UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO EM
TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

JULIANO OLIVEIRA DE ALMEIDA

METODOLOGIA DE AVALIAÇÃO TÉCNICO-CIENTÍFICA DE APLICAÇÕES BLOCKCHAIN: UM ESTUDO DE CASO NO SETOR ELÉTRICO

ARARANGUÁ
2021

JULIANO OLIVEIRA DE ALMEIDA

METODOLOGIA DE AVALIAÇÃO TÉCNICO-CIENTÍFICA DE APLICAÇÕES BLOCKCHAIN: UM ESTUDO DE CASO NO SETOR ELÉTRICO

Dissertação submetida ao Programa de Pós-Graduação em Tecnologias da Informação e Comunicação da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Tecnologias da Informação e Comunicação. Orientador: Prof. Dr. Roderval Marcelino. Coorientador: Prof. Dr. Martín Vigil.

ARARANGUÁ

2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Almeida, Juliano Oliveira de
Metodologia de avaliação técnico-científica de aplicações blockchain: um estudo de caso no setor elétrico / Juliano Oliveira de Almeida ; orientador, Roderval Marcelino, coorientador, Martín Augusto Gagliotti Vigil, 2021.
175 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Campus Araranguá, Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2021.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Blockchain. 3. Tecnologia de Contabilidade Distribuída. 4. Metodologia. 5. Avaliação. I. Marcelino, Roderval. II. Vigil, Martín Augusto Gagliotti. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Tecnologias da Informação e Comunicação. IV. Título.

JULIANO OLIVEIRA DE ALMEIDA

METODOLOGIA DE AVALIAÇÃO TÉCNICO-CIENTÍFICA DE APLICAÇÕES BLOCKCHAIN: UM ESTUDO DE CASO NO SETOR ELÉTRICO

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Jean Everson Martina, Dr.
Universidade Federal de Santa Catarina

Prof. Cristian Cechinel, Dr.
Universidade Federal de Santa Catarina

Prof. Juarez Bento da Silva, Dr.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Tecnologias da Informação e Comunicação.

Documento assinado digitalmente
Fernando Jose Spanhol
Data: 07/06/2021 20:16:15-0300
CPF: 642.656.419-20
Verifique as assinaturas em https://v.ufsc.br

Prof. Fernando José Spanhol Dr.
Coordenador do Programa

Documento assinado digitalmente
Roderval Marcelino
Data: 08/06/2021 08:12:21-0300
CPF: 832.867.489-00
Verifique as assinaturas em https://v.ufsc.br

Prof. Roderval Marcelino, Dr.
Orientador

Araranguá, 2021.

Este trabalho é dedicado à minha família, especialmente à minha esposa e filha.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois sem ele nada disso seria possível.

A minha esposa Vera Lúcia Cardoso e a minha filha Sofia Isabele da Rosa de Almeida pelo amor, companheirismo e incentivo para seguir em frente sempre. Amo muito vocês!

Ao meu orientador prof. Roderval Marcelino Dr. e coorientador prof. Martin Vigil Dr. que não mediram esforços para apoiar e orientar meus caminhos nesta jornada. Que foram além de parceiros de projeto, conselheiros e amigos. Vocês me ajudaram muito a crescer como profissional e como ser humano. Agradeço também a paciência e compreensão. Muito obrigado. Vocês são brilhantes. Minha admiração e respeito.

Aos parceiros de projeto prof. Guiliano Arns Dr., Solange Machado, Karoline Roversi, Felipe Tomao e Rafael Canal, que muito contribuíram no desenvolvimento da pesquisa e na concepção deste trabalho.

A Universidade Federal de Santa Catarina – Campus Araranguá e ao Programa de Pós-Graduação em Tecnologias da Informação e Comunicação.

A CPFL Energia pela escolha da UFSC como instituição de pesquisa e da nossa equipe de trabalho para composição deste projeto.

Aos que não foram citados, mas que de alguma forma fizeram parte desta dissertação, meus sinceros agradecimentos.

RESUMO

Desde a primeira implementação funcional da tecnologia de contabilidade distribuída, Bitcoin, chamada neste momento de blockchain, que o mundo passou a ver esta solução computacional muito promissora. Suas características como imutabilidade, consenso, segurança, arquitetura distribuída, *tokenização*, eliminação de agentes centralizados, dentre outras, mostraram alto potencial para inúmeras aplicações. Blockchain não é algo totalmente novo, entretanto a concatenação de diversas tecnologias computacionais tornam esta tecnologia inovadora e disruptiva. Por ser uma tecnologia nova, o desconhecimento e a falta de experiência dos envolvidos tornam a avaliação técnico-científica difícil. Muitos parâmetros computacionais de áreas diferentes estão relacionados à tecnologia blockchain. A atual literatura não apresenta uma metodologia de avaliação que sirva como ferramenta norteadora para especialistas avaliarem estas aplicações. Diante disso, este trabalho propôs uma metodologia de avaliação técnico-científica para as tecnologias de contabilidade distribuída. A pesquisa inicialmente trouxe um estudo mostrando o estado da arte das avaliações realizadas em aplicações blockchain. Em seguida foi mostrado a origem e extração dos indicadores utilizados na metodologia e sua contextualização. Ainda foi apresentado a construção da metodologia de avaliação técnico-científica, o instrumento criado para sua operacionalização e, por fim, um estudo de caso no setor elétrico onde a metodologia foi aplicada para avaliar seu potencial. Os resultados da aplicação da metodologia mostraram que em formato de instrumento de avaliação, com suas perguntas chaves e itens norteadores, tornou-se uma importante ferramenta para os envolvidos nestas novas soluções, levando a reflexão e avaliação de indicadores que poderiam passar despercebidos e consequentemente tornando a avaliação mais assertiva, colaborando nas melhorias e redução de problemas futuros.

Palavras-chave: Blockchain. Tecnologia de Contabilidade Distribuída. Metodologia. Avaliação.

ABSTRACT

Since the first functional implementation of distributed accounting technology, Bitcoin, now called blockchain, the world has come to see this very promising computing solution. Its characteristics such as immutability, consensus, security, distributed architecture, tokenization, elimination of centralized agents, among others, showed high potential for numerous applications. Blockchain is not something entirely new, however the concatenation of several computing technologies makes this technology innovative and disruptive. As it is a new technology, the lack of knowledge and lack of experience of those involved makes technical-scientific evaluation difficult. Many computational parameters from different areas are related to blockchain technology. The current literature does not present an evaluation methodology that serves as a guiding tool for specialists to evaluate these applications. Therefore, this work proposed a technical-scientific evaluation methodology for distributed ledger technologies. The research initially brought a study showing the state of the art of assessments carried out on blockchain applications. Then it was shown the origin and extraction of the indicators used in the methodology and its context. It was also presented the construction of the scientific technical evaluation methodology, the instrument created for its operationalization and, finally, a case study in the electric sector where the methodology was applied to evaluate its potential. The results of the application of the methodology showed that in an evaluation instrument format, with its key questions and guiding items, it became an important tool for those involved in these new solutions, leading to the reflection and evaluation of indicators that could go unnoticed and consequently making the most assertive assessment, helping to improve and reduce future problems.

Keywords: Blockchain. Distributed Ledger Technology. Methodology. Evaluation.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACL – Ambiente de Contratação Livre

ACR – Ambiente de Contratação Regulada

BaaS – *Blockchain-as-a-Service*

BFT – *Byzantine Fault Tolerance*

B2B – *Business-to-Business*

B2C – *Business-to-Consumer*

CCEE – Câmara de Comercialização de Energia Elétrica

CFT – *Crash Fault-Tolerant*

CPU – *Central Processing Unit*

DAG – *Directed Acyclic Graph*

DLT – *Distributed Ledger Techonology*

DPoS – *Delegated Proof-of-Stake*

EVM – *Ethereum Virtual Machine*

FAQ – *Frequently Asked Questions*

FIPS – *Federal Information Processing Standards*

ICO – *Initial Coin Offering*

IoT – *Internet-of-Things*

LAN – *Local Área Network*

LGPD – Lei Geral de Proteção de Dados Pessoais

LTS – *Long Time Support*

pBFT – *Practical Byzantine Fault Tolerance*

PoA – *Proof-of-Authority*

PoB – *Proof-of-Burn*

PoC – *Proof-of-Concept*

PoET – *Proof -of-Elapsed Time*

PoS – *Proof-of-Stake*

PoW – *Proof-of-Work*

PPGTIC – Programa de Pós-Graduação em Tecnologias da Informação e Comunicação

PRISMA – *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*

P2P – *Peer-to-peer*

RPCA - *Ripple Protocol Consensus Algorithm*

SDK – *Software Development Kit*

SPB – *Secure Private Blockchain*

VM – *Virtual Machine*

WAN – *Wide Área Network*

SUMÁRIO

1 INTRODUÇÃO

Na última década, a tecnologia blockchain emergiu como o grande impulsionador de novos ecossistemas tecnológicos para startups, empresas e governos (XU et al. 2019). Suas aplicações incluem, entre diversas outras, serviços de saúde e financeiros, gerenciamento de cadeia de suprimentos, internet das coisas, computação e armazenamento de dados e energia (XU et al., 2019; GUO et al., 2021, REYNA et al., 2018).

Com o advento dos protocolos blockchain se tornou possível construir uma nova geração de aplicativos transacionais que garantem confiança, responsabilidade e transparência, enquanto agilizam processos de negócios e restrições legais (CHENG; LIN, 2018; EHMKE; WESSLING; FREDRICH, 2018). Os protocolos blockchain embarcam tecnologias como encriptação assimétrica, redes *peer-to-peer*, livros-razão distribuídos, contratos inteligentes, algoritmos de consenso e outras tecnologias assistivas, juntos, forjando um arranjo computacional de alta complexidade protegido por criptografia. A disrupção desta tecnologia tem como característica a descentralização e imutabilidade dos dados.

Maull et al. (2017) afirmam que o blockchain vem reescrevendo as noções convencionais de transações de negócios, criando novas oportunidades para geração de valor. Por causa de seu vertiginoso ritmo de crescimento, muitos pesquisadores vêm desenvolvendo estudos envolvendo a tecnologia, entre eles encontram-se algumas revisões de literatura, propostas de *frameworks*, novos protocolos, avaliações de desempenho, algoritmos de consenso alternativos, estudos experimentais e comparativos. Embora existam artigos que trazem conhecimento relevante, em grande parte eles focam em resolver determinado problema ou sugestão de melhoria em um processo muito específico (GUO et al., 2021).

Brilliantova e Thurner (2019) apresentam pesquisas sistematizando as opiniões de especialistas do setor sobre as possibilidades da tecnologia blockchain. Para o mercado de energia, uma das principais implicações da adoção da mesma é a exclusão de intermediários entre geração e consumo de eletricidade. Segundo os autores, é provável que a adoção da blockchain reduza o papel das concessionárias, varejistas e mercados atacadistas de energia. Essa troca de energia sem intermediários resulta em menor consumo de energia, menores custos para o consumidor final, uma vez que os varejistas (“intermediários”) ficam estimados em 20% acima do valor da energia. Além disso, a integração do blockchain impactaria os

modelos de preços existentes nos mercados de energia. Portanto, a adoção do blockchain pode resultar em preços menores de energia promovendo a modicidade tarifária.

Carson et al. (2018) estruturam os casos de uso de blockchain em seis categorias princjpais: registros estáticos, gerenciamento de identidades, contratos inteligentes, registros dinâmicos, infraestrutura de pagamentos e outros. Os autores ainda classificam esses casos de uso em suas duas funções fundamentais – manutenção e transação de registros. Segundo os pesquisadores algumas indústrias têm aplicações em várias categorias, enquanto outras estão concentradas em apenas uma ou duas delas.

Para Jersin (2018) o potencial da blockchain se tornar um novo protocolo de padrão aberto para registros, identidade e transações confiáveis não pode ser simplesmente descartado. A tecnologia Blockchain pode resolver a necessidade de uma entidade estar encarregada de gerenciar, armazenar e financiar um banco de dados. Ganne (2018) aponta que os verdadeiros modelos P2P podem se tornar comercialmente viáveis devido à capacidade do blockchain de compensar os participantes por suas contribuições com *tokens*, além de oferecer a eles participação em qualquer aumento futuro do valor. No entanto, a mudança de mentalidade necessária e a ruptura comercial desse modelo e suas implicações são grandes.

Segundo Zhang (2019) no curto prazo, o valor estratégico da tecnologia Blockchain está principalmente na redução de custos. Para o pesquisador, a tecnologia pode ter o potencial disruptivo de ser a base de novos modelos operacionais, mas seu impacto inicial será impulsionar a eficiência operacional. O custo pode ser retirado dos processos existentes, removendo os intermediários ou o esforço administrativo de manutenção de registros e reconciliação de transações. Isso pode mudar o fluxo de valor capturando receitas perdidas e criando novas receitas para provedores de serviços de blockchain. Com base na quantificação do impacto monetário, proposta por ele, dos mais de 90 casos de uso analisados, estimam que aproximadamente 70% do valor em jogo no curto prazo seja em redução de custos, seguido por geração de receita e alívio de capital.

Na pesquisa de Di Silvestre et al. (2020), é proposto uma ampla perspectiva sobre a aplicação da tecnologia blockchain na área de sistemas de energia, esclarecendo alguns aspectos técnicos relativos a essa promissora tecnologia, os recursos e aplicações desenvolvidas até o momento, com foco no futuro de aplicações inovadoras no setor de energia elétrica. Para os autores, apesar de tantos potenciais, a aplicação da tecnologia

blockchain no setor de energia elétrica ainda apresenta grandes desafios para os técnicos. As limitações destacadas são escalabilidade, *throughput* e os altos custos de energia associados a blockchains públicas baseadas em prova de trabalho. Além desses desafios, os autores citam a segurança, pois ainda é um fator que permanece sem ser comprovada até que ela cresça o suficiente para ser resiliente a ciberataques. Outro risco é a falta de flexibilidade, pois uma vez que as cadeias de blocos são implantadas, é necessário um apoio significativo das partes interessadas antes que grandes atualizações possam ser feitas. Além disso, existem requisitos de facilidade e privacidade do usuário não resolvidos em relação ao gerenciamento de chaves e gerenciamento de dados. Os possíveis desafios de aplicativos dizem respeito à estrutura do setor elétrico e ao escopo na operação da rede.

Neste contexto esta pesquisa fez uma abrangente revisão sistemática para o estado da arte buscando por estudos que trouxessem um modelo ou método genérico, técnico e científico de se analisar e avaliar soluções computacionais blockchain. Todavia, esta busca exploratória revelou que não existem trabalhos científicos desta natureza. Em pesquisas correlatas, encontrou-se apenas a árvore de decisão de Chowdhury et al. (2018) utilizada na qualificação de projetos quanto a utilização ou não de blockchain e o *framework* de Moezkarimi, Abdollahei e Arabsorkhi (2019) que busca avaliar o nível de completude de recursos oferecidos por uma plataforma blockchain. Sendo assim, identificou-se a falta de uma metodologia que pudesse auxiliar especialistas e profissionais de TI na tomada de decisão quanto à adoção de projetos utilizando a tecnologia blockchain. Um instrumento ou ferramenta que servisse de base para construção de conhecimento e que assistisse estes profissionais em discussões mais esclarecidas a respeito desta tecnologia.

Tal problemática se tornou evidente quando um consórcio de agentes do setor elétrico formado por CPFL Energia, Engie Energia e Comerc Energia idealizou uma solução computacional, como prova de conceito de software – PoC – (do inglês *Proof-of-Concept*) blockchain, para comercialização de energia elétrica no Ambiente de Contratação Livre (ACL). A PoC é um ambiente para transações de compra e venda de energia elétrica no ACL, onde essas operações são negociadas livremente a partir de contratos bilaterais entre as partes envolvidas. Todavia os agentes se depararam com os seguintes questionamentos. Quais indicadores são relevantes? O que é necessário avaliar? A solução computacional desenvolvida atende a necessidade dos agentes envolvidos? Desta forma, observaram que

necessitavam de uma metodologia técnica e científica capaz de analisar, avaliar e dar um parecer acerca da aplicação desenvolvida.

Diante a esta perspectiva analisada, surge a pergunta: **Como avaliar técnica e cientificamente soluções computacionais utilizando a tecnologia blockchain?**

Considerando esta pergunta de pesquisa pontuou-se as seguintes hipóteses:

a) Pode-se analisar e avaliar, técnica e cientificamente, soluções computacionais utilizando a tecnologia blockchain através do desenvolvimento de um instrumento (método ou framework) computacional.
b) Pode-se analisar e avaliar, técnica e cientificamente, qualquer tipo de solução computacional, independente da aplicação, utilizando este instrumento.
c) Pode-se utilizar indicadores qualitativos e qualitativos encontrados na literatura como referência para análise e avaliação de aplicações blockchain.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver uma metodologia para análise e avaliação técnico-científica de aplicações blockchain.

1.1.2 Objetivos Específicos

Para atender o objetivo geral os seguintes objetivos específicos são necessários:

a) Estudar métricas para avaliação de projetos baseados na tecnologia blockchain;
b) Definir métricas, indicadores, parâmetros computacionais para validar soluções computacionais blockchain;
c) Desenvolver a metodologia de análise, avaliação técnica e científica de aplicações blockchain;
d) Experimentar a metodologia desenvolvida em uma prova de conceito;

1.2 JUSTIFICATIVA

No estudo de Wang et al. (2019), os autores mostram resultados promissores no gerenciamento de sistemas de energia distribuída para obter esquemas de comércio de energia e gerenciamento de demanda utilizando contratos inteligentes. De acordo com os pesquisadores os benefícios deste sistema são apresentados como maior transparência, redução de custos operacionais e negociação mais eficientes. No entanto, segundo os autores, este modelo de comercialização ainda está em desenvolvimento em comparação com o modo tradicional de negociação de energia. Pois para eles o conhecimento da base técnica da tecnologia blockchain e seus recursos ainda é imaturo para se adaptar às estruturas existentes. Os autores citam que poucas plataformas realmente consideram a implementação de hardware no nível físico e essas limitações de hardware têm impacto significativo no design do sistema. Destacam também os problemas de escalabilidade das redes blockchain onde o rendimento das transações pode não suportar o comércio de energia de alta frequência. Concluindo que na conjuntura atual as propostas de aplicação da tecnologia carecem de um procedimento técnico que permita uma análise consistente das plataformas blockchains.

Abdella e Shuaib (2018), apresentam uma revisão dos principais tópicos de pesquisa em torno da comercialização de energia e identificam que um dos principais obstáculos enfrentados na implantação deste modelo de negócio está na escolha da plataforma blockchain. Para eles até o momento, não está claro qual das plataformas é mais apropriada para os modelos de comercialização que vem sendo projetados. Segundo os pesquisadores, investigar e identificar qual solução blockchain é melhor para o ambiente de comércio de energia, levando em considerações várias propriedades, como escalabilidade, custo, eficiência computacional, tempo de resposta da transação, tamanho da transação, segurança e reversibilidade ainda é uma questão em aberto.

Maslin, Watt e Yong (2019) apresentam os desafios encontrados ao se pesquisar tecnologias digitais emergentes. Segundo os autores apesar da incerteza persistente sobre a capacidade das soluções blockchain para resolver os problemas de amanhã, o corpo de pesquisas nessas tecnologias está crescendo. No entanto, este é um campo dinâmico e especialistas com conhecimento especializado do design, uso e implicações da tecnologia são tão diversos quanto as plataformas nas quais suas contribuições são distribuídas. Um desafio

importante para os pesquisadores é, portanto, localizar informações valiosas e disponíveis publicamente. Para os pesquisadores, embora os especialistas em produtos e setores estabelecidos sejam facilmente identificados, os especialistas em tecnologias digitais emergentes não são, consequentemente, analisar e avaliar estas tecnologias não é uma tarefa trivial.

Examinando o estado da arte, pode-se observar que existe um consenso entre os autores com relação ao fato de que plataformas blockchains aplicadas ao mercado de energia elétrica promovem o processo de digitalização do setor, contribuindo para uma dinâmica contemporânea, desburocratizada e eficiente na cadeia de geração, transmissão, distribuição e comercialização e uso final da energia elétrica. Todavia, a imaturidade da tecnologia blockchain somada a escassez de profissionais capacitados para conceber e gerir soluções computacionais blockchain promove insegurança e incerteza quanto ao alcance dos objetivos esperados para novos projetos.

Hodiernamente existem variadas plataformas blockchains para os mais diversos propósitos e se desconhece como analisá-las e avaliá-las de modo a selecionar a mais adequada para uma determinada aplicação. Identificar se a mesma atende aos requisitos do projeto, se, por exemplo, oferece escalabilidade, resiliência e desempenho adequados, se atende aos critérios mínimos segurança e privacidade e ainda se a mesma dispõe de características técnicas como tamanho do bloco e tamanho da transação extensíveis ou configuráveis.

Desta forma este trabalho procurou preencher esta lacuna no que diz respeito ao *know-how* da tecnologia blockchain desenvolvendo uma metodologia para análise e avaliação técnico-científica de aplicações blockchain, experimentando a mesma em um estudo de caso do setor elétrico brasileiro.

1.3 ESCOPO DO TRABALHO

O intuito da pesquisa é estudar, definir e implementar quais qualificadores técnicos podem ser utilizados na construção de uma metodologia que permita a avaliação de soluções Blockchain aplicadas no setor elétrico. Busca-se, avaliar a viabilidade técnica e funcional estabelecendo um conjunto de indicadores que melhor caracterizam a aplicabilidade,

escalabilidade, funcionalidade e sustentabilidade de aplicações blockchain, assim como indicadores que permitem melhor identificar e antecipar pontos de inflexão ou de falha, suas limitações técnicas computacionais e operacionais.

Este estudo, contempla também, uma fase de experimentação da metodologia, onde o método será aplicado na avaliação de uma prova de conceito utilizando a tecnologia blockchain Corda no ambiente de comercialização de energia em uma companhia do setor elétrico.

Entre o público-alvo desta pesquisa, encontram-se o governo, agentes e instituições do setor elétrico, universidades e profissionais da tecnologia da informação.

1.4 ADERÊNCIA AO PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

O Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) busca resolver problemas de características interdisciplinares por intermédio das tecnologias computacionais (PPGTIC, 2018). Ele tem como área de concentração Tecnologia e Inovação, divida em três linhas de pesquisa, a saber: Tecnologia Computacional, Tecnologia, Gestão e Inovação e Tecnologia Educacional.

Esta pesquisa se integra ao programa na linha da Tecnologia Computacional. De acordo com PPGTIC (2018) o objetivo dos trabalhos “desta linha de pesquisa é desenvolver modelos, técnicas e ferramentas computacionais auxiliando na resolução de problemas de natureza interdisciplinar”. A contribuição social do programa também ocorre através do desenvolvimento de pesquisas de base tecnológica aplicada nas áreas de educação, gestão e inovação.

As características técnicas e científicas, que podem ser observadas ao longo deste trabalho, evidenciam a aderência desta dissertação ao PPGTIC. Assim, o desenvolvimento de uma metodologia para análise e avaliação técnico-científica na utilização da tecnologia blockchain, faz uso de tecnologias computacionais inovadoras, o que vai de encontro a proposta de interdisciplinaridade da linha de pesquisa, do programa e de outros trabalhos desenvolvidos dentro do PPTIC, como Rosa (2020).

Além do alcance tecnológico, pode-se destacar o impacto econômico obtido pela pesquisa, uma vez que a metodologia desenvolvida pôde compor um parecer sobre como uma aplicação blockchain com a finalidade de mitigar os custos dos seguros contratuais no ambiente de comercialização de energia se demonstra uma solução financeiramente atrativa.

Cabe destacar que a metodologia desenvolvida e seu instrumento de aplicação serão disponibilizados livre e publicamente, ficando a disposição das empresas do setor elétrico, centros de pesquisa, universidades, governo e comunidade.

Este estudo também colaborou de forma significativa para que as empresas participantes da pesquisa e seus parceiros pudessem compreender melhor esta nova tecnologia, vislumbrar novas aplicações e fomentar futuros projetos de pesquisa para a universidade.

Complementarmente, este trabalho, além de contribuir para o avanço da ciência nacional, também procurou inovar internacionalmente, pois como será apresentado no Capítulo 3 – Estado da Arte, não foi encontrado no Brasil e no mundo uma metodologia similar ou equivalente para avaliação de aplicações blockchain.

1.5 METODOLOGIA

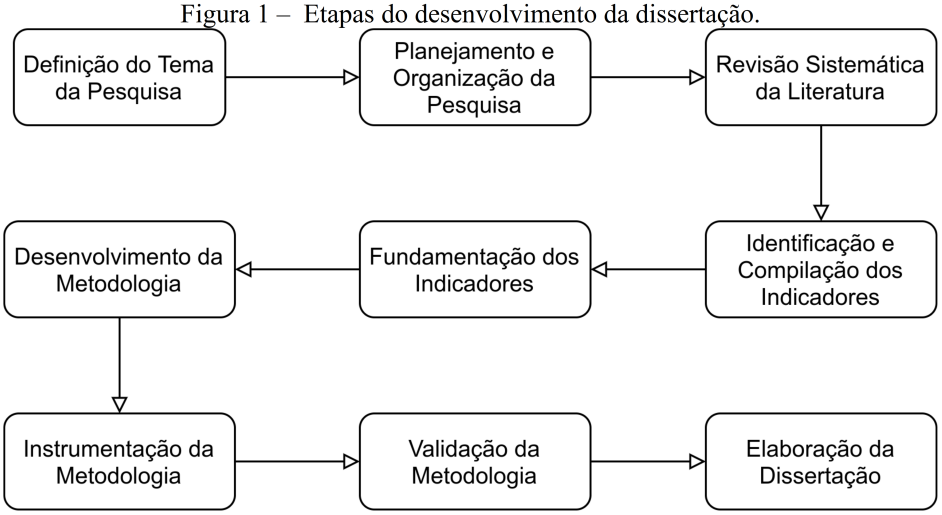
Para Silva e Menezes (2005), a pesquisa é um trabalho em processo não totalmente controlável ou previsível. Adotar uma metodologia significa escolher um caminho, um percurso global do espírito. O percurso, muitas vezes, requer ser reinventado a cada etapa. A Metodologia tem como função mostrar a você como andar no “caminho das pedras” da pesquisa, ajudá-lo a refletir e instigar um novo olhar sobre o mundo: um olhar curioso, indagador e criativo.

A construção deste trabalho seguiu uma metodologia de pesquisa baseada, fundamentalmente, nos critérios classificados e apresentados a seguir. Pode-se observar também, de forma sumária, na Figura 1, os pontos principais e o fluxo da pesquisa.

Quanto à área de conhecimento, classifica-se como interdisciplinar, mantendo afinidade com a proposta do PPGTIC, através do desenvolvimento de metodologias, técnicas, processos ou ferramentas computacionais que auxiliarão na resolução de problemas de caráter

interdisciplinar (PPGTIC, 2018). Permeando conhecimentos por várias disciplinas como Engenharias, Ciência da Computação e Tecnologias da Informação e Comunicação.

Figura 1 – Etapas do desenvolvimento da dissertação.



Fonte: Elaborado pelo autor.

Quanto à natureza, trata-se de uma pesquisa aplicada, pois, segundo Silva e Menezes (2005), "objetiva gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos". Visto que, os resultados obtidos serão utilizados na avaliação de uma solução Blockchain em operação em uma companhia do setor.

Quanto aos procedimentos técnicos, o referencial teórico está baseado na pesquisa bibliográfica que, do ponto de vista de Gil (2017), pode ser "elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e atualmente com material disponibilizado na internet". Por se tratar de um tema atual, a busca exploratória considerará também, importantes web sites relacionados à conferências, *journals* e relatórios técnicos, divulgados por comunidades e iniciativas blockchain, para coleta de publicações recentes e montagem do portfólio bibliográfico.

1.6 ESTRUTURA DO TRABALHO

A estrutura a ser apresentada nesta seção é o que se planeja para o desenvolvimento desta dissertação sendo constituída de 6 capítulos.

O capítulo 1 realiza a introdução do tema, os objetivos da pesquisa, além da justificativa, escopo e aderência ao programa.

O capítulo 2 aborda os conceitos computacionais aplicados para o desenvolvimento da pesquisa e da metodologia.

No capítulo 3 apresenta o estado da arte relativo a resultados relacionados a *benchmarks*, análises, avaliações ou desempenho de aplicações blockchain.

O capítulo 4 traz a metodologia desenvolvida. Apresentando o quadro dos indicadores compilados, suas fundamentações teóricas e o instrumento de análise e avaliação técnico-científico construído.

O capítulo 5 descreve a aplicação e experimentação da metodologia desenvolvida em um estudo de caso do ambiente de comercialização de energia do setor elétrico.

O capítulo 6 apresenta as considerações finais e os resultados obtidos a fim de prover subsídios para responder à pergunta da pesquisa e propor trabalhos futuros.

2 APORTES TEÓRICO-CONCEITUAIS

Buscando produzir conhecimento construtivo e argumentativo com esta pesquisa, se faz necessário a preleção de alguns conceitos e elementos que compõem e circundam as Tecnologias de Contabilidade Distribuída (DLTs)[1] e blockchains.

Apresentam-se e fundamentam-se, a seguir, as noções preliminares do estudo que auxiliarão no entendimento da pesquisa bem como a relação problema versus tecnologia.

2.1 FUNÇÕES DE *HASH* CRIPTOGRÁFICO

Uma função ***F*** de resumo criptográfico ou *hash* criptográfico é uma função matemática que recebe qualquer dado digital ***d*** (por exemplo, um arquivo texto, uma foto, etc) como entrada e calcula um número ***s = F(d)*** como saída. Chamaremos este número de saída ***s*** de ***hash*** daqui para frente. O *hash* ***s*** sempre tem a mesma quantidade de dígitos. Portanto, note que a quantidade de *hashes* distintos e possíveis $\mathbf{s_1 \neq s_2 \neq \ldots \neq s_k}$ é *finita* ($k = 10^n$, onde $n > 0$ é a quantidade de dígitos *decimais* do *hash*). Em contraste, a quantidade de dados digitais de entrada é *infinita*. Assim, espera-se que ocorram colisões, isto é, que existam dois dados de distintos $\boldsymbol{d \neq d'}$ tais que $\boldsymbol{F(d) = F(d')}$**.** Uma propriedade importante das funções de *hash* é ser *praticamente impossível* encontrar colisões.

Uma aplicação de funções de *hash* é auxiliar na verificação de integridade de arquivos. Relembrando, um arquivo é dito *íntegro* se ele *não foi modificado*. Assuma que você deseja manter um documento ***d*** em um computador público e se preocupa que ***d*** possa ser modificado sem sua autorização. Portanto, ao salvar o documento ***d*** pela última vez no computador, você calcula e anota o *hash* $\mathbf{s = F(d)}$ em um local seguro. No futuro, para verificar que ***d*** não foi modificado, ou seja, é o *mesmo* documento que você salvou, basta recomputar $\boldsymbol{s' = F(d)}$ e verificar que $\boldsymbol{s'}$ equivale ao *hash* ***s*** que você anotou anteriormente. Note que a probabilidade do documento salvo ***d*** e sua posterior modificação terem o mesmo

1 Segundo Natarajan (2017), *Distributed Ledger Technologies* ou DLTs referem-se à abordagem de rápida evolução no que diz respeito a gravação e compartilhamento de dados acerca de múltiplos bancos de dados (os *ledgers*). Essa tecnologia permite que transações e dados sejam gravados, compartilhados e sincronizados de forma descentralizada através de uma rede distribuída de participantes.

hash (isto é, ocorrer uma colisão) é *praticamente* nula. É comum na literatura autores se referindo ao *hash* **s = *F(d)*** utilizado para verificar integridade como *checksum*.

