidenciais nunca permaneçam em somente um banco de dados; em vez disso, podem estar dentro de nós de *blockchain* que têm imutabilidade e não podem ser modificados ou excluídos. A Figura 12 exibe um 2FA baseado em *blockchain*. Nesse sistema, os dispositivos do usuário serão autenticados por um provedor 2FA terceirizado por meio da rede *blockchain*. Cada parte da rede *blockchain* manterá as informações do *endpoint* com segurança e ativará o sistema 2FA para gerar a senha de segundo nível. Isso pode ser implantado no domínio público, *smart cities*, órgão de governo de qualquer nível ou mesmo em uma rede privada com uma chamada de API de terceiros (Gupta, 2018).

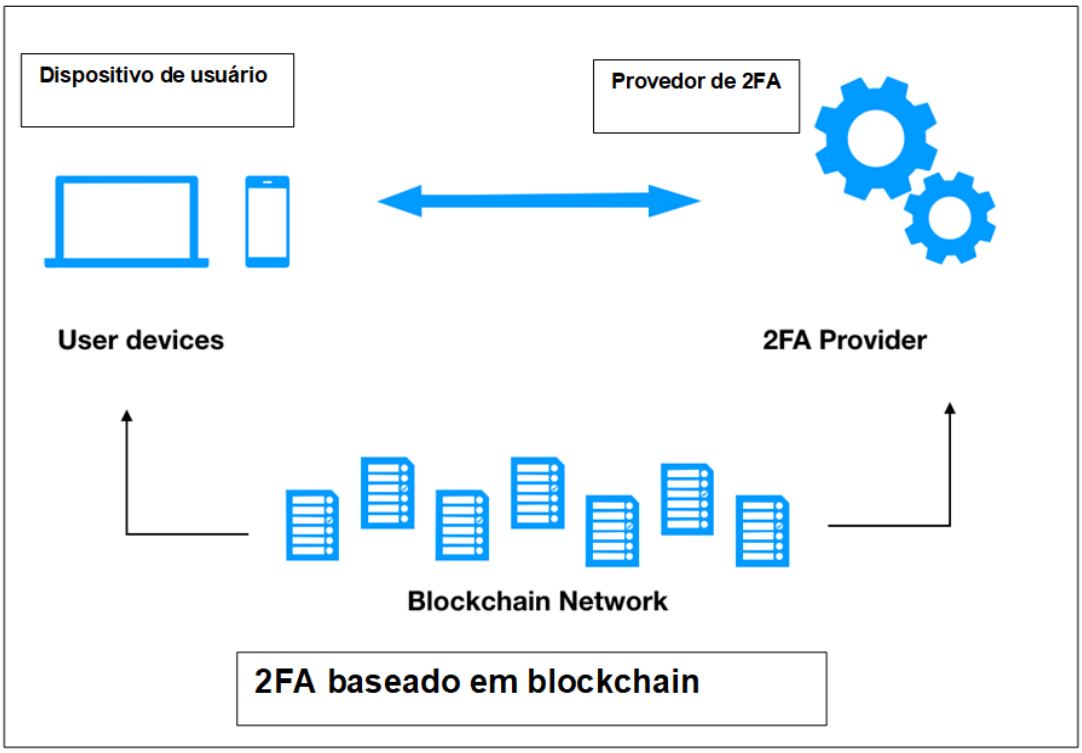

Figura 12
2FA baseado em *blockchain*.
Fonte: Gupta (2018). Tradução nossa.

2.4 Aplicações seguras

Uma característica da *blockchain* é a sua imutabilidade, o que significa, que uma vez que uma transação é registrada na cadeia, os dados não podem ser alterados

retroativamente. Com uma *blockchain* pública, pelo menos a maioria dos nós que computam a *blockchain* teria que conspirar para desfazer uma transação. É altamente improvável que isso ocorra na prática. Existem ameaças também, e elas serão vistas mais à frente. Chama-se a natureza distribuída dessa verificação de *blockchain* de "baseada em consenso".

Ao contrário dos sistemas convencionais, em que se confia na organização que executa o provedor de identidade ou na organização que executa a autoridade certificada (CA), diz-se que a *blockchain* pública cria um novo sistema baseado em confiança, estando essa confiança na rede de servidores e no *software* sistema, não em qualquer empresa em particular. A tecnologia de *blockchain* pública fornece o não repúdio a eventos por um grupo de servidores distribuídos, geralmente controlados por pessoas diferentes em locais diferentes. A maioria dos sistemas de *blockchain* públicos usa chaves e assinaturas para controlar quem pode fazer o quê no livro-razão compartilhado. Os nós da *blockchain* dentro da rede têm sua própria cópia do livro-razão e as transações adicionadas a este são públicas e transmitidas a todos os nós participantes, portanto, essa transação aparece em todas as cópias do bloco-cadeia.

De acordo com as regras acordadas pela rede, um, qualquer ou todos os participantes podem adicionar transações à *blockchain*. Os algoritmos de *blockchain* agregam transações em “blocos”, e os blocos são adicionados à cadeia de blocos existentes, usando uma assinatura criptográfica. Para *blockchains* públicos, essa assinatura inclui a prova de trabalho. Essa prova de trabalho torna criptograficamente improvável que qualquer pessoa, incluindo o fraudador de um *hacker*, possa alterar os bloqueios anteriores. A natureza pública e distribuída da *blockchain* torna difícil obter um bloco falso aceito pela rede (Treiblmaier & Beck, 2018b).

Entre as tecnologias promissoras da *blockchains* estão monitoramento de rede e serviços de segurança, incluindo autenticação, confidencialidade, privacidade, integridade e procedência. Atualmente, esses serviços são fornecidos por corretores terceirizados confiáveis ou usando abordagens distribuídas ineficientes. Como resultado, a segurança é um grande desafio para os atuais sistemas da rede. Por outro lado, a tecnologia *blockchain* pode fornecer garantias de segurança que resolvem

muitos desafios tradicionais, além de fornecer uma solução totalmente distribuída, comprovadamente segura e consensual. A Figura 13 ilustra as diferenças entre o controle de acesso tradicional e o baseado em *blockchain*. O mesmo conceito pode ser aplicado às demais garantias de segurança. Esta pesquisa enfoca o uso da tecnologia *blockchain* para fornecer serviços e aplicativos de segurança de rede em *smart cities,* mas pode-se usar em uma variedade de aplicações.

Então é apresentada como a tecnologia *blockchain* pode ser usada para resolver os desafios associados e destacar várias abordagens baseadas em *blockchain* com propostas que fornecem os serviços de segurança desejados (Salman, Zolanvari, Erbad, Jain & Samaka, 2019).

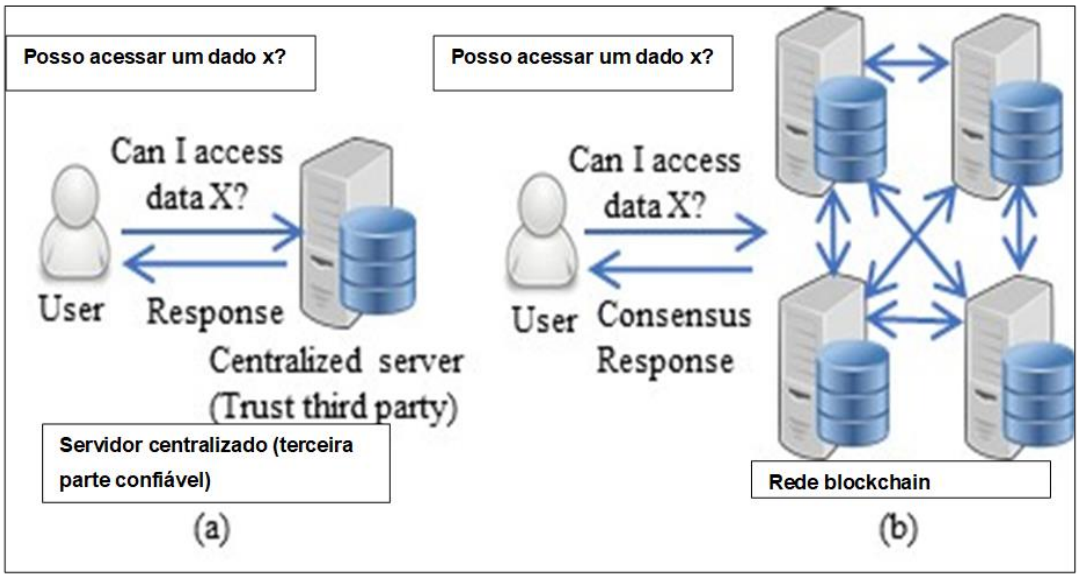

Figura 13
(a) Garantias de controle de acesso centralizado tradicional; (b) Garantias de controle de acesso com base em *blockchain*.
Fonte: Salman *et al*. (2019).

2.4.1 Abordagens de IoT segura por blockchain

Mohanta, Jena, Panda & Sobhanayak (2019) postulam que sistemas de transporte inteligentes (ITS) consistem em sete camadas, cada uma com alguns dispositivos de *hardware* ou serviços de aplicativo associados. Ao integrar com a tecnologia *blockchain*, aumenta a segurança do dispositivo e a privacidade dos dados. A *blockchain* pode fornecer um ecossistema ITS seguro, confiável e descentralizado.

Em ITS, o gerenciamento de chaves seguras é uma das questões importantes dentro da rede heterogênea. A camada física consiste em vários sensores físicos. A camada de dados consiste em blocos encadeados e técnicas relacionadas a criptografia e *hashing*. Na camada de rede, o ITS baseado em *blockchain* conecta os dispositivos no modelo pessoa a pessoa/parte a parte (P2P). Vários tipos de algoritmos de consenso são usados para que a validação de dados alcance confiança mútua entre os pares na camada de consenso. Em seguida, algum incentivo pode ser alocado de acordo com o algoritmo de consenso e o contrato inteligente é feito, a camada de aplicativo fornece serviços inteligentes e gerenciamento inteligente para o sistema. O algoritmo de consenso da prova de trabalho foi usado para atingir a *blockchain* específica do sistema.

Minoli & Occhiogrosso (2018) realçam que fundamentalmente a IoT pode utilizar *blockchain* para garantir a integridade dos dados. Eles mostram que a tabela seguinte descreve o possível uso de *blockchain* em várias camadas da estrutura da arquitetura de referência. Deve-se notar que os mecanismos envolvidos dão origem a certa complexidade, especialmente se a infraestrutura P2P é estabelecida globalmente, em todo um ecossistema de IoT. Devido às limitações típicas dos nós de IoT, nem sempre pode ser prático utilizar uma rede protegida por *blockchain* completa no âmbito de IoT genérico; no entanto, certos aplicativos críticos ou institucionais, como redes inteligentes, ITS, seguros e ambientes de contrato inteligente, podem ter recursos suficientes para suportar a funcionalidade.

As limitações potenciais da implementação de tais funções em nós de IoT genéricos para criar livros-razão distribuídos devido à capacidade limitada de processamento e armazenamento dos dispositivos de IoT são talvez evidentes, e os recursos de *blockchain* poderão ser implementados em elementos de rede (NEs) nela selecionados. Não se espera que um nó IoT de baixo custo, como um sensor ou atuador remoto, garanta a integridade de todos os dados do ecossistema; portanto, apenas alguns NEs selecionados podem assumir esse papel mais precioso. Outra abordagem é usar um livro-razão distribuído simples, no qual os blocos são assinados digitalmente ao longo do caminho, mas o processo de consenso mais elaborado não é implementado.

Minoli & Occhiogrosso, (2018) continuam:

a) *Blockchain* ponta a ponta - a fonte cria um bloco de transação contendo dados e também cria o primeiro bloco. Outros NEs irão anexar o próximo bloco na *blockchain*, conforme a informação viaja pela rede até seu destino, normalmente algum mecanismo analítico na nuvem para análise ou armazenamento. Aqui, o armazenamento também desfruta da proteção de integridade da *blockchain*. Essas transações podem ser reclamações, fotos de acidentes, etc.
b) Nível analítico/de armazenamento - isso é basicamente o mesmo que *blockchain* de ponta a ponta, exceto que a transação é "consumida" no mecanismo de análise, donde os dados são extraídos e utilizados. Aqui, o armazenamento não teria a proteção de integridade da *blockchain*, mas para algumas aplicações não críticas, por exemplo, amostragem de parâmetros ambientais, pode ser adequado.
c) Nível de *gateway* - nessa situação, os usuários individuais criam dados que não são protegidos imediatamente para integridade; entretanto, uma vez que os dados chegam ao *gateway*, eles são incorporados à *blockchain* junto com os dados de outros usuários, e assim ficam, também, protegidos. Uma motivação para essa abordagem é que os nós finais individuais podem não ter os recursos computacionais para criar *hashes* de (possivelmente grandes) blocos de dados.
d) No nível do *site* - para essa situação os usuários individuais em determinado local (por exemplo, sensores ou robôs no chão de fábrica) criam dados que não são protegidos imediatamente para integridade no nível do dispositivo; mas uma vez que os dados alcançam o nó de concentração local (por exemplo, um *switch* de camada 2, um ponto de acesso *Wi-Fi*, um roteador, um *firewall,* e assim por diante), eles são incorporados à *blockchain* junto com os dados de outros usuários *do* site. Novamente, uma motivação para essa abordagem é que os nós finais individuais podem não ter os recursos computacionais para criar *hashes* de (possivelmente grandes) blocos de dados, mas o NE baseado no local tem o poder computacional.

e) Nível do dispositivo - cada dispositivo individual tem a capacidade, bem como o requisito é, aqui, obrigatório de construir cadeias de blocos de dados a serem protegidos imediatamente.

Tabela 6

Mecanismos de segurança por camadas e usos da *blockchain* - conclui

Camadas	Descrição	Mecanismo de segurança
Camada 3 - *Fog networking*	Esta camada suporta *fog networking* (rede em névoa), isto é, a rede localizada (local ou vizinhança), que é o primeiro salto da conectividade do cliente IoT ("nuvem do dispositivo"). Normalmente, a rede de névoa é otimizada para o ambiente operacional dos clientes IoT e pode usar protocolos especializados. Pode ser um *link* com fio (por exemplo, em uma LAN de fábrica, digamos, em um aplicativo de robótica) ou um *link* sem fio (em uma LAN sem fio).	*Fog network*/ autorização e autenticação na borda da rede; criptografia e gerenciamento de chaves; gerenciamento de confiança e identidade (esses mecanismos estão sendo devidamente adaptados a essa camada do ecossistema IoT).
Camada 2 - Aquisição de dados	Esta camada abarca os recursos de "aquisição de dados". É fisicamente constituído de sensores (apropriados à "coisa" e à "aplicação" da camada superior), dispositivos embarcados, embutidos, *hubs* de sensores, e assim por diante. A camada 1 e a camada 2 podem ser vistas como estando em simbiose no mundo IoT, no sentido de que as coisas "casadas" com sensores se tornam clientes ou terminais IoT. As informações coletadas podem ser parâmetros de dados, voz, vídeo, multimídia, dados de localização, informações de poluição, etc.	*Blockchains* "no nível do *site*"; *link* de agregação, autorização e autenticação; criptografia e gerenciamento de chaves; gerenciamento de confiança e identidade (esses mecanismos estão sendo devidamente adaptados a essa camada do ecossistema IoT).
Camada 1 - Dispositivos (coisas)	Essa camada é composta do universo de "coisas" que estão sujeitas à automação oferecida pela IoT. Este é um grande domínio, incluindo (por exemplo) pessoas (com *wearables,* dispositivos de monitoramento médico *e/m-health,* etc.), *smartphones*, eletrodomésticos (por exemplo, geladeiras, máquinas de lavar, condicionadores de ar, etc.), casas e edifícios (incluindo HVAC e sistemas de iluminação), câmeras de vigilância, veículos (carros, caminhões, aviões, máquinas de construção), elementos da rede elétrica, e assim por diante	*Blockchains* de "nível de dispositivo"; autorização e autenticação no nível do dispositivo; criptografia e gerenciamento de chaves; gerenciamento de confiança e identidade (esses mecanismos estão sendo devidamente adaptados a essa camada do ecossistema IoT).