Outra propriedade importante das funções de *hash* é a seguinte. Possuindo *somente* um *hash* ***s*****,** é *praticamente* impossível descobrir um dado ***d*** tal que ***s = F(d).*** Uma aplicação desta propriedade é um sistema de autorização baseado em senhas. Quando você deseja se autenticar, você fornece uma senha ao sistema e ele compara se a senha fornecida é equivalente àquela previamente cadastrada no sistema. Para evitar que um invasor do sistema descubra sua senha, o sistema cadastra *somente* o *hash* de sua senha. Assim, quando você fornece sua senha, o sistema computa o *hash* da senha fornecida e verifica se ele equivale ao *hash* cadastrado. Note que um invasor do sistema não poderá descobrir sua senha a partir do *hash* cadastrado, pois é *praticamente* impossível encontrar a senha a partir do *hash* da senha.

As duas propriedades das funções de *hash* a) ser praticamente impossível encontrar colisões e b) ser praticamente impossível encontrar um dado a partir de um *hash* são suficientes para o leitor compreender este relatório. Existe outra propriedade importante para outros contextos. Caso o leitor tenha interesse em conhecê-la e suas aplicações, sugere-se a leitura de Schneier (2004) e Stinson (2006) respectivamente.

Um algoritmo de *hash* conhecido na literatura é o SHA-256. Ele foi proposto no ano 2000 como sendo uma nova geração de funções SHA, e em 2002 foi adotado como padrão FIPS[2] (do inglês *Federal Information Processing Standards*). O *hash* calculado pelo algoritmo tem tamanho de 256 bits e o algoritmo conta com uma função de compressão de 64 *rounds*[3]. Segundo Yoshida e Biryukov (2006), embora múltiplos estudos tenham sido feitos acerca da segurança do algoritmo, nenhuma fraqueza pôde ser encontrada para ele ou suas variantes até o momento. Ademais, nota-se que no momento de realização do atual estudo, o algoritmo SHA-256 pôde ser "quebrado", através de ataques, para apenas 46 de seus 64 *rounds*, mantendo sua segurança.

2.2 ESQUEMAS DE ASSINATURA DIGITAL

2 FIPS refere-se ao Padrão Federal de Processamento de Informações, uma norma do governo americano que descreve a criptografia e os requisitos de segurança relacionados com produtos do setor de tecnologia.
3 Rounds refere-se ao número de rodadas de execução da função de compressão.

Um esquema de assinatura digital consiste em três procedimentos. O primeiro procedimento cria um par de chaves: uma chave pública e outra privada. O segundo procedimento permite criar uma assinatura digital sobre um dado utilizando a chave privada. O terceiro procedimento permite verificar a assinatura sobre o dado a partir dele, da assinatura e da chave pública. Uma assinatura que pôde ser verificada com sucesso é dita *válida.* Um esquema de assinatura digital conhecido é o RSA, explicado e analisado a fundo em relação a segurança e eficiência conforme Buchmann (2004).

A chave privada é mantida em segredo para que somente seu detentor possa criar assinaturas. Em contraste, a chave pública é geralmente divulgada para que qualquer pessoa possa verificar uma assinatura. É praticamente impossível descobrir a chave privada a partir da pública.

Uma assinatura digital *válida* sobre um dado permite: a) afirmar que o dado não foi modificado após a assinatura (integridade); b) identificar que a assinatura foi criada pelo dono da chave pública (autenticidade); c) impedir que o signatário negue que criou a assinatura (não repúdio).

2.3 BLOCKCHAIN

Um livro-razão é uma ferramenta contábil que pode ser utilizada para apurar o saldo de contas. O livro-razão consiste de uma lista de transações. Uma transação é uma movimentação de recursos financeiros de uma conta para outra. Na literatura é comum se referir ao livro-razão como *ledger*.

A definição de blockchain apresentada a seguir é aquela introduzida por Nakamoto (2009) quando apresentava o Bitcoin. Um blockchain é um *ledger* digital onde somente pode-se adicionar novas transações. Não é possível alterar ou remover uma transação registrada. O blockchain é armazenado e atualizado de maneira *descentralizada.* Mais precisamente, voluntários chamados *nós* ou *nodos* armazenam réplicas do blockchain e as atualizam de modo a manter réplicas consistentes. A maneira é dita *descentralizada* pois não há um líder entre os voluntários instruindo como as atualizações devem ocorrer. Pelo contrário, os voluntários entram em consenso sobre as atualizações. A seguir detalham-se a construção do blockchain e a realização das atualizações.

Inicia-se com uma introdução sobre os participantes. Todo participante possui pelo menos um par de chaves. A chave pública do par serve para identificar *virtualmente* um participante e sua respectiva conta no *ledger*. Desconhece-se a identidade *real* de cada participante. Note que um participante pode ter inúmeras identidades virtuais e contas no blockchain. Diz-se que o blockchain oferece *pseudo-anonimato* aos participantes.

Os participantes se dividem em voluntários e usuários. Os voluntários são aqueles que mantêm o blockchain. Os usuários utilizam o blockchain para transacionar um ativo digital. Por exemplo, uma criptomoeda. Para isso, o usuário utiliza a chave privada, do par de chaves, para assinar uma transação autorizando que um ativo digital seja transferido de sua conta para a conta de outro usuário. Assinada a transação, o usuário deve enviá-la para os voluntários para que eles a adicionem ao blockchain. Dizemos que uma transação é válida se ela atende aos seguintes requisitos: a) a assinatura digital sobre a transação é válida; b) o emissor da transação tem saldo igual ao superior ao valor a ser transferido. Deve ser praticamente impossível para um usuário transferir o mesmo ativo para duas ou mais outras contas simultaneamente. Este tipo de transferência é conhecido na literatura *gasto duplo* e é considerado uma ameaça de segurança.

O blockchain consiste de uma sequência de blocos. Cada bloco contém uma lista de transações válidas e únicas. Uma mesma transação não ocorre em dois blocos distintos. A partir da lista de transações, é possível calcular o saldo atual de qualquer conta.

Adicionalmente, todo bloco, com exceção do primeiro, é criptograficamente *amarrado* ao bloco anterior. Mais precisamente, o *i-ésimo* bloco contém o *hash* do *i-1-ésimo* bloco, onde $i > 1$. Qualquer modificação num bloco, com exceção do último, pode ser percebida recalculando o *hash* do bloco alterado e comparando-o com o bloco seguinte. Por essa característica, diz-se que os dados gravados no blockchain são *imutáveis*. Portanto, é *praticamente impossível* remover transações registradas a fim de modificar o saldo final de uma conta.

Resta explicar como os voluntários atualizam o blockchain de modo consistente sem precisar de um líder. Para isso segue-se um *algoritmo de consenso* executado em rodadas da seguinte forma. A cada rodada um voluntário é escolhido para a) selecionar um conjunto de novas transações; b) verificar que as transações selecionadas são válidas; c) computar o *hash* do último bloco; d) criar um novo bloco contendo o *hash* computado e a lista de transações

válidas selecionadas; e) enviar o novo bloco para os demais voluntários. Os demais voluntários adicionam o novo bloco às suas réplicas do blockchain se e somente se: a) o novo bloco contém o *hash* do último bloco; b) o novo bloco contém somente transações novas e válidas. Perceba, todo bloco criado por um voluntário é conferido pelos demais. Portanto, o blockchain não depende que um voluntário específico seja confiável. Isso permite que usuários transacionem sem a necessidade de intermediários (DARIN; ASSUMPÇÃO, 2008).

A escolha do voluntário que cria o próximo bloco é fundamental para a segurança do blockchain. A título de análise, considere que o voluntário é escolhido por votação. Esta abordagem é insegura. Lembre-se que é impossível verificar a identidade *real* dos participantes e que um participante pode ter múltiplas identidades *virtuais.* Assim, não há como impedir que um participante utilize suas identidades *virtuais* para votar mais de uma vez.

Uma solução para o problema acima é oferecida pelo algoritmo de consenso conhecido por *Prova de Trabalho.* A cada rodada, todos os voluntários buscam uma prova de trabalho. Construir uma prova de trabalho requer uma busca ao acaso e dispende tempo. O primeiro voluntário a encontrar a prova de trabalho ganha o direito de criar o próximo bloco. Neste momento, os demais voluntários interrompem a busca e aceitam o novo bloco se ele a) contém o *hash* do bloco anterior; b) contém somente transações válidas; e c) contém a prova de trabalho encontrada. Caso contrário, continuam buscando a prova de trabalho.

Encontrar a prova de trabalho consome tempo, recursos computacionais e energia elétrica. Possuir distintas identidades virtuais em nada ajuda a encontrar a prova de trabalho e ter direito de propor o próximo bloco. Para compensar os custos de encontrar a prova de trabalho, o protocolo recompensa financeiramente o voluntário, lhe oferecendo a oportunidade de incluir no novo bloco uma transação especial criando e creditando um ativo digital para si mesmo. O custo da prova de trabalho atrelado à recompensa funciona como *incentivo* para os voluntários *somente* incluírem transações válidas no blockchain.

Como mencionado anteriormente, a descrição de blockchain segue aquela proposta pelo Bitcoin. Este tipo de blockchain é dito *público* pois qualquer indivíduo pode participar como voluntário ou usuário *sem comprovar sua real identidade*. Em contraste, existem blockchains *permissionados* onde participantes ou parte deles *devem comprovar sua identidade* (WALPORT, 2015). Neste tipo de blockchain, as provas de trabalho são

desnecessárias. Portanto, outros algoritmos de consensos podem ser aplicados (KOSTAREV, 2017; WALDMAN, 2018).

O assunto blockchain ainda é muito recente e tecnicamente surgiu da união de diversas tecnologias computacionais não sendo originalmente uma "nova" solução. Diante disso, muitos conceitos fundamentais são necessários para o entendimento desta tecnologia. Especificamente relacionado aos indicadores que serão apresentados neste estudo (Seção 4) faz-se necessário discorrer sobre algumas questões técnicas para o completo entendimento dos mesmos.

2.3.1 Tamanho do bloco

As transações em blockchains como o Bitcoin e o Ethereum são codificadas como sequências de *bytes* e armazenadas em blocos. O tamanho do bloco refere-se à capacidade *máxima* de armazenamento suportada por um bloco em determinada blockchain. Esta capacidade é definida em *bytes*. Por exemplo, no blockchain do Bitcoin as transações medem aproximadamente 250 *bytes* e os blocos podem medir *até* 1 MB (2^{20} bytes). Desta forma, um bloco pode armazenar por volta de 4.000 transações confirmadas (GOBEL; KRZESINSKI, 2017).

Cabe destacar que existem plataformas de contabilidade distribuída que utilizam bancos de dados de estados no lugar de blocos (ou de forma complementar ao blockchain) para registrar as transações. Entre as mais utilizadas atualmente estão o blockchain Corda e o Hyperledger Fabric.

2.3.2 *Throughput*

O *throughput* em um sistema blockchain pode ser entendido como a quantidade de transações que podem ser confirmadas por unidade de tempo. Comumente o *throughput* é representado em *transações por segundo* (TPS).

Em um blockchain o *throughput* depende, dentre outros fatores, da latência e do tamanho da transação e do tamanho e a frequência do bloco. No caso do Bitcoin, um novo

bloco é criado a cada aproximadamente 10 minutos, resultando em um *throughput* médio de 7 TPS (GOBEL; KRZESINSKI, 2017) e máximo de 10 TPS (TSCHORSCH; SCHEUERMANN, 2016).

2.3.3 Políticas de consenso

As aplicações comumente encontradas de blockchain privado são blockchains corporativos operadas por empresas ou entidades governamentais nas quais os usuários são conhecidos e credenciados, e possuem classes específicas de acesso de leitura e gravação. Exemplos destas aplicações incluem o Hyperledger, Ripple, Quorum e Corda. Cada uma destas plataformas, em versões empresariais, conduz seu processo de consenso adotando um mecanismo semelhante, porém, em particular diferente. De forma breve apresentam-se as políticas de consenso mais citadas na literatura.

Políticas de Endosso (Hyperledger Fabric): são recursos da tecnologia que permitem que os usuários definam políticas em torno da execução do código de um contrato inteligente. Essas políticas de endosso definem quais pares precisam concordar com os resultados de uma transação antes que ela possa ser adicionada ao *ledger*. Todo contrato inteligente possui uma política de endosso que especifica o conjunto de pares em um canal que deve executar o este contrato e endossar (avalizar) os resultados da execução para que a transação seja considerada válida. Como parte da etapa de validação da transação executada pelos pares, cada um dos pares de validação verifica se a transação contém o número apropriado de endossos e se eles são provenientes das fontes esperadas (ambos são especificados na política de endosso). As recomendações também são verificadas para garantir que sejam válidas (ou seja, assinaturas válidas de certificados válidos) (HYPERLEDGER, 2020d).

Validadores (Ripple): os validadores na rede Ripple são nodos (pares) que determinam se as transações atendem aos requisitos do protocolo e, portanto, são "válidas". Os validadores de serviço fornecem exclusivamente o agrupamento de transações em unidades solicitadas, concordando com um desses pedidos especificamente para evitar, principalmente, o gasto duplo (RIPPLE, 2020). Se um operador de nodo de validação assim escolher, ele também poderá votar em modificações da rede (*Amendments System*), taxas, reservas de carteira e outros fatores que afetam o *ledger*.

Serviços Notários (Corda): análogo a um agente cartorário, é um serviço de rede que fornece consenso de exclusividade, atestando que, para uma determinada transação, ele ainda não assinou outras transações que consomem qualquer um dos estados de entrada da transação proposta (CORDA, 2020). Ao ser solicitado a reconhecer uma transação, um serviço notarial pode a) assinar a transação se ainda não tiver assinado outras transações que consomem qualquer um dos estados de entrada da transação proposta ou b) rejeitar a transação e sinalizar que ocorreu uma tentativa de gasto duplo. Ao fazer isso, o serviço notário fornece o ponto final no estado do sistema. Até que a assinatura do serviço notarial seja obtida, as partes não podem ter certeza de que uma transação igualmente válida, mas conflitante, não será considerada como a tentativa "válida" de gastar um determinado estado de entrada. No entanto, após a obtenção da assinatura do serviço notarial, pode-se ter certeza de que os estados de entrada da transação proposta ainda não foram consumidos por uma transação anterior. Portanto, a notarização é o ponto final do estado do sistema.

2.3.4 Canais

Canais são estruturas de rede onde participam um subconjunto dos participantes de uma blockchain Hyperledger (HYPERLEDGER, 2020e). Um canal permite que o subconjunto comunique dados (e.g., transações) em sigilo (THAKKAR; NATHAN; VISWANATHAN, 2018). Isto é, quem não participa do canal não tem acesso aos dados trocados através dele. Canais são uma particularidade da tecnologia que estão presentes em alguns blockchains privados focados em soluções empresariais onde o nível de privacidade esperado é alto, como o Corda (redes de negócios) e o Hyperledger Fabric. Tal característica não existe, por exemplo, no blockchain do Bitcoin nem no Ethereum.

2.4 CONTRATOS INTELIGENTES

Szabo (1997) definiu um contrato inteligente como um software executado por computadores distintos que concordam com o resultado final da execução. Como tal, os contratos inteligentes operam como atores autônomos, cujo comportamento é completamente previsível. Contratos inteligentes podem ser usados para ajudar as partes que não confiam

uma na outra a celebrar um contrato sem depender de terceiros. Mais precisamente, as cláusulas do contrato são traduzidas para um contrato inteligente. Depois que as partes concordam com o contrato inteligente, ele é gerenciado por computadores. Neste ponto, as partes envolvidas não podem alterar o contrato inteligente nem interferir na sua execução.

A tecnologia Blockchain tem sido a infraestrutura necessária para executar contratos inteligentes. Mais precisamente, uma blockchain pode ser usada para armazenar e endereçar contratos inteligentes na forma de programas executáveis e imutáveis. Em contraste com as contas de blockchain, um contrato inteligente geralmente não é identificado por uma chave pública, mas por um *hash* do contrato inteligente. Uma transação endereçada a um contrato inteligente aciona sua execução pelos voluntários. Enquanto está sendo executado, um contrato inteligente pode mudar seu estado e originar novas transações. O histórico dos estados de um contrato inteligente, bem como as transações que ele recebeu e enviou, são armazenadas permanentemente no blockchain (PALMA; VIGIL; MARTINA, 2018).

2.5 PLATAFORMAS BLOCKCHAIN

O Bitcoin propôs o modelo precursor de blockchain. Entretanto, este modelo possui desvantagens. Por exemplo, o consumo de energia utilizado pelo algoritmo de consenso. Outro exemplo é que o modelo de blockchain do Bitcoin não suporta, nativamente, contratos inteligentes. A seguir apresentam-se modelos ou plataformas sucessores ao modelo proposto pelo Bitcoin. Nos referimos a essas plataformas, bem como aquela proposta pelo Bitcoin como Tecnologias de Contabilidade Distribuída.

2.5.1 Ethereum

O Ethereum é uma plataforma blockchain pública, lançada em 2015, que mantém a história de todas as transações dentro de uma rede P2P (do inglês *Peer-to-peer*). (NARAYANAN et al., 2016). Segundo Ferretti e D'Angelo (2019) a plataforma Ethereum pode ser considerada a principal blockchain programável do mundo. Nela os desenvolvedores podem construir uma gama de aplicativos descentralizados (*dapps*) utilizando sofisticados recursos dos contratos inteligentes com suporte nativo a moeda.

A plataforma Ethereum foi a primeira a introduzir o conceito de ativos digitais controlados diretamente por um código de computador que implementa regras arbitrárias, os contratos inteligentes, ou até mesmo controlados por uma Organização Autônoma Descentralizada baseada em blockchain, *DAOs*[4] (BUTERIN, 2015). Embora tenha sido promovido com uma blockchain pública, o código-fonte do Ethereum é open-source permitindo, a quem desejar, sua implementação em uma rede com controle de acessos, construindo assim uma blockchain privada.

2.5.2 Hyperledger Fabric

A plataforma blockchain Fabric é mantida pelo Projeto Hyperledger, um esforço colaborativo de código aberto criado para promover a tecnologia Blockchain para vários segmentos da indústria. O Projeto Hyperledger é uma associação global hospedada pela The Linux Foundation com mais de 130 membros, incluindo líderes em finanças, bancos, internet das coisas, cadeia de suprimentos, manufatura e tecnologia (SCHWENTKER, 2018). Com atualmente 16 projetos em andamento (Figura 2) o Projeto Hyperledger é uma comunidade de código livre focada no desenvolvimento de um conjunto de estruturas, ferramentas e bibliotecas estáveis para implantações de blockchain de nível empresarial. Ele serve como um local neutro para várias estruturas de livros distribuídos, incluindo Hyperledger Fabric, Sawtooth, Indy, bem como ferramentas como o Hyperledger Caliper e bibliotecas como o Hyperledger Ursa.

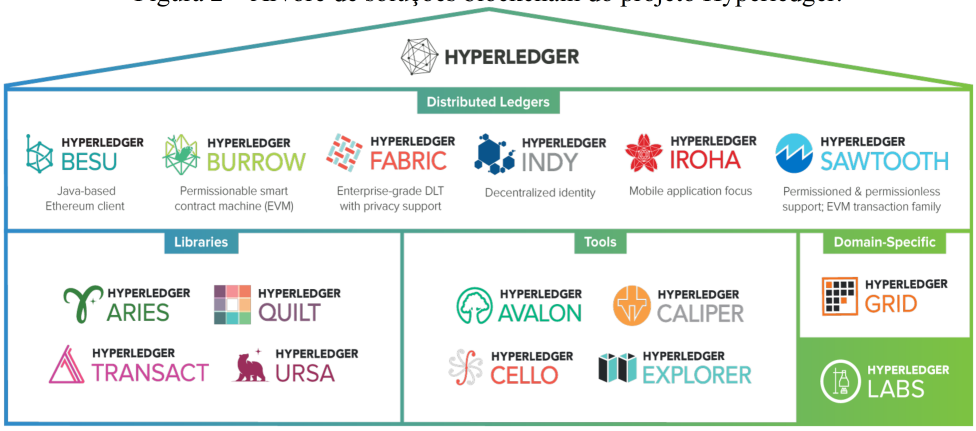
Essa iniciativa surgiu com o objetivo de atender aos requisitos do segmento corporativo que, segundo os membros, os atuais recursos das blockchain públicas seriam insuficientes em resolver, como escalabilidade e falta de suporte para transações privadas. A proposta do Hyperledger é justamente suprir esses requisitos a partir de uma série de casos de uso. Vale destacar que o Hyperledger tem o foco na indústria, mais especificamente nas relações B2B e B2C (HYPERLEDGER WIKI, 2020).

---

4 Uma Organização Autônoma Descentralizada ou DAO (do Inglês, *Decentralized Autonomous Organization*) é uma organização representada por regras codificadas como um programa de computador transparente, controlado pelos acionistas e não influenciado por um governo central. O registro de transações financeiras e as regras do programa de um DAO são mantidos em uma blockchain. Disponível em: https://en.wikipedia.org/wiki/Decentralized_autonomous_organization. Acesso em 05 de abr. de 2020.

O Hyperledger Fabric é uma plataforma de DLT de nível empresarial lançada em 2018 que oferece modularidade e versatilidade para uma ampla gama de casos de uso da indústria. A arquitetura modular do Fabric acomoda a diversidade de casos de uso de empreendimentos através de componentes modulares e de fácil utilização, como algoritmos de consenso, privacidade e serviços de filiação. (HYPERLEDGER, 2020b).

Figura 2 – Árvore de soluções blockchain do projeto Hyperledger.



Fonte: Hyperledger (2020a).

O Hyperledger Fabric é uma plataforma para soluções de contabilidade distribuída, sustentada por uma arquitetura modular que oferece altos níveis de confidencialidade, resiliência, flexibilidade e escalabilidade. Tal solução é projetada para suportar implementações conectáveis de diferentes componentes e acomodar as complexidades que existem em todo o ecossistema de DLT (HYPERLEDGER, 2020b). Para isso, utilizam-se diferentes canais que correm dentro da rede, bem como a divisão do trabalho, que caracteriza os diferentes nodos dentro da rede.

Como uma implementação de blockchain privada o Fabric conta com inúmeras propriedades únicas, dentre elas a possibilidade da geração de uma “rede de redes”, onde membros de diferentes redes com diferentes níveis de permissão e acesso podem atuar em conjunto e manter ainda assim sua privacidade e relacionamentos internos. Outras características da plataforma são sua flexibilidade na modelagem de contratos inteligentes, baixa latência de confirmação, suporte de múltiplas linguagens de contratos inteligentes (Go, Java, Javascript), suporte para EVM e Solidity, versionamento de contratos inteligentes e seu design visando operação contínua. (HYPERLEDGER, 2020c).

Inicialmente, o foco do Fabric estava centrado na indústria, entretanto, alguns casos de uso, relacionados ao gerenciamento de identidade ou propriedade, obtiveram grande sucesso e uniram adeptos ao desenvolvimento com apoio da Fundação Linux. Os projetos incluem, votação, dados de saúde, carteira para chaves privadas, identificação de cidadãos, propriedade intelectual, sistemas de credenciamento entre outros (HYPERLEDGER WIKI, 2020). Além disso, tais propostas, atualmente situam-se em estágio de incubação e compartilham suas soluções, permitindo sua clonagem para teste e experimentação.

2.5.3 Ripple

O Ripple é uma plataforma de pagamentos blockchain conhecido como XRP Ledger. Operando em uma rede P2P distribuída, o XRP Ledger enfrenta os mesmos desafios de outras moedas digitais na prevenção do gasto duplo de fundos e na garantia de consenso em toda a rede sobre o estado das contas e saldos dos usuários. Proposto pela primeira vez e depois implementado por Schwartz, Youngs e Britto (2014), o algoritmo subjacente ao XRP resolve esses problemas usando um protocolo de acordo tolerante a falhas bizantino sobre sub-redes coletivamente confiáveis, referido no *whitepaper*[5] como Ripple Protocol Consensus Algorithm ou RPCA (CHASE; MACBROUGH, 2018).

Abstratamente, a rede XRP Ledger é uma máquina de estado replicada. O estado replicado é o livro-razão mantido por cada nodo da rede e as transições de estado correspondem às transações enviadas pelos clientes da rede. Depois que os nodos concordam com os conjuntos de transações a serem aplicados ao estado, um protocolo de processamento de transações especifica regras determinísticas para ordenar as transações dentro de cada conjunto e como aplicar as transações para gerar o novo estado do livro-razão. Assim, o papel do RPCA é apenas fazer com que a rede chegue a um acordo sobre conjuntos de transações, não sobre o conteúdo ou o resultado dessas transações. Desde que os nós concordem com um conjunto de transações, o protocolo de processamento de transações garante que cada nodo gere um livro-razão consistente. Como um protocolo tolerante a falhas bizantino, o RPCA

5 *Whitepaper* refere-se ao documento que indica o problema que um projeto proposto (ou blockchain proposto) busca solucionar, a solução e uma descrição detalhada do produto, assim como sua arquitetura e suas interações com usuários. Disponível em: https://cointelegraph.com/ico-101/what-is-a-white-paper-and-how-to-write-it. Acesso em: 21 de maio de 2020.

deve operar mesmo na presença de participantes com falha ou mal-intencionados (CHASE; MACBROUGH, 2018).

Comparado a outros algoritmos de consenso descentralizados como prova de trabalho (PoW) ou prova de participação (PoS), o RPCA oferece menor latência de transação e maior rendimento. No entanto, sem um acordo uniforme sobre os participantes da rede, os usuários ainda precisam de uma maneira de determinar se sua escolha de pares de rede levará a um estado de rede consistente. Nesta configuração, cada usuário define individualmente uma lista de nós exclusiva ou UNL (*Unique Node List*), que é o conjunto de nodos cujas mensagens ele ouvirá ao tomar decisões sobre o estado da rede. É a interseção de qualquer par de UNLs de nodos corretos que determina a segurança da rede (CHASE; MACBROUGH, 2018).

2.5.4 Quorum

O Quorum foi desenvolvido pelo grupo JP Morgan como uma implementação privada e permissionada da plataforma Ethereum. O Quorum usa um algoritmo de consenso baseado em RAFT e atinge a privacidade de dados por meio da introdução de um novo tipo de transação “privada”.

A ideia básica por trás do Quorum é usar criptografia para evitar que todos, exceto aqueles que participam da transação, vejam dados confidenciais. A solução envolve um único blockchain compartilhado e uma combinação de arquitetura de software de contrato inteligente e customizações no Ethereum. Essas modificações na base de código do Ethereum incluem modificações na proposta de bloco e nos processos de validação. O processo de validação de bloco foi alterado de forma que todos os nodos validem as transações públicas e quaisquer transações privadas das quais eles façam parte, executando o código do contrato associado às transações. Para as demais “transações privadas”, um nodo simplesmente ignorará o processo de execução do código do contrato (QUORUM, 2018).

Isso resultará em uma segmentação do banco de dados do estado, ou seja, o banco de dados do estado é dividido em um banco de dados de estado privado e um banco de dados de estado público. Todos os nodos da rede estão em perfeito consenso de estado em seu estado público. Os bancos de dados privados de estado serão diferentes. Mesmo que o banco de

dados de estado do nodo cliente não armazene mais o estado de todo o banco de dados de estado global, o blockchain distribuído real e todas as transações nele são totalmente replicadas em todos os nodos e criptograficamente protegidos para imutabilidade (QUORUM, 2018).

2.5.5 Corda

Corda é uma plataforma blockchain criada pela empresa de tecnologia blockchain R3 LLC construída para registrar contabilmente transações sobre ativos financeiros (e.g., moedas, ações e títulos). Com o propósito de guardar e processar dados compartilhados, como contratos, foi projetado para implementar uma visão de contabilidade distribuída onde todo e qualquer ator econômico (empresas, indivíduos e máquinas) possa interagir, guardar e gerenciar seus acordos de forma segura, consistente, confiável, privada, auditável e autoritária, buscando otimização no nível de mercado, não de firmas (CORDA, 2018). O Corda foi concebido com

No Corda, diferentemente das plataformas blockchain apresentadas anteriormente que armazenam as transações em blocos, as transações são registradas como *states* (*estados)* em um banco de dados de *estados*. Estes estados representam os fatos compartilhados no livro-razão em um ponto específico de tempo, e podem representar qualquer objeto do mundo real, como ações, títulos de dívida, empréstimos e informações pessoais. *Estados* são objetos imutáveis, e consequentemente não podem ser modificados diretamente em reflexo de mudanças no mundo real. Para representar alterações e respostas ao mundo real então, os fatos "evoluem". Com a evolução dos fatos, novos *estados* vão substituindo os antigos, que são marcados como *históricos*. Outra forma de interpretar tal evolução é a análise de como os *estados* são substituídos, estes passam a ser marcados como gastos ou consumidos, que representam os *estados* com propósito de relatar transações, arquivamentos e auditoria. Os novos *estados*, marcados como não gastos ou não consumidos representam *estados* fungíveis disponíveis para gasto e estados lineares disponíveis para evolução ou transferência.

O Corda é uma rede privada e permissionada e composta por nodos, cada qual com uma instância do Corda e uma ou mais aplicações Corda (CorDapps) sendo executadas. Em contraste com tecnologias como o Bitcoin, as comunicações entre os nodos no Corda é feita

através de uma base de “necessidade de conhecimento”. Ou seja, as transações não estão acessíveis a todos os participantes conectados à rede, e sim, somente ao subgrupo dos participantes autorizados a recebê-las. Consequentemente, a comunicação não depende de transmissões globais. (R3, 2020). Somente os participantes envolvidos em um *estado* conhecem, acordam e assinam as transações para aquele *estado*. O Corda considera que uma transação é válida quando todos os participantes envolvidos assinam a transação. Não há validação da transação por terceiros através de um algoritmo de consenso. Para obter permissão e juntar-se a rede, um nó deve obter um certificado de um operador de rede. Este certificado mapeia a identidade conhecida do nodo (utilizada para representar este nodo em transações, por exemplo) para um IP e identidade legal no mundo real ou uma chave pública.

Segundo Nadir (2019), existem dois principais componentes na rede Corda, sendo eles o nodo Corda e o serviço de Notário. Os nodos são responsáveis por guardar a contabilidade e o serviço de Notário é uma forma de consenso portável que previne fraudes ligadas a realizar múltiplas transações envolvendo o mesmo ativo simultaneamente e também realiza a validação da transação. Notários são serviços plugáveis de rede que providenciam consenso de singularidade e o ponto de finalidade no sistema. Uma rede pode ter múltiplos notários com cada um rodando um algoritmo de consenso distinto. Serviços de notário podem ou não estar presentes nas transações.

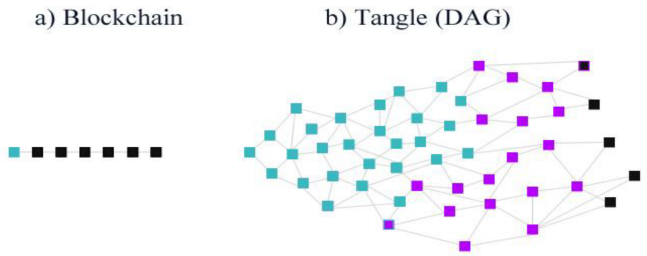
2.5.6 IoTa (Tangle)

Com o advento da tecnologia IoT (*Internet-of-Things*) e a incapacidade da Blockchain de resolver problemas de comunicação para esta nova tecnologia IoT, surgiu a IOTA (SILVANO; MARCELINO, 2020). Em 2016 Popov (2016) apresentou o documento que caracteriza a tecnologia por trás da IOTA, definindo também seus objetivos. O artigo nomeado “*The tangle*” indica que o projeto IOTA tem como foco oferecer uma infraestrutura de microtransações para o universo da IoT.

A IOTA tem uma abordagem diferente da tecnologia Blockchain, substituindo a Blockchain sequencial usada em sistemas como o Bitcoin (Figura 4), por um tipo de Grafos Acíclicos Dirigidos – DAG – (do inglês *Directed Acyclic Graph*) proposto e desenvolvido por seus fundadores, conhecido como Tangle (Figura 3). Na verdade a blockchain é

essencialmente uma versão restrita de um DAG, permitindo conexões apenas em uma única trajetória (RASCHENDORFER, 2019).

Figura 3 – Arquitetura blockchain tradicional *vs* IOTA–Tangle.



Fonte: Popov, 2016.

A Fundação IOTA traz uma tecnologia mais eficiente em valores energéticos, bem como aumenta a velocidade de transação e abre a possibilidade de transacionar valores e dados sem custo. Em vez de encadear as transações de maneira linear, como no Blockchain tradicional, cada nova transação na rede IOTA confirma duas transações anteriores, dessa forma sempre que um participante quiser adicionar uma nova transação ao Tangle-IOTA, seu remetente deverá aprovar duas transações previamente anexadas. Quanto mais transações anexadas a uma nova transação forem aprovadas, maior será a confiança na validade da transação. Com isso, o protocolo elimina a necessidade de mineradores da rede. (POPOV, 2016). O custo de uma transação envolve apenas o custo computacional para validar outras duas transações, ou seja, não há taxa de transação, o que é criticamente importante para o ecossistema IoT (SARFRAZ, 2019).

3 ESTADO DA ARTE

Uma busca sistemática foi realizada em 10 bases de dados científicas: IEEEXplore, EBSCO, Scopus, Gale, ScienceDirect, ResearchGate, SpringerLink, Wiley Online Library e Web Research. O IEEEXplore foi escolhido devido à sua importância estratégica para o domínio do tema blockchain, em particular, na área computacional e no setor elétrico. As pesquisas bibliográficas foram realizadas em março de 2020.

A escolha de palavras-chave para a pesquisa foi determinada concatenando pares de palavras nos domínios de interesse. O processo sistemático de pesquisa contou também com a utilização de caracteres curinga (*) visando ampliar o resultado das buscas. Os critérios de pesquisa utilizados foram: ***blockchain AND benchmark*, blockchain AND evaluat*, blockchain AND analys* e blockchain AND performa*.***

Cada par de palavras-chave pesquisadas nos respectivos bancos de dados e os resultados foram inseridos em uma matriz de síntese no documento Microsoft Excel. Seguiu-se a diretriz PRISMA[6], como mostra a Figura 4.

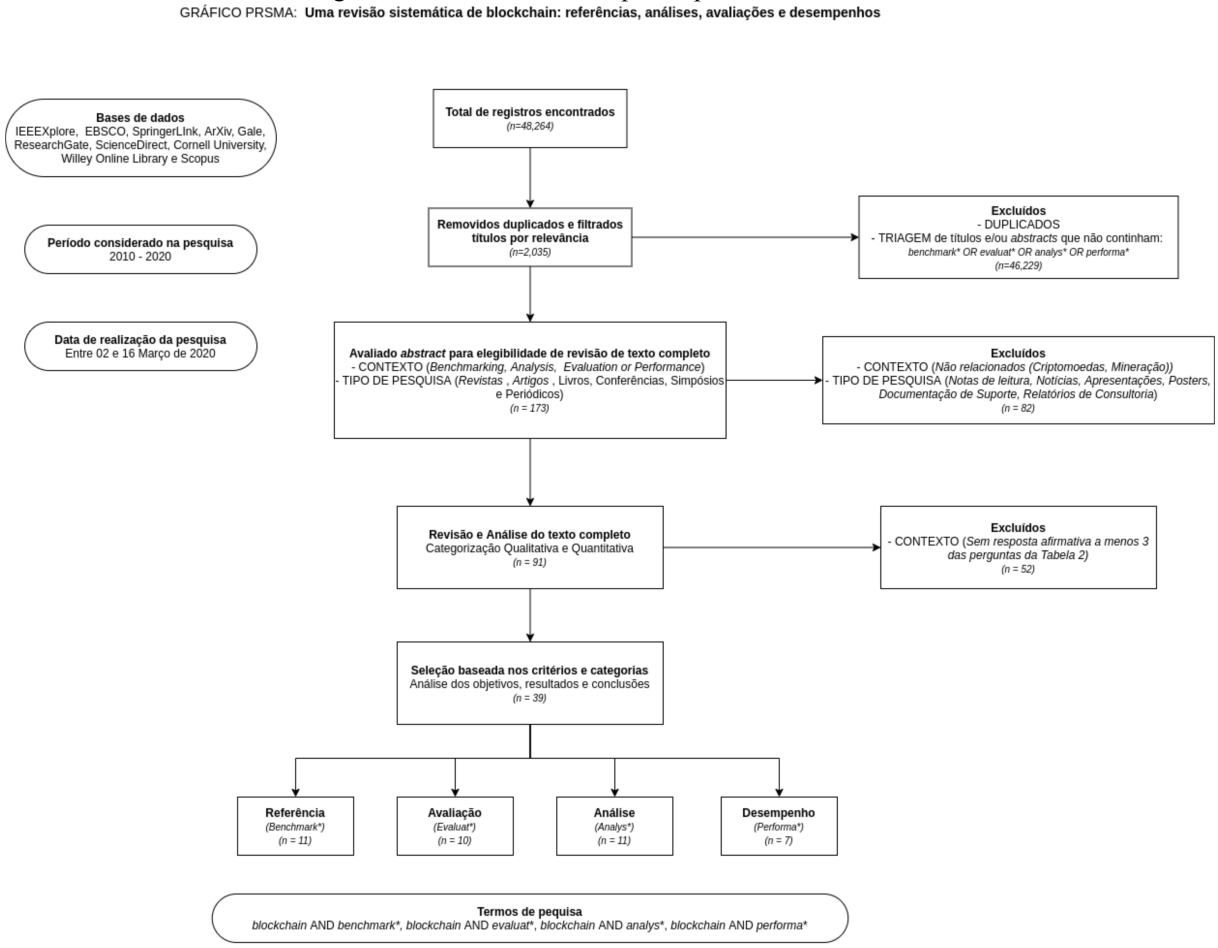
A popularidade da tecnologia blockchain começou após o lançamento do Bitcoin em 2009 e seu propósito inicial se concentrou no uso da blockchain no setor financeiro. A aplicação em outros setores, incluindo as avaliações, análises e trabalhos publicados relacionados, não era comum antes de 2010, isso justifica o período coberto por esta revisão, que é entre janeiro de 2010 e março de 2020. Onde o banco de dados permitia, todos os metadados foram selecionados para os critérios de busca e onde não era possível foi usada a melhor opção de pesquisa (palavra-chave, título e resumo).

Conforme pode ser verificado no gráfico prisma da Figura 4, foram encontrados 48.264 resultados nas buscas em todas as bases de dados. Na primeira triagem foram descartados os itens duplicados e os que não apresentavam no resumo relação com os critérios de busca, filtrando apenas os resultados relacionados a *benchmarks*, análises, avaliações ou desempenho de aplicações blockchain. Após esta etapa restaram 2.035 documentos. Na

6 PRISMA refere-se a "Principais itens para relatar Revisões sistemáticas e Meta-análises", uma recomendação criada em uma conferência em Ottawa, Canadá, em junho de 2005 atendida por 29 participantes, incluindo autores de revisões, metodologistas, clínicos, editores e um consumidor com finalidade de revisar e expandir o *checklist* e o fluxograma QUORUM (Qualidade dos Relatos de Meta-análises, guia criado em 1996 para tratar sobre subaproveitamento dos relatos de meta-análise). A recomendação PRISMA consiste basicamente em um *checklist* com 27 itens e um fluxograma de 4 etapas. (GALVAO; PANSANI; HARRAD, 2015).

segunda apuração foram descartados os itens relacionados a criptomoedas, mineração, algoritmos de consenso, desenvolvimento de contratos inteligentes entre outros, que não apresentavam associação ao escopo da pesquisa. Também foram descartadas as notas de leitura, notícias, apresentações, posters, documentação de suporte e relatórios de consultoria.

Figura 4 – Gráfico PRISMA para o processo de revisão.



Fonte: Elaborado pelo autor.

Mesmo realizando a filtragem da segunda etapa o número de documentos resultante ainda era grande (2.035 itens). Sendo assim aplicou-se outro filtro considerando o índice *h-index* do meio de publicação, o tipo de blockchain utilizado e o tipo de aplicação da tecnologia. Nesta filtragem também selecionaram-se os trabalhos que apresentavam o maior número de ocorrência dos critérios de busca por documento e foram descartadas publicações similares. Foi definido um limite de 50 publicações para leitura de resumos por critério de busca, bem como um mínimo de 10 selecionados, com exceção ao critério de busca

blockchain AND performa*, onde foram selecionados apenas 7. O que gerou a exceção foi o fato de que muitos dos resultados considerados relevantes retornados na consulta deste já haviam sido selecionados nos critérios de busca anteriores.

Neste momento resultaram 173 trabalhos distribuídos nos quatro critérios de busca e que se enquadravam nas condições de seleção definidas anteriormente. Realizou-se então a leitura dos resumos deste montante filtrando-os por contexto e tipo de pesquisa, como apresentado na Figura 1, restando 91 trabalhos selecionados. Esses então foram lidos na íntegra e, durante a leitura completa, foram filtrados aplicando as perguntas de elegibilidade apresentadas no Quadro 1. Nesta etapa mais 52 trabalhos foram descartados.

Quadro 1 – Perguntas de verificação para revisão de qualidade do *abstract* e do texto completo.

#	**Pergunta**	**Resposta**
P1	A publicação estuda referências, análises, avaliações ou desempenho de blockchain?	Sim/Não
P2	A publicação cita os critérios e os quantifica?	Sim/Não
P3	A publicação cita os critérios porém não os quantifica?	Sim/Não
P4	A publicação faz comparativo entre blockchains	Sim/Não

Fonte: Elaborado pelo autor.

O resultado final no funil da pesquisa, filtrando os registros de significante relevância, foram 39 publicações distribuídas em 11 de referências e de análises, 10 de avaliações e 7 de desempenho. O intuito da pesquisa era identificar indicadores e critérios técnicos que pudessem servir de métricas para construção de uma metodologia capaz de analisar e avaliar uma implementação blockchain independente da aplicação a qual ela fosse destinada. Desta forma optou-se, sobretudo, por considerar publicações que envolviam questões técnicas pertinentes à tecnologia blockchain, abstraindo suas aplicações.

Para atribuir coerência e coesão de forma geral aos números da pesquisa nas bases de dados, algumas considerações devem ser ponderadas:

a) O acentuado número de registros retornados nas buscas iniciais justifica-se pela concatenação do caractere curinga (*) às palavras-chave;
b) Observou-se uma considerável soma de registros duplicados, devido aos mesmos serem indexados por mais de uma base de dados;

c) Foi constatado o predomínio de publicações voltadas ao estudo de aplicações e implementações da tecnologia blockchain, e;
d) Observou-se uma significativa quantia de obras relacionadas a criptomoedas e mineração utilizando blockchain públicas.

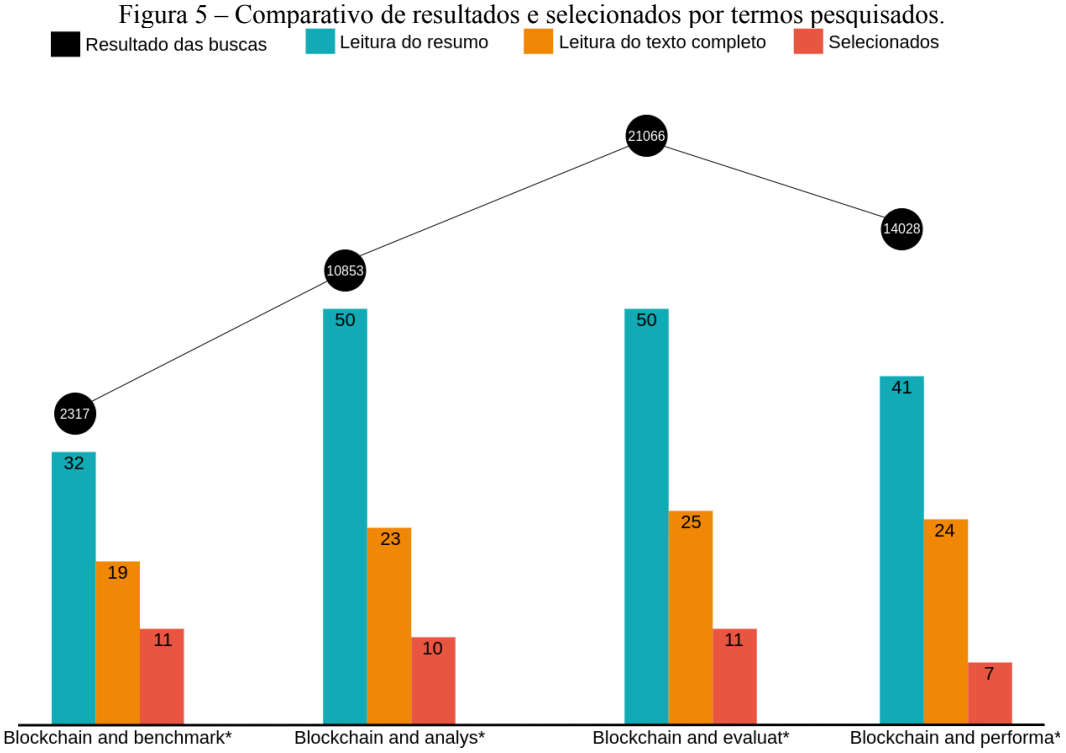
Métricas de qualidade: para garantir a qualidade do processo de revisão, as perguntas P1, P2, P3 e P4 do Quadro 1 serviram como métricas de verificação de qualidade para cada etapa da revisão. O título, as qualidades de revisão de resumo e de texto completo foram filtrados com essa métrica, como apresentado na Figura 4.

3.1 ORGANIZAÇÃO DA PESQUISA

Do número total de documentos considerados, que estudam referências, análises, avaliações ou desempenho de tecnologias blockchain, 173 tiveram os resumos lidos. Em 91 destes realizou-se a leitura do texto completo, e então 39 foram selecionados para composição desta pesquisa. Essas proposições amplamente incluíram a adoção da tecnologia em variados domínios de aplicação, contudo o objetivo deste estudo trata de procurar e identificar quais possíveis indicadores técnicos poderiam ser utilizados na definição de uma metodologia capaz de analisar e avaliar uma implementação blockchain independente de sua destinação final.

Observa-se na Figura 5 que se definiu o limite de 50 artigos para leitura de resumos por conjunto de palavras-chave, bem como um mínimo de 10 selecionados, com exceção ao termo ***blockchain AND performa****, onde foram selecionados apenas 7. O que motivou a seleção abaixo foi o fato de que muitos dos resultados considerados relevantes retornados na consulta deste já haviam sido selecionados e/ou analisados nos grupos de palavras-chave anteriores. Analisando ainda os apontamentos contábeis do gráfico, em somatório, foram lidos 173 resumos, deste montante, 52,60% seguiram para leitura do texto completo e desta segunda triagem foram selecionados 42,85%.

Figura 5 – Comparativo de resultados e selecionados por termos pesquisados.

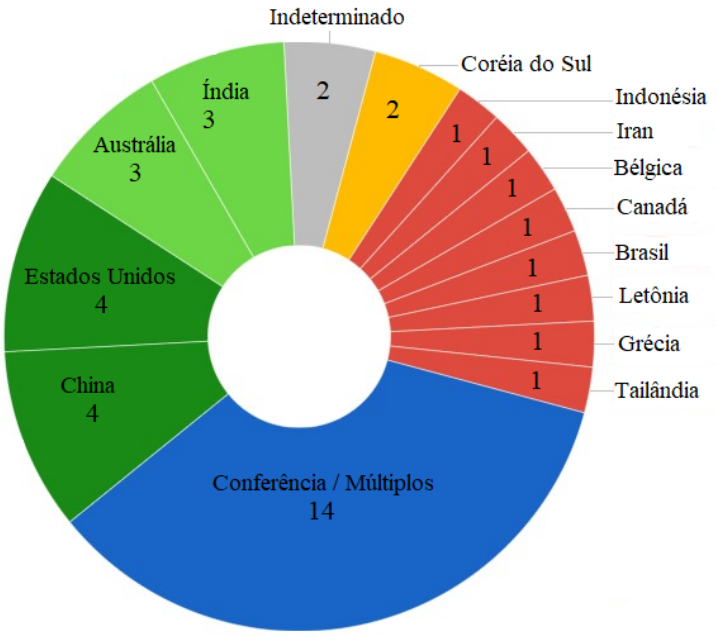


Fonte: Elaborado pelo autor.

3.2 DISTRIBUIÇÃO GEOGRÁFICA

Com relação à distribuição geográfica das publicações selecionadas, apurado na Figura 6, constatou-se que a maioria delas advém de conferências, simpósios, congressos entre outros eventos científicos que concentram autores de várias nacionalidades, não sendo possível determinar precisamente suas origens étnicas. Contudo, pode-se destacar, como esperado, a liderança de China e Estados Unidos, ambos com 4 trabalhos selecionados. Pode-se inferir também que a comunidade científica mundial vem buscando vigorosamente por conhecimento acerca da tecnologia blockchain e suas aplicações, haja vista que se observam estudos sendo desenvolvidos em todos os continentes, com exceção ao africano.

Figura 6 – Distribuição geográfica dos documentos selecionados.

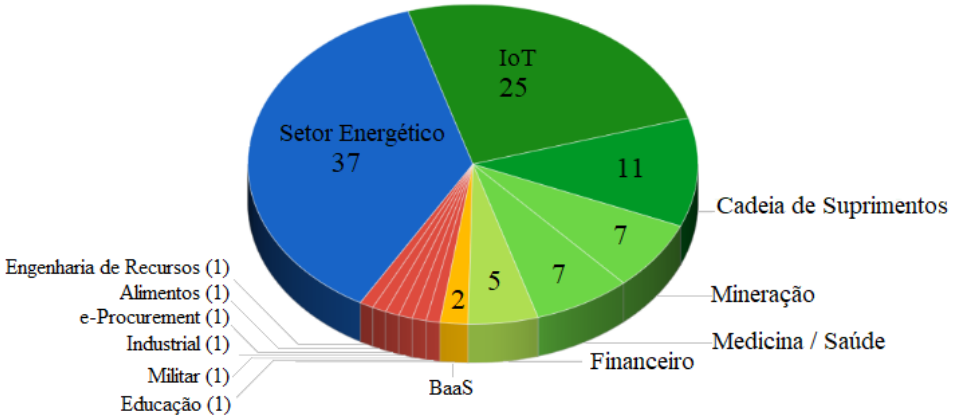


Fonte: Elaborado pelo autor.

3.3 SEGMENTOS DE APLICAÇÃO

Dentre os grupos mostrados na Figura 7 pode-se ir mais a fundo e analisar as aplicações específicas dos mesmos, como por exemplo *Smart Grids*, trocas de energia P2P e discussões acerca de Veículos Elétricos para o Setor Energético, ou Testes de Capacidade, Análise de Sistemas Sem Fio, Análises de Segurança e Performance e Integração com Ajuda Humanitária e Cadeia de Suprimentos no caso do IoT.

Figura 7 – Distribuição funcional dos artigos lidos.



Fonte: Elaborado pelo autor

Nota-se também grande foco em análises e avaliações de diversas plataformas blockchain, muitas vezes de forma comparativa e sob diversos escopos, como Tempo Real, Operação em Nuvem e Análise de Tempo Discreto, ou para funções específicas, como Setor Médico, Financeiro, *Smart Contracts*, Bancos de Dados Relacionais e Setor *Mobile*.

Analisou-se também os documentos em relação a aplicações da blockchain, e nota-se majoritariamente discussões ligando blockchain ao Setor Energético (n = 37) e ao conceito de Internet das Coisas – IoT (n = 25).

3.4 AVALIAÇÕES DAS TECNOLOGIAS BLOCKCHAIN ENCONTRADAS

Embora o escopo desta pesquisa seja a experimentação da metodologia no setor elétrico, mais especificamente em um estudo de caso da aplicação da tecnologia blockchain no sistema de comercialização de energia elétrica, o desenvolvimento deste estudo inaugural não se limitou na busca por publicações relacionadas ao setor elétrico nem ao mercado de energia elétrica. Tal comportamento da pesquisa deu-se por se considerar necessário desenvolver uma metodologia ampla e genérica capaz de analisar, avaliar e/ou mensurar o desempenho de soluções computacionais baseadas em blockchain.

Ao optar-se por explorar a revisão sistemática abstraindo a aplicação destinada da tecnologia, conseguiu-se identificar um número maior de indicadores, bem como ampliar os horizontes da pesquisa. Foi possível inferir também quais indicadores estão mais ou menos conectados ao tipo de aplicação ou a plataforma blockchain utilizada. Além disso se obteve um nível mais abrangente e profundo de conhecimento técnico e científico acerca destes indicadores.

Os recursos técnicos das plataformas blockchain são divididos em recursos funcionais e não funcionais. Para Moezkarimi, Abdollahei e Arabsorkhi (2019) recursos funcionais, como indicadores de consenso, estrutura de blockchain, bloco e transação, ativos nativos e tokenização, extensibilidade, segurança e confidencialidade, códigos-fonte, gerenciamento de identificadores e, finalmente, sistemas de recompensa e incentivo foram examinados.

Hintzman (2017) considera o objetivo ou aplicação de uma blockchain como o indicador mais relevante a ser percebido na avaliação da tecnologia. O pesquisador acredita

que diferentes objetivos na implementação da blockchain podem levar ao desenvolvimento de uma variedade de plataformas e, portanto, o primeiro indicador de avaliação deve ser o esclarecimento do objetivo da implementação da blockchain. O parâmetro seguinte seria a facilidade de participação no blockchain usando a plataforma fornecida pela tecnologia. Por exemplo, o pré-requisito para ingressar em uma rede de algumas das cadeias de blocos é que o nodo em questão seja um nodo completo; enquanto em outras instâncias da blockchain, os usuários também podem se conectar através de nodos leves (*light nodes*). Ainda segundo o pesquisador, o próximo indicador é o tipo de blockchain ser público ou privado e se a plataforma é de código aberto ou software proprietário.

De acordo com Moezkarimi, Abdollahei e Arabsorkhi (2019) outro referencial é a governança da blockchain que especifica quem e como lidar com o domínio e as regras da blockchain, quem gerencia o acesso ao ecossistema e se os usuários entenderão quem toma essas decisões. Outro indicador importante é o desempenho da plataforma blockchain. Considerando a natureza desse indicador e para estimá-lo, é possível combinar métodos como medir a velocidade de aceitação da transação na rede, a quantidade de largura de banda usada na rede, a quantidade de dados necessários para armazenar na rede e como armazenar dados na blockchain. Ainda segundo Moezkarimi, Abdollahei e Arabsorkhi (2019), outros indicadores que devem ser medidos em uma avaliação de plataforma são a velocidade de adicionar blocos à blockchain, o tamanho dos blocos e transações, bem como a taxa de manipulação de transações.

Em 2018 Grakov (2018) realizou um estudo comparativo entre as plataformas blockchain mais difundidas até então. Na pesquisa foram analisados indicadores que incluem recursos disponíveis, linguagem de programação, modelos de licenciamento de código, modelo e algoritmo de consenso, estrutura de implementação de contratos inteligentes, governança de plataforma, moeda nativa, tipo de blockchain, tempo de confirmação de transação, taxa de transação e confidencialidade.

Na pesquisa conduzida por Dinh et al. (2017) ponderam-se indicadores como o número de transações por segundo (TPS), o tempo médio de transação (latência), a tolerância a faltas por indisponibilidade do nodo, a escalabilidade por número de nodos e cargas de trabalho para a plataforma privada estudada.

Macdonald, Liu-Thorrold e Julien (2017) examinam os recursos da blockchain, com foco nas plataformas blockchain. No trabalho desenvolvido por estes pesquisadores, os recursos propostos, como tipo licenciamento de código, facilidade de uso, suporte técnico e documentação, mecanismos de motivação e consenso, moedas suportadas, segurança, usabilidade, escalabilidade e desenvolvimento foram sugeridos como indicadores gerais para comparar e avaliar plataformas blockchains.

Fundamentados por uma extensa mineração na literatura disponível até o momento este trabalho apresenta como principais contribuições:

a) Compilação dos indicadores técnicos e científicos mais relevantes encontrados nos estudos relacionados à análise, avaliação, desempenho e *benchmark* de plataformas e soluções utilizando a tecnologia blockchain.
b) Metodologia de análise e avaliação de aplicações computacionais blockchain.
c) Instrumento como ferramenta de aplicação da metodologia de análise e avaliação.

3.5 COMPLEMENTOS

De modo a se oferecer uma maior clareza no entendimento dos resultados obtidos por esta pesquisa, os artigos selecionados foram indexados em um catálogo (Tabela 1) que contém o índice numérico, o título, o link da publicação e a quantidade de indicadores citados nos trabalhos. O objetivo da criação deste índice foi determinar um relacionamento entre os artigos selecionados e os indicadores depurados durante o estudo e o nível de relevância aparente entre as publicações.

Sucessivamente, utilizando-se da indexação preliminar, construiu-se o Quadro 2 onde cada um dos indicadores foi relacionado ao índice de artigos do catálogo. Através deste esforço foi possível aprofundar o nível de granularidade dos indicadores por artigos, de forma que se pôde identificar, principalmente, quais indicadores são mais discutidos por outros pesquisadores e quais artigos abordam um número maior de indicadores, inferindo-se com isso posições de relevância tanto dos indicadores quanto dos artigos selecionados.

Tabela 1 – Catálogo de artigos selecionados. continua

Índice	Título	Link	Qtd. de indicadores citados
1	BBB: Make Benchmarking Blockchains Configurable and Extensible	https://ieeexplore.ieee.org/document/8952155	4
2	Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform	https://ieeexplore.ieee.org/document/8526892	12
3	Sharing Blockchain Performance Knowledge for Edge Service Development	https://ieeexplore.ieee.org/document/8998488	12
4	Proposing a Framework for Evaluating the Blockchain Platform	https://www.researchgate.net/publication/334565211_Proposing_a_Framework_for_Evaluating_the_Blockchain_Platform	20
5	A Survey on Challenges and Progresses in Blockchain Technologies: A Performance and Security Perspective	https://www.researchgate.net/publication/337098879_A_Survey_on_Challenges_and_Progresses_in_Blockchain_Technologies_A_Performance_and_Security_Perspective	16
6	Benchmark and comparison between hyperledger and MySQL	http://journal.uad.ac.id/index.php/TELKOMNIKA/article/view/13743/pdf_1372	7
7	OpBench: A CPU performance benchmark for ethereum smart contract operation code	https://ieeexplore.ieee.org/document/8946199	3
8	Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation	https://www.researchgate.net/publication/314213424_Predicting_Latency_of_Blockchain-Based_Systems_Using_Architectural_Modelling_and_Simulation	11
9	Effective scaling of blockchain beyond consensus innovations and Moore's law	https://arxiv.org/abs/2001.01865	13
10	Peer-to-Peer EnergyTrade: A Distributed Private Energy Trading Platform	https://arxiv.org/abs/1812.08315	12
11	Performance Evaluation of the Quorum Blockchain Platform	https://arxiv.org/abs/1809.03421	11
12	Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability	https://ieeexplore.ieee.org/document/8946222	13
13	Blockchain Architectures for P2P Energy Trading Between Neighbors	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8939856	8
14	A Distributed Energy Trading Authentication Mechanism Based on a Consortium Blockchain.	https://www.researchgate.net/publication/334711440_A_Distributed_Energy_Trading_Authentication_Mechanism_Based_on_a_Consortium_Blockchain	9
15	Blockchain for Peer-to-Peer Energy Exchanges: Design and Recommendations	https://ieeexplore.ieee.org/document/8443042	6
16	A Financial Evaluation Framework for Blockchain Implementations	https://ieeexplore.ieee.org/document/8936297	5
17	Evaluating Usability of Permissioned Blockchain for Internet-of-Battlefield Things Security	https://ieeexplore.ieee.org/document/9020736	11
18	Blockchain Energy Market Place Evaluation: An Agent-Based Approach	https://ieeexplore.ieee.org/document/8614924	9
19	Evaluating Suitability of Applying Blockchain	https://www.researchgate.net/publication/323204410_Evaluating_Suitability_of_Applying_Blockchain	5
20	Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload	https://www.researchgate.net/publication/332379108_Towards_a_Performance_Evaluation_of_Private_Blockchain_Frameworks_using_a_Realistic_Workload	9
21	Discrete-Time Analysis of the Blockchain Distributed Ledger Technology	https://ieeexplore.ieee.org/document/8879453	9

conclusão

22	A Method for Blockchain Transactions Analysis	https://ieeexplore.ieee.org/document/8931194/algorithms#algorithms	3
23	A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations	https://ieeexplore.ieee.org/document/8922632	14
24	A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors	https://www.sciencedirect.com/science/article/pii/S0268401219305067	12
25	Review of the Blockchain Technology in the Energy Sector	https://www.sciencedirect.com/science/article/pii/S1364032118307184	6
26	Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions	https://ieeexplore.ieee.org/document/8939186	13
27	Blockchain-Powered Applications for Smart Transactive Grids	https://www.researchgate.net/publication/337510619_Blockchain-Powered_Applications_for_Smart_Transactive_Grids	5
28	A Comparitive Study of Blockchain Applications for Enhancing Internet of Things Security	https://ieeexplore.ieee.org/document/8944446	8
29	Performance analysis and comparison of PoW, PoS and DAG based blockchains	https://www.sciencedirect.com/science/article/pii/S2352864819301476	8
30	SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading	https://ieeexplore.ieee.org/document/8767089	8
31	A Comparative Analysis of Distributed Ledger Technologies for Smart Contract Development	https://ieeexplore.ieee.org/abstract/document/8904256	14
32	A Comparative Analysis of Distributed Ledger Technology Platforms	https://ieeexplore.ieee.org/abstract/document/8902067/	16
33	Operating Permissioned Blockchain in Clouds: A Performance Study of Hyperledger Sawtooth	https://ieeexplore.ieee.org/document/8790849	12
34	Performance Analysis of Private Blockchain Platforms in Varying Workloads	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8038517	9
35	Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)	https://ieeexplore.ieee.org/document/8548070	10
36	A Detailed and Real-Time Performance Monitoring Framework for Blockchain Systems	https://ieeexplore.ieee.org/document/8449244	8
37	Power Trading Blockchain using Hyperledger Fabric	https://www.researchgate.net/publication/326125058_Blockchain_Technology_Hyperledger_Framework_in_the_Internet_of_Energy	10
38	Exploring blockchain for the energy transition Opportunities and challenges based on a case study in Japan	https://www.sciencedirect.com/science/article/pii/S1364032119306963	16
39	Blockchain for Internet of Energy management: Review, solutions, and challenges	https://arxiv.org/pdf/1909.02914.pdf	10

Legenda
blockchain AND benchmark*
blockchain AND evaluat*
blockchain AND analys*
blockchain AND performa*

Fonte: Elaborado pelo autor.

Quadro 2 – Classificação de artigos em relação a indicadores que mencionam.