HVAC: *Heating, ventilation, and air conditioning.*
Fonte: Minoli & Occhiogrosso (2018). Tradução e adaptação nossas.

Os autores finalizam exemplificando, com a Figura 14, um aplicativo de segurança IoT *e-health*, cujo dispositivo de nível de *gateway* cria uma *blockchain* para as informações médicas a serem transmitidas (a criptografia do conteúdo original também deve ser implementada).

Blockchains podem e devem ser usadas no nível do aplicativo para validar todos os tipos de transações que necessitam de segurança. Por exemplo, o pagamento de uma taxa de estacionamento à medida que passa pelas várias entidades financeiras que

apoiam a transação, fotografia, imagem, vídeo ou formulário de dados de hospitais. Além disso, as informações podem incluir dados de sensores médicos, reclamações médicas, capturas de tela de vigilância internas em vídeo, e assim por diante.

Blockchains também podem ser usadas na camada inferior do modelo de comunicação para fornecer integridade para transferência de informações através de um número encadeado de *links*, convergindo da borda para um mecanismo de análise centralizado ou um servidor baseado em nuvem.

Os dispositivos IoT precisam se comunicar e sincronizar uns com os outros. Usando-se *blockchain,* podem-se controlar e configurar dispositivos IoT (por exemplo, gerenciar chaves usando criptossistemas de chave pública Rivest, Shamir e Adleman (RSA), em que as chaves públicas são armazenadas em um local seguro da rede e as chaves privadas são salvas em dispositivos individuais).

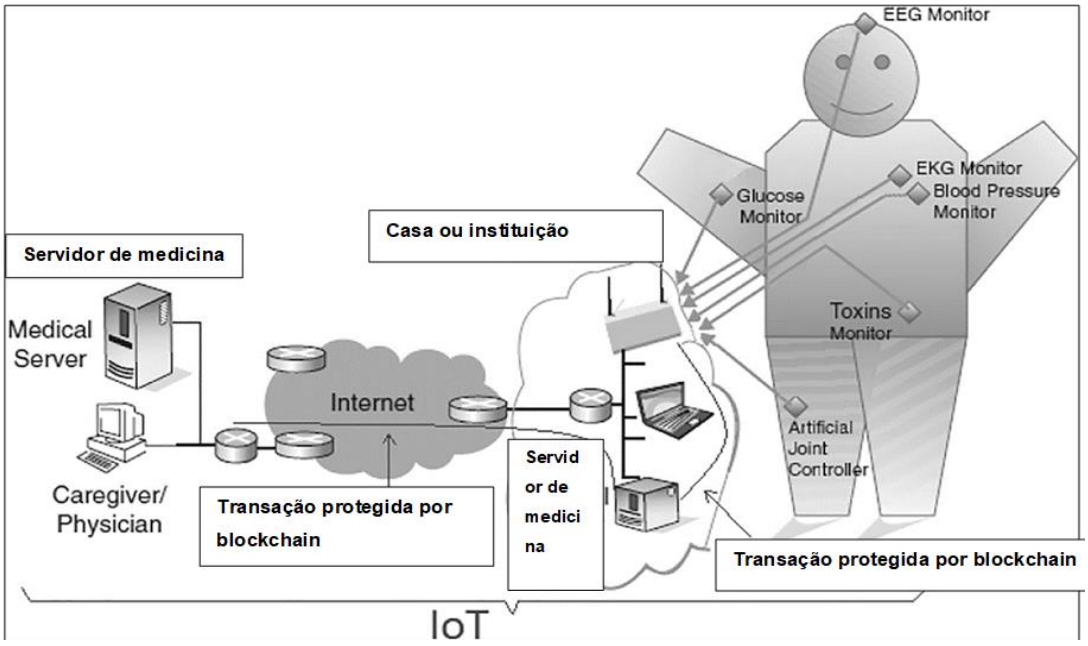

Figura 14
Exemplo: *e-health* - aplicação de *blockchain.*
Fonte: Minoli & Occhiogrosso (2018).

Nakamura & Geus (2007) explanam que a autenticação exerce papel fundamental para a segurança de ambientes virtuais ao validar a identificação dos usuários. Após a autenticação, o sistema pode conceder a autorização para o acesso aos recursos. A autenticação pode ser realizada com base em alguma coisa que o usuário sabe, em

algo que o usuário possui ou em determinada característica do usuário. O controle de acesso, que tem como base a autenticação dos usuários, também desempenha papel essencial em qualquer ambiente e pode ser usado em diferentes níveis ou camadas. A identificação é a função em que o usuário declara determinada identidade para um sistema, enquanto a autenticação é a função responsável pela validação dessa declaração de identidade do usuário. A autenticação ou a validação da identificação do usuário que oferece a autorização pode ser realizada utilizando-se três métodos, conforme Nakamura & Geus (2007):

a) Com base no que o usuário sabe: senha, chave criptográfica ou *personal identification number* (PIN).
b) Com base no que o usuário possui: *token*, cartão ou *smart card*.
c) Com base nas características do usuário: biometria (seção 11.1.3), ou seja, reconhecimento de voz, impressão digital, geometria das mãos, reconhecimento da retina, reconhecimento da íris, reconhecimento digital de assinaturas, etc. (Nakamura & Geus, 2007).

Rotuna, Gheorghita, Zamfiroiu & Smada (2019) também abortam esse assunto usando a norma *International Organization for Standardization* (Isso) de 2019. Para eles, a identidade digital é a informação sobre uma entidade, utilizada pelos sistemas de informação para representar um agente externo, que pode ser uma pessoa, uma organização, um aplicativo ou um dispositivo. A ISO/IEC 24760-1 (2019) define identidade como um "conjunto de atributos relacionados à entidade". Os dados de identidade digital permitem a autenticação automática de um usuário interagindo com um sistema e possibilita o acesso aos serviços fornecidos pelo sistema.

Identidade autossoberana (SSI) é um tipo de identidade digital que permite ao usuário o controle total e final de sua identidade. Por meio da SSI, os usuários ou empresas podem armazenar seus dados de identidade em seus dispositivos e podem fornecê-los com eficácia para aqueles que precisam validá-los. Assim, o usuário gerencia por meio de um aplicativo, no celular ou no computador, os elementos que compõem a identidade e controla o acesso a esse conjunto de informações. Os dados de identidade podem incluir datas de nascimento, cidadania, diplomas universitários ou

licenças. Dentro do aplicativo, o usuário recebe inicialmente um número de identificação autogerado derivado da chave pública e uma chave privada correspondente. Esse par de chaves é diferente da combinação de nome de usuário e senha, porque depois de criado pelo usuário, cálculos matemáticos automáticos são realizados sobre ele, o que torna a descriptografia quase impossível.

Rotuna *et al.* (2019) reforçam que esse tipo de identidade pode ser implementado para identificar os cidadãos de uma cidade inteligente usando a tecnologia *blockchain,* que garante armazenamento, registro de data e hora seguros e hospedagem descentralizada. Esse modelo elimina a necessidade de senhas e garante autenticação com alto grau de segurança.

As soluções de identidade digital com base pública giram em torno da cidadania e do uso na interação com instituições públicas e privadas. Os governos fornecem aos indivíduos uma variedade de serviços diferentes que estão se tornando cada vez mais disponíveis *online*. A digitalização do serviço governamental inclui a necessidade de uma identidade digital segura, portátil e de fácil acesso. Atualmente, o único caso de uso implementado “de cima para baixo” de uma identidade nacional baseada em *blockchain* é a Estônia, que estabeleceu um dos sistemas de carteira de identidade nacionais mais avançados tecnologicamente. O cartão obrigatório permite o acesso a todos os serviços eletrônicos seguros (Sullivan & Burger, 2017 como citado em Zwitter, Gstrein & Yap, 2020), incluindo viagens dentro da União Europeia, seguro saúde nacional, acesso a contas bancárias, votação eletrônica, administração de registros médicos e até mesmo reclamações fiscais.

O cartão físico é protegido com criptografia de chave pública - criptografia de curva elíptica (ECC) de 384 *bits* e que também pode ser usado em ambiente digital para verificação. Ele utiliza a tecnologia *blockchain* para garantir a validade das informações pessoais, permitindo total controle e portabilidade. Embora a identidade às vezes seja considerada “autossoberana”, uma vez que o fluxo de informações é totalmente controlado pelo proprietário da identidade, existem restrições em termos de uso. Portanto, pode-se argumentar que esse sistema não representa uma

personificação pura do conceito de identidade autossoberana e não deve ser considerado como tal (Zwitter *et al*., 2020).

2.4.1.1 *Edge / Fog computing*

Recentemente, houve mudança nas arquiteturas dos sistemas de informação, surgindo a computação de névoa. O que essa tecnologia faz é processar os dados sensíveis ao tempo na borda da própria rede, ou seja, mais perto de onde os dados estão sendo gerados, para que as ações apropriadas possam ser tomadas a tempo. Alguns recursos principais desse modelo são: minimizar a latência, conservar a largura de banda da rede, resolver o problema de privacidade e segurança dos dados e aumentar a confiabilidade (Mohamed, 2019).

O autor prossegue: a computação de borda significa ter alguma computação local que funcione com a nuvem pública de forma híbrida.

A Tabela 7 compara computação/*networking* nuvem e névoa em termos de localização, tamanho e aplicações. A arquitetura de computação de névoa é mostrada na figura 15. A IoT é composta de três camadas: nuvem, névoa e camadas de dispositivo.

Tabela 7

Comparação entre computação em nuvem e névoa

	Nuvem	**Névoa**
Localização	Centralizado em um pequeno número de *big data centers*	Frequentemente distribuído em muitos locais, potencialmente em grandes áreas geográficas, mais perto dos usuários. Os nós e sistemas de névoa distribuídos podem ser controlados de maneiras centralizadas ou distribuídas.
Tamanho	Os *data centers* em nuvem são muito grandes, cada um contendo normalmente dezenas de milhares de servidores.	Uma névoa em cada local pode ser pequena (por exemplo, um único nó de névoa em uma fábrica ou a bordo de um veículo) ou tão grande quanto necessário para atender às demandas do cliente. Um grande número de pequenos nós de névoa pode ser usado para formar um grande sistema de névoa.
Aplicação	Normalmente oferece suporte a aplicativos que podem tolerar atrasos de ida e volta da ordem de alguns segundos ou mais.	Suporta significativamente mais aplicativos de tempo crítico que requerem latências abaixo de dezenas de milissegundos ou até menos.

Fonte: Mohamed (2019).

As nuvens são compostas de servidores e cada um deles mantém aplicações com serviços de computação e armazenamento. A camada do dispositivo é composta de sensores e atuadores. Os dados do sensor coletados por sensores são entregues a servidores em redes e são finalmente entregues aos nós de névoa da borda na camada de névoa. Com base nesses dados, as ações a serem realizadas pelos atuadores são decididas na IoT. Os atuadores recebem ações dos nós de névoa de borda e executam as ações no ambiente físico. Além disso, um nó de névoa toma uma decisão sobre quais ações os atuadores devem realizar com base nos dados do sensor. Em seguida, os nós de borda emitem as ações para os nós atuadores. Um nó de névoa também é equipado apropriadamente para armazenar dados. Assim, os dados e processos são distribuídos não apenas para servidores, mas também para nós da névoa no modelo de computação em nuvem, enquanto centralizados em servidores de nuvens no modelo de computação em nuvem (Mohamed, 2019).

O autor finaliza pontuando que dados de IoT são produzidos em curto tempo e em grandes quantidades, apresentando uma variedade de distribuições esporádicas ao longo do tempo. Além disso, em alguns casos, em tempo real ou quase em tempo real. Uma tendência em aplicativos de internet das coisas que aborda o conceito de IoT *analytics* é ao uso de computação em névoa, que pode descentralizar o

processamento de fluxos de dados de IoT e apenas realizar a transferência de dados de IoT filtrados dos dispositivos da borda da rede para a nuvem.

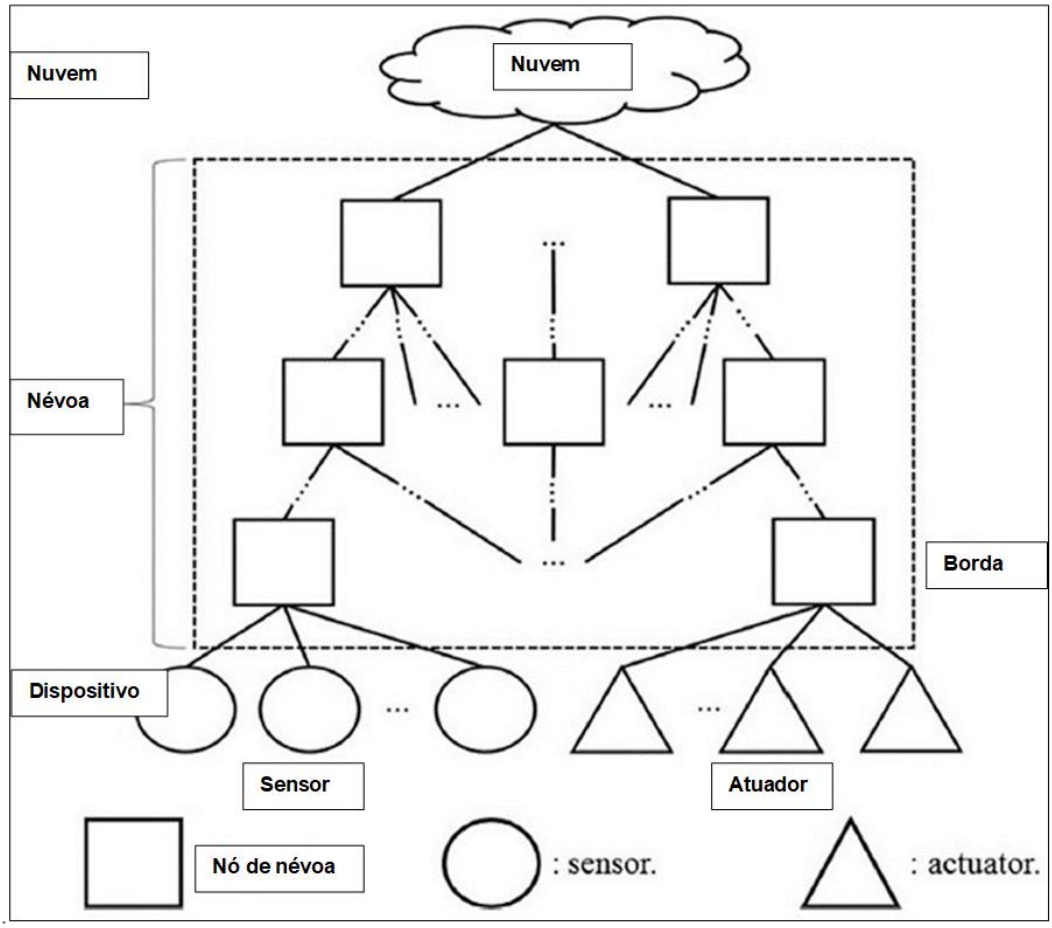

Figura 15
Arquitetura IoT com três camadas: *cloud*, *fog* e dispositivos conectados.
Fonte: Mohamed (2019).