Indicador	**Índice do Trabalho**
Aplicação	2, 3, 5, 7, 8, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 25, 26, 27, 28, 31, 32, 33, 37, 38, 39
Documentação	4, 14, 31
Participação do fornecedor/comunidade	4, 23, 24, 38
Tamanho do time de desenvolvimento	4, 16
Tamanho do bloco	2, 4, 6, 10, 12, 14, 21, 24, 32, 35
Tamanho do *mempool*	4, 6, 8, 11, 12, 14, 21, 29, 31, 33, 34, 35, 37
Tamanho da transação	2, 4, 6, 8, 10, 11, 12, 21, 29, 32, 36
Escalabilidade	1, 3, 4, 5, 9, 10, 12, 13, 19, 23, 24, 25, 26, 27, 28, 31, 32, 33, 35, 36, 38, 39
Interoperabilidade	3, 4, 9, 23, 38
Algoritmo de consenso	2, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 23, 25, 26, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39
Tipo de licenciamento	4, 12, 23, 24, 32
Tempo de confirmação de bloco	4, 9, 21, 24, 29, 34, 36
Alocação de recursos	2, 3, 4, 5, 17, 18, 20, 29, 31, 32, 33, 34, 35, 36, 38
Presença de banco de dados de estado	2, 5, 12, 23, 26, 38
Throughput	1, 2, 3, 5, 6, 8, 9, 10, 11, 12, 14, 17, 18, 19, 20, 23, 24, 26, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39
Latência da transação	1, 2, 3, 5, 6, 8, 9, 10, 11, 12, 14, 26, 31, 32, 34, 37, 38, 39
Desempenho	2, 5, 18, 24, 29, 30, 33, 34, 35
Tempo de finalidade	2, 8, 9, 20, 21, 34, 35, 36, 37
Tempo de espera da validação	3, 4, 8, 9, 17, 18, 20, 21, 35
Resiliência	5, 15, 28, 30, 32
Tolerância a faltas	1, 5, 11, 13, 15, 16, 17, 22, 23, 24, 26, 28, 30, 31, 38, 39
Topologia da rede	3, 4, 5, 9, 17, 18, 22, 23, 24, 26, 28, 30, 33, 37, 38
Tipo de blockchain	2, 4, 5, 8, 9, 10, 11, 12, 13, 16, 17, 18, 20, 23, 24, 26, 28, 30, 31, 32, 33, 37, 38, 39
Custo	3, 4, 7, 8, 9, 10, 11, 13, 16, 17, 21, 23, 25, 26, 27, 30, 31, 32, 39
Segurança	3, 4, 5, 10, 14, 15, 16, 19, 20, 23, 24, 25, 26, 27, 28, 30, 32, 33, 38
Privacidade	3, 4, 5, 10, 11, 12, 13, 15, 19, 23, 24, 25, 26, 30, 32, 38, 39
Suporte a moeda ou *token*	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 20, 21, 22, 23, 26, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39

Fonte: Elaborado pelo autor.

4 METODOLOGIA DE AVALIAÇÃO TÉCNICO-CIENTÍFICA

Durante a leitura das 91 publicações na íntegra, na revisão sistemática, foi-se construindo um quadro com os indicadores de referência que eram apresentados pelos autores. Embora houvesse uma procura em destaque por indicadores relacionados aos aspectos técnico-computacionais, identificou-se a existência de indicadores relacionados a governança, suporte, segurança e facilidade de uso que são complementarmente importantes para o desenvolvimento da metodologia objetivo da pesquisa. Logo, tais indicadores também foram selecionados. Finalizada a revisão deste montante, foram colecionados 27 indicadores dentre os mais relatados e abordados pelos pesquisadores.

Posteriormente observou-se que dentre os indicadores compilados existiam determinadas características que se assemelhavam em alguns deles e que eram distintas dos demais. Percebendo tal comportamento inferiu-se que tais indicadores, embora relacionados, faziam parte de grupos distintos de predicados assim como de medidas, o que levou ao entendimento de que dever-se-ia agrupá-los em 4 dimensões (viz., arquitetura, objetivo, suporte e governança) e 2 subdimensões (qualitativo e quantitativo). O Quadro 3 apresenta a compilação dos indicadores.

A dimensão de arquitetura engloba majoritariamente indicadores sobre o desempenho das tecnologias blockchain. Devido ao desempenho poder ser avaliado ou afetado por diferentes parâmetros, distintos indicadores qualitativos e quantitativos são listados nesta dimensão. Ainda, a dimensão inclui indicadores que têm a ver com a forma como a tecnologia blockchain pode estar ligada a outras tecnologias (interoperabilidade) ou pela comunidade de usuários (tipo de licenciamento).

Em relação ao objetivo ou aplicação de uma blockchain observa-se, de modo geral, consistir principalmente em criptomoedas, contratos inteligentes e estruturas para o desenvolvimento de aplicativos. Devido à aplicação de cada plataforma, os recursos e componentes esperados variam. Por exemplo, plataformas desenvolvidas com o objetivo de implementar contratos inteligentes requerem um sistema para compilar e executar esses contratos.

A dimensão suporte pode ser considerada como um dos principais fatores na avaliação de produtos de software de código aberto, especialmente para plataformas. Quanto

mais documentação uma tecnologia tiver, mais usuários poderão utilizá-la e mais desenvolvedores poderão aprimorá-la. Além disso, o tamanho do grupo de desenvolvimento é outro critério importante para avaliar a continuação do desenvolvimento da plataforma. Investimentos e parcerias corporativas também são considerados como critério de suporte ao produto e, é claro, alto valor no mercado.

Quadro 3 – Estrutura metodológica adotada e seus indicadores.

Dimensão	**Indicadores**	
	Qualitativo	**Quantitativo**
Arquitetura	Resiliência Escalabilidade Interoperabilidade Alocação de recursos Tipo de licenciamento Algoritmo de consenso Desempenho Tolerância a faltas Presença de banco de dados de estado	Tamanho do bloco Tamanho do *mempool* Tamanho da transação Latência da transação Throughput Tempo de finalidade Tempo de espera da validação Tempo de confirmação de bloco
Objetivo	Aplicação	
Suporte	Documentação Participação do fornecedor/comunidade Tamanho do time de desenvolvimento	
Governança	Segurança Privacidade Topologia da rede Tipo de blockchain Suporte a moeda ou token	Custo

Fonte: Elaborado pelo autor.

Quanto à governança de uma blockchain, a definição de regras e a concessão de permissões de leitura, gravação e confirmação são determinadas, geralmente, por um administrador ou grupo de administradores da plataforma. As entidades ou organizações, que podem ser públicas, privadas ou consórcios, diferenciam-se em termos de participação no blockchain, permissões, funções de nodos na rede e componentes da plataforma que serão implantados em diferentes nodos.

Cabe compreender que, embora tenha sido feito o dimensionamento e classificação dos indicadores para fins de organização e pesquisa, uma dependência intrínseca existe entre

eles. Tal dependência pode ser observada em métricas como o tempo de criação do bloco, as taxas de transação, tamanho do bloco e o tamanho da transação, que de forma conjuntas desempenham papéis importantes na determinação do desempenho de um sistema blockchain. Ressalta-se ainda que especificidades acerca das dependências entre indicadores variam dentre diferentes plataformas (CHOWDHURY et al., 2019).

4.1 FUNDAMENTAÇÃO DOS INDICADORES

Nesta seção serão contextualizados os indicadores selecionados para a construção da metodologia computacional, suas dimensões e subdimensões. Para cada indicador uma explicação será desenvolvida e pareceres dos diversos autores pesquisados serão expostos para servir de análise e avaliação de futuras aplicações blockchain.

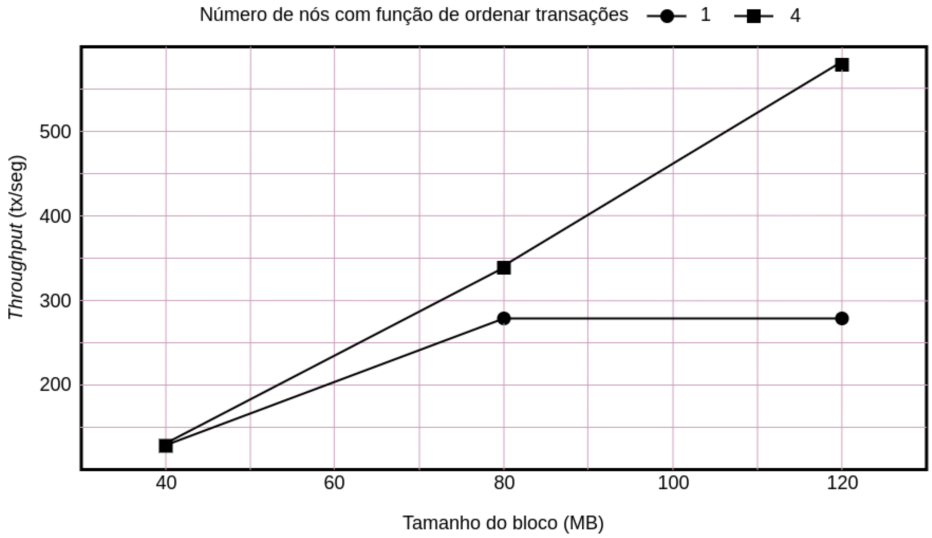
4.1.1 Dimensão Arquitetura

4.1.1.1 Quantitativo

4.1.1.1.1 Tamanho do bloco

Constatou-se ao analisar as publicações estudadas a existência de um consenso entre os autores quanto a uma forte relação entre este indicador e a performance de uma solução blockchain. Sukhwani et al. (2018) apontam que alguns reveses de desempenho existentes em plataformas blockchain privadas, como o tempo para ordenação das transações e o tempo de confirmação das transações no livro razão podem ser atenuados quando se utiliza um bloco de tamanho maior. Embora esta técnica promova um aumento na latência média, sua implementação consegue obter um ganho de performance. Contudo cabe destacar que existe um tamanho considerado ideal e que ele varia de acordo com outros indicadores das dimensões: objetivo, arquitetura e governança. Esta relação entre os indicadores pode ser observada na Figura 8, onde o *throughput* aumenta em relação ao tamanho do bloco, mas também depende da topologia da rede. Verifica-se que apesar de haver um aumento no tamanho do bloco, o desempenho é limitado pelo número de nodos que ordenam as transações na rede, que é definido por uma política de governança existente em blockchain privadas.

Figura 8 – Relação entre tamanho do bloco e *throughput*.

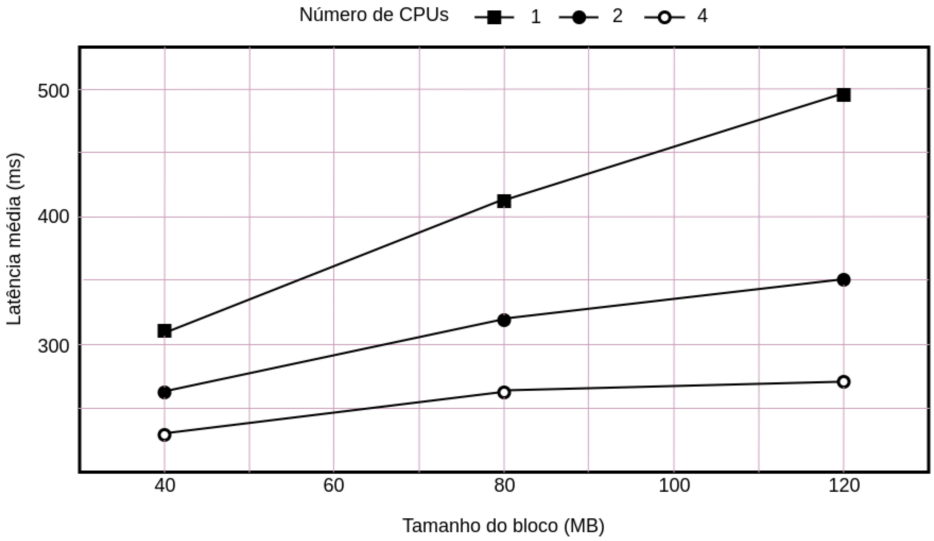


Fonte: Adaptado de Sukhwani et al. (2018).

Outra relação entre os indicadores pode ser percebida na Figura 9, onde a latência média aumenta em relação ao tamanho do bloco. Todavia pode-se mitigar esta degradação da latência aumentando o número de unidades de processamento (CPUs) na rede, por exemplo, com a entrada de novos participantes ou incremento da infraestrutura de hardware. Entretanto este comportamento pode não ocorrer em blockchain públicas e tem forte relação com o algoritmo de consenso utilizado. Então, analisando os cenários sob diferentes pontos de vista pode-se inferir que, embora conseguiu-se construir uma representação visual dimensionada dos indicadores compilados no Quadro 3, todos são estreitamente relacionados e dependentes.

Thakkar, Nathan e Viswanathan (2018) identificaram em sua pesquisa, também utilizando a plataforma Hyperledger Fabric, que em redes com grande volume de transações, tamanhos maiores de bloco resultam, de mogo geral, em um maior *throughput* e menor tempo de espera (validação e confirmação das transações), onde mesmo com o detrimento da latência média, obtiveram ganhos de desempenho. Na pesquisa foram utilizados blocos de tamanhos variados de 10 a 100 transações. Cabe salientar que quando se projeta uma blockchain privada, independente da plataforma, algumas configurações, incluindo o tamanho do bloco, podem ser definidas baseadas no seu caso de uso, garantindo a otimização dos recursos e um melhor desempenho da rede.

Figura 9 – Relação entre tamanho do bloco e latência média.



Fonte: Adaptado de Sukhwani et al. (2018).

Na comparação de implementações blockchain proposta por Hintzman (2017) o autor julga que tamanho de bloco é essencial para controlar a performance da blockchain, e nota que o Bitcoin conta com limitação de 1 MB como tamanho de bloco máximo. Em relação ao Ethereum, o autor explica que o tamanho de bloco é apenas limitado pela quantidade de *gas*[7] em circulação, e também aponta que no momento no estudo (2017) esta quantidade era de aproximadamente de 3 milhões de *gas,* o que reflete em um tamanho máximo de bloco de aproximadamente 89 kB. Nota-se também constante aumento de *gas* em circulação, e que 2019 este valor já alcançava 10 milhões, o que reflete na possibilidade teórica de maiores blocos. Ná prática, o tamanho médio dos blocos varia entre 20 e 30 kB. (ETH GAS STATION BLOG, 2019).

4.1.1.1.2 Tamanho do *mempool*

Mempool refere-se ao local onde todas as transações pendentes esperam para ser confirmadas pela rede blockchain e acrescentadas no próximo bloco, e consequentemente em termos gerais um *mempool* de grande tamanho indica grande tráfego na rede. (BLOCKCHAIN.COM, 2020).

---

7 *Gas* refere-se a um custo computacional teórico para os mineradores executarem uma transação na plataforma Ethereum. Proporcionalmente ao custo despendido, compensam-se os mineradores utilizando a criptomoeda própria do Ethereum denominada de *Ether*.

No Bitcoin, o *pool* de memória (*mempool*) atua como um repositório de todas as transações não confirmadas. Depois que um usuário gera uma transação, ela é transmitida para toda a rede e armazenada no *mempool*, onde aguarda confirmação. Se a taxa de transações recebidas for superior ao *throughput* da rede, será criada uma lista de transações a serem confirmadas. As transações que permanecem não confirmadas por um longo período acabam sendo rejeitadas.

Em 11 de novembro de 2017, o tamanho do *mempool* do Bitcoin excedeu 115k transações não confirmadas, resultando em US$ 700 milhões em transações paralisadas (MEMORIA, 2017). As inundações do *mempool* criam incerteza entre os usuários, para que paguem taxas mais altas de mineração para impedir que suas transações sejam rejeitadas.

Ecoinomic (2018) explica que, em blockchain públicas, como o Bitcoin e o Ethereum, *mempools* mais congestionados implicam em aumento dos incentivos monetários para execução de transações, visto que tal incentivo pode ser entendida como um fator de prioridade para executar determinada transação. Transações cujos incentivos são maiores em relação a média geral são confirmadas com maior rapidez, e em caso de congestionamento do *mempool*, nota-se que transações com incentivos inferiores podem ser atrasadas por horas ou dias ou até rejeitadas.

Cabe ressaltar que o *mempool* não está presente em todas as blockchains e sua aplicabilidade vai depender da plataforma e do modelo de negócio que se deseja utilizar. O Quadro 4 classifica algumas das principais plataformas existentes atualmente em relação a presença do *mempool* considerando sua configuração padrão.

Quadro 4 – Classificação de plataformas em relação ao *mempool*.

Presença do *mempool*	**Plataformas**
Possui	Bitcoin, Multichain, Neo, Ripple, Monero, Stellar, IOTA, Ethereum
Não possui	Corda, Hyperledger Fabric, Hyperledger Sawtooth, EOS

Fonte: Elaborado pelo autor.

De modo geral, os documentos selecionados apresentam este indicador inserido no contexto funcional do sistema. Pois o *mempool* passa a existir a partir do momento que uma rede blockchain é iniciada, mais precisamente quando um nodo da rede é instanciado e transações passam a ser criadas. Este indicador pode ser usado como um monitor de

comportamento da rede, onde se pode inferir *throughput*, tempo de espera (validação e confirmação) e opcionalmente custo, uma vez que o tamanho do *mempool* reflete o nível de saturação da rede. Cao et al. (2020) estudam o comportamento operacional de três soluções baseadas em DLTs quando expostas a diferentes níveis de tráfego de transações e analisam a probabilidade de tolerância a falta no sistema quando o *mempool* é sobrecarregado. Tal estudo aponta que tanto DLTs que utilizam o *Proof-of-Work (PoW)* quanto *Proof-of-Stake (PoS)* apresentaram faltas quando submetidas à situação apresentada, já a DLT baseada em DAG manteve probabilidade nula de faltas, como esperado devido a sua arquitetura.

4.1.1.1.3 Tamanho da transação

Em um blockchain, cada transação que é adicionada ao *mempool* aumenta o tamanho da fila de transações em uma unidade, enquanto cada bloco gerado diminui o tamanho dessa fila pela confirmação de várias transações em um lote. O número de transações incluídas em cada bloco é determinado pela distribuição dos tamanhos das transações e pelo tamanho máximo do bloco. Utilizando uma instância privada do blockchain Ethereum em um ambiente fechado, Geissler et al. (2019) avaliam o impacto de diferentes tamanhos de transações na capacidade de processamento (geração de blocos) da plataforma, fornecendo uma descrição detalhada do modelo e validação com base nos valores de medição obtidos. Baseado no estudo dos pesquisadores pode-se inferir que, entre outros aspectos, o tamanho da transação influencia diretamente no:

a) Tamanho da Fila: Conhecer a menor diferença D, para $D \geq 0$, entre o tamanho do bloco T_B e o somatório dos tamanhos das transações T_{Tx} dado pela fórmula: $D = T_B - \Sigma T_{Tx}$ otimiza a utilização do bloco e a capacidade de consumo da fila, consequentemente o *throughput* da rede. (Observe que se a diferença for zero ($D = 0$) o bloco está completamente ocupado.)
b) Tempo de espera: Geissler et al. (2019) examinam o efeito de diferentes tamanhos de transação no tempo médio de espera. Para compreender o resultado obtido pelos pesquisadores, cabe destacar que como a fila de transações pendentes do blockchain avaliado não tem limite de tamanho, nenhuma transação seria descartada e o tamanho da fila divergiria para $+\infty$.

> Portanto, o modelo foi limitado a cargas do sistema (*system load*) de [8]$\rho < 1$, caso contrário, o tamanho da fila não convergiria. Como pode ser observado na Figura 10 o tempo médio de espera $E[W]$ não aumenta continuamente com o aumento do tamanho das transações, mas depende da utilização do bloco. No experimento para um bloco de tamanho $\beta = 1{,}5$ kB as transações 60, 150 e 210 *bytes* apresentam um agrupamento mais eficiente do que as de 90, 120 e 180 *bytes*. Logo, como uma utilização mais precisa do bloco leva a um empacotamento mais eficiente das transações no espaço disponível dentro de cada bloco, mais transações podem ser confirmadas em cada ciclo, garantindo tempos de confirmação mais rápidos.

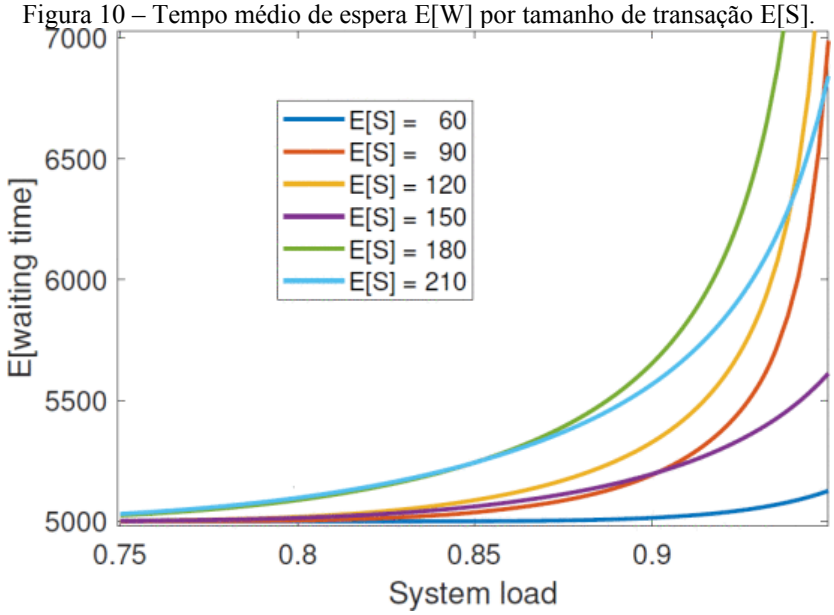
Cabe compreender que embora se tenha feito o dimensionamento e classificação dos indicadores para fins de organização e pesquisa, uma dependência intrínseca existe entre eles. Consoante ao observado por Chowdhury et al. (2019), que citam algumas métricas como o tempo de criação do bloco, as taxas de transação, o tamanho do bloco e o tamanho da transação e ressaltam que todos desempenham papéis importantes na determinação do desempenho de um sistema blockchain e que isso variará entre diferentes plataformas. Destacam ainda que é importante entender as características e os recursos da plataforma para selecionar a mais adequada para uma aplicação específica.

A análise comparativa de Hintzman (2017) infere que o tamanho da transação, assim como o tamanho de bloco, é de elevada importância no desempenho de plataformas blockchain. O autor sinaliza as variações no tamanho das transações para alguns projetos. O Bitcoin que conta com um mínimo de 200 bytes por transação. A plataforma Steem que opera com uma média de 100 bytes por transação e a plataforma Lisk que possui um máximo de 1223 bytes por transação. Observa-se também, que na configuração padrão, a plataforma Multichain dispõe a maior capacidade entre as apresentadas no estudo, de 4MB por transação. Sobre a plataforma Ethereum, o autor ressalta que assim como o tamanho de bloco, o tamanho de transação é limitado apenas pela quantidade de gas em circulação, que resulta em uma transação com tamanho máximo de aproximadamente 89KB.

---

8 ρ = Carga do sistema como proporção entre a taxa de chegada e processamento de transações. Requer $\rho < 1$ para que a fila seja estável.

Figura 10 – Tempo médio de espera E[W] por tamanho de transação E[S].



Fonte: Geissler et al. (2019).

Como observado, diferentes plataformas possuem diferentes tamanhos e limitações em relação aos tamanhos das transações devido a diversos fatores, como o tipo da blockchain, estrutura e tipo da transação, arquitetura da cadeia, etc. A Tabela 2 traz um compilado deste indicador entre algumas das principais plataformas conhecidas atualmente.

Tabela 2 – Relação entre o tamanho da transação e a plataforma.

Plataforma	**Limite (configuração padrão)**
IOTA	2673 *trytes* (aprox. 1.6kB)
Cardano	8kB
Quorum	32kB
Bitcoin	100kB
Neo	102.4kB
Multichain	4MB
Corda	4MB
EOS	Tempo de execução máximo de 30ms
Ethereum	Quantidade de *gas* disponível
Hyperledger Fabric	Configurável
Hyperledger Sawtooth	Configurável

Fonte: Elaborado pelo autor.

4.1.1.1.4 Latência da transação

O termo latência, no entendimento abstrato, é um intervalo de tempo entre uma requisição e sua resposta ou, de um ponto de vista mais amplo, um atraso de tempo entre a causa e o efeito de alguma mudança física no sistema que está sendo observado. A definição precisa de latência depende do sistema que está sendo observado e da natureza da operação. Por exemplo, em telecomunicações, na terminologia VoIP, o tempo gasto para conversão de voz em dados e vice-versa é conhecido como latência de comutação. Em um computador, latência de disco é o atraso entre o momento em que os dados são solicitados ao dispositivo de armazenamento e o momento em que os dados começar a ser retornados.

Em sistemas blockchain o termo latência refere-se a dois intervalos associativos de tempo: latência de rede e latência da operação.

a) Latência de rede (L_R): Purbo et al. (2020) apontam que a latência de rede está relacionada ao tempo necessário para se enviar mensagens de uma extremidade a outra em uma rede de comunicação. A latência de rede também pode ser o intervalo de tempo necessário para a entrega de pacotes de dados do remetente ao destinatário. Quanto maior o atraso ou a latência, maior o risco de falha no acesso. A latência da rede também é frequentemente interpretada como o nível de atraso na entrega em redes de comunicação de dados e voz. A latência é medida estritamente na forma de tempo. Por exemplo, uma rede para enviar mensagens leva 24 milissegundos (ms) de uma extremidade à outra. Em geral, existem três componentes de latência a saber: atraso de propagação, trânsito e fila.
b) Latência de operação (L_o): Purbo et al. (2020) definem latência de operação como a medida de tempo que uma rede blockchain leva para identificar, validar e confirmar cada transação. Em particular, o tempo despendido por um participante do sistema para processar cada transação recebida e disponibilizar seu resultado para a rede. O Grupo de Trabalho sobre Desempenho e Escalabilidade em blockchains mantido pela The Linux Foundation define latência de operação como qualquer tempo de trabalho da rede devido ao mecanismo de consenso em vigor (HYPERLEDGER, 2018).

Desta forma, este estudo considera latência da transação (L_T) em uma rede blockchain como o somatório entre a latência de rede (L_R) e a latência de operação (L_o), dado pela fórmula: L_T=L_R+L_O, passando a utilizar o termo *latência da transação* ou apenas *latência* para definir este indicador.

Latência de transação é uma visualização em toda a rede da quantidade de tempo necessário para que o efeito de uma transação seja utilizável em toda a rede. A medida inclui o tempo desde o momento em que um evento é emitido até o ponto em que o resultado está amplamente disponível na rede. Isso inclui o tempo de propagação e qualquer tempo de trabalho realizado em favor do mecanismo de consenso do sistema. Tempo de trabalho este que contempla, entre outros atrasos, o tempo de espera e validação da transação e o tempo de confirmação do bloco. Para levar em conta esses fatores e fornecer uma visão geral da rede, a latência deve ser medida usando todos os nodos participantes deste sistema (HYPERLEDGER, 2018).

Para Duan et al. (2019) em sistemas de grande escala (geo-) distribuídos, a latência da rede desempenha um papel significativo, pois geralmente há uma interação complexa entre a latência e o mecanismo de tempo limite, o que afetaria o desempenho ou até a confiabilidade do sistema. Os pesquisadores destacam ainda que a latência afeta diretamente o *throughput* em uma rede blockchain, apontando que o rendimento de uma rede blockchain diminui à medida que a latência aumenta.

Yasaweerasinghelage, Staples e Weber (2017) apontam que a latência em sistemas baseados em blockchain é uma limitação. Uma plataforma blockchain que usa o *Consenso de Nakamoto*[9] pode levar segundos (e.g., Ethereum) ou minutos (e.g., Bitcoin) para que uma transação seja incluída em um bloco. Essas transações nunca são absolutamente confirmadas, pois a garantia de imutabilidade é fornecida pelos blocos subsequentes, conhecidos como blocos de confirmação. A latência para inclusão inicial de uma transação em uma blockchain é maior do que nos sistemas tradicionais, e um grande número de blocos de confirmação multiplicará esse atraso. A latência também pode ser afetada por atrasos na rede, taxa de

9 Consenso de Nakamoto pode ser entendido como o conjunto de regras e incentivos proposto por Satoshi Nakamoto, criador do Bitcoin, que ajuda a governar o mecanismo de consenso em um sistema distribuído onde os participantes envolvidos não precisam se conhecer ou confiar uns nos outros ou em terceiros para que o sistema funcione. Disponível em: https://golden.com/wiki/Nakamoto_consensus. Acesso em: 20 junho 2020.

transação oferecida, número de transações sendo processadas e decisões estratégicas tomadas pelos mineradores. Portanto, os tempos de inclusão da transação podem variar bastante.

Outro ponto de atenção observado por Yasaweerasinghelage, Staples e Weber (2017) é em relação ao tempo entre a criação de dois blocos consecutivos (tempo entre blocos) ou frequência de criação dos blocos (frequência do bloco). Na teoria, cada rede possui sua própria frequência do bloco definido. Por exemplo, a frequência do bloco da rede Bitcoin é de cerca de 10 minutos, enquanto a frequência do bloco da rede Ethereum é de cerca de 20 segundos. Embora esses valores variem na prática, alguns autores consideram que em uma blockchain pública o tempo entre blocos é conceitualmente fixo. No entanto, cabe instruir, que o momento exato de concepção do próximo bloco é incognoscível. Contudo, quando se parte para blockchains privadas, este tempo pode ser configurado como uma opção de design ou tomada de decisão arquitetônica. Isso reduz o tempo de inclusão da transação, o que pode atenuar a latência no nível do sistema. Tal constatação pôde ser observada no experimento de Yasaweerasinghelage, Staples e Weber (2017), onde utilizando uma implementação privada da plataforma Ethereum apuraram que para os tempos de blocos de 2.3s, 6.3s e 13.6s (tempo padrão da plataforma) as latências médias foram de 28.1s, 64.7s e 132s respectivamente, utilizando os mesmos cenários de avaliação.

Zheng, Zhu e Si (2019) analisam quatro plataformas em relação a sua latência, conforme a Tabela 3.

Tabela 3 – Comparação de plataformas blockchain em relação a latência.

Plataforma	**Latência**
Ethereum (Geth)	Em torno de 100 segundos
Parity	Alguns segundos
Hyperledger Fabric	Dezenas de segundos
IOTA	Aproxima-se de 0 a partir de certo tamanho de rede

Fonte: Adaptado de Zheng, Zhu e Si (2019).

Pondera-se também que a latência de transação pode apenas ser considerada relevante quando comparada entre plataformas com transações de natureza similar e com restrições idênticas. Várias tecnologias blockchain também diferem em relação a definição de transação. (ZHENG; ZHU; SI, 2019).

Thakkar, Nathan e Viswanathan (2018) demonstram grande preocupação com o desempenho das plataformas blockchain permissionadas e sua capacidade de lidar com um enorme volume de transações com baixa latência, e também citam preocupação em relação à riqueza de linguagens na descrição de transações. Ressalta-se, porém, que diferentes plataformas permissionadas, como o Quorum e o Corda, tendem a lidar com esses problemas se utilizando de técnicas distintas no domínio de sistemas distribuídos, e que o Hyperledger Fabric, foco do estudo, lida com essas preocupações através de um alto grau de especificabilidade, contando com um design modular e componentes plugáveis.

Che et al. (2019) e Kuzlu et al. (2019) realizam avaliações utilizando a plataforma Hyperledger Fabric, e em ambos os experimentos propostos observa-se que até atingir o ponto de saturação de taxa de envio de transações (200 TPS e 250 TPS respectivamente) a plataforma manteve uma performance estável, com aumento linear de latência. Após o ponto de saturação, em ambos os casos houve um considerável aumento de latência conforme a taxa de envio progredia.

Hassan, Yuen e Niyato (2019) julgam que aplicações ligadas à *smart energy* necessitam de baixa latência para garantir um monitoramento e controle suaves e operação de aparelhos, equipamentos e processos. Eles apontam também que a latência em algumas aplicações críticas, como às necessárias para estabilização da rede, deve ser medida em milisegundos. Essas considerações levaram os autores a reconhecer que para áreas como Monitoramento de Rede, Gerenciamento de Energia e Gerenciamento Distribuído de Energia algoritmos baseados em *Proof-of-Authority*[10] são essenciais, visto suas vantagens em relação a latência e utilização de recursos. Os pesquisadores ressaltam, porém, que tal algoritmo não se mostrou tão eficiente em outras aplicações para cumprir os requisitos de latência.

4.1.1.1.5 *Throughput*

Em termos gerais, *throughput* pode ser compreendido como taxa de produção, taxa de transferência, vazão média, trabalho realizado ou a taxa na qual determinada operação é processada. Quando empregado no contexto de redes de comunicação, como a Internet, o *throughput* pode ser definido como a taxa de entrega *bem-sucedida* de mensagens em um

10 Em algoritmos baseados em autoridades (*Proof-of-Authority, PoA)* nodos autorizados (confiáveis) criam blocos de maneira *round-robin*. Algoritmos PoAu eliminam trocas de mensagem entre nodos utilizadas na obtenção de consenso. (HASSAN; YUEN; NIYATO; 2019).

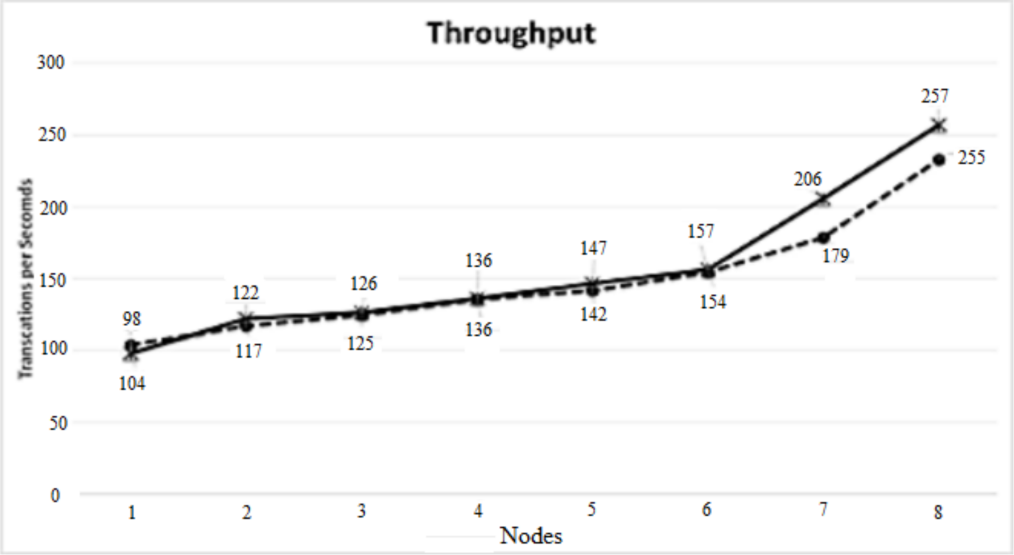
canal de comunicação. Quando analisado em um ambiente sistêmico o *throughput do sistema* é o somatório das taxas de dados entregues a todos os terminais em uma rede (MIAO et al., 2016). Logo, assim como latência, a definição de *throughput* depende do sistema que está sendo observado e da natureza da operação.

Em blockchain, *throughput* é a taxa na qual as transações válidas são confirmadas pela rede em um determinado intervalo de tempo. Esta taxa é medida em transações por segundo (TPS). Lembrando que o número de transações inválidas deve ser descontado do total de transações confirmadas. Cabe salientar que o *throughput* leva em consideração a operação de todo o sistema e não a nodos individuais. (HYPERLEDGER, 2018).

Purbo et al. (2020) definem *throughput* como "o número de transações bem-sucedidas por segundo" em um sistema blockchain. Em ciência da computação está associado a algum tempo de computação utilizado para resolver determinada tarefa.

Zheng, Zhu e Si (2019) também definem o *throughput* como o montante de transações efetivadas que uma plataforma blockchain consegue processar por segundo. Os autores ressaltam também que mesmo sendo um indicador chave na avaliação de performance de uma plataforma blockchain, o *throughput* é apenas relevante quando comparado entre plataformas com transações de natureza similar em um conjunto idêntico de restrições.

Figura 11 – Relação entre número de nodos e *throughput* no Hyperledger Fabric.



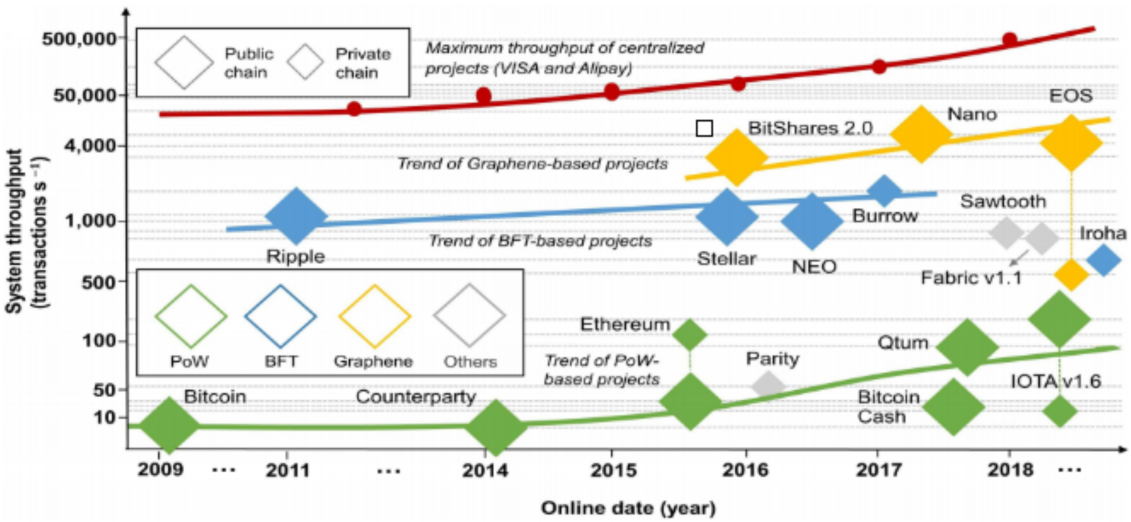
Fonte: Purbo et al. (2020).

Observa-se também que as atuais limitações de *throughput* das plataformas blockchain são bem expressivas quando comparadas a sistemas de bancos de dados tradicionais, e que esta deficiência deve ser mitigada para que uma maior adoção e aplicação da tecnologia em ambientes de produção real ocorra. Notam-se também diversos trabalhos acadêmicos voltados para estudo e análise de técnicas de paralelismo de dados voltadas para otimização do *throughput* em blockchains. (ZHENG; ZHU; SI, 2019).

Verifica-se também que na plataforma Hyperledger Fabric o *throughput* depende principalmente de dois parâmetros: o tamanho e a frequência do bloco, e que para aumentar o *throughput* do Fabric pode-se aumentar o tamanho dos blocos ou reduzir a frequência entre eles. Além disso, nota-se que o aumento no número de participantes da rede também tende a aumentar o *throughput*, conforme a Figura 11. (PURBO et al., 2020).

Liu et al. (2020) realizam uma análise temporal da performance das principais plataformas blockchain, apresentando entre os indicadores analisados, o *throughput*.

Figura 12 – *Throughput* de pico das principais plataformas blockchain com o tempo.



Fonte: Liu et al. (2020).

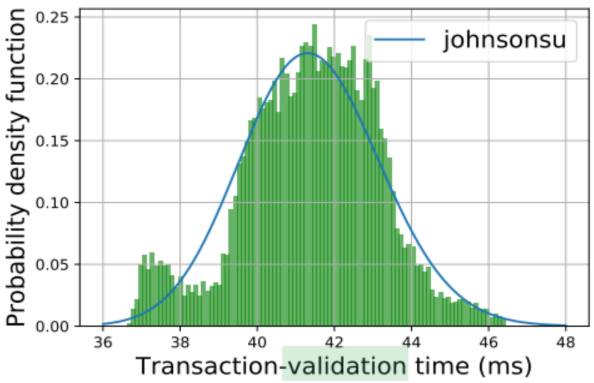
Conforme mostra a Figura 12, observa-se que mesmo com as melhorias implementadas durante o passar dos anos, as plataformas com algoritmos baseados em PoW mantêm baixos *throughputs*, variando de 3.3 – 6.67 TPS no Bitcoin a aproximadamente 250 TPS no IOTA, enquanto que plataformas com algoritmos mais leves, como o BFT (*Byzantine Fault Tolerance*) alcançam picos de 1000 à 1500 TPS. Nota-se também que a partir de 2015

começam a surgir algoritmos baseados no framework Graphene, que utiliza de criações de bloco geo-ordenadas por produtores de blocos permissionados como forma de atingir *throughputs* superiores a 3500 TPS. Os designs baseados em Graphene são, porém, considerados questionáveis em termos de descentralização e segurança. (LIU et al., 2020).

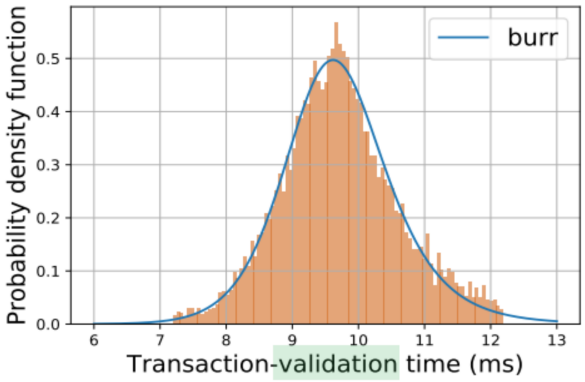
4.1.1.1.6 Tempo de espera da validação

Oliveira et al. (2019) definem que o tempo de validação de transação representa o intervalo de tempo desde a submissão de uma transação já assinada por um usuário para um nodo, até que este nodo realize o processo de validação da transação. Para computar esse tempo, os autores consideram a latência entre o instante de submissão da transação e o instante do recebimento de uma resposta válida.

Figura 13 – Histogramas de tempo de validação de transação.



(a) Parity



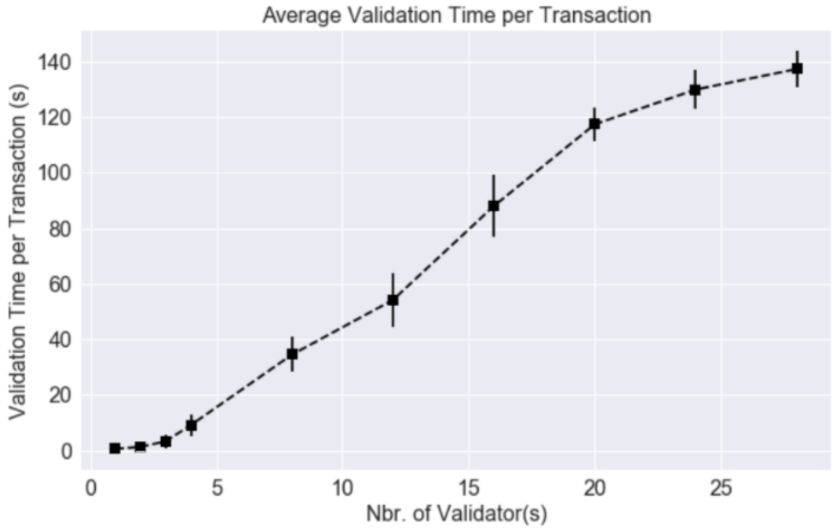
(b) Multichain

Fonte: Oliveira et al. (2019).

O estudo de Oliveira et al. (2019) realiza uma comparação de desempenho entre as plataformas Multichain e Parity quando submetidas a uma carga de trabalho com distribuição probabilística de chegada de transações baseada na rede Bitcoin no período de Junho de 2017 a Junho de 2018. Os resultados obtidos foram plotados em histogramas, conforme a Figura 13, e nota-se que a distribuição do tempo de validação de transação Parity segue uma distribuição Johnson's SU (variação da distribuição normal), enquanto que o Multichain segue uma distribuição de Burr (log-logistica).

Observa-se também que o tempo de validação variou de 37 a 46 ms na plataforma Parity, com maior concentração transações no intervalo entre 41 e 43 ms. Na plataforma Multichain o tempo variou de 7 a 12 ms, com maior concentração na faixa entre 9 e 10 ms, o que indica que o Multichain é em média quatro vezes mais rápido que o Parity no processo de validação de transações.

Figura 14 – Tempo de médio de validação (*vs*. número de nodos validadores).



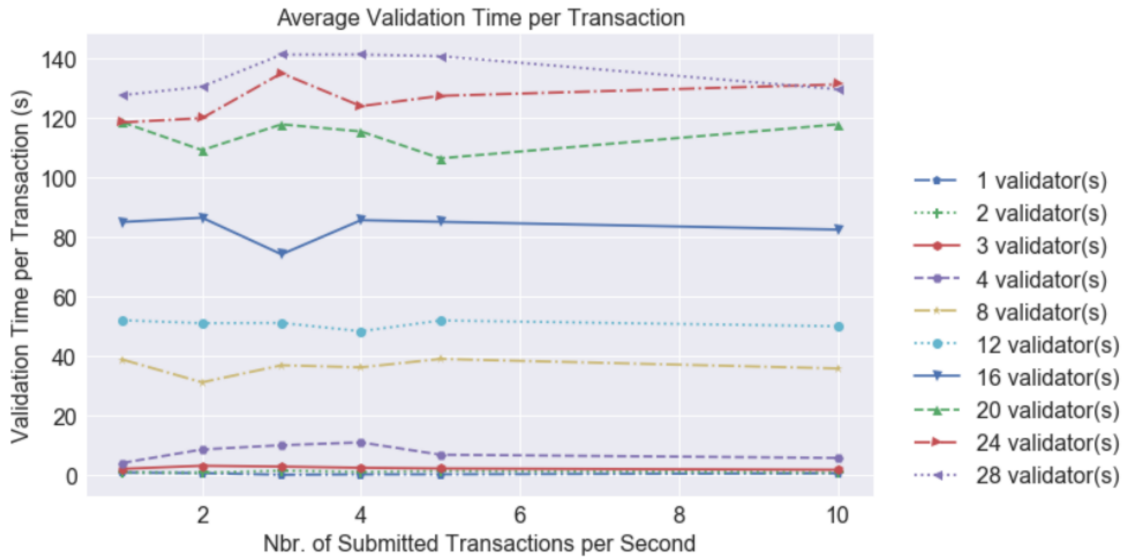
Fonte: Brousmichc et al. (2018).

Brousmichc et al. (2018) propõe um *framework* de simulação para avaliar diversos modelos de mercados energéticos locais baseados em blockchain. Os autores utilizam o *Ethermint* (combinação do Ethereum e *Tendermint)*, escolha justificada por seu menor consumo energético e maior velocidade na validação das transações. No estudo os pesquisadores apontam que quanto mais transações enviadas por segundo, mais a rede acumula atrasos na validação. Em um experimento onde são enviadas 10 transações por

segundo, uma rede de 1, 2, 3 ou 4 nodos validadores conseguem realizar a validação das mesmas em um segundo ou menos, enquanto que para redes com 8, 12, 16 ou 20 validadores a blockchain leva vários segundos. Entre os resultados obtidos, o estudo revela na Figura 14 que quanto maior o número de nodos validadores, maior o tempo de validação de uma transação.

Sob outra perspectiva, Brousmichc et al. (2018) analisam o impacto da variação do volume de transações no tempo de validação, para um número constante de nodos validadores, como mostra a Figura 15. Os resultados indicam que o tempo médio é apenas ligeiramente afetado pelo aumento do número de transações, e os autores explicam que isso ocorre pelo empilhamento de transações no *mempool* do *Tendermint*, onde todas as transações recebidas são armazenadas antes de serem validadas.

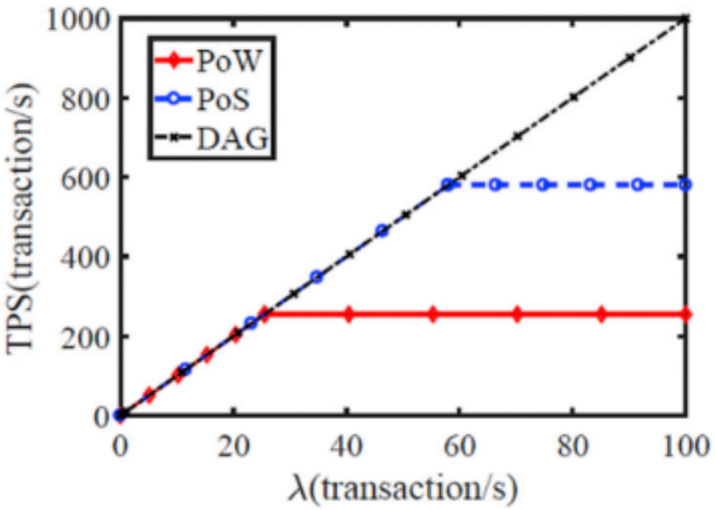
Figura 15 – Tempo médio de validação de transações (*vs*. número de TPS).



Fonte: Brousmichc et al. (2018).

Cao et al. (2020) utilizam de uma métrica denominada de *Delay* de Confirmação, que avalia a taxa de processamento desde a chegada de uma nova transação até sua confirmação final. Os autores realizam uma análise de performance dos algoritmos PoW, PoS e DAG quanto a este indicador, apresentada na Figura 16. Na simulação realizada pelos pesquisadores utilizou-se uma rede blockchain com dez nodos com capacidades computacionais semelhantes.

Figura 16 – Delay de confirmação dos algoritmos analisados.



Fonte: Cao et al. (2020).

Os autores notam que com o aumento de recursos computacionais, o consenso pode ser obtido com maior rapidez, além de sinalizarem que diferenças no *delay* de confirmação podem decorrer dos diferentes requisitos para confirmação por parte de cada plataforma (6 confirmações para o Bitcoin/PoW, 10 para Nxt/PoS e 200 para o Tangle). Os pesquisadores ainda ressaltam que o processo de confirmação no algoritmo DAG difere dos demais, visto que a transação é apenas confirmada quando seu peso atinge o patamar cumulativo de confirmação (W), e consequentemente o *delay* de confirmação depende do valor de W e da taxa de chegada de transações.

4.1.1.1.7 Tempo de confirmação de bloco

Binance Academy (2020) define tempo de confirmação de bloco como o tempo decorrido entre o momento que uma transação blockchain é submetida à rede e o tempo em que a mesma é validada e inserida no próximo bloco confirmado. Representa então, o tempo total que um usuário deve esperar até que sua transação seja coletada e confirmada por um nodo minerador. Cabe salientar que o tempo de confirmação de bloco, em alguns blockchains públicos, pode variar de acordo sua prioridade que é baseada no valor do incentivo financeiro oferecido para o processamento de determinada transação.

Na análise de Moezkarimi, Abdollahei e Arabsorkhi (2019) abordam-se dez plataformas observando este indicador; Liu et al. (2020) também analisam diversas blockchains e sua evolução a respeito do mesmo; e Chowdhury et al. (2019) apontam que o tempo de confirmação é dependente do algoritmo de consenso utilizado no sistema, e complementam as argumentações dos outros pesquisadores com análises semelhantes em algumas plataformas. Os resultados dos estudos foram compilados e compõem a Tabela 4.

Tabela 4 – Classificação de plataformas por tempo de confirmação.

Tempo de Confirmação (segundos)	**Plataformas**
< 5	Waves, Ripple, Steem, Corda, Stellar e Burrow
5 a 59	Ethereum, Cardano, Nano, Parity, BitShares, Iota, Iroha, Lisk
60 a 599	Zcash, Neo, Litecoin, Dogecoin
>= 600	Bitcoin, Bitcoin Cash e Counterparty
Variável / Configurável	Multichain, Elements, Hyperledger Sawtooth e Hyperledger Fabric

Fonte: Adaptado de Moezkarimi, Abdollahei e Arabsorkhi (2019), Liu et al. (2020), Chowdhury et al. (2019) e Hintzman (2017).

Sob outro prisma, Zheng et al. (2018) equacionam o tempo de confirmação de bloco nomeando-o de *Average Response Delay*, e salientam que sua não quantificação no estudo se justifica pela utilização de redes locais (LANs) para realização dos testes, e que os resultados do *Delay* seriam mais significativos em redes de longa distância (WANs) com trânsito pela internet.

4.1.1.1.8 Tempo de finalidade

Conceitualmente, entende-se por tempo de finalidade como o tempo necessário para que uma transação seja considerada probabilisticamente finalizada ou irreversível. Ou seja, que determinada transação já possua um número mínimo de confirmações que assegure sua imutabilidade.

Em termos gerais, plataformas blockchain contam com diferentes tipos de atraso, como apresentado na seção latência, que consequentemente implicam diferentes tempos de finalidade. O tempo de irreversibilidade de uma transação decorre de fatores específicos da

plataforma blockchain, principalmente em relação a ataques, como a existência de nodos maliciosos e até mesmo a probabilidade de blocos serem criados e submetidos simultaneamente, como explica Buterin (2015). Nota-se também que o tempo de finalidade varia com o tipo de algoritmo de consenso utilizado, e que algoritmos baseados em BFT mostram-se mais eficientes em relação aos tradicionais PoW e PoS.

Buterin (2015) realiza uma análise de casos da plataforma Ethereum a respeito deste indicador e questões de segurança, e estima que o tempo de finalidade para que uma transação na plataforma seja considerada segura (com 99,9% de chance de não reversão) é algo próximo de 3 minutos, ou 10 confirmações. O autor assume um tempo de confirmação de bloco de aproximadamente 17 segundos. Atualmente o tempo de confirmação do bloco se aproxima de 15 segundos, e que necessita de cerca de 12 confirmações, totalizando em um tempo de finalidade ainda próximo de 3 minutos.

Algumas plataformas contam também com algoritmos de consenso classificados como determinísticos, como o Hyperledger Fabric, o que resulta em qualquer bloco validado pelo nodo ordenador pode ser considerado final, reduzindo de forma significativa o tempo de finalidade. (HYPERLEDGER, 2020f).

De forma similar ao Fabric, o Algorand conta com finalidade imediata de transações, onde todo bloco criado pode ser considerado seguro e final. No Algorand, não existe a possibilidade de ocorrer *fork* na blockchain devido ao fato de que em cada *round* apenas um bloco pode ter o limite necessário de votos de comitê. Quando o algoritmo de consenso decide um bloco a ser adicionado, a decisão não pode ser alterada, e em caso de possíveis partições de rede, um nodo malicioso nunca é capaz de convencer outros 2 nodos honestos a aceitarem 2 blocos diferentes no mesmo *round*. (ALGORAND, 2019).

Na plataforma Corda, o tempo de finalidade é variável, visto que os serviços notários podem ou não se utilizar de algoritmos baseados em finalidade probabilística. Corda (2018) expõe que no âmbito empresarial um tempo de finalidade curto é quase sempre "não-negociável", o que torna a utilização de algoritmos baseados em BFT a opção mais favorável.

A Tabela 5 conta com uma relação de algumas das principais plataformas blockchain do mercado e seus respectivos tempos de finalidade considerados seguros.

É importante ressaltar também que, no caso de plataformas com algoritmos baseados em finalidade probabilística os blocos tornam-se "mais e mais finais" conforme novos blocos

são criados e confirmados, e consequentemente diferentes usuários e corretoras podem optar por níveis maiores ou menores de segurança, o que reflete em variações nos tempos de finalidade conforme a necessidade.

Tabela 5 – Relação entre plataformas blockchain e o tempo de finalidade.

Plataforma	**Num. de confirmações**	**Tempo (segundos)**
Bitcoin	6	600
Ethereum	12	180
EOS	330	180
IOTA	-	141
Algorand	1	5
Cardano	15	-
Hyperledger Fabric	-	Configurável
Multichain	-	Configurável
Corda	Variável	Variável

Fonte: Elaborado pelo autor.

4.1.1.2 Qualitativo

4.1.1.2.1 Resiliência

Quando trata-se de resiliência no meio tecnológico e cibernético refere-se a habilidade de uma entidade de entregar continuamente o resultado esperado, apesar de eventos cibernéticos adversos. O conceito também inclui a habilidade de se restaurar aos padrões regulares após tais eventos e de se modificar continuamente se necessário em face de novos riscos. (BJÖRCK et al., 2015).

Vangulick, Cornelusse e Ernst (2018) abordam resiliência à ataques cibernéticos voltados especificamente para a área de blockchain ligado à trocas de energia *peer-to-peer*, dividindo os ataques em duas categorias: Ataques gananciosos (de interesse próprio) e ataques de extorsão. A primeira categoria envolve participantes da rede que de forma maliciosa buscam benefício próprio às custas da comunidade ou de outros participantes. Os autores citam ataques como roubo de energia (que julgam ser resolvido pelo próprio design da aplicação), gasto duplo (que devido à rastreabilidade da energia e ao consenso julga-se sem risco de ocorrência) e ataques do tipo *Sybil* (que mesmo com custo-benefício insignificante

são tratados pelos autores junto com a categoria de ataques). A categoria de ataques de extorsão refere-se a cenários que buscam causar perturbações e solicitar compensação como forma de resgate para finalizar ou evitar repetição do ataque. Os autores propõem duas formas de resolver esta forma de ataques, uma matemática através do evitamento de concentração de "riquezas" e recomendações de pesos para variáveis propostas no estudo, e outra forma a partir da criação de motivações e punições para os nodos participantes.

Quadro 5 – Conclusões sobre a resiliência de plataformas blockchain.

Plataforma	**Conclusão**
Bitcoin	Forte resiliência contra imutabilidade de dados graças ao algoritmo de consenso utilizado e grande adoção da plataforma.
Ethereum	Forte resiliência contra imutabilidade de dados e código graças ao algoritmo de consenso utilizado e grande adoção da plataforma.
EOS	Menos resiliência que o Ethereum devido a utilização de apenas 21 validadores com a possibilidade de colusão e corrupção entre os validadores. Se os produtores de blocos agirem segundo as regras, o EOS pode providenciar resiliência contra imutabilidade de dados e código.
Cardano	Resiliência depende do número de eleitores. Se o número de eleitores for abaixo do proposto pelo protocolo pode haver colusão e corrupção entre os mesmos. Se os eleitores seguirem o protocolo estritamente, o Cardano pode providenciar resiliência contra imutabilidade de dados e código.
Hyperledger Fabric	Resiliência depende do número de endossantes e de ordenadores.
Hyperledger Sawtooth	Resiliência depende do número de validadores.
IOTA	A IOTA possui forte resiliência contra imutabilidade após um período de adaptação. O algoritmo de consenso favorece o acúmulo de peso na cadeia principal (poder de hash) tornando inviável qualquer modificação. Além disso, o esquema de assinatura implementado dentro do protocolo IOTA fornece forte resistência a ataques, inclusive a ataques de computadores quânticos.
Multichain	Resiliência depende do número de validadores.
Corda	Resiliência depende do número de validadores.

Fonte: Adaptado de Chowdhury et al. (2019).

Dorri et al. (2019a) propõem uma rede blockchain privada e segura (SPB) para solucionar diversos problemas ligados à troca de energia distribuída. A SPB proposta é

avaliada de forma qualitativa em relação a uma ampla gama de ataques, e segundo os autores pode ser considerada segura e resiliente. Alguns dos ataques avaliados são: Produtor Malicioso, Consumidor Malicioso, ataque de Certificado de Existência (onde o nodo malicioso finge ser um *smart meter* a partir de um *meter* real) e Nodo de *Backbone* Malicioso (onde o nodo de suporte principal (*backbone)* está comprometido e não entrega as transações para os nodos comuns).

Chowdhury et al. (2019) fazem comparações entre as 9 principais plataformas blockchain em relação a diversos critérios, dentre eles resiliência. As conclusões em relação a este indicador estão exibidas no Quadro 5.

4.1.1.2.2 Interoperabilidade

Para O'Neal (2019), interoperabilidade em blockchain refere-se em termos gerais à habilidade de compartilhar informações através de diferentes redes e plataformas blockchain, sem restrições. O atual cenário conta com dezenas de novos projetos surgindo a cada ano, competindo entre si com fim de desenvolver a "melhor" blockchain. Em geral, porém, cada projeto representa uma nova blockchain isolada, o que de certa forma contradiz a ideia base da tecnologia que a sustenta, a descentralização.

Ressalta-se também a contemporaneidade da tecnologia como um todo, e nota-se que diversas soluções e novas plataformas com foco em interoperabilidade vêm sendo propostas, como *Polkadot, Cosmos, Chainlink, Wanchain* e *Quant,* e que este indicador é algo essencial para a aplicação da tecnologia blockchain em diversos setores do mercado. (O'NEAL, 2019).

Rydzi e Truong (2019) mencionam um estudo de Zhang et al. (2017) focado na área de saúde que explica melhorias e desafios de interoperabilidade ligados ao blockchain na área. Menciona-se também que os desafios poderiam ser mitigados através da utilização de padrões familiares de software, como *Abstract Factory, Flyweight, Proxy* e *Publisher-Subscriber.*

Para Ahl et al. (2020) interoperabilidade é algo que não se deve deixar de lado quando pensa-se na implantação de blockchain no setor elétrico, e notam-se incertezas quando fala-se de interoperabilidade de sistemas digitais e *smart grids* legadas em larga escala, e propõem-se ajustes graduais nos Sistemas P2P[11]. Citando exemplos como Ethereum e

11 O termo "Sistema *P2P"* refere-se a sistemas de troca energética *peer-to-peer*, ou pessoa-a-pessoa, onde ocorre a compra e venda de energia entre duas ou mais partes participantes da *grid* elétrica. Disponível em: https://www.infiniteenergy.com.au/peer-to-peer-energy-trading/ Acesso em: 22 de maio de 2020.

Multichain os autores também colocam em questionamento se os atuais sistemas energéticos japoneses seriam capazes de suportar uma solução blockchain escalável. Grande importância também é dada quando fala-se de interoperabilidade de contratos inteligentes com leis de contrato de jurisdição.

Liu et al. (2020) buscam em seu estudo explorar as estratégias de escalabilidade para as tecnologias blockchain da próxima geração a partir da realização de *benchmarks* em larga escala. Os autores constatam que as técnicas de *Parallel-chain* (como *side-chain, cross-chain* e *child-chain*) têm entre outras intenções a de habilitar a interoperabilidade dentre múltiplas blockchains. Tais técnicas são explicadas no estudo, porém fogem ao escopo deste documento. Além disso, os autores também mencionam que um dos pontos negativos da escalabilidade voltada para a topologia de rede seria a perda da interoperabilidade.

4.1.1.2.3 Alocação de recursos

A Alocação de Recursos é uma atividade de gerenciamento intimamente relacionada ao gerenciamento estratégico (de recursos). O valor dos programas de alocação de recursos está no cumprimento dos objetivos organizacionais. A relação entre recursos e estratégia é uma via de mão dupla. A estratégia determina quais recursos são necessários, mas a disponibilidade de recursos também pode limitar uma estratégia (KANG et al., 2019).

O Blockchain se tornou uma estrutura promissora de gerenciamento de dados distribuídos e foi aplicada a muitos cenários de sistema distribuído. No entanto, o processamento em redes blockchain geralmente consome muitos recursos de computação. Segundo Sun et al. (2019) atualmente, o problema da alocação de recursos nas redes blockchain é um grande desafio.

Embora boas perspectivas possam ser esperadas, existem alguns problemas associados à adoção em ambientes de produção da tecnologia blockchain. Como apontado por Pongnumkul, Siripanpornchana e Thajchayapong (2017), é computacionalmente intensivo e consome muita energia implementar a técnica atual de blockchain (especialmente a baseada em PoW), mas a maioria dos sistemas pode não ter a capacidade de computação necessária, espaço de memória ou suprimento de energia para executar e armazenar blockchain.

Zheng et al. (2018) observaram em sua pesquisa, que durante a execução de contratos inteligentes, ele consome muitos recursos da CPU. O grau de consumo da CPU é

determinado pela lógica de negócios implementada no contrato. Rotinas de criptografia ou *loops* consomem muitos recursos da CPU. A ação de confirmar o bloco, computando o *hash* do estado mundial, também consome muitos recursos da CPU. Observe que diferentes sistemas de blockchain estão sendo executados nos pares equipados com diferentes CPUs. Portanto, dependendo do modelo de negócio implementado no blockchain, um indicador como métrica para monitorar a utilização da CPU ao executar os contratos inteligentes, talvez seja necessário.