Do ponto de vista de Mohamed (2019), a IoT pode se beneficiar muito da funcionalidade fornecida pela *blockchain* e ajudará a desenvolver as tecnologias IoT atuais. É importante notar que ainda há muitos desafios de pesquisa e questões em aberto que precisam ser estudados a fim de usar perfeitamente essas duas tecnologias.

Mukherjee, Matam, Shu, Maglaras, Ferrag, Choudhury & Kumar (2017) reportam que *fog computing*, também chamado de computação de borda (*edge*), é uma plataforma altamente virtualizada que permite a computação e o armazenamento entre os usuários finais e o *data center* da computação em nuvem tradicional. Sem os terceiros, os dispositivos *fog* podem se comunicar uns com os outros. No entanto, a técnica de *blockchain* pode ser usada para facilitar a comunicação entre nós de névoa e

dispositivos IoT. E mostram, na Figura 16, uma visão mais detalhada das três camadas de arquitetura de *fog computing.*

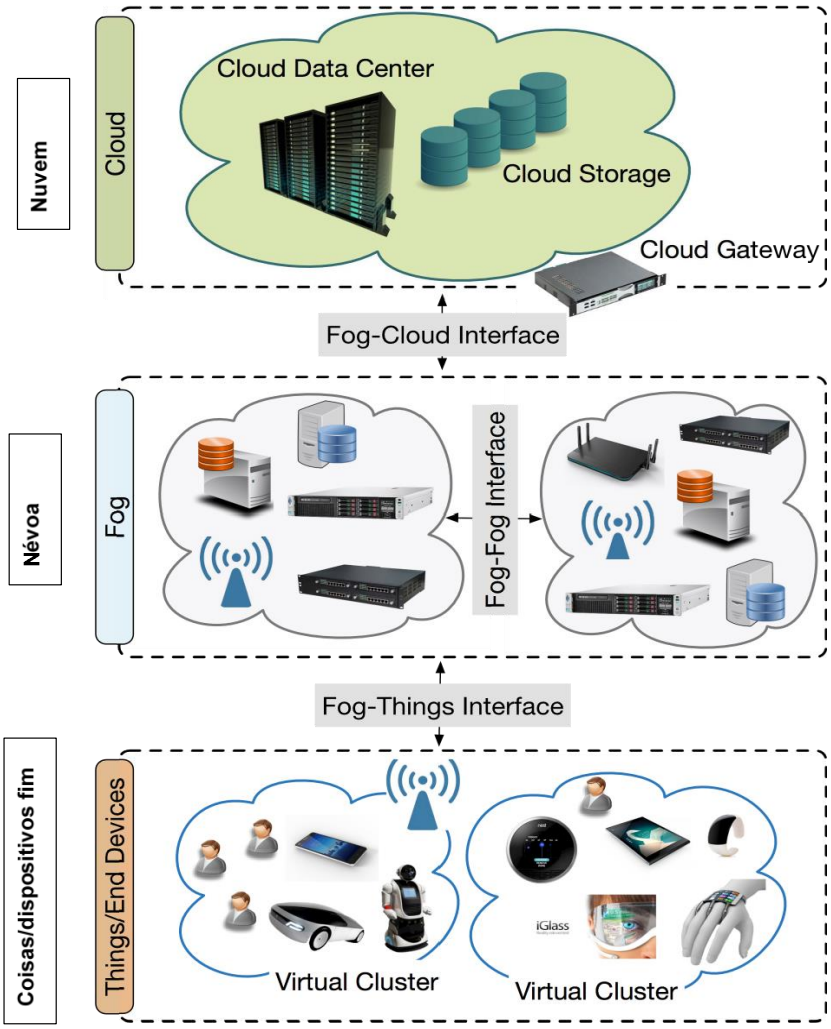

Figura 16
As três camadas de arquitetura de *fog computing*.
Fonte: Mukherjee *et al*. (2017).

Outros autores, como Rejeb, Keogh & Treiblmaier (2019), no mesmo diapasão, identificam que, ao combinar a tecnologia *blockchain* e IoT, os parceiros de intercâmbio obtêm *insights* novos e oportunos em sua cadeia, em tempo real, com informações mais precisas e confiáveis sobre os principais processos, eventos e atributos monitorados. Essa fusão de tecnologia IoT e *blockchain* pode ajudar a melhorar a rastreabilidade de ponta a ponta em uma cadeia de suprimentos de um município, por exemplo, e permitir recursos de *recall* rápido de bens rastreados.

Blockchains permitem a agregação descentralizada de grandes quantidades de dados gerados a partir de dispositivos conectados de IoT e garantem que os benefícios

sejam compartilhados de forma mais equitativa entre os participantes da rede em uma cidade, por exemplo.

Na Figura 17 constatam-se as principais áreas de pesquisa na interseção entre a tecnologia IoT e *blockchain*, incluindo escalabilidade, segurança, imutabilidade e auditoria, eficácia e eficiência do fluxo de informações, rastreabilidade, interoperabilidade e qualidade.

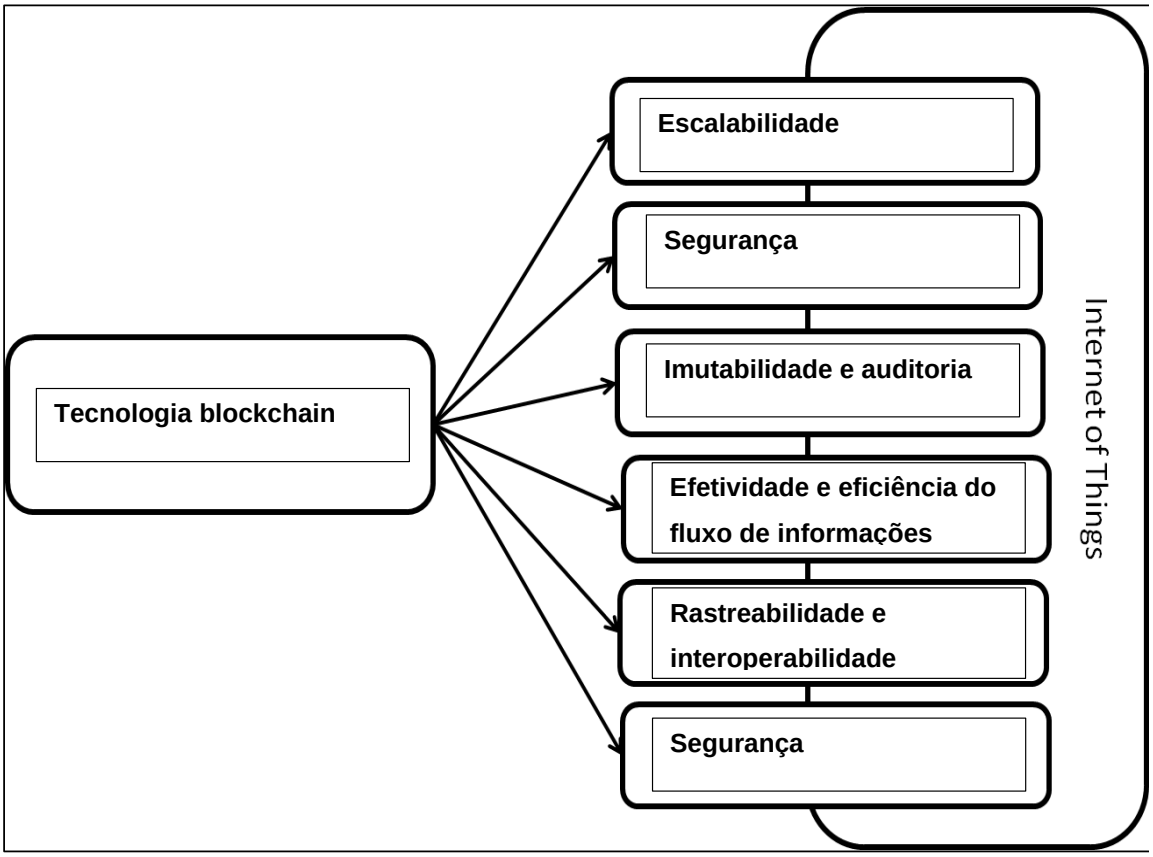

Figura 17
O impacto da tecnologia *blockchain* nas características de IoT.
Fonte: Rejeb *et al*. (2019). Traduções nossas.

2.4.2 Sistemas de reputação

Callegaro e Hornburg (2011) apregoam que muitos autores fazem um *mix* entre confiança e reputação.

a) Confiança: é uma medida individual de confiança que um agente tem sobre outros agentes. Basicamente, se o agente tem um relação direta de confiança,

ele usa essa medida. Caso o valor não seja confiável, então ele usa a reputação.

b) Reputação: é uma medida social de confiança que um grupo de agentes ou uma sociedade tem sobre agentes ou grupos (social). É um mecanismo para computar a confiança individual – “poderei confiar em agentes com melhor reputação Minha reputação afeta a confiança que os outros têm em mim”. É uma ferramenta social com o objetivo de reduzir a incerteza de interagir com indivíduos de atributos desconhecidos.

Mui, Mohtashemi & Halberstadt (2002 como citado em Callegaro & Hornburg, 2011) definem reputação como a percepção criada pelos agentes sobre ações passadas, sobre suas intenções e normas e em relação às expectativas dos outros agentes. Desse modo, é possível compreender que a reputação é um componente da confiança e isso é representado como um valor numérico que representa a opinião de uma comunidade sobre um indivíduo. Exemplos: Mercado Livre, *eBay*, *Airbnb*, *Booking*.

O sistema de reputação tradicional em uma rede P2P tem muitas desvantagens, como atualização de dados, precisão, grande sistema de arquivos mantido e mudanças dinâmicas na rede (Mohanta *et al*., 2019). As redes também enfrentam ataques como *collusion attack* (ataque de conluio) e *sybil attack* (ataque *sybil*). O sistema de reputação baseado em *blockchain* supera os principais desafios presentes no sistema. Dennis & Owen (2016) discutiram inicialmente os sistemas de reputação atuais e apresentam o primeiro sistema de reputação generalizado que pode ser aplicado a várias redes e que é baseado na *blockchain*.

As contribuições feitas por Yasin & Liu (2016) indicam que é uma estrutura sistemática para agregar identidade *online* e informações de reputação, para fornecer uma abordagem holística para avaliações comportamentais *online* pessoais. As principais contribuições incluem: um mecanismo de agregação de identidade baseado em rede de dependência social, uma estrutura de gerenciamento de contrato inteligente referindo-se a avaliações pessoais *online* com base na identidade digital agregada e uma implementação experimental baseada na tecnologia *blockchain*, com exemplos ilustrativos e avaliações teóricas para a abordagem.

De acordo com Nãsulea & Mic (2018), a identidade digital criada por meio de um protocolo *blockchain* já está disponível e pode ser usada como assinatura eletrônica. O exemplo mais notável agora é o programa *Estonian e-Residency* (*Republic of Estonia e-Residency*, 2017), que permite aos usuários criar uma identidade digital que pode ser usada para abrir uma empresa na Estônia até por cidadãos de fora da União Europeia. Combinar identidades digitais com ativos inteligentes significa que se podem autorizar coisas que se possui, que estão registradas na bloc*k*chain, para iniciar transações no próprio nome. Ativos inteligentes que não possuem inteligência artificial (IA), mas estão registrados na *blockchain*, ainda apresentam benefícios, pois a propriedade sobre esses ativos é fácil de identificar usando *blockchain*.

2.4.3 Integração blockchain com smart cities

Smart city é considerado um sistema que conecta grupos de dispositivos que produzem e compartilham grande quantidade de informações. Por causa dessa grande quantidade de dados que trafegam entre os dispositivos deve haver uma estrutura organizacional para organizar e gerenciar esse movimento. As características básicas desse sistema são transparência, descentralização, autonomia e imutabilidade. Todas essas propriedades podem ser fornecidas pela tecnologia *blockchain* (Melhem, AlZoubi, Yassein & Mardini, 2019).

Conforme Nãsulea & Mic (2018), a *blockchain* permite que relacionamentos entre indivíduos funcionem de maneira distribuída, sem a necessidade de um coordenador ou planejador central. Existem três unidades principais dentro do modelo de uma cidade inteligente baseada em *blockchain* que interagem entre si por meio de processos que moldam o *design* operacional do sistema: a cidade inteligente, a comunidade inteligente e o indivíduo. Na camada individual, as implementações de *blockchain*, como identidades digitais ou ativos inteligentes, aprimoram e melhoram as vidas dos “ecidadadões” da cidade inteligente. Os sistemas de suporte de votação, decisão e negociação baseados em contratos inteligentes e *blockchain* aprimoram e otimizam a operação da comunidade inteligente.

Por fim, a própria cidade inteligente colhe os benefícios de mais eficiência de interações automatizadas com seus “ecidadadões” e distribuição otimizada de ativos inteligentes. Um modelo é apresentado na Figura 18 sobre uma *blockchain* no centro de *smart cities* e comunidades inteligentes.

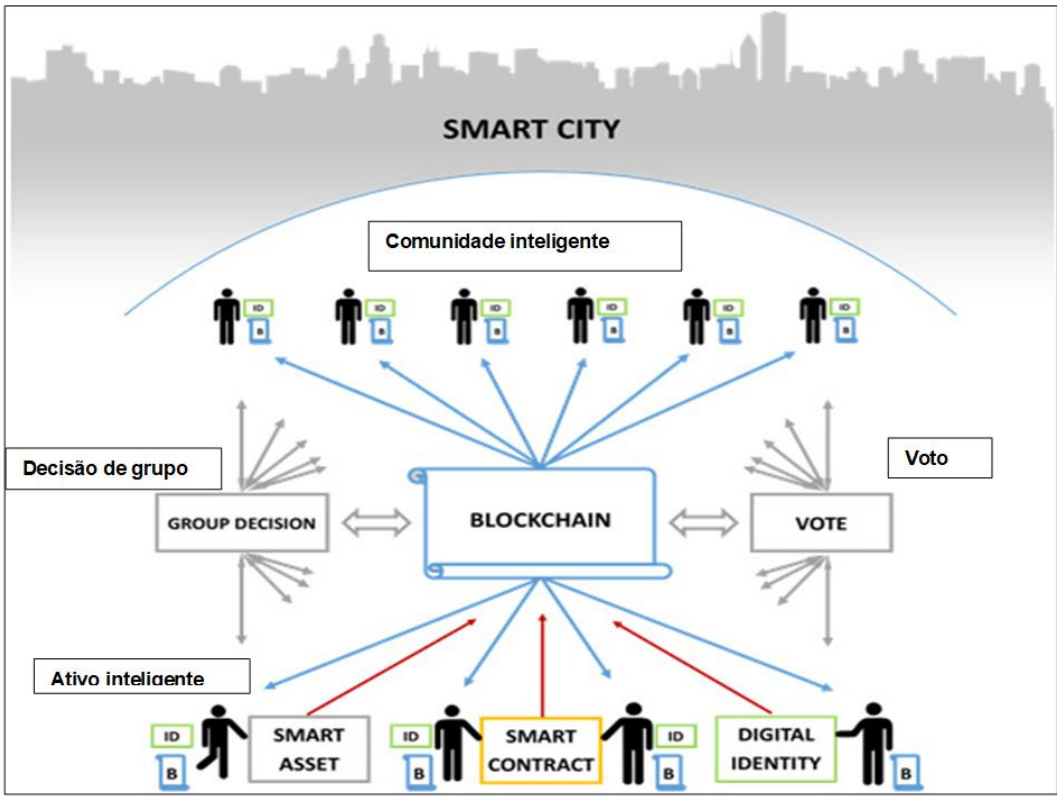

Figura 18
Blockchain no centro de *smart cities* e comunidades inteligentes.
Fonte: Nãsulea & Mic (2018).

O livro-razão da *blockchain* está no centro do modelo aprimorado de *smart city e smart community*. O acesso ao livro-razão é compartilhado por todos os membros da comunidade, sendo que cada um possui sua própria cópia sincronizada do livro-razão compartilhado (azul). Cada membro da comunidade possui uma identidade digital que é usada para autenticar o indivíduo em transações que envolvem o livro razão compartilhado (verde). A criação de uma nova identidade digital, contrato inteligente ou ativo inteligente é registrada no livro razão da *blockchain* (vermelho). Ativos inteligentes e decisões de grupo são tratados usando o livro razão *blockchain* (cinza).

Embora a tecnologia *blockchain* possa ser usada como uma solução de estrutura para

ampla variedade de problemas enfrentados por uma cidade inteligente, o grau em que ela é usada na prática dependerá das preferências da comunidade e da administração da cidade. Algumas cidades podem, com o tempo, transferir o controle da maioria das funções para novas tecnologias inteligentes automatizadas, enquanto outras optarão por manter o controle e confiar em soluções tradicionais de gestão de cidades. Seja qual for a escolha, é importante garantir que amplo espectro de opções esteja disponível para as cidades. A desregulamentação e a transferência de poderes da administração regional para a local são essenciais para esse fim. Há muito pouco sentido em discutir o benefício de contratos inteligentes ou sistemas de votação baseados em *blockchain* se a legislação nacional determina que os contratos só são juridicamente vinculativos se forem assinados por um Cartório de Notas ou se a lei eleitoral exigir que os cidadãos coloquem um carimbo no papel em todos os tipos de eleições (Nãsulea & Mic (2018).

2.4.3.1 Registro imobiliário seguro

Shrivas (2019) assegura que o *Lantmäteriet* (cartório) sueco testou com sucesso uma plataforma *blockchain* para registro de terras com a ajuda de SBAB Stockholm *Bank* (SBAB), *Telia Company*, *Landshypotek Bank*, *Kairos Future* e *ChromaWay*. A *Lantmäteriet* produz bancos de dados geográficos e mapas e é encarregada de ajudar a garantir a segurança e a confiança no registro notarial das propriedades e no uso sustentável de longo prazo de terras (imóveis) e águas da Suécia. *Lantmäteriet* tem cerca de 2.000 funcionários em 60 cidades. Sua sede fica em Gävle.

O Sistema de Registro de Imóveis, conforme a Figura 19, armazena notas de compra/venda e contratos, assinaturas de partes, seus documentos de identidade e informações de propriedade em *blockchain*. A edição de registros é permitida apenas por meio da interface administrativa, mas registra todas as transações na *blockchain*, que pode ser visualizado por todos os interessados como compradores, vendedores, agentes, bancos, inclusive públicos (Kempe, 2016). O governo de Gana e a IBM assinaram um Memorando de Entendimento (MoU) para desenvolver a plataforma baseada em *blockchain*. Governo estadual indiano, Andhra Pradesh, também testou

o registro de terras e registrou 100.000 registros de terras em *blockchain* (Haridas 2018 como citado em Shrivas, 2019).

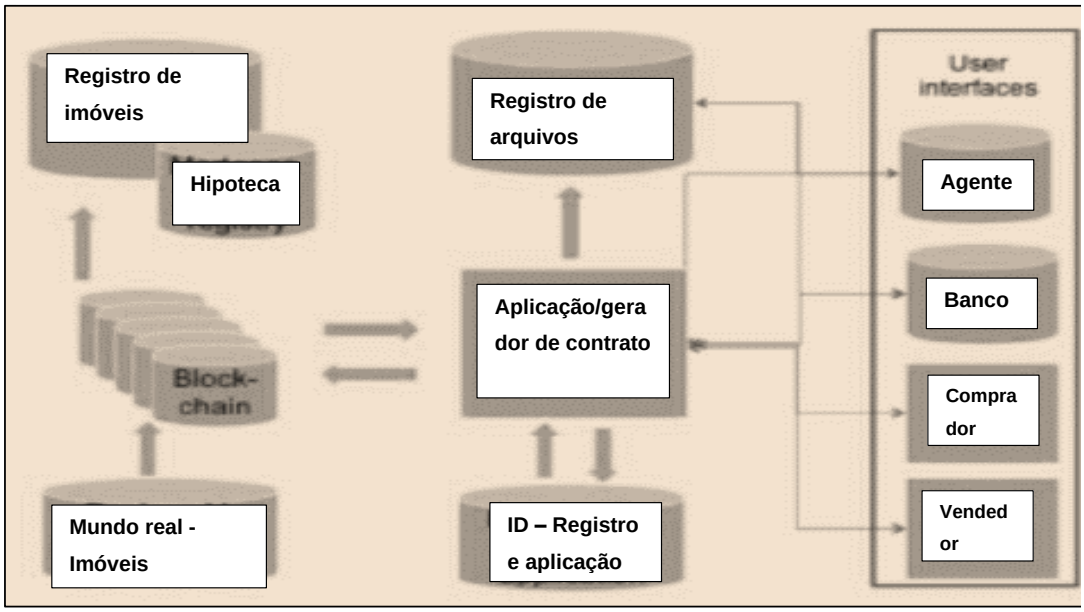

Figura 19
Esquema de registro de imóveis
Fonte: Shrivs (2019). Tradução nossa.

2.4.3.2 Eleições seguras

Xie, Tang, Huang, Yu, Xie, Liu & Liu (2019a) documentam que a tecnologia *blockchain* melhora significativamente as cidades inteligentes. A seguir, é usado um sistema geral de votação eletrônica baseado em *blockchain*, indicando com um caso de uso para mostrar como a tecnologia *blockchain* pode ser usada para promover a implementação de uma cidade inteligente confiável, segura, transparente e democratizada. Conforme se vê na Figura 20, um sistema de votação eletrônica baseado em *blockchain* geralmente consiste em cinco etapas distintas, incluindo a criação da eleição, registro de eleitor, transação de voto, contagem de votos e verificação de votos:

a) Criação de eleições - o administrador eleitoral que gerencia o ciclo de vida de uma eleição cria-a usando um aplicativo descentralizado de administração (DApp). O administrador eleitoral especifica o tipo de eleição, define as políticas eleitorais, define uma lista de candidatos e decide a duração da eleição. Em

seguida, o administrador DApp cria um contrato inteligente de eleição e o implanta na *blockchain*.

b) Registro de eleitor - quando uma eleição é criada, o administrador da eleição deve determinar uma lista de eleitores elegíveis. Usando um componente de verificação de identidade do governo, o administrador eleitoral pode autenticar e autorizar eleitores qualificados. Se um cidadão for um eleitor elegível, ele recebe uma chave digital segura. E então uma carteira correspondente é gerada para o eleitor elegível. A carteira é única para cada eleitor e pode ser usada para votar.

c) Transação de voto - quando um eleitor seleciona um candidato e dá seu voto, a seguir o eleitor assina a transação usando a chave digital segura. Depois que os dados do voto são assinados, a carteira do eleitor irá interagir com o contrato inteligente da eleição. O contrato inteligente processa apenas votos legais, o que significa que se o eleitor é elegível e não votou antes, o voto é lançado durante o período eleitoral. Se a votação for legal, o contrato inteligente transmitirá os dados do voto como uma transação para todos os nós da *blockchain*. Se a maioria dos nós da *blockchain* concordar com os dados da votação, é alcançado consenso para a votação específica. Em seguida, a transação que contém os dados do voto é anexada à *blockchain* permanentemente e o ID da transação é enviado ao eleitor correspondente.

d) Cálculo dos votos - a contagem da eleição é feita automaticamente pelo contrato inteligente de eleição de acordo com as transações de voto que são armazenadas na *blockchain*. Terminada a eleição, o resultado final é publicado.

e) Verificação de voto - como mencionado anteriormente, cada eleitor elegível recebe o ID da transação de seus dados de voto. O ID da transação pode ser usado pelos eleitores para acessar a *blockchain* e localizar a transação correspondente. Os eleitores podem, portanto, ver seus dados de voto, verificar a validade do processo de contagem eleitoral e confirmar a exatidão dos resultados eleitorais.

A partir da descrição detalhada de um sistema de votação eletrônica baseado em *blockchain* geral, concluiu-se que a tecnologia *blockchain* pode ser usada para criar um sistema de votação seguro, transparente, rastreável, verificável e democrático. Em

primeiro lugar, o sistema descentralizado torna o processo de votação menos vulnerável à manipulação e ataque, e só permite que indivíduos elegíveis votem em uma eleição. Em segundo lugar, todas as transações de voto armazenadas na *blockchain* são públicas para todos os eleitores, tornando o processo de votação transparente, rastreável e verificável. Terceiro, as transações de voto armazenadas na *blockchain* são acordadas por todos os nós da *blockchain,* usando algoritmos de consenso.

O contrato eleitoral inteligente permite que o armazenamento de dados de votos, a apuração de uma eleição e a determinação de um resultado eleitoral sejam feitos automaticamente. Assim, nenhuma entidade pode controlar o processo de votação e manipular os dados do voto, o que torna o processo de votação mais democrático. Embora o caso de uso se concentre no sistema de votação eletrônica, situações semelhantes baseadas em *blockchain* podem ser derivadas para outros aspectos em cidades inteligentes, como transporte, educação, saúde, etc. (Xie *et al*., 2019a).

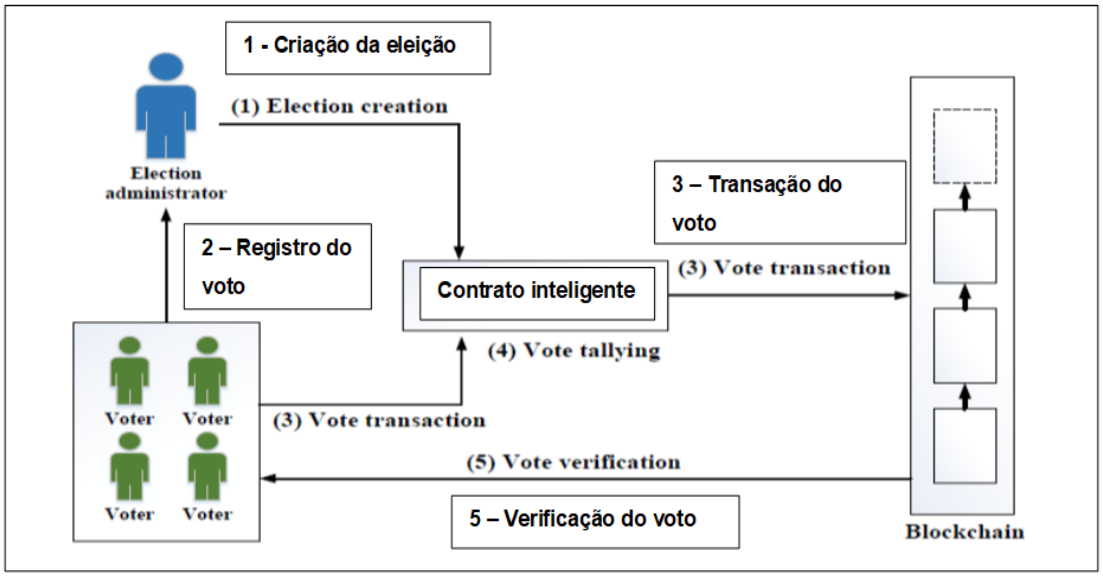

Figura 20.
Votação segura com *blockchain.*
Fonte: Xie, Tang, Huang, Yu, Xie, Liu & Liu (2019b). Tradução nossa.

2.4.3.3 Gerenciamento e carregamento de veículos elétricos

Xie *et al*. (2019b) afirmam que, atualmente, a fim de desenvolver sistemas de transporte “verdes”, os veículos elétricos têm atraído atenção generalizada e têm sido implantados em muitos países. Para garantir a condução diária de veículos elétricos, estações de carregamento e a infraestrutura de carregamento estão sendo amplamente implantadas, especialmente em áreas urbanas. Em geral, após o processo de carregamento de uma estação de carregamento, o veículo elétrico precisa pagar à estação de carregamento certa quantia. *Blockchain* e *smart contracts* podem ser usados para facilitar e agilizar o comércio de eletricidade entre veículos elétricos e estações de recarga.

Knirsch *et al*. (2017 como citado em Xie *et al*., 2019a) sugerem um protocolo de quatro estágios para permitir que veículos elétricos carreguem a partir das estações elétricas de carregamento. Conforme mostrado na Figura 21, as quatro etapas são: exploração, licitação, avaliação e cobrança.

O trabalho de Kang *et al*. (2017 como citado em Xie *et al*., 2019a) descreve um sistema de comércio de eletricidade P2P baseado em *blockchain* chamado PETCON, para melhorar o comércio de eletricidade entre veículos elétricos híbridos *plug-in* (PHEVs). As informações da transação de eletricidade são registradas em um razão (livro) compartilhado. Uma abordagem iterativa de leilão duplo é apresentada para otimizar os preços da eletricidade e a quantidade de eletricidade comercializada entre os PHEVs, com o objetivo de maximizar o bem-estar social.

Huang, Xu, Wang & Liu (2018) propõem um modelo de negociação baseado em *blockchain* denominado LNSC, que inclui as fases de registro, programação, autenticação e cobrança. As informações de transação entre veículos elétricos e estações de carregamento são armazenadas na *blockchain*. Contratos inteligentes são usados para permitir um processo de negociação automático.

A Figura 21 traz um protocolo de carregamento de veículos elétricos baseado em *blockchain*. Na fase de exploração, um veículo elétrico envia uma solicitação à

blockchain, que contém parâmetros como a quantidade de energia, o intervalo de tempo e a região geográfica. Em seguida, as estações de carregamento próximas enviam lances para essa solicitação na fase de licitação. Na fase de avaliação, uma estação de carregamento ideal é selecionada pelo veículo elétrico. Na fase de carregamento, a transação acordada é executada pela estação de carregamento selecionada para fornecer a quantidade de energia por determinado preço durante definido período (Xie *et al*., 2019b).