Além disso, um blockchain possui espaço de armazenamento separado no disco rígido para armazenar os dados, incluindo o estado do livro razão. Além disso, consome os recursos de E/S (Entrada/Saída) enquanto mantém a blockchain (por exemplo, confirmação de bloco, execução de contrato).

Com o objetivo de permitir que os usuários saibam como os recursos são consumidos em todas as etapas e ajudar os desenvolvedores a otimizar o desempenho, Zeng et al. (2018) criaram um processo *daemon* para coletar e analisar logs nos pares. A intenção era coletar os dados sobre o consumo de hardware em blockchain (por exemplo, uso da CPU, memória, soquete de rede e leitura de disco). Os autores relatam, em trabalhos futuros, que vêm desenvolvendo um *upgrade* da ferramenta para fazer o monitoramento em tempo real.

Cabe mencionar que, como pode ser observado em sites de empresas que fornecem hardware para servidores empresariais, como Dell, IBM, Intel e AMD, os componentes que compõem a arquitetura deste super-computadores possuem um valor bem expressivo, podendo tornar a tarefa de preparar um ambiente ou atualizá-lo para a utilização da tecnologia blockchain, um tanto custoso para as organizações. Diante disso, e surgindo como uma oportunidade de negócio, empresas prestadoras de serviço em nuvem como AWS, IBM e Microsoft, passaram a oferecer uma nova modalidade de serviço conhecida como *Blockchain-as-a-Service* (BaaS) ou Blockchain como Serviço.

O BaaS pode ser entendido como um serviço fornecido para criação e o gerenciamento de rede de terceiros baseadas em nuvem para empresas no ramo de criação de aplicativos blockchain. Permite às empresas “desenvolver, operar, governar e expandir um ecossistema blockchain de forma rápida e econômica em uma plataforma flexível baseada na nuvem.” (IBM, 2020). Tal serviço oferece às empresas a possibilidade execução de tarefas que demandem uso intensivo de computação, memória, e E/S.

4.1.1.2.4 Tipo de licenciamento

Quando a tecnologia blockchain se tornou pública, foi alvo principalmente do setor financeiro. Em particular, o Bitcoin em seu *whitepaper* descrito como um sistema que permite aos utilizadores transferir dinheiro do ponto A para o ponto B, sem ter que depender de canais tradicionais.

No entanto, a blockchain já se espalhou além do financiamento, e suas aplicações são aparentes em gerenciamento de dados, *e-commerce*, e-governança, votação online, energia, jogos e outros setores. Na esteira destas novas aplicações, várias plataformas blockchain comerciais estão fazendo a sua criação. Durante o mesmo tempo, as comunidades blockchain *open-source* lançaram projetos de código aberto para o avanço da indústria. Pode-se dizer que foram estas iniciativas *open-source* que abriram o caminho e impulsionaram a adoção global da tecnologia.

Considerando-se a predominante difusão das plataformas blockchain *open-source*, houve homogeneidade quanto a este indicador entre os autores dos documentos selecionados. (MOEZKARIMI; ABDOLLAHEI; ARABSORKHI, 2019; KUZLU et al., 2019; SYED et al., 2019; JANSSEN et al., 2020; e CHOWDHURY et al., 2019).

Em plataformas de código aberto (*open-source*) como Bitcoin e Ethereum os mecanismos de governança são geralmente democráticos, onde usuários e mineradores em geral têm a palavra final sobre como os sistemas DLT podem evoluir. Ambos os sistemas apóiam a noção de responsabilidade e transparência. Devido a todos esses atributos positivos, há um forte nível de confiança em ambos os sistemas e eles foram amplamente utilizados para interromper as abordagens tradicionais em vários domínios de aplicativos.

Um aspecto interessante nos sistemas DLT públicos é o mecanismo de governança correspondente. Todos eles são *open-source* e com pouca diferença na maneira como as melhorias são realizadas. Bitcoin, Ethereum e Cardano permitem que qualquer pessoa envie propostas de melhoria que são então aprovadas por diferentes mecanismos.

Segundo Valkenburgh (2017), o design *open-source* é algo essencial para construir confiança e segurança nas redes blockchain, visto que isso implica um projeto produzido de forma colaborativa, transparente e desenvolvido para ser um bem da comunidade, não uma propriedade de uma empresa ou pessoa singular. O resultado de softwares *open-source*

geralmente reflete códigos extremamente resilientes feito por usuários para usuários, visto que estes buscam melhorias e constante eliminação de redundâncias dos mesmos.

Como exemplos de blockchains *open-source* pode-se citar o Bitcoin, Ethereum, Neo, Hyperledger Sawtooth, Hyperledger Fabric, Ripple e Cardano.

Embora haja a predominância na utilização de blockchains de código aberto, algumas das instituições ou fundações que mantém o código-fonte e atualizações destas plataformas oferecem soluções para empresas, com um *upgrade* da versão *open-source*. Nestas versões diferenciadas, são oferecidos serviços de suporte a atualizações, implantações e correção de *bugs,* mão de obra de desenvolvedores e arquitetos blockchain, consultoria especializada, apoio e customizações para adequação ao modelo de negócio da empresa, além do fornecimento em primeira mão de novas versões e funcionalidades personalizadas ao cliente empresarial. Esse adicional pode ser contratado junto às mantenedoras do blockchain mediante contratos de prestação de serviços e ou licenciamento de software específico, caso necessário (ETHEREUM, 2020; R3, 2020; IBM, 2020).

4.1.1.2.5 Algoritmos de consenso

Uma das principais características da tecnologia Blockchain é sua arquitetura descentralizada. Múltiplos nodos interagem entre si sem um elemento central. Desta forma, para que as transações sejam consideradas válidas no *ledger* um algoritmo de consenso precisa ser implementado. Este consenso é uma forma dinâmica de encontrar um acordo em grupo. Os algoritmos de consenso procuram garantir que as regras do protocolo sejam seguidas, assegurando-as para todas as transações, tornando o sistema Blockchain confiável e garantindo que a transação aconteça uma única vez. (ZHENG; ZHU; SI, 2019).

Para Sankar et al. (2017) um algoritmo de consenso é uma sequência de passos que os participantes de um sistema distribuído seguem para tomar uma decisão conjunta e unânime.

Para Cao et al. (2020) o algoritmo de consenso em uma Blockchain tem por objetivo fazer a rede chegar a um acordo na presença de faltas, sendo a chave para criar confiabilidade distribuída entre os usuários. Ainda comenta que o mecanismo de consenso desempenha um papel fundamental na performance do Blockchain.

Existem vários algoritmos de consenso e continua sendo um desafio para desenvolvedores e pesquisadores estudá-los e aperfeiçoá-los. Os mais utilizados são PoW,

PoS e DPoS (Delegated Proof-of-Stake). Entretanto existem outros como Raft, pBFT, PoA, PoB (BAIRD, 2016; BARINOV; BARANOV; KHAHULIN, 2018; CASTRO; LISKOV, 1999).

a) *Proof-of-Work (PoW):* A prova de trabalho é o mecanismo de consenso mais clássico principalmente devido à sua aplicação no Bitcoin. Neste tipo de consenso aparece a Figura dos mineradores. Palavra singular que lembra a busca pelo ouro que geralmente não é tarefa fácil. A ideia central é que os mineradores, membros do sistema, competem entre si usando todo seu poder computacional para resolver um quebra-cabeça criptográfico baseado em funções de *hash* (e.g., SHA-256). O competidor que encontrar primeiro uma solução para o quebra-cabeça é o vencedor e consequentemente tem direito de inserir um novo bloco na blockchain e receber uma recompensa. Esta recompensa normalmente é em dinheiro, ou melhor, criptomoedas como Bitcoin. Neste tipo de solução se consome uma grande carga computacional (CAO et al., 2020)

b) *Proof-of-Stake (PoS):* Com o objetivo de aliviar a carga computacional do PoW devido a tentativa de solucionar o quebra-cabeça complexo baseado em funções de *hash*, surgiu a prova de participação (PoS). Este tipo de mecanismo propõe o conceito de idade da moeda, que é um ativo não gasto multiplicado pela sua duração, desde o último momento vencedor até a hora atual. Este processo também tem base no *hash* e numa maior idade da moeda que levará a uma maior probabilidade de ganhar o direito de criar um novo bloco. Neste tipo de mecanismo os usuários candidatos a participar do processo de construção dos blocos precisam bloquear uma quantidade de suas criptomoedas como participação (*Stake*). O tamanho da participação é uma espécie de aposta que aumenta as chances de ser o ganhador e ter direito a criar o bloco seguinte. Além deste critério e para não privilegiar sempre os mesmos ganhadores, outros critérios são adotados como a seleção da idade da moeda e seleção aleatória de blocos citados acima. (CAO et al., 2020; MAESA; MORI, 2020; ZHENG; ZHU; SI, 2019).

c) *Delegated Proof-of-Stake (DpoS):* Apesar do mecanismo PoS apresentar avanços comparados ao PoW, principalmente na redução da carga computacional, novos problemas surgiram. Um deles é chamado de "*Nothing at Stake*". Suponha que exista uma pequena rede Blockchain vazia derivada de uma principal. No PoW todos os nodos trabalharão na rede mais longa porque seria um desperdício de energia computacional trabalhar na mais curta. No protocolo PoS, um minerador malicioso pode minerar na cadeia mais curta, porque não terá risco de perder participação, logo o protocolo não pode evitar quebras de cadeias. Uma melhoria neste mecanismo provocou o surgimento de sua derivação chamada de *DPoS* (*Delegated Proof-of-Stake*), em Português, prova de participação delegada. Neste mecanismo o consenso depende do poder de votação das partes interessadas, onde as partes interessadas podem eleger qualquer número de testemunhas e os blocos são gerados pelas testemunhas eleitas em uma ordem sequencial sem um acordo global. Com este mecanismo o consenso torna-se mais rápido, eficiente e mais flexível comparado com o PoS. Há críticas entretanto com relação a centralização quando houver um baixo número de testemunhas. (CAO et al., 2020).

d) *Practical Byzantine Fault Tolerance (pBFT):* Este mecanismo de consenso, usado pela rede Blockchain Hyperledger Fabric, todos os nodos se comunicam tendo como objetivo alcançar um consenso através de um acordo entre a maioria. Sua vantagem é a redução da carga computacional, entretanto é indicado para grupos de trabalho pequeno e consequentemente pouca escalabilidade. (CAO et al., 2020).

A Tabela 6 mostra os algoritmos mais importantes segundo Zheng et al. (2018) e traz um comparativo referente a BFT, CFT (*Crash Fault-Tolerant)*, verificação de velocidade, TPS, escalabilidade e as plataformas que os utilizam.

Dorri et al. (2019b) propuseram uma aplicação de Blockchain para o setor elétrico implementando um diferente mecanismo de consenso. Nesta aplicação o foco era o sistema distribuído de energia onde os envolvidos no consumo e produção de energia poderiam fazer negócio tendo o Blockchain como suporte. Com o objetivo de reduzir a falta de privacidade,

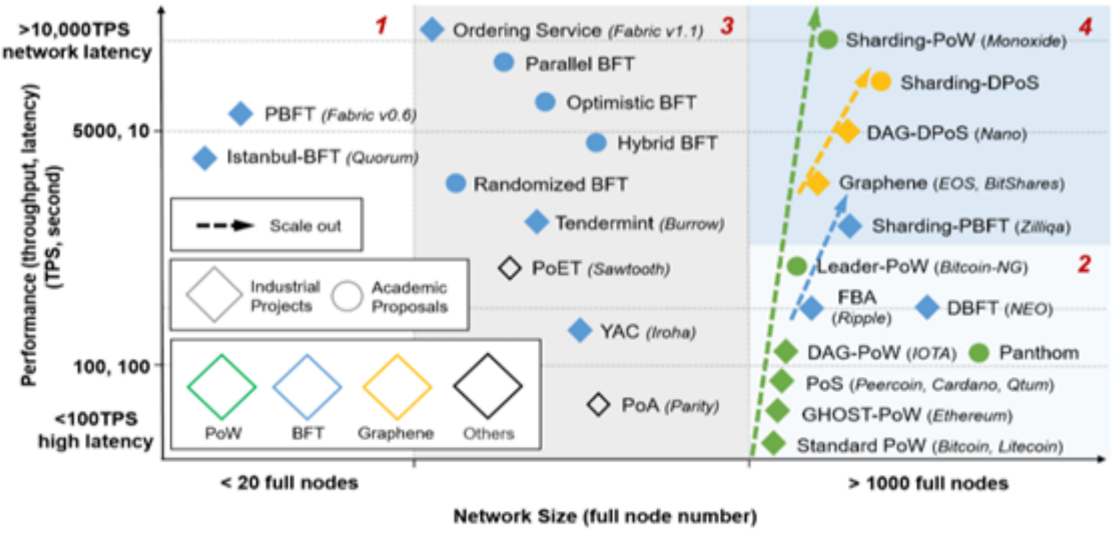
capacidade de processamento e sobrecargas dos pacotes os autores propõem a utilização do mecanismo de consenso DTC (*Distributed Time-based Consensus*) dentre outras detalhes específicos da aplicação. No DTC, o minerador pode criar um bloco somente a cada período de tempo previamente acordado. Maiores detalhes do mecanismo de consenso pode ser obtido em Dorri et al. (2019b).

Tabela 6 – Análise de algoritmos de consenso.

Característica	**PoW**	**PoS**	**DPoS**	**Raft**	**pBFT**
BFT	50%	50%	50%	-	33%
CFT	50%	50%	50%	50%	33%
Velocidade de verificação	>100 s	< 100 s	< 100 s	< 10 s	< 10 s
TPS	< 100	< 1000	< 1000	> 10000	< 2000
Escalabilidade	Forte	Forte	Forte	Fraca	Fraca
Plataformas típicas	Bitcoin	Ethereum	BitShares	Quorum	Hyperledger Fabric

Fonte: Zheng et al. (2018).

Figura 17 – Correlação entre performance *vs* tamanho da rede.



Fonte: Li et al. (2020).

Li et al. (2020) realizam um interessante estudo comparativo entre alguns algoritmos de consenso e suas relações com a performance e o tamanho da rede. Para a performance leva-se em conta o trabalho realizado, latência da rede e transações por segundo. Para o tamanho da rede foi levado em consideração o número de nodos. A Figura 17 mostra este comparativo. Importante destacar que os mecanismos mais sofisticados estão na região 4,

onde têm-se melhores performances e maior números de nodos. Os autores salientam que nesta região 4 os mecanismos são derivações dos tradicionais como pode ser visto na imagem. Estes algoritmos de consenso são constituídos de projetos industriais e também de propostas acadêmicas, sendo alguns modelos ainda nunca implementados fora do laboratório. Entre parênteses pode-se verificar os tipos de Blockchain que implementam os respectivos mecanismos de consenso.

4.1.1.2.6 Escalabilidade

Zheng, Zhu e Si (2019) definem escalabilidade como o indicador que avalia as mudanças de *throughput* e latência de transação quando uma blockchain experimenta aumento de nodos e de cargas de trabalho concorrentes (transações a serem validadas). Os autores avaliam os cinco principais algoritmos de consenso quando tratamos de escalabilidade, e os autores classificam os algoritmos PoW, PoS e DpoS como algoritmos de forte escalabilidade, e os algoritmos Raft e pBFT como de fraca escalabilidade. Também trata-se do armazenamento de dados, e menciona-se que bancos de dados relacionais são menos escaláveis que bancos não relacionais, porém são adequados para *datasets* consistentes e de crescimento vagaroso. Na análise de plataformas blockchain populares em relação a escalabilidade, os autores afirmam que a performance da implementação do Ethereum conhecida por Parity mantém-se constante enquanto a implementação Go Ethereum degrada linearmente em função do número de transações ou nodos. Portanto. Ainda, o Hyperledger pode escalar até apenas 16 nodos e o IOTA possui aumento de escalabilidade conforme o número de usuários aumenta. Conclui-se também que a fraca escalabilidade da tecnologia blockchain é um dos principais fatores que dificultam a adoção da tecnologia em larga escala no setor comercial e financeiro.

Para Moezkarimi, Abdollahei e Arabsorkhi (2019) escalabilidade é um dos fatores considerados importantes e efetivos na avaliação da plataforma. Limitantes deste critério, segundo os autores seriam restrições no número de transações por segundo, número de nodos participantes nos processos da rede principal, número de usuários e tempo de validação de bloco.

Para avaliar a escalabilidade da plataforma Hyperledger Fabric, Kuzlu et al. (2019) explicam que em uma rede blockchain escalabilidade pode ser medida de diferentes formas,

como: baseado no número de canais, no número de pontos de acesso, número de organizações, número de nodos, número de transações e algoritmo de consenso. Os autores optam por utilizar o número total de transações como critério de escalabilidade em sua avaliação. A partir dos testes realizados concluiu-se que o tipo de transação tem uma influência significativa na performance da blockchain, e que um aumento nas transações simultâneas também afeta significativamente a performance da blockchain, principalmente quanto a latência, porém nota-se que a taxa de transação não foi afetada pelo mesmo.

Thakkar, Nathan e Viswanathan (2018) apontam que no Fabric, do ponto de vista do consumo de recursos, o nível de complexidade das políticas de aprovação das transações controla a escalabilidade da rede. Mesmo com um grande número de organizações ou pares, se as políticas definidas envolverem apenas algumas organizações, o desempenho não será afetado. Isso ocorre porque a transação precisa ser simulada em um número pré-definido de nodos pré estabelecidos (ambos especificados na política de endosso) na rede para coletar as aprovações. A escalabilidade também pode ser definida em termos de número de nodos geograficamente distribuídos e latência na disseminação de blocos entre eles. Ainda, segundo os pesquisadores, o número de nodos de serviço de pedidos e a escolha do protocolo de consenso usado entre eles também afetariam a escalabilidade.

4.1.1.2.7 Desempenho

O Blockchain foi projetado para uso em um ambiente onde não há partes confiáveis e administração central, mas a imutabilidade de dados e segurança é importante. Devido à natureza inerentemente distribuída e ponto a ponto da tecnologia, as transações baseadas em blockchain só podem ser concluídas quando todas as partes atualizam seus respectivos livros contábeis, o que pode ser um processo lento. Portanto, a implementação do blockchain é cara e muitas de suas funções também são fornecidas por soluções tradicionais de gerenciamento de bancos de dados centralizados, ou seja, por um banco de dados relacional. No entanto, o desempenho da blockchain em termos de *throughput* é significativamente mais lento em comparação com bancos de dados relacionais. Por exemplo, o *throughput* do Bitcoin e do Ethereum é de apenas 4 TPS e 20 TPS, respectivamente, enquanto o *throughput* médio da Visa e do PayPal é de 1667 TPS e 193 TPS, respectivamente (MECHKAROSKA; DIMITROVA; POPOVSKA-MITROVIKJ, 2018). A perda de desempenho é negociada por

uma vantagem do blockchain, pois fornece uma maneira confiável, robusta e segura de armazenar dados sem interferências de terceiros.

Embora blockchains possam parecer semelhantes aos bancos de dados distribuídos, elas geralmente são implementadas sem uma autoridade central e um repositório central. Portanto, as blockchains fornecem algumas diferenças únicas em relação a tudo o que veio antes. Um blockchain sobrevive a falhas e ataques usando verificação redundante em vários nodos (HYPERLEDGER, 2018). Essa resiliência vai muito além da replicação, pois ocorre na rede sem nenhum coordenador ou intermediário central.

Em alguns outros sistemas em rede, como camadas da web, adicionar nodos serve para dividir o trabalho entre mais recursos e aumentar o desempenho. Isso geralmente é o inverso em blockchains, onde mais nodos aumentam a resiliência do sistema em termos de integridade e disponibilidade, geralmente com algumas despesas para o desempenho. Mesmo essa noção simples pode ser complicada quando analisamos a amplitude do blockchain. Algumas blockchains especializam as funções de nodos. Nesses sistemas, um nodo pode não mais implicar um participante exclusivo (como uma empresa) com uma parcela da carga de resiliência. Isso torna muito difícil medir e comparar o desempenho entre diferentes blockchains (HYPERLEDGER, 2018).

Observa-se no estudo de Thakkar, Nathan e Viswanathan (2018) que em blockchains privadas a) a verificação de política de endosso, b) a validação de política sequencial de transações em um bloco e c) a validação e confirmação das transações no banco de dados de estado foram os três principais gargalos de desempenho, considerando plataformas blockchain que possuem transações do tipo *transação de endosso*.

Dinh et al. (2017) apontam em seu estudo que os indicadores: *throughput*, latência, escalabilidade e a capacidade de tolerância a faltas de um blockchain são os principais responsáveis por gargalos de desempenho em um sistema blockchain.

Zheng, Zhu e Si (2019) evidenciam que todas as preocupações com segurança e desempenho são devidas ao chamado "*Scalability Trilemma*" (em tradução livre, Trilema da Escalabilidade), onde um sistema Blockchain tenta oferecer escalabilidade, descentralização e segurança, sem comprometer nenhuma delas.

No estudo apresentado por Rydzi e Truong (2019) pode-se observar que existem problemas complexos e tipos de conhecimento sobre desempenho que um desenvolvedor

precisa entender para projetar e definir implantações adequadas de recursos de blockchain. Isso ocorre devido à falta de uma padronização ou metodização que auxilie esses profissionais no compartilhamento e recomendação de recursos e tecnologias utilizados no desenvolvimento de aplicativos baseados em blockchain.

Faz-se necessário também algumas considerações acerca dos desafios de desempenho enfrentados pela implantação da tecnologia blockchain nos setores industriais. As atuais escalas de aplicação na indústria são geralmente volumosas, o que requer das plataformas de blockchain processar transações com um *throughput* muito alto. A grande maioria das plataformas de blockchain de ponta não podem lidar com altas taxas de transações e com isso o desempenho será severamente degradado. Especialmente para os serviços financeiros, a baixa escalabilidade e os altos atrasos no processamento de transações da blockchain se tornam o principal gargalo de desempenho (ZHENG; ZHU; SI, 2019). Para aplicativos de IoT, o gargalo é diferente. Samaniego e Deters (2017) avaliam o desempenho de uma blockchain hospedada em nuvem e borda, em que a blockchain é proposta como um serviço para a IoT. Em seu trabalho mostram que a latência da rede é o fator de desempenho dominante quando a blockchain é adotada nos sistemas de IoT. A escalabilidade se tornou um problema premente com o rápido crescimento no tamanho do aplicativo e nos volumes de transações.

4.1.1.2.8 Tolerância a faltas

Segundo Silva (2013) uma falha de sistema ocorre quando o serviço prestado se desvia de cumprir sua função conforme a especificação do sistema. Falhas são causadas por erros. Erros ocorrem em tempo de execução quando alguma parte do sistema entra em um estado inesperado devido a ativação de uma falta. Faltas são defeitos, um passo incorreto, processo ou definição de dados que faz com que o sistema passe a se comportar de forma não intencional ou imprevista. Faltas podem ser um *bug* em um programa, um problema de configuração e/ou uma interação originada de um sistema externo ou um usuário. Um erro não necessariamente provocará uma falha, por exemplo, uma exceção pode ser lançada e o funcionamento global do sistema continuará em conformidade com a especificação. De maneira geral, uma falta, quando ativada, pode levar a um erro que pode levar ou a outro erro ou a uma falha.

Em sistemas distribuídos tanto os processos quanto os canais de comunicação podem divergir do comportamento correto (ou desejável), caracterizando uma falta.

Hadzilacos e Toueg (1994) fornecem uma taxonomia que distingue as faltas em:

a) Faltas por omissão – Casos onde um processo ou um canal de comunicação deixa de executar as ações que deveria.
b) Faltas arbitrárias (ou bizantinas) - Descreve uma semântica onde qualquer tipo de erro pode ocorrer.
c) Faltas de sincronização (ou temporização) - Aplicáveis aos sistemas distribuídos síncronos onde limites de tempo são estabelecidos para o tempo de execução dos processos. Estas falhas podem ser:
    i) No processo, por exemplo, o relógio local ultrapassa os limites de sua taxa de desvio em relação ao tempo físico.
    ii) No canal, por exemplo, a transmissão de uma mensagem demora mais do que o limite definido

As faltas dos processos podem ocorrer tanto no domínio do tempo quanto no domínio dos valores. As faltas que ocorrem no domínio do tempo são mais simples de se tratar. Já as faltas que ocorrem no domínio dos valores são chamadas arbitrárias ou bizantinas (LAMPORT; SHOSTAK; PEASE, 1982).

Uma falta bizantina (ou arbitrária) é uma condição dos sistemas de computação distribuídos, onde os nodos podem falhar e os nodos maliciosos podem existir; e não há conhecimento sobre se um nodo falhou ou é um nodo malicioso. Um protocolo de consenso BFT é tolerante a faltas bizantinas se puder funcionar em um ambiente com nodos maliciosos e nodos com falha, enquanto um protocolo que não é tolerante a faltas bizantinas (*non*-BFT) funciona apenas para nodos com falha, não sendo capazes de identificar a atividade de nodos maliciosos. Alguns algoritmos de consenso da blockchain são tolerantes a faltas bizantinas, onde nodos honestos ainda podem chegar a um acordo com a existência de nodos maliciosos. Algoritmos de consenso não foram projetados para funcionar em um ambiente malicioso e supõem que todos os nodos são honestos e só podem tolerar falhas gerais do sistema.

Faltas ou comportamentos maliciosos em nodos são ocorrências comuns em um sistema distribuído e, portanto, é importante estudar a capacidade de tolerância a faltas de um blockchain. No estudo de Thakkar, Nathan e Viswanathan (2018), testando a plataforma

Fabric, os pesquisadores apontam que as faltas no nodo não afetam o desempenho (durante casos sem sobrecarga), pois o cliente pode receber as aprovações de outros nodos disponíveis. Entretanto, com cargas mais altas (saturação de transações), eles observam que os nodos que reingressam na rede após uma falha e a sincronização do livro razão devido à falta de blocos apresentam grandes atrasos. Isso ocorre porque, embora a taxa de processamento de bloco no nodo reconectado estivesse no pico, outros nodos continuam adicionando novos blocos na mesma taxa de processamento de pico.

4.1.1.2.9 Presença de banco de dados

Para o armazenamento das transações são utilizados os SGBD (sistemas gerenciadores de banco de dados). Os tipos mais usados são os bancos de dados relacionais e não relacionais. Em Blockchain menciona-se que bancos de dados relacionais são menos escaláveis que bancos não relacionais, porém são adequados para datasets consistentes e de crescimento vagaroso.

De forma simplificada, para o Hyperledger, Banco de Dados de Estado refere-se a uma visão indexada dos *logs* de transações, e consequentemente pode ser gerado e regenerado da blockchain a qualquer momento. Bancos de dados de estado armazenam os últimos valores de todas as *keys*, e são utilizados para tornar mais eficientes as interações *chaincode*[12], visto que estas executam transações com base no estado atual dos dados. (HYPERLEDGER, 2020g).

No estudo de Thakkar, Nathan e Viswanathan (2018) realiza-se a comparação acerca de dois bancos de dados de estado para a plataforma Hyperledger Fabric, sendo eles o GoLevelDB e o CouchDB. Os resultados mostraram que a taxa de transações quando utilizando-se do LevelDB foi três vezes maior que quando se utilizou o CouchDB, e os autores explicam que isso se dá decorrente de que o primeiro é um banco de dados embutido para pares de processos, enquanto que o segundo se acessa através de *REST APIs* em um servidor *HTTP* seguro.

Saraf e Sabadra (2018) realizam uma análise comparativa das principais plataformas Ethereum, Hyperledger, Corda e de seus derivados. Os autores entram em detalhes sobre o

12 *Chaincode* é um pedaço de código instalado e instanciado em uma rede de nodos do Hyperledger Fabric que possibilita interações com o *ledger* da rede. Disponível em: https://fabrictestdocs.readthedocs.io/en/latest/chaincode.html. Acesso em: 04 de maio de 2020.

funcionamento de todas as plataformas abordadas, e definem o banco de dados de estado presente no Hyperledger Fabric como algo que guarda o atual estado do par chave-valor do *ledger*. Segundo os autores, o banco de dados de estado auxilia no aumento de eficiência de transações, visto que este possibilita a extração do último par chave-valor de forma fácil.

Na análise de Saraf e Sabadra (2018) aborda-se também a plataforma Corda, como mencionado, e nota-se a existência de um Objeto de Estado na plataforma, que se assemelha de certa forma ao banco de dados de estado proposto para o Fabric. Os autores conceituam o objeto de estado como sendo um documento digital que guarda a existência, conteúdo e atual estado de um acordo entre duas ou mais partes.

Hassan, Yuen e Niyato (2019) avaliam duas possíveis forma de gerenciamento de dados, *On-chain* e *Off-chain*, e as analisam conforme vantagens e desvantagens, conforme mostra o Quadro 6.

Quadro 6 – Comparativos de gerenciamento de dados para blockchain.

Tipo	**Descrição**	**Vantagens**	**Desvantagens**
On-chain	Todas as transações validadas são guardadas na blockchain	Maior transparência, auditabilidade e disponibilidade de dados	Fardo grande de armazenamento, menos escalável e não eficiente para nodos com recursos limitados
Off-chain	Apenas os hashes de dados importantes são armazenados na blockchain	Menos requisitos de armazenamento, eficiente para nodos com recursos limitados	Bancos de dados convencionais são necessitados para hospedar dados *off-chain*

Fonte: Adaptado de Hassan, Yuen e Niyato (2019).

Chowdhury et al. (2018) realizam um estudo aprofundado visando comparar métodos de bancos de dados convencionais com métodos blockchain. Os autores também realizam uma revisão de escopo das aplicações blockchain no período de cinco anos prévios ao estudo e, por fim, propõem uma árvore de decisão para verificar se o caso de uso em questão deve ou não utilizar a tecnologia blockchain, e caso sim, qual tipo de tecnologia blockchain deve ser utilizada.

Na comparação proposta por Chowdhury et al. (2018) analisam-se cinco principais critérios: a) construção de confiança; b) confidencialidade e privacidade; c)

robustez/tolerância a faltas; d) performance; e) segurança. A partir destes critérios, elaborou-se o Quadro 7.

Por fim, Chowdhury et al. (2018) julgam que blockchain não é uma tecnologia com propósitos gerais, mas que quando aplicada corretamente exibe diversos benefícios. Propõe-se então uma árvore de decisão (Figura 18) que pode ser utilizada por parte de analistas de negócios ou arquitetos de sistemas para a decidir a viabilidade da adoção da tecnologia blockchain.