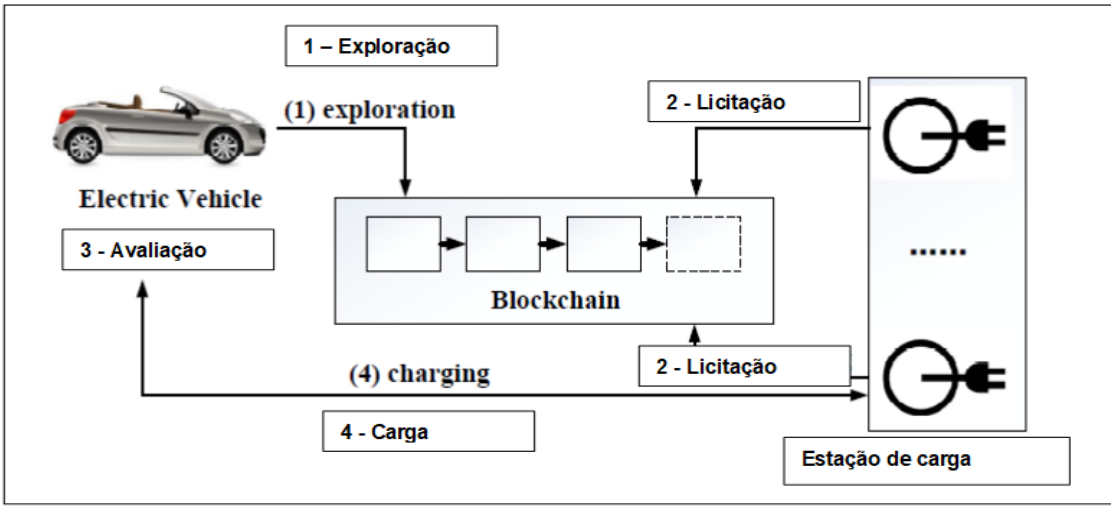

Figura 21
Protocolo para gerenciamento e carregamento de veículos elétricos.
Fonte: Xie et al. (2019b). Tradução nossa.

2.4.3.4 DDoS *attacks*

De acordo com Gupta (2018), um ataque DDoS é uma tentativa maliciosa de interromper o tráfego legítimo para um servidor, sobrecarregando o alvo com uma enxurrada de solicitações de sistemas geograficamente dispersos, conseguindo-se, assim, deixá-lo fora de alcance na internet. Tem-se primeiro que entender como funciona um ataque de negação de serviço (DoS). Durante os ataques DDoS, os invasores bombardeiam a máquina-alvo com grande quantidade de solicitações que levam ao esgotamento dos recursos do servidor e, como resultado, falha nas solicitações de usuários legítimos. Em um ataque DoS, um agente de ameaça usa uma única máquina para esgotar o servidor de destino; no entanto, um ataque DDoS

é muito mais poderoso, pois milhões de máquinas podem ser usadas para exaurir e derrubar um servidor de destino na rede.

O referenciado autor diz que nos últimos anos tem-se observado aumento nesses tipos de ataques. Conforme relatório da *Radware*, 43% das organizações sofreram ataques desse tipo, mas o restante nem sabia se foram atacadas. Os invasores estão adaptando várias técnicas emergentes e táticas complexas para comprometer a rede-alvo.

Em 28 de fevereiro de 2018, o GitHub, o *site* de hospedagem de código, foi atingido com o maior ataque DDoS de todos os tempos, registrado a 1,35 *terabits* por segundo (Tbps). Como os ataques DDoS se enquadram na categoria de ameaças cibernéticas, isso torna inviável a implantação de qualquer mecanismo de prevenção de segurança, visto que as vulnerabilidades do sistema estão sob o controle das organizações, mas as ameaças não podem ser controladas. O *front-end* do aplicativo da *web* permanece centralizado para todos os usuários; portanto, deixa um único ponto de falha para as organizações, que podem ser órgãos de governo de qualquer nível, bem como em *smart cities*.
Por definição, *blockchain* é uma rede descentralizada que permite que partes independentes se comuniquem sem qualquer envolvimento de terceiros. Para proteger as redes de ataques DDoS, as organizações podem distribuir seus sistemas entre vários nós de servidores que fornecem alta resiliência e removem o ponto único de falha. Existem duas vantagens principais em usar a *blockchain*: a tecnologia *blockchain* pode ser usada para implantar um livro-razão descentralizado para armazenar IPs na lista negra. A tecnologia *blockchain* elimina o risco de um único ponto de falha (Gupta, 2018).

O referido autor segue dizendo que para implantar a plataforma de proteção DDoS baseada em *blockchain* como exemplo real, é necessário preparar o ambiente de teste com *Node.js* e *Truffle* com *blockchain Ethereum*. Nesse ponto, Gupta (2018) demonstra a implementação da técnica usando um projeto existente de *blockchain* para defender uma rede de um ataque DDoS. O *link* do projeto pode ser encontrado em https://github.com/gladiusio/gladius-contracts.

Como a implementação de técnicas foge ao escopo desta pesquisa, entende-se que esse assunto poderá ser tratado em futuras pesquisas complementares.

2.4.3.5 Auditagem

A tecnologia de *blockchain* pode também ser usada quando há necessidade de conformidade das atividades das empresas/órgãos com os regulamentos, pois garante uma trilha de auditoria, ou seja: *compliance*. A *blockchain* pode ser usada como base para a verificação das transações realizadas. Exemplo: em vez de pedir extratos bancários aos clientes ou enviar solicitações de confirmação a terceiros, os auditores podem verificar facilmente as transações em livros de *blockchain* disponíveis publicamente. A automação desse processo de verificação irá impulsionar a eficiência de custos e a celeridade no ambiente de auditoria. O que distingue o uso da *blockchain* de outras formas de carimbo de data/hora e autenticação de dados é que os documentos e outros conjuntos de dados na *blockchain* são provas descentralizadas. É garantir que os dados não possam ser apagados ou modificados por alguém, nem por sua própria empresa nem por concorrentes, terceiros ou governos (Findlay, 2015 como citado em Abreu, Aparício & Costa, 2018).

De acordo com um estudo de Gao & Srivastava (2012 como citado em Abreu *et al*., 2018), documentos/informações ocultas, documentos alterados, documentos falsos e conluio com terceiros totalizam 81% dos esquemas de evidências, por meio dos quais a gestão cria ou oculta evidências para perpetrar a fraude. O reconhecimento prematuro de receitas, receitas fictícias, ativos supervalorizados e despesas subestimadas, despesas/passivos omitidos ou subestimados totalizam 78% dos esquemas de contas, por meio dos quais a administração comete fraude ao manipular saldos de contas ou divulgações. Ter um sistema de *blockchain* em que os contadores devem inserir as demonstrações financeiras das empresas em um livro-razão seguro e resistente a modificações, que possa ser usado em tempo real tem considerável impacto positivo na redução desse tipo de fraude e corrupção em geral.

Outra abordagem diferente, mas também importante, é que os algoritmos embutidos nos *softwares* determinam se as regras são atendidas e as transações estão corretas. Esses “algoritmos se tornam cada vez mais autônomos e invisíveis, tornam-se mais difíceis para o público detectar e examinar seu *status* de imparcialidade” (Janssen & Kuk, 2016, p. 371 como citado em Ølnes, Ubacht & Janssen, 2017).

Portanto, é necessário armazenar e auditar os algoritmos da *blockchain*. O código-fonte aberto, do *software* está sempre aberto ao público. Embora os proponentes argumentem que disponibilizar o código-fonte permite ao público revisar o código e melhorar a qualidade, isso é questionável, pois ambos os lados podem estar certos, dependendo das circunstâncias (Ven, Verelst & Mannaert, 2008 como citado em Ølnes *et al.*, 2017).

2.5 Desvantagens, limitações e ameaças a *blockchains*

Niranjanamurthy, Nithya & Jagannatha (2019) citam que a *blockchain* tem algumas desvantagens ou limitações se comparada às tecnologias convencionais, por exemplo:

a) Primeiramente, cita-se o desempenho: devido à natureza das *blockchains*, elas sempre serão mais lentas do que bancos de dados centralizados. Numa transação, uma *blockchain* precisa fazer todas as mesmas coisas similarmente ao banco de dados normal, mas também carrega três cargas adicionais:
   - Verificação de assinatura: toda transação *blockchain* deve ser assinada digitalmente usando-se um esquema de criptografia público-privado. Isso é necessário porque as transações se propagam entre os nós de forma ponto a ponto, portanto, sua origem não pode ser provada de outra forma. A geração e verificação dessas assinaturas são computacionalmente complexas e constituem o principal gargalo;
   - mecanismos de consenso em um banco de dados distribuído como *blockchain*: um esforço deve ser despendido para garantir que os nós na rede alcancem consenso. Dependendo do mecanismo de consenso usado,

isso pode envolver uma comunicação significativa de ida e volta e/ou lidar com bifurcações e suas reversões consequentes;

- redundância: não é sobre o desempenho de um nó individual, mas a quantidade total de computação que uma *blockchain* requer. Enquanto os bancos de dados centralizados processam as transações uma ou duas vezes, em uma *blockchain* elas devem ser processadas independentemente por cada nó da rede. Logo, muito mais trabalho está sendo feito para o mesmo resultado final.

b) Tecnologia nascente: resolver desafios como velocidade de transação, processo de verificação e limites de dados será crucial para tornar a *blockchain* amplamente aplicável.
c) Grande consumo de energia: os mineradores da rede Bitcoin *blockchain* estão tentando 450 mil trilhões de soluções por segundo em esforços para validar transações, usando quantidades substanciais de poder de computador.
d) Controle, segurança e privacidade: enquanto existem soluções, incluindo *blockchain* privada ou permitida e criptografia forte, ainda existem questões de segurança cibernética que precisam ser abordadas antes que o público em geral confie seus dados pessoais a uma solução *blockchain*.
e) Questões de integração: os aplicativos *blockchain* oferecem soluções que requerem mudanças significativas ou substituições completas dos sistemas existentes. Para fazer a troca, as empresas devem criar estratégias para a transição.
f) Adoção cultural *blockchain* representa uma mudança completa para uma rede descentralizada que requer a adesão de seus usuários e operadores.
g) *Blockchain* oferece representativa economia em custos de transação e tempo, mas o alto custo de capital inicial pode ser um fator limitante.

Já Reyna *et al*. (2018) citam outro fator limitante importante: capacidade de armazenamento e escalabilidade. Esses quesitos têm sido profundamente questionados na *blockchain*. Nessa tecnologia, a cadeia está sempre crescendo, à taxa de 1 MB por bloco a cada 10 minutos em Bitcoin, e há cópias armazenadas entre os nós da rede. Embora apenas nós completos (um nó que pode validar totalmente transações e blocos) armazenem a cadeia completa, os requisitos de armazenamento

são significativos. Conforme o tamanho aumenta, os nós exigem mais e mais recursos, reduzindo assim a escala de capacidade do sistema. Além disso, uma cadeia superdimensionada tem efeitos negativos no desempenho, por exemplo, aumenta o tempo de sincronização para novos usuários.

Ainda no entendimento de Reyna *et al*. (2018), o ataque mais importante é o de 51% ou majoritário. Ess ataque pode ocorrer se um participante do *blockchain* for capaz de controlar mais de 51% do poder de mineração. Nessa situação, ele pode controlar o consenso na rede. O *boom* e a rápida evolução dos *pools* de mineração aumentaram a probabilidade de esse ataque acontecer, o que, por sua vez, pode comprometer a integridade de uma rede *blockchain*. Além disso, autores como Zhu, Gai & Li (2019) e Narayanan, Bonneau, Felter, Miller & Goldfeder (2016 como citado em Reyna *et al*. (2018) discutem a possibilidade de atingir a maioria do poder de mineração por meio de suborno. O incentivo de mineração solo ou mineração P2P ajuda a aliviar esse problema.

Taxa de transferência e latência são outras limitações exploradas por Cui *et al*. (2019). A velocidade de geração de blocos e processamento de transações do *blockchain* aumenta a latência e limita a taxa de transferência de um sistema que usa *blockchain*. Esse problema se torna mais grave para o esquema de IoT, pois o sistema *blockchain* leva tempo para chegar a consenso, mesmo para uma pequena infraestrutura de IoT com taxa de transação limitada. O sistema precisa de certo tempo para anexar os novos dados à *blockchain*, e essa latência mínima não pode ser eliminada.

2.5.1 Soluções para smart cities baseadas em blocos pós-quânticos

Os computadores quânticos vêm sendo desenvolvidos rapidamente. O *Google* conseguiu criar um computador com a dita supremacia quântica, chamado "*Sycamore*". O computador usa 53 *qubits* (unidade básica de informação) e foi capaz de resolver em 200 segundos um cálculo complexo que levaria 10.000 anos para ser concluído usando os supercomputadores mais poderosos da atualidade. O *Google* não está sozinho na corrida *quantum*. A IBM abriu a "IBM Q *Network*", que é uma comunidade global de empresas, instituições acadêmicas, *startups* e laboratórios de

pesquisa que trabalham juntos para melhorar e avançar a computação quântica. *Apple*, Intel, *Microsoft*, *Amazon* e muitas outras empresas de tecnologia se juntaram à competição para desenvolver o futuro dos computadores. Esses computadores certamente são capazes de computar os algoritmos mencionados em tempo exponencial, o que ameaça a segurança de quase todos os algoritmos de criptografia, incluindo aqueles nas quais as seguranças de *blockchain* são baseadas. Assim, medidas de segurança devem ser tomadas antes que as ameaças se tornem realidade. Azzaoui & Park (2020) apresentam alguns dos algoritmos e métodos recém-desenvolvidos que foram comprovados com base nos trabalhos relacionados relevantes, como propensos a conter ataques quânticos em *blockchain*:

2.5.1.1 *Lattice-based Cryptography*

Lattice-based cryptography: criptografia baseada em rede foi adotada em inúmeras pesquisas, pois se acredita ser protegido contra computadores quânticos. Normalmente, ele pode ser usado para proteger a *blockchain* contra os ataques quânticos que podem quebrar curvas elípticas criptográficas. Torres *et al*. (como citado em Azzaoui & Park, 2020) propuseram um esquema baseado em rede com uma assinatura de anel vinculável única. Esse esquema proposto permite ao público verificar se duas ou mais assinaturas foram geradas pelo mesmo signatário, garantindo o anonimato e segurança usando o número inteiro curto suposição de dureza/dificuldade de rede de solução.

A proposta concebe também um novo protocolo de preservação de privacidade de criptomoeda chamado *Lattice RingCT* v1.0 usando o *post-quantum* como base para a construção de blocos junto com o compromisso homomórfico primitivo para garantir as transações confidenciais seguras do *post-quantum*. Gao *et al*. (como citado em Azzaoui & Park, 2020) propuseram um esquema de assinatura com base no problema de rede também e usaram o algoritmo de delegação baseado em rede para gerar chaves secretas selecionando um valor aleatório. A mensagem é assinada pelo algoritmo de amostragem de pré-imagem. Além disso, para reduzir a correlação entre a mensagem e a assinatura, um assinatura dupla foi adotada usando o primeiro e o último *design* de assinatura. Aplicando esse esquema de assinatura em *blockchain*

cria-se um *post quantum blockchain* (PQB). A análise feita mostra que o esquema da criptomoeda/*blockchain* proposta é capaz de resistir a ataques de computação quântica.

Enquanto os métodos de criptografia tradicionais baseiam-se na álgebra, a criptografia em rede utiliza a dimensão geométrica - indo em dimensões diferentes em muitas direções diversas. O resultado é um sistema muito mais difícil de "*crackear*", que oferece mais segurança a todos (Micciancio & Ristenpart, 2020).

2.5.1.2 Chave distribuída quântica

Outra abordagem para encontrar uma solução sujeita a ataques *quantum* é usar uma *quantum distributed key* (QDK). A QDK geralmente usa fótons individuais para trocar dados de chaves criptográficas entre os usuários. Cada fóton representa um único *bit* de dados, que pode ser um ou zero. Com base na teoria da Física Quântica, o valor de cada *bit* é determinado com base no estado do fóton (o *spin* e a polarização). É necessário gerar uma série de fótons únicos. O fóton deve estar em estado de polarização, horizontal ou vertical, e esse estado será medido novamente na extremidade receptora. Esse método é considerado altamente seguro, pois se um bisbilhoteiro tentar medir o estado de um único fóton, o fóton será destruído. Além disso, um invasor nunca pode gerar o mesmo fóton novamente com a mesma polarização e o mesmo *spin*. Assim, o receptor notará um erro na série de fótons recebidos. A QDK está por trás do princípio da incerteza de Heisenberg, que afirma que é impossível medir a velocidade e a posição de certas partículas quânticas ao mesmo tempo.

A QDK garante a segurança teórica e incondicional da informação com base nas leis da Física Quântica. Numerosas pesquisas e trabalhos implantaram essa técnica para proteger a rede *blockchain*. Kiktenko *et al*. (como citado em Azzaoui & Park, 2020) também usaram QDK para gerar uma chave secreta entre duas partes conectadas por um canal *quantum* para transmitir o estado *quantum* e um canal clássico público para procedimentos de pós-processamento. O documento fundiu a camada de rede QKD no sistema *blockchain* atual para proteger o subalgoritmo relevante contra

ataques quânticos. Consequentemente, a tecnologia que habilita as redes QDK foi demonstrada em experimentos e agora está disponível por intermédio de fornecedores comerciais. As aplicações potenciais da QDK incluem a segurança de infraestruturas críticas, como redes inteligentes, financeiras, instituições e defesa nacional. No entanto, a QDK pode não ser viável para proteger um sistema de criptomoeda em grande escala, pois consome mais poder de computação para o procedimento de criação do bloco, mas ainda pode ser muito útil para proteger um banco de dados distribuído de menor escala (Azzaoui & Park, 2020).

2.5.1.3 Emaranhamento quântico no tempo

O termo emaranhamento foi usado na mecânica quântica após o famoso artigo publicado por Einstein, Podolsky e Rosen em 1935. Eles afirmam que em sistemas quânticos separados espacialmente havia uma "ação fantasmagórica à distância", como Einstein *et al.* a descreveram. Essa ação assustadora envolve correlações não clássicas. Rajan *et al*. (como citado em Azzaoui & Park (2020) implantaram essa ramificação para criar uma *quantum blockchain*. Esse método é baseado na codificação de *blockchain* em um estado temporal de fótons de Greenberger-Horne-Zeilinger (GHZ) que não pode coincidir ao mesmo tempo. Os autores substituíram os componentes de uma *blockchain* clássica por um sistema quântico, no qual usaram um conceito de codificação superdenso para usar a *blockchain* quântica e converter as informações clássicas em estados de Bell espacialmente emaranhados (que são estados quânticos específicos de dois *qubits* que representam os exemplos mais simples - e máximos - de emaranhamento quântico).

O entrelaçamento baseado em *blockchain quantum* no tempo é uma solução forte para proteger cidades inteligentes baseadas em *blockchain*. Implementando esse método, os registros ainda existem e podem ser lidos, mas eles não podem ser tocados porque os fótons que os contêm não existem mais. E isso garantirá a integridade e confidencialidade das *smart cities* baseadas em *blockchain* (Azzaoui & Park, 2020).

Nessa linha existem diversas implementações, como, por exemplo, a qTESLA, que é uma família de esquemas de assinaturas pós-quânticas comprovadamente segura

com base na dureza/dificuldade do problema de aprendizagem com erros de anel de decisão. O esquema é uma variante eficiente do esquema de assinatura de Bai-Galbraith, que por sua vez é baseado na estrutura “Fiat-Shamir com abortos” de Lyubashevsky (Zhang, Wang, Wang, Fu & Wang, 2021).

Nesse sentido, sugere-se incluir essa matéria, também, em futuros estudos.

3 Procedimentos Metodológicos

Nesta pesquisa, o foco foi a natureza dos assuntos trabalhados, como *blockchain* e segurança da informação em *smart cities.* E para abordar o escopo desta investigação foi necessário realizar uma pesquisa tridimensional. Daí surgiu o ambiente de estudo para segurança da informação em *smart cities,* resultado da relação de três dimensões interdependentes: *blockchain*, internet da coisas (IoT) e *smart cities.* Estas últimas ainda se relacionam a outras tecnologias, ferramentas e *add-nos*.

A dimensão tecnológica exigiu a aquisição de conhecimentos para entender como o fenômeno ocorre na prática, bem como suas implicações nesse ambiente de TIC. Foi feita, então, uma prospecção de estudos para se atingirem os objetivos propostos.

A conjunção dessas três dimensões atuando em um ambiente de TIC constituiu um *corpus* teórico e conceitual que permitiu apurar qual o relacionamento do nível de segurança da informação nessas estruturas baseadas em *blockchain*.

Revisão sistemática, segundo Kitchenham & Charters (2007) é interpretada, como uma revisão sistemática de literatura que é uma forma de estudo secundário e utiliza uma metodologia bem definida para identificar, analisar e interpretar todas as evidências disponíveis a respeito de uma questão de pesquisa particular de maneira imparcial e repetível.

Ainda segundo Kitchenham & Charters, sua metodologia basicamente se divide em três etapas: planejamento da revisão, condução da revisão e relato.

Como defendem Dewan & Singh (2020), existem muitos tipos de pesquisa científica na literatura. Esse número de tipos de pesquisas decorre do fato de existirem diferentes abordagens e métodos de pesquisas que podem ser usados para conduzir esses estudos. Em outras palavras, há muitas metodologias diferentes que podem ser usadas para abordar as questões com as quais os pesquisadores precisam trabalhar. É possível para os pesquisadores usar qualquer um dos diferentes tipos ou formatos de pesquisa existentes.

A seguir, Dewan & Singh (2020) apresentam breve descrição de algumas das formas comuns de pesquisas que estudantes e pesquisadores têm à mão para escolher. As formas mais comuns de pesquisa são as quantitativas e as qualitativas. Existe uma diferença muito clara entre elas, no entanto, ambas são relacionadas entre si, pois sempre que um pesquisador realiza uma pesquisa, ele tem que escolher um dos dois tipos, sendo que, em pesquisa, os estudos/fenômenos contêm aspectos que os tornam qualitativos ou quantitativos.

Em muitos casos, porém, os pesquisadores podem optar por incorporar os dois elementos das duas formas de pesquisa. A necessidade de incluir os aspectos das duas formas de pesquisa pode surgir da natureza complexa do estudo que está sendo trabalhado. Assim, é sempre deixado para o pesquisador decidir se deve incluir os critérios qualitativo ou quantitativo ou ambos, dependendo da natureza do fenômeno e do enfoque a ser estudado. Desnecessário será dizer que a essência da pesquisa quantitativa é que o pesquisador deliberadamente concentra-se na medição de conteúdo de natureza quantitativa. O pesquisador que optar pelo estudo quantitativo deve ter certeza de que os problemas que ele está examinando podem ser medidos com precisão de maneira discreta. Por outro lado, prossegue o autor, a pesquisa qualitativa é definida pela maneira como está focada na avaliação de um fenômeno usando métodos específicos.

A segunda categoria de pesquisa inclui estudos empíricos e conceituais como forma de investigação. É geralmente conduzida de forma que o pesquisador considere os vários modelos teóricos existentes. Em estudos empíricos, o pesquisador simplesmente busca atingir os objetivos do estudo coletando e medindo dados. O processo de coleta e medição dos dados é normalmente realizado com o objetivo de testar uma hipótese. Por outro lado, pesquisa conceitual é geralmente conduzida para fornecer mais informações sobre uma teoria do conhecimento. Por exemplo, um estudo pode ser realizado para fornecer mais informações sobre uma teoria específica de determinada disciplina. Nesse caso, o pesquisador não está interessado em testar alguma hipótese, mas em fornecer mais informações sobre certa área do conhecimento (Dewan & Singh, 2020).

O terceiro tipo é referido como pesquisa aplicada. Para entender sua essência, é importante considerar o oposto desse tipo, que é chamado de pesquisa fundamental. Pesquisa fundamental ou básica é qualquer estudo realizado com o objetivo de obter conhecimento que é usado para cobrir as lacunas existentes no conhecimento que já existe e que ainda não é completo ou pleno. Em muitas ocasiões, a investigação pode levar conduzir um estudo porque percebeu que falta alguma informação/complementação sobre determinado problema. Já a pesquisa aplicada, por sua vez, usa pesquisas científicas para desenvolver tecnologias ou novas técnicas para intervir/alterar fenômenos em estudo (Dewan & Singh, 2020).

Isso posto, resume-se que a tipologia desta pesquisa ficou classificada como: a) do procedimento técnico, bibliográfica; b) da natureza, básica; c) do objetivo, descritiva; d) da abordagem, qualitativa.

3.1 Planejamento da revisão sistemática da literatura

Etapas foram realizadas na revisão sistemática da literatura segundo metodologia de Kitchenham & Charters (2007). Aqui foi escolhido o processo de pesquisa individual a ser implementado.

(a)	Planejar	1	Identificadas as necessidades da revisão
		2	Especificadas as questões de pesquisa
		3	Desenvolvido um protocolo de revisão
(b)	Conduzir	4	Identificada a pesquisa
		5	Selecionados os estudos primários
		6	Avaliada a qualidade do estudo
		7	Extraídos e monitorados os dados
		8	Sintetizados os dados
(c)	Relato		

3.2 A questão de pesquisa

Com a finalidade de validar a questão de pesquisa, aderiu-se à ferramenta de pesquisa muito usada na área médica, baseada em evidências, *Population, Intervention, Comparison, Outcome, Study type* (PICOS).

O mnemônico PICO foi originalmente empregado para ajudar a guiar uma forma padronizada e disciplinada de formular uma pergunta de pesquisa clínica, realizando pesquisa bibliográfica completa para responder a essa pergunta (particularmente por meio do *Medical Literature Analysis and Retrieval System On-line*/Publicações Médicas (MEDLINE/PubMed) e, como resultado, gerar uma resposta baseada em evidências para a consulta clínica construída (Saaiq & Ashraf, 2017).

Os elementos da pergunta PICO incluíam “P” para problema ou paciente ou população, “I” para intervenção ou exposição, “C” para comparação e “O” para resultados. A pergunta PICO foi recomendada para ser formulada em cadeias de pesquisa apropriadas para descobrir toda a literatura relevante publicada de qualidade disponível no ciberespaço. A estrutura PICO é absolutamente louvável para o propósito para o qual foi originalmente introduzida. Posteriormente, o modelo foi incrementado PICOS para estender ainda mais sua utilidade científica para a descrição lógica e completa da parte metodológica dos manuscritos científicos. A adição defendida de “S” ao mnemônico PICO o modifica para PICOS, garantindo reprodutibilidade e expressão mais robusta do protocolo de estudo seguido em qualquer pesquisa científica particular (Saaiq & Ashraf, 2017).

O conceito crucial de análises em estudos de pesquisa está bem estabelecido, no entanto, muitas vezes os pesquisadores desconhecem seu significado e implicações lógicas. Consequentemente, seus estudos relatados sofrem com a falta de reprodutibilidade e tradução robustas para a população em geral. A abordagem PICOS proposta tem a intenção de servir como um guia para os pesquisadores e ajudá-los a descrever de forma eficiente e completa sua metodologia de pesquisa. Além disso, também servirá como um guia de lista de verificação para que os revisores e editores revisem mais detalhadamente os manuscritos sob sua avaliação e,

portanto, garantam sua validade científica e robustez. Ao assegurar padrões metodológicos uniformes e objetividade, o valor científico geral da literatura publicada certamente aumentará (Saaiq & Ashraf, 2017).

No caso deste estudo ficou:

P: *Population* (população) - em *smart cities*
I : *Intervention* (intervenção) - *blockchain*
C: *Comparison* (comparação) – segurança da informação
O: *Outcome* (resultado) - qualidade
S: *Study type* (tipo de estudo) – qualitativo

Daí surgiu a pergunta a ser investigada: quais técnicas de *blockchain* podem contribuir para aumentar o nível segurança da informação em *smart cities*?

3.3 Desenvolvimento do protocolo de revisão

Foram identificadas as fontes de pesquisa usadas via *Web*:

a) *Scopus* (Elsevier);
b) *Scientific Electronic Library Online* (SciElo);
c) *ScienceDirect*;
d) IEE*EXplore*r;
e) *Association for Computing Machinery* (ACM) *Digital Libray*;
f) outros.

Foram verificados os artigos quanto à sua completude (*completeness*) e criticidade. Uma vez que se está tratando de tecnologia neste trabalho, esse aspecto foi considerado crítico. Dadas, porém, as limitações da pesquisa, a investigação deverá ser maximizada nesse quesito.

Em resumo, foi trabalhado com o seguinte protocolo:

a) Palavras-chave: *smart cities*, cidades inteligentes, internet das coisas, IoT, *blockchain*, segurança da informação.
b) A *string*: *blockchain and* (“*smart cities*” or “*Internet of Things*” or IoT).
c) 1º Critérios de inclusão: Que atende à *string* especificada. Artigos primários, artigos integrais. A seleção inicial é feita no título do artigo e/ou resumo.
d) Critérios de exclusão: revisão. Publicados antes de 2016 que tratam de cryptomoeda. Bitcoin etc.
e) Período estudado: de 2016 em diante, para eliminar artigos com ênfase integral em cryptomoedas.
f) Língua: qualquer.
g) Tipos de artigos: periódicos, *Journals* e anais de eventos científicos da área. Ter sido aprovado por banca examinadora quando se referir a trabalhos de conclusão de curso, mestrado ou doutorado.
h) Período de realização: a partir de 13 de junho de 2020 até 26/02/2021.
i) Seleção e catalogação das publicações: via aplicativo *Mendeley*.
j) 2º Critérios de inclusão: Que o corpo do artigo contenha a sentença: “segurança da informação” ou *Cybersecurity* ou citação de qualquer tipo de *cybertreats*.

Considera-se que a *string* definida não é muito complexa a ponto de reduzir demais a base de artigos nem muito simples para não gerar uma base de artigos muito extensa a ponto de comprometer o tempo de análise dos artigos.

4 Apresentação e Discussão dos Resultados

Os resultados estão trazendo respostas à questão de pesquisa: quais as técnicas de *blockchain* que podem ser adotadas para contribuir para o aumento do nível de segurança da informação em *smart cities?*

A investigação trouxe diversas repostas, com diferentes tecnologias, ferramentas e aplicações que podem satisfazer as questões iniciais, atendendo aos objetivos da pesquisa.