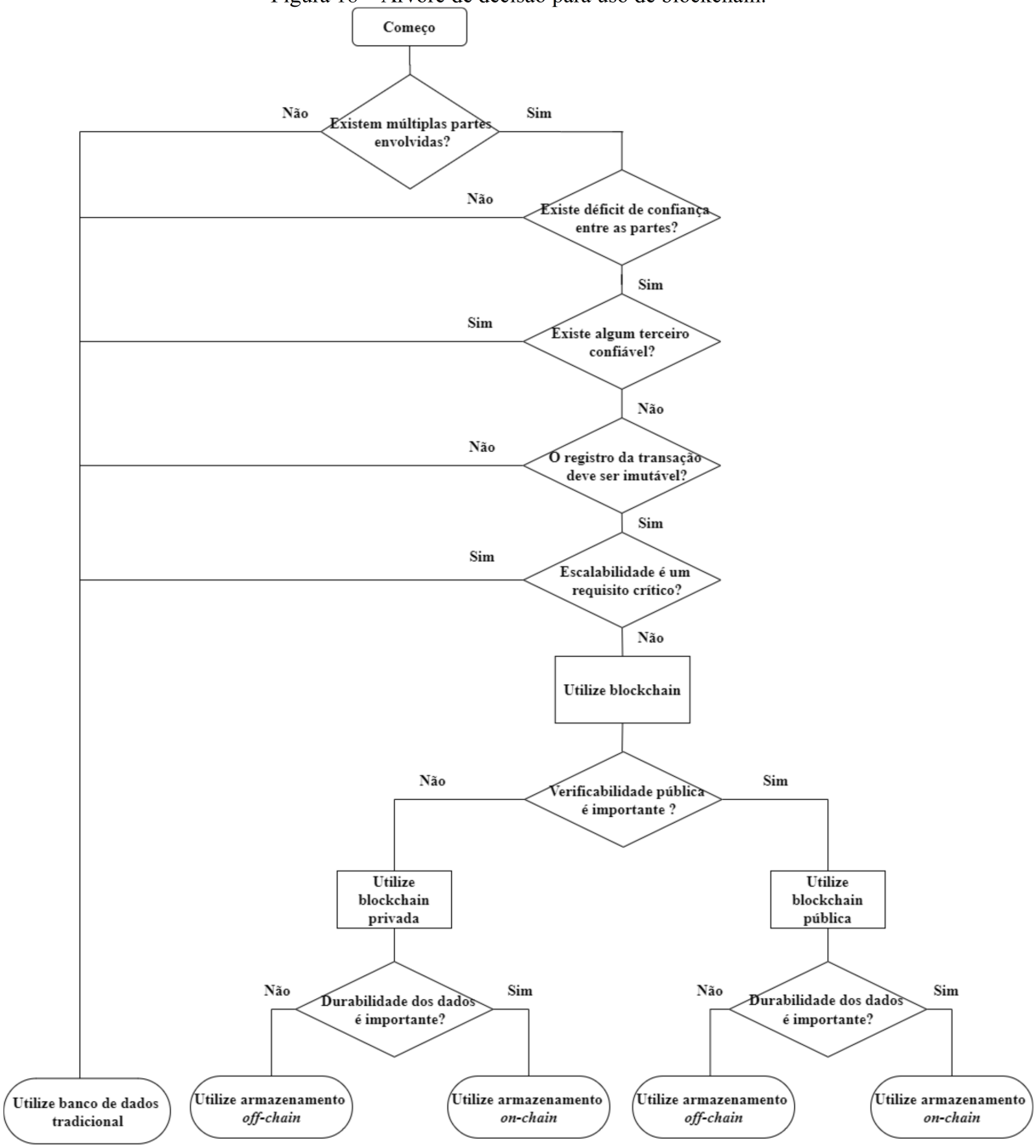
Quadro 7 – Comparação de métodos tradicionais e tecnologia blockchain.

Problema	**Blockchain**	**Banco de dados central**	**Vantagem**
Construção de Confiança	Pode operar sem qualquer confiança entre os envolvidos	Necessita de uma parte central confiável	Blockchain
Confidencialidade dos dados	Todos os nodos têm visibilidade dos dados (por padrão)	Restringe acesso à pessoal autorizado	Banco de dados
Robustez/ Tolerância à Faltas	Dados distribuídos pelos nodos	Dados armazenados no banco de dados central	Blockchain
Performance	Leva certo tempo para alcançar consenso (e.g. 10 min para o Bitcoin)	Execução/atualização imediata	Banco de dados
Redundância	Cada nodo participante tem a última cópia (por padrão)	Apenas a parte central tem uma cópia dos dados	Blockchain
Segurança	Usa medidas criptográficas (por padrão)	Controle de acesso tradicional	Blockchain

Fonte: Chowdhury et al. (2018).

Segundo Chowdhury et al. (2018) a tecnologia blockchain é útil em casos de uso onde existe mais de uma autoridade administrativa e onde existe déficit de confiança entre as mesmas. Como exemplos típicos os autores citam o gerenciamento de cadeias de suprimentos e um possível consórcio entre empresas independentes trabalhando em conjunto em um projeto para o governo. Para a decisão acerca de blockchains do tipo público ou privado os autores ressaltam que se existe necessidade de que os dados armazenados na blockchain sejam de visibilidade pública, deve-se optar por uma blockchain pública, e que se os dados são apenas para partes específicas então deve-se optar por uma blockchain privada.

Figura 18 – Árvore de decisão para uso de blockchain.



Fonte: Adaptado de Chowdhury et al. (2018).

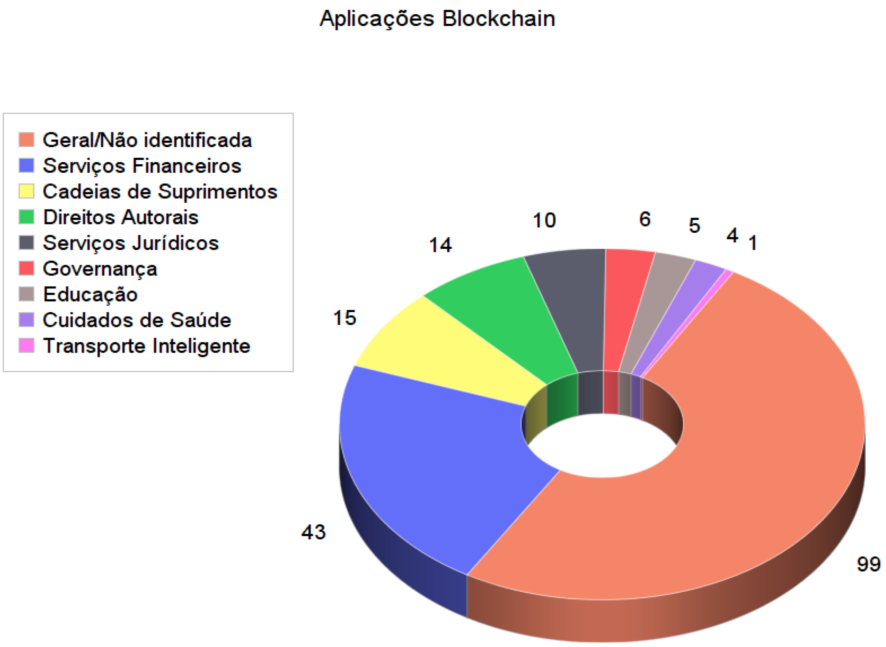
4.1.2 Dimensão Objetivo

4.1.2.1 Qualitativo

4.1.2.1.1 Aplicação

Espera-se que as tecnologias blockchain impulsionem inovações, melhorem os processos existentes ou desbloqueiem novas tecnologias. Gigantes da indústria, tecnologia e finanças como Tesla, IBM e JP Morgan, respectivamente, figuram dedicadas ao desenvolvimento de novos aplicativos baseados em blockchain. No início de 2019, haviam 197 provedores de serviços de blockchain registrados na *Cyberspace Administration of China* (ZHANG, 2019). Os serviços foram agrupados em nove categorias, como mostra a Figura 19. Entre esses provedores, cerca da metade fornece uma plataforma geral de blockchain ou serviços de blockchain não reconhecidos. A segunda maior categoria é de serviço financeiro, que inclui 43 provedores e é obviamente a aplicação mais comum do blockchain. As seguintes categorias são serviços de cadeia de suprimentos, proteção de direitos autorais e serviços jurídicos. Existem também alguns fornecedores focados em governança, saúde, educação e transporte inteligente.

Figura 19 – Aplicações blockchain registradas na *Cyberspace Administration of China.*



Fonte: Elaborado pelo autor.

Para Moezkarimi, Abdollahei e Arabsorkhi (2019) o objetivo ou aplicação de uma blockchain consiste essencialmente em criptomoeda, contratos inteligentes e da existência de uma estrutura para o desenvolvimento de aplicativos. Devido à aplicação de cada plataforma,

os recursos e componentes esperados variam. Por exemplo, plataformas desenvolvidas com o objetivo de implementar contratos inteligentes exigem um componente para compilar e executar esses contratos. Ainda segundo os pesquisadores, se as plataformas forem mais gerais e não projetadas para atingir um objetivo ou aplicativo específico, serão mais úteis. Essas plataformas gerais, que os pesquisadores definem como plataformas flexíveis, podem ser usadas por uma maior variedade de aplicativos.

Hearn (2016) apresenta o blockchain Corda como um banco de dados global descentralizado com confiança mínima entre os nodos. De acordo com o projetista, esta tecnologia visa atender a várias aplicações; financeiras, comerciais, rastreamento da cadeia de suprimentos entre outras, fornecendo uma plataforma para o desenvolvimento descentralizado de aplicativos baseada em contratos inteligentes.

Segundo Thakkar, Nathan e Viswanathan (2018) a aplicação ou o objetivo que se deseja atingir com uma implementação blockchain estão intimamente relacionados às especificações dos indicadores. Segundo eles, dependendo do aplicativo e dos requisitos, pode ser necessário avaliar alguns questionamentos como: *Qual deve ser o tamanho do bloco para obter uma menor latência? Quantos canais podem ser criados e qual deve ser a alocação de recursos? Que tipos de política de endosso são mais eficientes? Qual é a diferença de desempenho entre determinados bancos de dados de estados?* A preocupação dos pesquisadores é pertinente ao fato de que se deve observar se a solução blockchain escolhida é realmente a mais apropriada ao tipo de negócio que se deseja executar, partindo da aplicação para a tecnologia e não o inverso. Em outras palavras, deve-se ter claramente definido o objetivo da solução, para então buscar pela tecnologia blockchain ideal. Adotando esse tipo de abordagem, entende-se que se deve adaptar o modelo de negócio à tecnologia e não customizar/modificar a tecnologia para atender ao modelo de negócio.

O Blockchain pode adicionar valores significativos a variadas aplicações em diferentes domínios comerciais e industriais e pode habilitar novos modelos de negócios que antes não eram possíveis. De acordo com Zheng, Zhu e Si (2019), atualmente, os modelos de negócios baseados em blockchain mais propostos estão relacionados a moedas criptografadas. Recursos de blockchain, como identidade digital, segurança distribuída, acordos do tipo consenso e operação sem intermediários, são capazes de aprimorar os recursos competitivos e

a flexibilidade de muitos setores. Portanto, é importante considerar como novos modelos de negócios podem ser desenvolvidos, implantados e medidos.

4.1.3 Dimensão Suporte

4.1.3.1 Qualitativo

4.1.3.1.1 Documentação

Documentação de software pode ser entendida como um conjunto de documentos que instruem algum público sobre um software. Destacamos aqui dois tipos de documentação. A primeira é a documentação de usuário, que instrui como *usar* o software (HORCH, 2003). A segunda é a documentação dos desenvolvedores, que descreve o design e requisitos do software em desenvolvimento (HORCH, 2003) e auxilia os desenvolvedores a solucionar eventuais problemas que surjam durante o desenvolvimento do software. (JAMES, 2008).

Segundo Moezkarimi, Abdollahei e Arabsorkhi (2019), possuir um extenso suporte e boa documentação, como descrição dos designs e aspectos da plataforma, relatórios técnicos de implementação, tutoriais e amostras de exemplo podem ser considerados vantagens e levam ao uso de forma otimizada da plataforma pelo usuário. Além disso, quanto mais documentação uma plataforma possuir, mais os usuários e desenvolvedores podem utilizar e trabalhar para melhorar as mesmas.

Benahmed et al. (2019) realizam um estudo comparativo de diversas plataformas blockchain e utilizam-se da documentação para analisar a usabilidade da plataforma e quão fácil ou difícil é sua utilização. São levados em conta a extensão da documentação, sua situação de manutenção (constantes atualizações ou documentação descontinuada) e existência de amostras e exemplos de utilização.

Com relação a documentação deve-se considerar também o fluxo e frequência de atualização dos repositórios do código da plataforma blockchain, como o GitHub ou Bitbucket. Se a tecnologia fornece uma documentação detalhada do projeto, recursos para testes (massa de testes) como processadores de transação de amostra e se disponibiliza projetos completos que são mantidos atualizados ao longo das versões. Também se a tecnologia oferece modelos de configurações de rede, APIs e contratos inteligentes de

exemplo que contemplem casos de uso gerais e específicos para o processo de desenvolvimento.

Algumas plataformas disponibilizam recursos como kits de desenvolvimento (SDKs), bibliotecas e interfaces de linha de comando (CLI) para gerenciamento e interação com nodos, carteiras e a rede blockchain. Outras fornecem também binários pré-compilados para desenvolvimento devido aos altos requisitos de compilação que facilitam a configuração do ambiente e a implantação final. Tais ferramentas reduzem a curva de aprendizado e aceleram o desenvolvimento e implantação de provas de conceito ou protótipos de redes blockchain. Esses recursos geralmente vem acompanhados de larga documentação e alguns até oferecem suporte a vários idiomas, o que torna os projetos blockchain mais atraentes (JANSSEN et al., 2020).

Macdonald, Liu-Thorrold e Julien (2017) classificam como importante, para a avaliação de um blockchain, a qualidade e a quantidade de documentação e recursos ao desenvolvedor para cada plataforma. Isso inclui explicações sobre o design e os recursos da plataforma, detalhes técnicos da implementação, tutoriais e exemplos. Essa documentação é importante para permitir que os usuários tirem o máximo proveito de uma plataforma. Eles destacam que, em geral, quanto mais documentação melhor, principalmente se a documentação visa vários usuários (por exemplo, desenvolvedores, mineradores, usuários de aplicativos).

Também podem ser consideradas como documentação útil, publicações como FAQs, tutoriais, exemplos, explicações, propostas de design e guias escritos pelas comunidades de desenvolvedores das plataformas. Documentos que sugerem aos desenvolvedores e administradores de sistemas ferramentas, ou uma combinação delas, para colocar os aplicativos blockchain em funcionamento no tempo mínimo também são relevantes.

4.1.3.1.2 Participação do fornecedor/comunidade

A participação de quem desenvolve e da comunidade para Moezkarimi, Abdollahei e Arabsorkhi (2019) pode ser considerada importante para o suporte do produto (ou plataforma) e para criar alto valor de mercado. Os autores também avaliam que o histórico de desenvolvimento da plataforma é importante, se este for mais longo se assume melhor desenvolvimento. O tamanho da comunidade de desenvolvedores também é um importante

indicador, e segundo os autores, quanto maior esta comunidade, maior a chance de continuidade do processo de desenvolvimento da plataforma. Realiza-se também uma classificação de diversas plataformas acerca deste indicador, conforme adaptado no Quadro 8.

Quadro 8 – Classificação de plataformas blockchain em relação a participação de empresas.

Nível de Participação Empresarial	**Plataforma**
Alto	Multichain, Hyperledger Sawtooth, Hyperledger Fabric e Cardano
Moderado	Bitcoin e Ripple
Baixo	Ethereum, Zcash e Waves

Fonte: Adaptado de Moezkarimi, Abdollahei e Arabsorkhi (2019).

Syed et al. (2019) tratam a participação do fornecedor como algo essencial para a sobrevivência do blockchain no setor empresarial, dito que este impõe as propriedades demandadas, como integridade de dados e algoritmo de consenso. Os autores também notam que no setor de saúde, os fornecedores por vezes aparentam demonstrar mais interesse em discutir o blockchain e sua segurança em si que focar nos problemas que poderiam ser resolvidos pela tecnologia. Este estudo também analisa brevemente a participação dos fornecedores nos setores de cadeia de suprimentos e indústria automotiva.

Para Porru et al. (2017) o número de contribuintes voluntários atesta a atratividade do software blockchain diante do cenário *open-source*[13]. Uma larga base de voluntários pode ser considerada um fator pivotal para o sucesso e evolução da blockchain. Para alcançar um desenvolvimento sustentável e obter melhorias na qualidade do software são recomendadas práticas específicas voltadas para aumentar a sinergia entre sistema e comunidade.

Janssen et al. (2020) por sua vez analisam os impactos da tecnologia blockchain na indústria e no mercado como um todo, suas dificuldades e necessidades por parte do governo e dos fornecedores. Enquanto nota-se que a dependência de um intermediário nas transações tende a se tornar obsoleta, também evidencia-se que ainda há necessidade de uma governança para projetar, operar e manter o sistema dentre os participantes. Menciona-se também que a tecnologia blockchain em si pode ser considerada muito disruptiva, e que pode ser moldada

13 O termo *open-source* refere-se a softwares desenvolvidos de forma colaborativa, compartilhados livremente, publicados de forma transparente e desenvolvidos com finalidade de ser um bem comunitário, sem ser propriedade de uma pessoa ou empresa. (VALKENBURGH, 2017).

conforme a influência de fornecedores e do mercado, expondo ainda mais a importância da participação do fornecedor. Nesse estudo também ressalta-se que ainda existe uma grande falta de entendimento dos consumidores, autoridades e fornecedores quanto aos potenciais casos de uso da tecnologia blockchain e seus impactos sociais.

O estudo de Hyrynsalmi et al. (2019) mostra que as empresas participantes do estudo julgam que a construção de uma comunidade começa antes mesmo da publicação do *white paper* ou antes mesmo da empresa possuir um site. A criação da comunidade, segundo os autores, deve começar quando a ideia é formulada, e não deve finalizar enquanto a firma continuar em operação. Todas as empresas participantes do estudo também concordaram que encontrar apoiadores que acreditem no projeto, compartilhem de sua missão ou visão e estejam dispostos a disseminar a ideia em suas próprias redes é importante para o projeto e especialmente para o sucesso da *Initial Coin Offering (ICO)*[14]. Algumas empresas também julgam que o gerenciamento da construção de comunidade é importante, e que se deve interagir com a comunidade em nível de membros ou investidores individuais, e buscar encorajá-los e incentivá-los.

4.1.3.1.3 Tamanho do time de desenvolvimento

Segundo Moezkarimi, Abdollahei e Arabsorkhi (2019), o tamanho do time de desenvolvimento pode ser considerado um importante indicador para prever a continuidade de desenvolvimento e evolução de uma plataforma. Os autores propõem três principais categorias para classificar os times de desenvolvimento, sendo elas time pequeno (menos de 50 desenvolvedores), médio (de 50 a 100 desenvolvedores) e grande (mais de 100 desenvolvedores). Os autores também classificam as plataformas abordadas no estudo acerca deste critério, como mostra o Quadro 9.

Amsden e Schweizer (2018) abordam a chance de sucesso de uma ICO a partir de múltiplos fatores, dentre eles a qualidade do empreendimento, que segundo os autores é diretamente associada ao tamanho do time de desenvolvimento. Para os autores, a preparação e lançamento de uma ICO necessita de extensivo trabalho, como na criação do *whitepaper*, comercialização da oferta, gerenciamento de mídias sociais e comunicação com os

14 *Initial Coin Offering* refere-se à forma de arrecadar fundos através de blockchain para desenvolvimento do projeto através da venda de ações, *tokens* (criptomoeda que necessita da utilização de uma blockchain separada para operar) ou moedas ligadas ao mesmo. (AMSDEN e SCHWEIZER, 2018).

investidores. Consequentemente, quanto maior o time de desenvolvimento maior a chance destas preparações e gerenciamentos serem bem-sucedidos. Os autores também notam que o tamanho do time serve como sinal de confiança geral no projeto, e que capital humano pode ser medido pelo número de membros no time.

Quadro 9 – Classificação de plataformas blockchain em relação ao tamanho do time de desenvolvimento.

Tamanho do time	**Plataformas**
Grande	Bitcoin, Ethereum, Hyperledger Fabric, Cardano
Médio	Waves, Neo, Multichain, Hyperledger Sawtooth
Pequeno	Zcash, Ripple

Fonte: Adaptado de Moezkarimi, Abdollahei e Arabsorkhi (2019).

Ante, Sandner e Fiedler (2018) também abordam o tamanho do time relacionado à ICO, e notam que o capital humano de um projeto atua como um sinal para potenciais investidores, visto que este é um importante recurso para sucesso organizacional. Estudos também indicam que capitalistas de risco dão valor a critérios do capital humano, como experiências prévias, educação e experiência de liderança em gerenciamento (apud HALL; HOFER, 1993; MUZYKA; BIRLEY; LELEUX, 1996; SHEPHERD; ZACHARAKIS, 1999). Os autores também notam que possíveis investidores também dão valor a critérios com relação indireta ao tamanho do time, como tamanho da rede do time (alcance da rede *LinkedIn* dos membros) e dispersão do time (número de diferentes nacionalidades presentes nos times).

Hyrynsalmi et al. (2019) julga que o tamanho do time de desenvolvimento, mesmo que não extensamente estudado, pode ter impacto positivo na ICO do projeto. Em geral, CEOs com grandes redes no *LinkedIn* (500+) tendem a ter impacto positivo, e grandes times de desenvolvimento tiveram impacto positivo em um estudo e impacto nula em outro. Os autores também analisam oito casos de empresas que optaram por se manter anônimas, e nota-se uma média de 15 participantes por equipe (variação de 7 a 29 membros). Segundo as empresas, times maiores tendem a passar maior credibilidade, visto que em geral estes cumprem mais tarefas simultaneamente, porém as empresas também ressaltam a necessidade de qualidade sobre quantidade.

4.1.4 Dimensão Governança

4.1.4.1 Qualitativo

4.1.4.1.1 Documentação

Segurança de um sistema computacional consiste em proteger os recursos de um sistema (hardware, software, dados e telecomunicações) contra violações de integridade, disponibilidade e confidencialidade (NIELES; DEMPSEY; PILLITTERI, 2017). Tais conceitos são definidos por Stallings e Brown (2015) da seguinte forma. Integridade é a garantia de que dados não foram alterados sem autorização e que um sistema funciona conforme concebido, sem manipulações. Disponibilidade é a garantia do sistema responder prontamente a todos a seus usuários. Confidencialidade é a garantia que não há acesso não autorizado a dados.

Em relação a Segurança é importante ressaltar que quando se fala de segurança em blockchain públicas refere-se a tornar a adulteração de dados algo inviável através do armazenamento de dados no máximo de localizações possíveis em ambientes descentralizados sem uma autoridade central. (ZHENG et al., 2018). No caso de blockchains privadas e permissionadas porém segurança é abordada de maneira diferente, através de uma camada de segurança baseada em funções que restringe as operações à funções e dados à usuários privilegiados para o dado específico. (DEMIR; TURETKEN; FERWORN, 2019).

No estudo de Moezkarimi, Abdollahei e Arabsorkhi (2019) avalia-se a segurança em diversos níveis, como segurança dos dados das transações, anonimidade do usuário e segurança do ecossistema da blockchain como um todo. Os autores notam também que se espera evolução em relação a segurança de uma plataforma conforme a mesma se torna "madura", e tal amadurecimento depende, entre outros fatores, do investimento recebido, e este por sua vez depende diretamente do número de usuários que utilizam a plataforma.

Vangulick, Cornelusse e Ernst (2018) abordam segurança para a aplicação da blockchain no setor elétrico, mais especificamente voltado para comércio *peer-to-peer* e proteção do *ledger* e transações em relação a ataques cibernéticos, desconsiderando o risco de adulterações ligadas ao *meter* diretamente. O ponto de vista destes autores foi abordado de forma aprofundada na seção 3.3.3.1.1 Resiliência.

Janssen et al. (2020) tem uma abordagem voltado para adoção da tecnologia blockchain como um todo pelo mercado, e ressaltam que mesmo que um dos principais pontos fortes da tecnologia seja sua segurança, ainda há insegurança do mercado em relação a o quão nova é a tecnologia, e Kshetri (2018) argumenta que como a tecnologia blockchain ainda não foi suficientemente utilizada, a mesma ainda não foi testada seriamente para poder ser considerada livre de erros.

Segundo Hassan, Yuen e Niyato (2019) o indicador de segurança, quando falando de aplicações no setor elétrico, depende de quatro principais requisitos:

a) Autenticação: preocupa-se com a determinação da identidade de um nodo emum sistema visando bloquear acessos não autorizados.
b) Autorização: trata do gerenciamento de acesso e privilégios dos nodos na rede. Em sistemas inteligentes de energia nodos possuem funções variadas, e consequentemente necessitam de níveis variados de autorização em aplicações individuais.
c) Integridade de dados: refere-se à detecção de alterações não autorizadas nos dados. No caso dos sistemas inteligentes de energia auditabilidade é necessária para corrigir responsabilidade em caso de funcionamentos defeituosos ou conflitos, garantir interesses comerciais e financeiros e cumprir requisitos reguladores.
d) Auditabilidade: preocupa-se com a habilidade de reconstruir um histórico completo de um determinado evento ou ação a partir de registros históricos.

Urmila, Hariharan e Prabha (2019) realizam um estudo comparativo de aplicações blockchain voltadas para IoT, e ressaltam a importância dada para segurança nessa área, o que torna a resiliência da tecnologia blockchain algo de grande valor. Para reforçar este ponto os autores fazem um comparativo da segurança cibernética padrão e da segurança da tecnologia blockchain, e notam riscos de falhas reduzidas do último em relação ao primeiro, além de robustez elevada e vantagens relacionadas a não necessidade de manutenção. Conclui-se por fim que o blockchain como meio de segurança para IoT é mais adequado que outras formas tradicionais.

Na análise comparativa de Chowdhury et al. (2019) também leva-se em consideração a segurança das 10 plataformas analisadas, entrando em detalhes sobre como cada uma garante tal indicador. Conclui-se também que todas as plataformas analisadas (Bitcoin, Ethereum, EOS, Cardano, Hyperledger Fabric, Hyperledger Sawtooth, IOTA, Multichain, Corda e Waltonchain) possuem um alto grau de robustez em relação a diferentes tipos de ataques e erros sem precedente.

No estudo de Ahl et al. (2020) com foco no setor elétrico japonês nota-se preocupações dos autores em relação aos desafios tecnológicos que a tecnologia blockchain enfrenta, e em relação a segurança os autores ressaltam que mesmo com benefícios quando comparada a segurança cibernética tradicional, ainda existem riscos e possibilidades de ataques, como o ataque de 51%, gasto-duplo, falsificação dos dados e *bugs* no contrato inteligente. Nota-se também que o caso de uso examinado pelos autores trata-se de uma blockchain privada, e que consequentemente esses riscos são reduzidos, porém que em caso de necessidade de escalonamento do sistema os riscos e topologia podem mudar. Segundo os autores, topologia também é um fator de alta importância quando se fala de segurança.

Ahl et al. (2020) também mencionam brevemente como integrações da tecnologia blockchain e de inteligência artificial poderiam contribuir positivamente para a segurança de plataformas blockchain, principalmente no âmbito de contratos inteligentes.

4.1.4.1.2 Privacidade

No contexto de segurança da computação, privacidade é garantia de que um indivíduo controla quais informações a seu respeito podem ser coletadas e armazenadas, bem como por quem e para quem essas informações podem ser cedidas (STALLINGS; BROWN, 2015).

Privacidade foi um dos fatores chaves na adoção e sucesso dos primórdios da tecnologia blockchain, porém após anos de estudos e escrutínio relacionados a sua privacidade, desenvolveram-se heurísticas poderosas capazes de analisar transações e inferir um usuário comum, e em muitos casos obter a identidade real do usuário. No atual estado, o Bitcoin e suas *altcoins* irmãs podem ser considerados menos privados que o sistema bancário tradicional. Propuseram-se ao longo do tempo diversos protocolos buscando ampliar a

privacidade e resolver o problema exposto, todos porém dependentes de redes de comunicação anônimas externas, como o Tor[15]. (HENRY; HERZBERG; KATE, 2018).

Henry, Herzberg e Kate (2018) propõe a resolução deste problema através da utilização de uma primitiva criptográfica chamada de *private information retrieval (PIR)* ou recuperação de informações privadas. A técnica PIR, segundo os autores, por mais adequada que seja, é notavelmente ineficiente e é constante alvo de estudos e pesquisas que visam sua melhoria e implementação de protocolos viáveis que se utilizam da mesma.. Nota-se também que novos desafios ligados à privacidade são introduzidos conforme novas soluções para o problema da escalabilidade vem sendo propostas.

Para Dorri et al. (2019a) as soluções existentes para o mercado energéticos baseados em blockchain sofrem principalmente de três problemas: a) dependência de terceiros confiáveis que garantam que ambos os lados da troca energética cumpram seus comprometimentos, b) falta de privacidade, considerando que possíveis atacantes podem obter informações privadas e sensíveis de qualquer usuário ligando múltiplas transações do mesmo ou monitorando os padrões de geração de transação dos nodos, e c) despesas gerais como negociações entre produtores e consumidores são transmitidos para todos os participantes. O *framework* implementado em Ethereum proposto pelos autores (SPB) busca resolver estes problemas, entre outros.

Segundo Hassan, Yuen e Niyato (2019) uma análise das aplicações blockchain no setor elétrico mostra que em vários sistemas inteligentes de energia existe uma grande necessidade de manter os dados e as identidades dos nodos privados, visto que dados referentes aos *smart meters* revelam informações privadas em relação aos hábitos, cronograma e comportamento dos usuários.

No estudo de Baliga et al. (2018) analisa-se unicamente a plataforma Quorum, e nota-se que o indicador de privacidade foi um dos objetivos do design da plataforma, e que esta permite que subconjuntos de membros de um consórcio realizem transações uns com os outros sem tornar as mesmas públicas para os membros não envolvidos. A privacidade do Quorum é possibilitada através da divisão do *ledger* público principal em um *ledger* público e outro privado. O *ledger* público e suas transações podem ser visualizadas por todos os

15 Tor é um software livre e de código aberto que proporciona a comunicação anônima e segura ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade. Disponível em: https://en.wikipedia.org/wiki/Tor_(anonymity_network) Acesso em: 08 de maio de 2020.

membros da rede, enquanto que o *ledger* privado e suas transações são visíveis apenas para os envolvidos. Nota-se porém que os membros não envolvidos na transação têm acesso apenas a um hash referente à mesma.

Na avaliação de aptidões de aplicação da tecnologia blockchain em diversas áreas propostas por Lo et al. (2017), nota-se que problemas ligados a escalabilidade e privacidade são os principais fatores ligados a sua não utilização no mercado de ações de grande volume, e que privacidade é algo que atualmente se deve abrir mão quando pensando em aplicações na área da saúde, porém que deve ser levado em consideração.

Chowdhury et al. (2019) classifica as 10 principais plataformas blockchain em relação a sua privacidade, como mostra o Quadro 10, e ressalta que plataformas e sistemas que contam com privacidade tendem a ter uma maior probabilidade de adoção em larga escala.

Quadro 10 – Classificação de plataformas em relação à privacidade.

Classificação	**Plataformas**
Transações ligadas via identificadores pseudônimos. Transações, códigos de contratos inteligentes e outros dados visíveis para todos	Bitcoin, Ethereum, EOS e Cardano
Forte suporte à privacidade utilizando o *ledger* privado para usuários autorizados / conhecidos	Hyperledger Fabric e Hyperledger Sawtooth
Utilização de pseudônimos	IOTA
Suporte de privacidade através de gerenciamento integrado das permissões dos usuários	Multichain, Corda
Tag RFID	Waltonchain

Fonte: Adaptado de Chowdhury et al. (2019).

4.1.4.1.3 Topologia da rede

Topologia da rede refere-se ao arranjo dos nodos ou pontos que participam de uma rede e de suas respectivas conexões (KENYON, 2002).

No estudo de Rydzi e Truong (2019) propõe-se um *framework* com objetivo de compartilhar e sugerir informações e conhecimento sobre blockchain. Nota-se que para o desenvolvimento deste *framework* os autores realizaram 324 *benchmarks* com topologias

variadas a partir de 250 padrões de implantação de redes, e que por fim o *framework* pode retornar uma topologia recomendada conforme o objetivo do usuário.

Duan et al. (2019) destacam que para uma maior assertividade na avaliação de uma topologia da rede blockchain, deve-se levar em consideração sua implantação em um ambiente distribuído fisicamente. Segundo esses pesquisadores, todas as ferramentas de *benchmarking* de rede estudadas são executadas diretamente em máquinas físicas ou virtuais em uma rede relativamente estável (principalmente dentro do mesmo *datacenter* ou *cluster*). No entanto, isso está longe de ser uma configuração prática. A tecnologia Blockchain foi projetada para permitir que várias partes ou entidades troquem informações (por exemplo, transações em um setor financeiro ou registros em uma rede da cadeia de suprimentos), e é altamente provável que aplicativos ou mesmo componentes diferentes da rede estejam localizados em diferentes locais físicos.