Por definição, *blockchain* é uma rede descentralizada que permite que partes independentes se comuniquem sem qualquer envolvimento de terceiros. Para proteger as redes, as organizações podem distribuir seus sistemas entre vários nós de servidores que fornecem alta resiliência e removem o ponto único de falha (Gupta, 2018).

Assim, fazendo uma releitura de Gupta (2018), pode-se ver que o mais importante é que a *blockchain*, uma vez implementada, sempre vai melhorar as condições de segurança da informação nos sistemas. Singh & Michels (2018) alertam que muito do interesse em DLs decorre de sua capacidade de descentralizar e desintermediar, removendo a necessidade de terceiros (confiáveis). Em muitos casos, é a natureza descentralizada das DLs que traz considerações de segurança, resiliência e integridade de dados.

Resta ao analista/arquiteto de rede medir sua necessidade de *blockchain* e qual a relação custo/benefício que ele pode trabalhar na sua entidade diante das várias variáveis que estão em jogo em uma tomada de decisão desse tipo. Nesse ponto, a tecnologia não é única e vai depender da aplicação/ferramenta usada e de qual o resultado pretendido, parâmetros críticos, tempo de resposta, custo, etc.

Em se tratando de casos específicos, pode-se citar uma aplicação em cadeia de suprimentos alimentares: conforme entendimento de Reyna *et al*. (2018), a integração de tecnologias promissoras como IoT e computação em nuvem provou ser

inestimável. A *blockchain* pode enriquecer a IoT, fornecendo um serviço de compartilhamento confiável, cujas informações são confiáveis e podem ser rastreadas. As fontes de dados podem ser identificadas a qualquer momento e os dados permanecem imutáveis ao longo do tempo, aumentando sua segurança. Nos casos em que as informações devem ser compartilhadas com segurança entre muitos participantes, essa integração representa uma revolução. Por exemplo, uma rastreabilidade exaustiva em vários produtos alimentares é um aspecto fundamental para garantir a segurança alimentar. A rastreabilidade dos alimentos pode exigir o envolvimento de muitos participantes: fabricação, alimentação, tratamento, empacotamento, distribuição, e assim por diante. Um vazamento de dados em qualquer parte da cadeia pode levar a uma fraude e retardar todo o processo. O que pode afetar seriamente a vida dos cidadãos.

Essa aplicação pode ser implementada em indústrias de alimentos, bem como órgãos de governo para fiscalização sanitária desses alimentos. Isso garante empecilhos às fraudes e ameaças à segurança alimentar nas cidades.

Cao *et al*. (2019) também citam exemplo em cadeia de suprimentos, mais especificamente para contêineres. Na indústria baseada em cadeia de suprimentos existem modelos de cadeia de suprimentos habilitados para *blockchain*. Nesse modelo, as informações armazenadas na *blockchain* podem servir como um log de entrega para embarques/desembarques de contêineres.

Em sistemas de transporte inteligentes (ITS), com a integração à tecnologia *blockchain*, aumenta a segurança do dispositivo e a privacidade dos dados. A *blockchain* pode fornecer um ecossistema ITS seguro, confiável e descentralizado. Em ITS, o gerenciamento de chaves seguras é uma das questões importantes dentro da rede heterogênea (Mohanta *et al*., 2019).

Essa aplicação em cadeia de suprimentos pode estar sendo usada para aquisição, fiscalização, distribuição e auditagem para casos de vacina. Como atualmente está acontecendo na preparação para a vacinação contra o coronavírus no Brasil, há um saldo de qualidade nesse processo.

Minoli & Occhiogrosso (2018) exemplificaram e mostraram um aplicativo de segurança baseado em IoT, o *e-health*, no qual o dispositivo de nível de *gateway* cria uma *blockchain* para as informações médicas a serem transmitidas (a criptografia do conteúdo original também deve ser implementada). *Blockchains* podem e devem ser usadas no nível do aplicativo para validar todos os tipos de transações que necessitam de segurança. Por exemplo, o pagamento de uma taxa de estacionamento à medida que passa pelas várias entidades financeiras que apoiam a transação, fotografia, imagem, vídeo ou formulário de dados de hospitais. Além disso, as informações podem incluir dados de sensores médicos, reclamações médicas, capturas de tela de vigilância internas em vídeo, e assim por diante. Os dispositivos IoT precisam se comunicar e sincronizar-se uns com os outros usando *blockchain.* Podem-se controlar e configurar dispositivos IoT (por exemplo, gerenciar chaves usando criptossistemas de chave pública RSA em que as chaves públicas são armazenadas em um local seguro da rede e as chaves privadas são salvas em dispositivos individuais).

A autenticação tem papel fundamental na segurança de ambientes virtuais ao validar a identificação dos usuários. Após a autenticação, o sistema pode conceder a autorização para o acesso aos recursos. Nakamura & Geus (2007) mostram que os dados de identidade digital permitem a autenticação automática de um usuário interagindo com um sistema e possibilita o acesso aos serviços fornecidos pelo sistema. Identidade autossoberana (SSI) é um tipo de identidade digital que permite ao usuário o controle total e final de sua identidade. Baseada em *blockchain*, a Estônia estabeleceu um dos sistemas de carteira de identidade nacionais mais avançados tecnologicamente. O cartão obrigatório permite o acesso a todos os serviços eletrônicos seguros (Sullivan & Burger, 2017 como citado em Zwitter *et al*. (2020), incluindo viagens dentro da União Europeia, seguro saúde nacional, acesso a contas bancárias, votação eletrônica, administração de registros médicos.

Năsulea & Mic (2018) informam que a identidade digital criada por meio de um protocolo *blockchain* já está disponível e pode ser usada como assinatura eletrônica.

Outra aplicação importantíssima com *blockchain* é o Sistema de Registro de Imóveis, que, armazena notas de compra/venda e contratos, assinaturas de partes, seus

documentos de identidade e informações de propriedade em *blockchain*. A edição de registros é permitida apenas por meio da interface administrativa, mas registra todas as transações na *blockchain*, que pode ser visualizada por todos os interessados como compradores, vendedores, agentes, bancos, inclusive públicos (Kempe, 2016).

No Brasil ainda existem muitos cartórios não digitalizados, e somente em 2015 o Conselho Nacional de Justiça (CNJ) editou o Provimento n° 47, de 19 de junho de 2015 (CNJ, 2015), que estabelece diretrizes gerais para o sistema de registro eletrônico de imóveis em Brasília. Destaca-se, ainda, que a *blockchain* oferece um nível de segurança maior do que os cartórios digitalizados atuais. Logo, é a oportunidade de se implantar o cartório já usando *blockchain*.

Xie *et al*. (2019b) acreditam que a tecnologia *blockchain* melhora significativamente as cidades inteligentes e expõem como é usado um sistema geral de votação eletrônica baseado em *blockchain*, indicando um caso de uso para mostrar como a tecnologia *blockchain* pode ser usada para promover a implementação de uma cidade inteligente confiável, segura, transparente e democratizada e com o voto seguro rastreável e auditável. O sistema descentralizado torna o processo de votação menos vulnerável à manipulação e ataque e só permite que indivíduos elegíveis votem em uma eleição. Todas as transações de voto armazenadas na *blockchain* são públicas para todos os eleitores, tornando o processo de votação transparente e verificável. Por fim, as transações de voto armazenadas na *blockchain* são acordadas por todos os nós desta, usando-se algoritmos de consenso.

O rol de aplicações de *blockchain* em *smart cities* é praticamente infinito, pois, como já foi dito, essa tecnologia é genérica (Brasil, 2020b) e acessível. Não sendo exaustivo, outra importante aplicação para órgãos de governo e empresas em geral é usá-la como ferramenta de auditagem e *compliance*, inclusive a Lei geral de proteção de dados (LGPD). A *blockchain* pode ser usada como base para a verificação das transações realizadas. Os auditores podem averiguar facilmente as transações em livros de *blockchain* disponíveis publicamente.

O que distingue o uso da *blockchain* de outras formas de carimbo de data/hora e autenticação de dados é que os documentos e outros conjuntos de dados na *blockchain* são provas descentralizadas. Garante que os dados por ninguém podem ser apagados ou modificados, nem por sua própria empresa nem por concorrentes, terceiros ou governos (Findlay, 2015 como citado em Abreu *et al*., 2018).

Quanto aos computadores quânticos, estes representam uma grande ameaça à criptografia clássica e aos protocolos de segurança das redes, incluindo *blockchain*. *Smart cities* baseadas em *blockchain* são uma instância crítica que precisa ser protegida contra futuros ataques quânticos, pois mantém dados de informações confidenciais sobre cidadãos, servidores e usuários em diferentes níveis. Neste trabalho, apresentou-se uma visão geral para compreender os potenciais riscos futuros das *smart cities* baseadas em *blockchain* frente aos computadores quânticos.

A seguir elaborou-se a Tabela 8 contendo o resumo dos achados que foram abordados nesta pesquisa.

Tabela 8

Aplicações práticas com *blockchain* em *smart cities*

	Base/uso		
Aplicações	**Iot**	***Smart cities***	**Referência**
Transações financeiras *online*	V	V	Lewis, 2018; Nakamoto, 2008; Panda *et al*., 2018
Cadeia de suprimentos	V	V	Rejeb *et al*., 2019; Restuccia *et al*., 2019
Telemedicina	V	V	Minoli & Occhiogrosso, 2018
Comércio de energia de veículos	V	V	Xie *et al*., 2019b
Gerenciamento de identidade digital de cidadãos	V	V	Gupta, 2018; Nãsulea & Mic, 2018
Governança			
Sistemas de transportes inteligentes	V	V	Mohanta *et al*., 2019; Huang *et al*., 2018
Monitoramento de rede e serviços de segurança, incluindo autenticação, confidencialidade, privacidade, integridade e procedência.	V	V	Salman *et al*., 2019; Minoli & Occhiogrosso, 2018; Nakamura & Geus, 2007; Rotuna *et al.*, 2019
Votação segura	V	V	Xie *et al*., 2009b; Nãsulea & Mic, 2018
Cartorial	V	V	Shrivas, 2019; Kempe, 2016
Proteção ataque DDos/DOS	V	V	Gupta, 2018
Auditagem/*copliance*/governança	V	V	Findlay, 2015

Fonte: dados da pesquisa (2021).

5 Considerações Finais

Conforme os resultados alcançados com esta pesquisa, pôde-se concluir que a *blockchain* é reconhecida como uma das tecnologias mais revolucionárias e inovadoras que existem. É uma tecnologia genérica. Ela pode ser aplicada em amplo espectro tecnológico do mesmo modo que a inteligência artificial o é.

Do mesmo modo que inteligência artificial leva inteligência às tecnologias aplicadas, a *blockchain* leva segurança à informação onde é implementada. Por isso que se pode dizer que ela pode ser aplicada em ambientes que trabalhem em TIC, quer seja em ambiente empresarial, corporativo, médico, governo (*smart cities*), educacional ou militar.

Em cada ambiente, porém, haverá um tipo de tecnologia, uma técnica, uma ferramenta diferente, pois cada aplicação tem suas peculiaridades e necessidades que serão satisfeitas. Mesmo assim, pode ser acolhida por um tipo ou outro da tecnologia, que atenderá à demanda satisfatoriamente, conjugada com um aplicativo ou outro, até com um *mix* deles, para atender melhor ao quesito segurança da informação em *smart cities.*

Ao longo do estudo, discorreu-se sobre quais os vários tipos de aplicações e as tecnologias que podem atender a determinada necessidade de segurança da informação, ficando a cargo do analista definir bem esse casamento. O mais importante é que a *blockchain*, uma vez implementada, sempre vai melhorar as condições de segurança da informação no sistema. Resta ao analista/arquiteto medir a necessidade da *blockchain* e qual a relação custo/benefício que ele pode trabalhar no seu sistema, diante das várias variáveis que estão em jogo em uma tomada de decisão desse tipo.

Pela natureza descentralizada da *blockchain,* infere-se que uma gama de problemas/ameaças é evitada/minimizada só se considerando essa característica. Um fator muito importante é que nas como visto, a auditoria pode ser feita em tempo real.

Assim, os fatores críticos descritos para a auditoria têm considerável impacto positivo na redução de fraudes e corrupção em geral, bem como seria desestimulante para pessoas mal-intencionadas. Esse tipo de aplicação melhora muito o grau de transparência em *smart cities* e órgãos de governo. Essa técnica, com certeza, como já implementada em outros países, acaba com a maioria dos problemas de licitação no Brasil, estados e cidades. Esse seria o grande destaque trazido pelos estudos.

Em relação ao objetivo principal, foi alcançado por diversas maneiras: quais seriam as técnicas mais indicadas para aumentar a segurança da informação em *smart cities*? Constatou-se que há aplicações, na prática, em que se pode usar *blockchain* para garantir a segurança da informação em cadeia de suprimentos, telemedicina, eleições, identificação digital, cartórios, sistemas de transporte inteligentes, *compliance* e ainda em auditagem, entre outros que impactam a qualidade de vida dos cidadãos em uma *smart cities.* Portanto, a investigação respondeu ao problema de pesquisa. Ficou evidenciado que os objetivos específicos, tais como: apresentação de características principais de *blockchain*, análise de parâmetros e detecção de aplicações e usos foram explorados e alcançados em exemplos e tabelas ao longo do estudo, em *smart cities* com visões de autores diversos para satisfazer quesitos relativos à segurança da informação.

Ressalta-se que essa tecnologia tem suas desvantagens, também, como custo, problema ambiental devido ao alto consumo energético e velocidade de pré-processamento, que precisam ser levadas em consideração, entre outros

Outro ponto importante é que, com o uso de BaaS, o cliente pode implementar aplicações seguras em nuvens, bem como gerenciamento e operação com vários níveis de complexidade sem serem necessários profundos conhecimentos técnicos de TI.

De acordo com a metodologia exposta, esta pesquisa que foi aplicada para s*mart cities*, baseada em *hardware* de IoT, usou somente literatura disponível na internet. Acredita-se que deva haver limitações no estudo, pois alguns provedores de literatura científica só permitem acesso às instituições credenciadas, outros só fornecem

publicações científicas mediante pagamento. Por isso estas duas últimas opções não estão incluídas na pesquisa.

Percebeu-se que as justificativas e o tema para conduzir este estudo foram baseados na situação do país em relação ao assunto segurança da informação. O Brasil ocupa a segunda posição no *ranking* em perdas econômicas devido a ataques cibernéticos. Por isso, o país exarou diversas iniciativas, entre elas a publicidade da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética, a *E-Ciber*, em fevereiro de 2020.

Além dessa, outra justificativa é que o governo federal vem envidando esforços para tornar o país moderno, ágil, com burocracia mínima, transparente e seguro, atingindo o estágio de maturidade tecnológica e de atendimento às necessidades do país em segurança cibernética, considerando aspectos relativos ao ecossistema digital no âmbito nacional e internacional.

Com a finalidade de prevenção contra ataques de computadores quânticos, aqui se apresentou a estrutura clássica de *smart cities* baseada em *blockchain* e sugeriram-se algumas das soluções pós-quânticas eficazes, como criptografia baseada em rede, distribuição de chaves quânticas e emaranhamento em *blockchain* quântica com base no tempo. Essas soluções são suscetíveis aos ataques quânticos e são auspiciosas para serem implantadas em *smart cities* baseadas em pós-*quantum blockchain* antes que ocorra o avanço dos computadores quânticos em larga escala nos mercados.

Diante desse panorama, apreendeu-se que a contribuição deste trabalho vem ao encontro dos anseios dos governos, que é garantir que a informação seja segura, principalmente nas *smarts cities,* em cujo ambiente o cidadão é o que mais fica exposto ao crime. O momento é bem adequado, pois no dia 8 de dezembro de 2020 o governo acabou de lançar, iniciativa inédita, que é a “Carta Brasileira para Cidades Inteligentes”, na qual foram colocadas as diretrizes e pilares para implementação de *smart cities* sustentáveis e seguras no país. Outro ponto interessante refere-se à importância desta pesquisa para os meios acadêmicos, pois o Brasil, como entendido,

está em início de jornada para desenvolvimento dessa ideia. Essa pesquisa vem contribuir para esse desenvolvimento.

Como trabalhos futuros e promissores, tais como no campo da auditagem e anticorrupção, pode-se relacionar a associação de *blockchain* com inteligência artificial, que assim poderão dar continuidade à pesquisa, pois a tecnologia é recente e ainda está em desenvolvimento

.

Referências

Abreu, P. W., Aparicio, M., & Costa, C. J. (Jun. 2018). Blockchain technology in the auditing environment. *Anais do Iberian Conference on Information Systems and Technologies, CISTI*, 1–6. https://doi.org/10.23919/CISTI.2018.8399460.

Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K. K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications*, *144*, 13–48. https://doi.org/10.1016/j.jnca.2019.06.018.

Ahmed, S., Shah, M. A., & Wakil, K. (2020). Blockchain as a trust builder in the smart city domain: A systematic literature review. *IEEE Access*, *8*, 92977–92985. https://doi.org/10.1109/ACCESS.2020.2993724.

Angelidou, M. (2017). The role of smart city characteristics in the plans of fifteen cities. *Journal of Urban Technology*, *24*(4), 3–28. https://doi.org/10.1080/10630732.2017.1348880.

Angrishi, K. (2017). *Turning internet of things (IoT) into internet of vulnerabilities (IoV) : IoT Botnets*. 1–17. http://arxiv.org/abs/1702.03681.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99–109. https://doi.org/10.1109/TMSCS.2015.2498605.

Azzaoui, A.-E., & Park, J. H. (2020). Post-quantum blockchain for a scalable smart city. *Journal of Internet Technology*, *21*(4), 1171–1178. https://doi.org/10.3966/160792642020072104025.

Banco Nacional de Desenvolvimento Econômico e Social - BNDES. (2017). *Produto 7A: Aprofundamento de Verticais – Cidades*. Brasília: BNDES.

Brasil. (2020a). Presidência da República. *Decreto nº 10.222, de 5 de fevereiro de 2020*. Brasília: Casa Civil.

Brasil (2020b). Tribunal de Contas da União - TCU. *Levantamento da tecnologia blockchain*. (p. 7). Recuperado de: https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm.

Cabaj, K., & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: The case of cryptowall. *IEEE Network*, *30*(6), 14–20. https://doi.org/10.1109/MNET.2016.1600110NM.

Callegaro, R. F., & Hornburg, J. E. (2011). *Confiança e Reputação em SMA*.

Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z., & Peng, M. (2019). When

Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *IEEE Network*, *33*(March), 133–139. https://doi.org/10.1109/MNET.2019.1900002.

Conselho Nacional de Justiça - CNJ. (2015). *Provimento n° 47, de 19 de junho de 2015*. Brasília: CNJ.

Costa, J. A. F., & Sola, F., & Garcia, M. A. F. (2020). Telemedicina e uberização da saúde: médicos operários ou consumidores? *Cuadernos Iberoamericanos de Derecho Sanitario*, *9*(3), 72–88.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, *6*, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985.

Cunha, M. A., Przeybilovicz, E., Macaya, J. F. M., & Burgos, F. (2016). *Smart cities: Transformação Digital de cidades* (v. 16). http://linkinghub.elsevier.com/retrieve/pii/S026427519800050X.

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076–8094. http://files/1359/Blockchain for Internet of Things A survey.pdf

Dewan, S., & Singh, L. (2020). Use of blockchain in designing smart city. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/SASBE-06-2019-0078.

El Ioini, N., & Pahl, C. (2018). A review of distributed ledger technologies. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).* 11230 LNCS (November), 277–288. https://doi.org/10.1007/978-3-030-02671-4_16.

European Comission. (2014). *Smart Cities.* Retrieved from: https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

Gaur, N., Desrosiers, L., Novotny, P., Ramakrishna, V., O'Dowd, A., & Baset, S. (2018). *Hands-on blockchain with hyperledger: Building decentralized applications with hyperledger fabric and composer*. Packt Publishing.

Georgescu, M., & Popescul, D. (Dec. 2016). The importance of internet of things security for smart cities. *Smart Cities Technologies*. https://doi.org/10.5772/65206.

Giffinger, R., Fertner, C., Meijers, E., & Kramar, H. (2007). City-ranking of European medium-sized cities. *Semantic Scholar*. Corpus ID: 16115224.

Gupta, R. (2018). *Hands-on cybersecurity with blockchain*. Packt Publishing Ltd.

Haroon, A., Ali, M., Asim, Y., Naeem, W., Kamran, M., & Javaid, Q. (2016). Constraints in the IoT: The world in 2020 and beyond. *International Journal of Advanced Computer Science and Applications*, *7*(11), 252–271. https://doi.org/10.14569/ijacsa.2016.071133.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045.

Hitachi. (2014). *Smart sustainable city overview*. Retrieved from: http://www.hitachi.com/product.

Holbrook, J. (2020). *Architecting enterprise blockchain solutions*. John Wiley & Sons.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015*, 21–28. https://doi.org/10.1109/SERVICES.2015.12.

Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access*, *6*, 13565–13574. https://doi.org/10.1109/ACCESS.2018.2812176.

Instituto Nacional de Telecomunicações - Inatel. (2019). *Smart cities*: conceitos e aplicações. Fundação Instituto Nacional de Telecomunicações (v. III).

International Standardization for Organization/ International Electrotechnical Commission - ISO/IEC (2019). *ISO/IEC 24760*.

International Telecommunication Union/Comissão Econômica das Nações Unidas para a Europa - ITU/UNECE. (2017). *Sustainable Smart Cities*. Retrieved from: https://unece.org/sustainable-smart-cities.

International Telecommunication Union - ITU. (2012). *Measuring the Information Society.* Retrieved from: https://www.itu.int/en/itu-d/statistics/documents/ publications/mis2012/mis2012_without_annex_4.pdf.

International Telecommunication Union - ITU-T. (2014). Smart water management in cities. *ITU-T Focus Group on Smart Sustainable Cities*. Retrieved from: https://smartnet.niua.org/sites/default/files/resources/TR-SWM-cities.pdf.

Kempe, M. (Jul. 2016). *The land registry in the blockchain*. 42. Retrieved from: http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf.

Khan, J. Y. (2019). Internet of things (IoT): Systems and applications. *Jenny Stanford Publishing*.

Khrais, L. T. (2020). IoT and blockchain in the development of smart cities. *International Journal of Advanced Computer Science and Applications*, *11*(2), 153–159. https://doi.org/10.14569/ijacsa.2020.0110220.

Kim, S., & Deka, G. C. (2020). *Studies in Big Data 60 advanced applications of blockchain technology*. Universiteitgent.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering.*

Raj, K. (2019). *Foundations of blockchain protocols*. Packt Publishing.

Lee, I., & Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008.

Lewis, A. (2018). *The basics of bitcoins and blockchains.* E-book loja Kindle (pp. 603–623).

Liao, K., Zhao, Z., Doupe, A., & Ahn, G. J. (2016). Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin. *ECrime Researchers Summit, ECrime*. https://doi.org/10.1109/ECRIME.2016.7487938.

Lisdorf, A. (2020). *Demystifying Smart Cities*. E-book Kaufen. https://doi.org/10.1007/978-1-4842-5377-9

Meijer, A., & Rodríguez Bolívar, M. P. (2013). Governing the smart city: Scaling-Up the Search for socio-techno synergy. *EGPA Annual Conference*, *2013*, 1–13. Retrieved from: http://medcontent.metapress.com/index/A65RM03P4874243N.pdf%5Cnhttps://www.scss.tcd.ie/disciplines/information_systems/egpa/docs/2013/BolivarMeijer.pdf

Melhem, A., AlZoubi, O., Yassein, M. B., & Mardini, W. (Dec. 2019). Applications of blockchain in smart cities. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3368691.3368726

Micciancio, D., & Ristenpart, T. (2020). Advances in cryptology - CRYPTO 2020. *Anais do 40th Annual International Cryptology Conference, CRYPTO 2020*. Springer Nature.

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1–2*, 1–13. https://doi.org/10.1016/j.iot.2018.05.002.

Mohamed, K. S. (2019). *The era of internet of things*. https://doi.org/10.1007/978-3-030-18133-8.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*, 100107. https://doi.org/10.1016/j.iot.2019.100107.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940. Retrieved from: www.ijarcs.info

Moore, C., Rainwater, B., & Stahl, E. (2018). *Blockchain in Cities*. National League of cities, 31.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: challenges. *IEEE Access*, *5*, 19293–19304. https://doi.org/10.1109/ACCESS.2017.2749422.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*, 1–6. https://doi.org/10.2139/ssrn.3440802.

Nakamura, E. T., & Geus, P. L. (2007). *Segurança de redes em ambientes cooperativos*. São Paulo: Bekerley.

Nãsulea, C., & Mic, S.-M. (2018). Using blockchain as a platform for smart cities. *Journal of E-Technology*, *9*(2), 37. https://doi.org/10.6025/jet/2018/9/2/37-43.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, Applications and challenges. *IEEE Communications Surveys and Tutorials*, *22*(4), 2521–2549. https://doi.org/10.1109/COMST.2020.3020092.

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*(2), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007.

Onik, M. M. H., & Miraz, M. H. (2019). Performance analytical comparison of Blockchain-as-a-service (BaaS) platforms. *ArXiv*, 1–17.

Panda, P. S., Dhameja, G., & Singhal, B. (2018). *Beginning blockchain A beginner's guide to building blockchain solutions*. Apress.

Perwej, A., Haq, K., & Perwej, Y. (2013). Blockchain and its influence on market. *International Journal of Computer Science Trends and Technology*, *7*(5), 82–91. Retrieved from: www.ijcstjournal.org.

Pourahmad, A., Ziari, K., Hataminejad, H., & Parsa, S. (2018). Explanation of concept and features of a smart city. *Bagah-E-Nazar*, *15*(58), 5–26.

Pukkasenung, P. (2020). *Internet of things (IoT): A basic concept and analysis Security Issues*. *18*(11), 1–10.

Quiniou, M. (2019). *Blockchain: the advent of disintermediation*. Wiley (164 p.).

Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, *11*(7), 1–22. https://doi.org/10.3390/fi11070161.

Restuccia, F., Kanhere, S. D., Melodia, T., & Das, S. K. (2019). Blockchain for the Internet of Things: present and future. *ArXiv Preprint ArXiv:1903.07448*. http://files/1289/2019.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*(2018), 173–190. https://doi.org/10.1016/j.future.2018.05.046.

Rotuna, C., Gheorghita, A., Zamfiroiu, A., & Smada, D.-M. (2019). Smart city ecosystem using blockchain technology. *Informatica Economica*, *23*(4/2019), 41–50. https://doi.org/10.12948/issn14531305/23.4.2019.04.

Saaiq, M., & Ashraf, B. (2017). Modifying “pico” question into “picos” model for more robust and reproducible presentation of the methodology employed in a scientific study. *World Journal of Plastic Surgery*, *6*(3), 390–392. Retrieved from: http://www.ncbi.nlm.nih.gov/pubmed/29218294%0Ahttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC5714990.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security services using blockchains: A state of the art survey. *IEEE Communications Surveys and Tutorials*, *21*(1), 858–880. https://doi.org/10.1109/COMST.2018.2863956

Santos, B. P., Silva, L. A. M., Celes, C. S. F. S., Borges Neto, J. B., Peres, B. S., Augusto, M., Vieira, M., Vieira, F. M., Goussevskaia, O. N., & Loureiro, A. A. F. (2016). Internet das coisas: da teoria à prática. *Anais do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, *50*. Retrieved from: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf.

Santos, M., & Moura, E. (2019). *Hands-On IoT solutions with blockchain*. eBook Kindle.

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650–655. https://doi.org/10.1016/j.future.2018.04.060.

Shrivas, M. K. (2019). The disruptive blockchain: types, platforms and applications. *Texila International Journal of Academic Research*, *6*, 17–39. https://doi.org/10.21522/tijar.2014.se.19.01.art003.

Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning blockchain.* https://doi.org/10.1007/978-1-4842-3444-0.

Soni, D., & Makwana, A. (Apr. 2017). A survey on mqtt: a protocol of internet of things(IoT). *International Conference on Telecommunication, Power Analysis and Computing Techniques (Ictpact - 2017)*, 0–5. https://www.researchgate.net/publication/316018571_A_SURVEY_ON_MQTT_A_PROTOCOL_OF_INTERNET_OF_THINGSIOT.

Statista. (2020). Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030. Retrieved from: https://www.statista.com/statistics/802690/worldwide-connecteddevices-by-access-technology/

Treiblmaier, H., & Beck, R. (2018a). Business transformation through blockchain: Volume II. *In Business Transformation through Blockchain: Vol. I*. https://doi.org/10.1007/978-3-319-99058-3.

Treiblmaier, H., & Beck, R. (2018b). Business transformation through blockchain: Volume II. In *Business Transformation through Blockchain: Vol. II*. https://doi.org/10.1007/978-3-319-99058-3.

United Nations. (2014). *Revision of the World Urbanization Prospects*. Department of Economic and Social Affairs/Population Division.

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1–32.

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. In *International Journal of Communication Systems* (v. 25, Issue 9). https://doi.org/10.1002/dac.2417.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019a). A Survey of Blockchain Technology Applied to Smart Cities : Research Issues and Challenges Blockchain-based. *IEEE Communications Surveys & Tutorials*, *PP*(c), 1. https://doi.org/10.1109/COMST.2019.2899617

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019b). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794–2830. Recuperado de: http://files/1411/8642861.html.

Yasin, A., & Liu, L. (2016). An online identity and smart contract management system. *Proceedings - International Computer Software and Applications Conference*, *2*, 192–198. https://doi.org/10.1109/COMPSAC.2016.2.

Zhang, P., Wang, L., Wang, W., Fu, K., & Wang, J. (2021). A blockchain system based on quantum-resistant digital signature. *Security and Communication Networks*, (2). https://doi.org/10.1155/2021/6671648.

Zhu, L., Gai, K., & Li, M. (2019). *Blockchain technology in internet of things*. https://doi.org/10.1007/978-3-030-21766-2.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (May 2020). Digital identity and the blockchain: Universal Identity management and the concept of the “self-sovereign” individual. *Frontiers in Blockchain*, *3*, 1–14. https://doi.org/10.3389/fbloc.2020.00026.