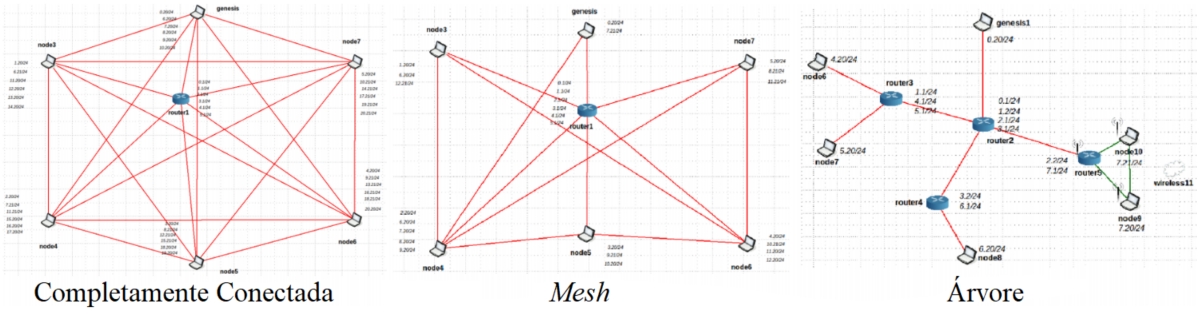
O estudo de Liu et al. (2020) avalia a escalabilidade da tecnologia blockchain e suas perspectivas para o futuro, e reconhece a escalabilidade baseada em topologia como essencial, visto que técnicas *multi-chain* podem otimizar a eficiência de recursos de uma rede *peer-to-peer*. Os autores também exploram métodos como realizar descarregamento de cargas de trabalho (utilizando técnicas *off-chain*), habilitação de interoperabilidade entre plataformas blockchain e particionamento de rede (que divide a carga de trabalho em um número razoável de *peers* interconectados que agem como blockchains independentes, através da utilização de técnicas de *sharding).* Os autores também pontuam sobre os pontos negativos de tal escalabilidade, e ressaltam a existência do "trilema" blockchain, que implica a redução de segurança e descentralização em troca desta escalabilidade.

Macedo, Rosales e Garcia (2019) propõem um método de análise de transações blockchain (focados em transações derivadas de ataques por *ransomware)* a partir de três principais tipos de análise: a) rastreio, b) análise de redes e c) análise estadístico. A análise de redes proposta busca permitir a visualização do histórico de transações como sendo uma rede direcionada, onde as direções serão consideradas nodos e o sentido do pagamento será considerado enlace. Consequentemente, o montante do pagamento representa o peso do enlace. A visualização da rede gerada permitiria a obtenção de informações acerca da dinâmica de transações, dos nodos de maior importância e de possíveis estratégias para melhorar o pseudo-anonimato da blockchain.

Shi et al. (2019) buscam analisar a performance da plataforma Hyperledger Sawtooth implantada em serviços de nuvens e instanciados em máquinas virtuais – VMs – (do inglês *Virtual Machines*). Os testes foram realizados nas plataformas Amazon Web Service (6 *datacenters* espalhados pelo mundo) e *ExoGENI (*6 *datacenters* nos Estados Unidos), e buscam analisar problemas de consistência de performance, de estabilidade de performance e de escalabilidade de performance. Nota-se que os autores utilizaram três diferentes tipos de instância para cada provedor (pequeno, médio e grande). Segundo os autores a VM foi instalada no sistema operacional Ubuntu 16.04, e apenas um nodo foi implantado por nuvem em VM, visto que a implantação de mais de um nodo por VM poderia existir congestionamento entre os mesmos. Visando uma análise ampla, realizou-se variação no número de instâncias de VMs (de 3 a 15), que acarreta consequente variação do número de nodos nos testes. Os resultados implicam pouco impacto gerado pela variação de nodos, visto que o algoritmo utilizado (PoET) tem seu *design* voltado para redes grandes.

Buenrostro et al. (2019) avaliam a usabilidade da plataforma Hyperledger Sawtooth para operações militares em um campo de batalha através de simulações no *Common Open Research Emulator (CORE)*, um *software* utilizado para simular diversos tipos de redes. Os autores colocam grande importância na configuração da rede em ambientes militares, então realizam testes em três topologias distintas: a) completamente conectada, b) *mesh*, e c) árvore. conforme mostra a Figura 20.

Figura 20 – Topologias relevantes para avaliação do blockchain no setor militar.

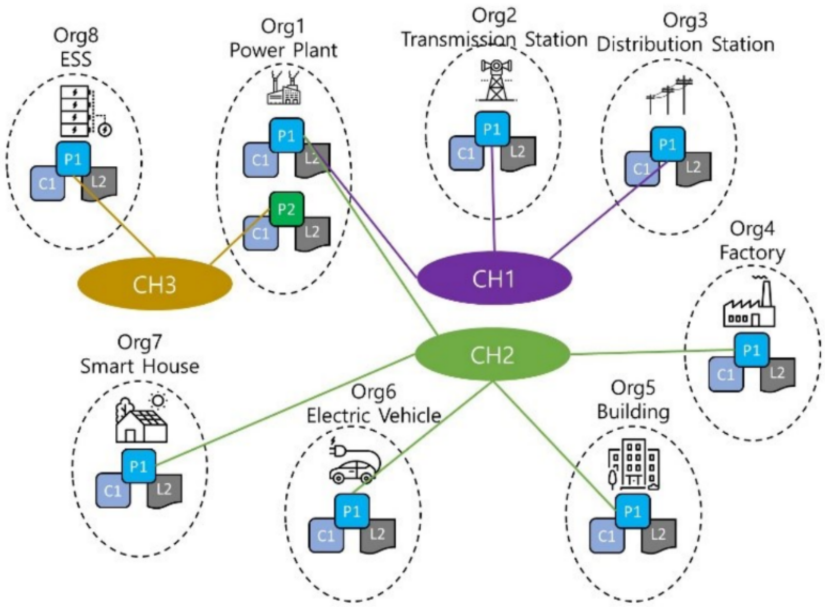


Fonte: Adaptado de Buenrostro et al. (2019).

Também foram realizados 90 testes utilizando bandas-largas variadas e concluiu-se que topologias de conectividade completa e *mesh* são mais efetivas quando comparadas à de árvore, e ainda que conectividade completa se sobressai em alguns aspectos.

Zhang et al. (2018) analisam a utilização da plataforma Hyperledger Fabric em trocas de energia, e propõem uma topologia própria através da incorporação do Fabric em uma típica rede de *smart grid*. Os autores propõem a criação de três canais com diferentes funções e diferentes organizações participando em cada um deles, como mostra a Figura 21.

Figura 21 – Topologia de rede *smart grid* proposta.



Fonte: Zhang et al. (2018).

Os autores explicam as funcionalidades individuais e coletivas de cada canal:

a) Canal 1: Compartilha dados sobre perdas energéticas em transações distribuídas com *ledgers* distribuídos. Consiste basicamente de uma Usina Elétrica (Org1), uma Subestação de Transmissão (Org2) e uma Subestação de Distribuição (Org3). O objetivo deste canal é o registro e gerenciamento eficiente de perdas energéticas.
b) Canal 2: Compartilha dados sobre utilização de energia em transações distribuídas com *ledgers* distribuídos. Consiste de uma Usina Elétrica (Org1), uma Fábrica (Org4), um Prédio (Org5), um Veículo Elétrico (Org6) e uma Casa (Org7). O objetivo deste canal é enviar e receber dados sobre utilização energética e guardar e utilizar energia em geração eficiente de eletricidade.
c) Canal 3: Neste canal os dados de capacidade remanescente e capacidade para

backup de energia são compartilhados para *ledgers* distribuídos. Consiste em uma Usina Elétrica (Org1) e um Sistema de Armazenamento de Energia (ESS) (Org8). O objetivo deste canal é que usuários compartilhem dados sobre capacidades e gerenciem dados sobre eletricidade com flexibilidade.

As análises de performance realizadas pelos autores demonstram que a topologia e sistema propostos possuem performance viável para serem utilizados em diversas aplicações, incluindo *smart grids*.

4.1.4.1.4 Tipos de blockchain

Devido à constante evolução da tecnologia blockchain, atualmente há diferentes blockchains disponíveis. Aqui sugere-se classificar as blockchains existentes em tipos para melhor entender as possíveis aplicações da tecnologia blockchain e suas diferentes necessidades.

Existe uma certa divergência sobre como classificar blockchains na literatura. Neste trabalho se abordou primeiramente a taxonomia proposta Oliveira et al. (2019) e Xu et al. (2017) devido à clareza oferecida e por ser a mais comum. Em seguida, apresentam-se tipos alternativos. Por fim, considerações de outros autores.

a) Tipos principais de blockchain

Oliveira et al. (2019) e Xu et al. (2017) classificam as tecnologias blockchains usando a combinação das duas seguintes formas:

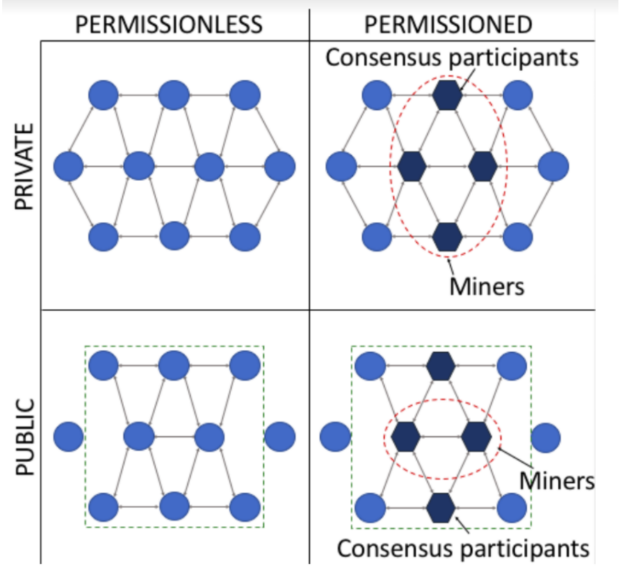
Pública vs. Privada: uma blockchain pública é aquela onde não existe controle de acesso a rede do blockchain e, portanto, qualquer um pode se conectar à rede da blockchain. Em contraste, uma blockchain privada exige algum controle de acesso e somente um conjunto pré-determinado de indivíduos pode se conectar à rede do blockchain.

Permissionada vs. Não-Permissionada: uma blockchain permissionada é aquela cujos participantes são identificados e seus respectivos papéis podem ser diferenciados. Por exemplo, um subconjunto dos participantes é autorizado a validar transações enquanto todos os participantes podem criar transações. Já em blockchains não permissionadas, inexiste

distinção entre os papéis dos participantes. Ou seja, todos os participantes exercem os mesmos papéis.

A Figura 22 ilustra os tipos acima apresentados. Nas linhas têm-se blockchain privadas e públicas. Na blockchain pública, somente os participantes (nodos) no interior do retângulo tracejado estão conectados à rede pública. Na blockchain privada, somente os nodos conectados são ilustrados. O papel dos nodos é identificado por sua forma geométrica e circunscrição na elipse em vermelho tracejada. Note que nas blockchains não permissionadas os nodos conectados assumem os mesmos papéis (forma circular). Nas blockchains permissionadas há nodos que participam do algoritmo de consenso (hexágono) e nodos que mineram blocos (circunscritos pela elipse tracejada).

Figura 22 – Análise taxonômica dos tipos de blockchain.



Fonte: Oliveira et al. (2019).

Vale destacar algumas implicações de blockchains públicas e privadas. Em geral, blockchains públicas são abertas e transparentes, e sua segurança depende em parte da adesão pelos participantes dos protocolos, regras e métodos de segurança propostos. Algumas das vantagens de blockchains públicas são: a) confiabilidade (visto que os nodos não precisam ter confiança entre si para o funcionamento da rede), b) segurança (quanto maior número de participantes, maior a distribuição de registros e mais difícil a atuação de hackers) e c) transparência (devido a grande distribuição de registros, o sistema inteiro pode ser

considerado transparente, visto que não é possível exibir uma falsa transação ou escondê-la). Desvantagens de blockchains públicas são seu número reduzido de transações por segundo (consequente do grande número de nodos e da verificação de transações), problemas de escalabilidade (também consequente do grande número de nodos visto que o tempo para completar a transação escala com o crescimento da rede) e alto consumo energético (o processo de consenso possui alto consumo energético e necessita de sistemas de hardware especializados para operar).

No Quadro 11 apresentam-se exemplos dos tipos de blockchain supracitados.

Quadro 11 – Classificação de plataformas blockchain por tipo.

Tipo	**Não Permissionada**	**Permissionada**
Privada	Hyperledger	Ripple, Neo, Multichain, Symbiont, Corda
Pública	Bitcoin, Ethereum, Litecoin, Zcash	Stellar, Sovrin, EOS

Fonte: Elaborada pelo autor.

Diferentemente, blockchains privadas podem ser entendidas como um sistema não "completamente" descentralizado e distribuído, visto que estes são controlados por organizações e indivíduos. Consequentemente, blockchains privadas são consideradas muito menos seguras que as públicas e sofrem das brechas de segurança de um sistema centralizado. (ZHENG; ZHU; SI, 2019).

Como este tipo de blockchain é geralmente utilizado dentro de organizações e empresas, apenas membros selecionados participam da rede, e a organização controladora gerencia o nível de segurança, autorizações, permissões, acessibilidade e a possibilidade de decidir a qual usuário ou grupo fornecer ou não o direito de mineração.

Algumas das possíveis aplicações de blockchains privadas são implementações voltadas para votos, gerenciamento de cadeia de suprimentos, identidades digitais e controle de ativos. Como vantagens, blockchains privadas contam com uma velocidade transacional superior às públicas (maior número de transações por segundo devido ao número limitado de nodos, o que acelera o processo de consenso e verificação) e maior escalabilidade (em geral blockchains privadas podem escalar de forma flexível conforme as necessidades da entidade controladora). Desvantagens de blockchains privadas são a necessidade de confiança entre os usuários, segurança reduzida (devido ao número reduzido de participantes, a rede torna-se

mais propícia às brechas de segurança, visto que se o sistema central de gerenciamento da entidade controladora é comprometido, o invasor pode ter acesso a todos os nodos e informações da rede), maior centralização e necessidade de um sistema de gerenciamento de acesso para seu funcionamento de forma correta (o sistema conta com direitos de monitoramento e gerenciamento, tendo permissão de adicionar novos nodos na rede ou decidir o nível de acesso dos nodos participantes).

b) Tipos alternativos de blockchain

Outras classificações menos comuns também podem ser encontradas na literatura. Elas são blockchains híbridas e consórcios. Uma blockchains híbrida é uma combinação de blockchains pública e privada que oferece um balanço entre privacidade, escalabilidade e rastreabilidade de dados. Para tal, um subconjunto dos dados de blockchain privadas são gravados em uma blockchain pública. Com uma rede híbrida usuários podem controlar quem tem acesso e quais dados tais usuários têm acesso, possibilitando a existência de apenas parte dos dados e da rede em forma pública. Transações neste tipo de rede geralmente são verificadas internamente à rede privada, porém podem ser publicamente verificadas e disponibilizadas se essa for a vontade da entidade controladora (BLOCKCHAIN COUNCIL, 2019; DATAFLAIR TEAM, 2019; PACKT, 2017). Um exemplo de aplicação de blockchain híbrida é dado por Kuvshinov et al. (2017), onde universidades gravam registros escolares sigilosos em suas blockchains privadas, cujos hashes dos blocos são gravados numa blockchain pública. Exemplos de blockchains híbridas são Dragonchain, VeChain e Aergo.

Outra classificação de blockchain são os consórcios. Um consórcio é uma blockchain controlada por duas ou mais organizações. O foco desta classificação está na *governança* e não na distinção entre pública vs. privada e permissionada vs. não permissionada. Tanto é que parece não haver consenso na literatura sobre como um consórcio se posicionaria na Figura 6. Por exemplo, Xu et al. (2017) define consórcio como blockchains privadas mas alerta para a dificuldade de diferenciar uma blockchain privada entre consórcio e não consórcio. Por outro lado, Rajput, Thakur e Basha (2019) definem consórcios como uma combinação de blockchains públicas e privadas. Similarmente, Blockchain Council (2019), Dataflair Team (2019) e Packt (2017) definem que assim como o tipo de blockchain híbrida, blockchains consórcio são combinações de blockchains públicas e privadas, com diferença de que estas

são controladas por mais de uma organização, e cada organização controladora tem direito de autorizar transações e supervisionar o processo de consenso, além de poder atuar como nodo na troca de informações e mineração. Um dos objetivos desse tipo de blockchain é a cooperação das organizações controladoras visando solucionar problemas em comum. Consórcios blockchain são tipicamente utilizados por bancos e organizações governamentais. Exemplos de blockchains do tipo consórcio são *Cardano, Energy Web Foundation, R3, Quorum, Bankchain, Voltron e Fisco.*

c) Outras considerações

Zheng, Zhu e Si (2019) abordam os tipos de blockchain de forma analítica e comparativa, analisando vantagens e desvantagens das blockchains públicas, privadas e de consórcio (denominada de federativa pelos mesmos), além de questões gerais de ambiente e segurança, como mostra o Quadro 12.

Quadro 12 – Comparação de blockchains públicas e privada/consórcio.

Critério	**Blockchain Pública**	**Blockchain Privada/Consórcio**
Acesso	Leitura e escrita aberta	Leitura e escrita permissionada
Velocidade	Lenta	Rápida
Segurança	*Proof-of-Work, Proof-of-Stake,* outros algoritmos de consenso	*Proof-of-Byzantine-Fault-Tolerance*, Raft, *Proof-of-Authority*
Filiação	Anonimato ou pseudo-anonimato	Identidades conhecidas
Ambiente	Sem confiança entre membros	Com confiança entre membros

Fonte: Adaptado de Zheng, Zhu e Si (2019).

O estudo de Yasaweerasinghelage, Staples e Weber (2017) busca realizar predições de latência da plataforma Ethereum (especificamente Geth) através da modelagem e simulação de performance arquitetural do sistema. Os autores ressaltam que a justificativa da utilização de uma rede privada do Ethereum se dá para evitar o *flooding*[16] da rede pública, reduzir custos e poder variar o tempo inter-bloco da rede.

Buenrostro et al. (2019) analisam a utilização da tecnologia blockchain na área militar com integração à IoT, e optam por analisar a performance da plataforma Hyperledger

16 *Flooding* refere-se ao ato de enviar múltiplas informações de forma a causar um alto fluxo de dados em um curto período de tempo.

Sawtooth especificamente. Segundo os autores, a opção deu-se em função das características customizáveis da plataforma, como gerenciamento de identidades baseado em funções, taxa de transação e tamanho de buffer. Plataformas públicas também foram analisadas como possíveis escolhas, porém os autores acreditam que características ligadas principalmente à não existência de restrição de entrada na plataforma tornam-a não válida para a aplicação.

Hassan, Yuen e Niyato (2019) analisam profundamente a aplicação de blockchains públicas, privadas e de consórcio em diversas áreas do setor elétrico, e concluem que para a área de Infraestrutura Inteligente existe fraca necessidade de *throughput* e latência de transação, porém sua grande necessidade de privacidade torna blockchains privadas ou de consórcio preferenciais nesta aplicação. No domínio de trocas de energia existe relativamente pouca necessidade de privacidade, e consequentemente os autores sugerem a utilização de blockchains públicas ou de consórcio. Para aplicações voltadas para Gerenciamento de Energia os autores sugerem a utilização de tecnologias semelhantes às de Infraestrutura Inteligente.

4.1.4.1.5 Suporte a moeda ou token

Brousmichc et al. (2018) definem uma moeda digital como uma unidade de informação criptográfica usada para facilitar uma transação no mundo real. Bitcoin e Ethereum são duas blockchains que oferecem moedas digitais nativas. Transações de moedas digitais podem ser feitas de uma pessoa para outra. No entanto, nenhuma moeda física se move quando são enviadas ou recebidas (HASSAN; YUEN; NIYATO, 2019).

O Bitcoin foi a primeira moeda virtual, criada em 2009 como software de código aberto por uma pessoa ou grupo conhecido por Satoshi Nakamoto. O *whitepaper* creditado a Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, propôs um sistema alternativo aos regulamentos tradicionais, canais de negócios e licenças, permitindo que duas partes pudessem negociar diretamente entre si sem a necessidade de um terceiro confiável. De acordo com o *whitepaper*, o objetivo inicial dessa criptomoeda era desenvolver um sistema P2P que evite a supervisão e as despesas transacionais impostas por terceiros não interessados.

A aplicação da tecnologia blockchain além das moedas digitais necessitava de novos desenvolvimentos na própria tecnologia (DIEDRICH, 2016). Em 2013, um grupo de

desenvolvedores liderados por Vitalik Buterin iniciou um projeto chamado Ethereum para expandir os recursos da tecnologia blockchain. Eles reconheceram os limites da blockchain Bitcoin. O Bitcoin por design era principalmente um aplicativo – ou uma plataforma com recursos muito limitados. Eles queriam que a Ethereum se tornasse uma plataforma de desenvolvimento de uso geral que pudesse ser usada para criar aplicativos descentralizados e tokens digitais (BUTERIN, 2014; WOOD, 2014) A plataforma Ethereum foi lançada em 2015 e a comunidade Ethereum vem crescendo rapidamente, provocando uma nova onda de inovação. Os desenvolvedores usaram a plataforma para criar uma ampla variedade de aplicativos descentralizados, bem como tokens digitais que podem ser usados para interagir com aplicativos descentralizados. Através do Ethereum, os desenvolvedores agora podem tokenizar quase todos os tipos de ativos, principalmente os ativos escassos. No processo de tokenização de ativos escassos, empreendedores e inovadores começaram a perceber o poder disruptivo de longo alcance da tecnologia e dos tokens de blockchain. Os tokens podem ser criados sobre uma blockchain e podem ser usados para representar uma ampla gama de ativos além das moedas.

Desta forma, um ativo digital pode ser uma moeda ou um token digital. Tecnicamente existem duas abordagens populares para definir ativos digitais na maioria das soluções de blockchain: o modelo UTXO sem estado, em que os saldos das contas são codificados em registros de transações anteriores; e o modelo de conta, onde os saldos das contas são mantidos no espaço de armazenamento do estado no *ledger* (HYPERLEDGER FAQ, 2017).

As blockchain públicas com suporte nativo a ativos digitais, como Bitcoin, Ethereum, Cardano, Litecoin e Monero utilizam o modelo baseado em UTXO, enquanto as blockchain privadas como Hyperledger Fabric, Corda, Quorum, que não incluem suporte nativo a ativos digitais, podem utilizar tanto uma quanto outra abordagem, fazendo uso de um banco de dados de estado.

Entretanto, embora não ofereçam suporte nativo, as plataformas privadas citadas acima podem gerar ativos digitais através de contratos inteligentes e transacioná-los como em um blockchain público, garantindo também a rastreabilidade, a proteção contra o gasto duplo entre outras características presentes nas plataformas públicas.

4.1.4.2 Quantitativo

4.1.4.2.1 Custo

Analisando-se a operação de uma rede blockchain, o custo pode ser associado aos encargos de qualquer transação que envolvem o processamento ou armazenamento de dados no *ledger*. Comumente definido como *taxa da transação*. (CHOWDHURY et al., 2019).

No âmbito deste estudo, este indicador ainda abordará os custos de implementação e utilização de redes blockchain em provedores de serviços de nuvem.

Na análise da plataforma Ethereum realizada por Aldweesh et al. (2019) observa-se que, da perspectiva de mineradores, espera-se que o custo energético da execução de contratos inteligentes seja heterogêneo em diferentes implementações da plataforma, visto que o tempo de execução dos *opcodes* individuais tende a diferir entre as mesmas. Nota-se também que os mineradores podem optar por realizar suas operações baseados na otimização do custo-benefício. Um dos objetivos da plataforma proposta pelos autores seria o de auxiliar na seleção da melhor implementação para o uso desejado. Vale ressaltar também que no estudo os autores analisam o custo através da utilização de CPU, acesso ao armazenamento e *gas*.

Dorri et al. (2019b) exprimem o custo como a representação total do valor monetário que um usuário deve pagar como taxa de transação em uma troca energética no setor elétrico. Recordando que cada transação envolve uma taxa que serve como incentivo para o minerador processar e registrar as transações em um blockchain. Os autores ainda ponderam que o tamanho da blockchain influência no custo de gerenciamento da mesma.

Yasaweerasinghelage, Staples e Weber (2017) salientam em seu estudo que custos de hardware e componentes em sistemas blockchain podem ser modelados e simulados de forma convencional (apud GOOIJER; JANSEN; KOZIOLEK E KOZIOLEK, 2012), porém sinalizam a existência de outros custos, como do *gas* utilizado na execução de contratos inteligentes na plataforma Ethereum e possíveis taxas de transação.

O estudo de Hassan, Yuen e Niyato (2019) evidencia que uma das principais barreiras da aplicação da tecnologia blockchain em sistemas inteligentes de energia são as altas despesas iniciais, contudo observam que devido as tecnologias desatualizadas em que esses sistemas operam, a adoção da blockchain resultaria na redução de diversos custos operacionais.

Kouveliotis-lysikatos et al. (2019) desenvolvem uma aplicação para simulação de transações energéticas e focadas no Ethereum, avaliando a aplicabilidade da plataforma no setor. Os autores realizam testes na implantação de contratos inteligentes por diferentes métodos, e aferem os custos de *gas* dos métodos individualmente. A Tabela 7 apresenta os resultados obtidos considerando a cotação do Ether e do Euro na data do estudo.

Cabe esclarecer que os contratos inteligentes utilizados nas simulações de Kouveliotis-lysikatos et al. (2019) foram desenvolvidos utilizando a linguagem Solidity e implantados e testados utilizando o *Truffle Software Framework* (para a simulação de uma rede Ethereum local utilizou-se o *Ganache*, que faz parte do *Truffle*). Os contratos foram executados assumindo 4 nodos participantes.

Tabela 7 – Consumo de *gas* para métodos de implantação de contratos inteligentes.

Métodos		Limite de *gas* por bloco: 6721975		
		Cotação: 1 Ether = 102,75 Euro		
Contrato	**Método**	***Gas* médio**	**Num. de chamadas**	**Valor em Euro**
Smart Meter	Registrar *Meter*	43900	4	0,01
	Cancelar *Meter*	14482	4	0,00
Fornecedor	Período de declaração	52656	4	0,00
	Finalizar	13484	1	0,00
	Período de pagamento	37281	4	0,01
	Cadastrar usuário	125865	4	0,03

Fonte: Adaptado de Kouveliotis-lysikatos et al. (2019).

Chowdhury et al. (2019) realizam uma análise comparativa entre algumas das plataformas mais populares em relação a existência de custos e taxas. Os resultados conciliados formam o Quadro 13.

Quadro 13 – Classificação de plataformas blockchain em relação a custo/taxa.

Presença de custo/taxa	**Plataformas**
Com custo/taxa	Bitcoin, Ethereum, Multichain, Waltonchain, Cardano
Sem custo/taxa	Hyperledger Fabric, Hyperledger Sawtooth, IOTA, Corda, EOS

Fonte: Adaptado de Chowdhury et al. (2019).

Demir, Turetken e Ferworn (2019) propõem um *framework* para analisar, do ponto de vista financeiro, os custos de uma implementação blockchain, e consequentemente os custos de manutenção e gerenciamento de plataformas do tipo pública e privada. Os autores estimam o custo mínimo do hardware em torno de US$1000 para uma presumível participação na rede Bitcoin, além de um custo mensal médio por volta de US$100 com o consumo de energia elétrica.

Por outro lado, o custo para manter uma rede privada utilizando um provedor de serviços em nuvem como Amazon Web Services (AWS), Microsoft Azure e IBM Cloud, pode ser uma alternativa apropriada a depender do caso de uso e do nível de exigência computacional do projeto. Visto que estes provedores além de oferecer escalabilidade, alta disponibilidade e armazenamento confiável, eximem despesas com infraestrutura e pessoal de TI nas organizações. Demir, Turetken e Ferworn (2019) calculam o custo para manter dois nodos da plataforma Hyperledger Fabric na AWS. O estudo apresenta valores inferiores à US$2/hora para sustentar uma rede de produção e custos até 70% menores para redes de teste.

A Tabela 8 apresenta os valores praticados atualmente pelos principais provedores de serviços em nuvem para implantação ou utilização de soluções blockchain. Os custos foram estimados utilizando a configuração padrão das plataformas oferecidas em 730 horas de utilização mensais.

Tabela 8 – Comparação de valores de soluções blockchain em nuvem.

Fornecedor	**Plataforma**	**Custo (USD/hora)**	**Custo Mensal (USD)**
Oracle	Oracle Blockchain	0,5 a 0,75	372 a 558
Microsoft Azure	Quorum	1,01	733,92
IBM Cloud	IBM Blockchain	1,90	1387
Alibaba Cloud	Hyperledger Fabric	1,01 a 7,20	735 a 5254
SAP Cloud	Hyperledger Fabric	1,81	1324
AWS	Hyperledger Fabric	1,93	1408,90
AWS	Hyperledger Sawtooth	0,40	292
AWS	Corda Enterprise VM	0,096	70,08
Chainstack	Corda	0,61	446,40

Fonte: Elaborado pelo autor.

4.2 DESENVOLVIMENTO DO INSTRUMENTO DE AVALIAÇÃO

Sumariamente, cabe refletir algumas considerações importantes definidas e seguidas neste estudo e que delinearam as atividades da pesquisa e da produção do conhecimento. Entre elas, a premissa relacionada ao escopo da aplicação, ambiente e tecnologia. Para que o universo coberto pela metodologia fosse o mais amplo e genérico possível, não se restringiu ao tipo ou plataforma blockchain, o objetivo de aplicação na qual a tecnologia foi utilizada nem qual o ambiente onde a tecnologia foi implantada. Ou seja, este estudo buscou alcançar o conjunto de possibilidades mais abrangente e exequível, projetando a metodologia para ser aplicada na maioria das plataformas blockchain, qualquer modelo de negócio e qualquer ambiente (teste ou produção).

Assim sendo, é pertinente e interessante destacar que embora se tenha utilizado um estudo de caso no setor elétrico para experimentação desta metodologia, o objetivo deste trabalho foi o desenvolvimento de uma metodologia ampla e genérica capaz de avaliar qualquer solução desenvolvida utilizando tecnologias blockchain.

No entanto, escolher ou avaliar determinada tecnologia é um aspecto técnico-científico. Do mesmo modo que projetar e desenvolver um método complexo também requer ciência. Segundo Brooks (1994) ciência e tecnologia são altamente interdependentes, contudo, possuem objetivos bem diferentes. Chavda (2012) apresenta uma relação entre a ciência e tecnologia como sendo, respectivamente, a pesquisa e aplicação, onde uma depende da outra.

Ciência desenvolve tecnologia, já a tecnologia aplicada gera inovação. A tecnologia por si só não possui finalidade, é um conceito vazio sem aplicação (KOSTOFF, 2001). Ela deve ser entendida como um meio para alcançar determinado fim que gere valor para as pessoas. A tecnologia é uma ferramenta. Instrumento técnico desenvolvido através da ciência para ajudar pessoas a resolver problemas ou melhorar processos. Ciência e tecnologia se misturam, pois existe um fluxo contínuo ao longo do processo de inovação.

O instrumento de análise e avaliação técnico-científico foi desenvolvido com o propósito de servir como um guia para especialistas ao se examinar uma solução computacional baseada em blockchain. O objetivo do instrumento é orientar o especialista na reflexão a respeito dos meandros da solução observada, auxiliando-o na construção de

conhecimento capaz de formar um entendimento esclarecido que o permita analisar e avaliar a solução desenvolvida.

Todavia, embora o instrumento desenvolvido tenha sido conceitualmente testado, o mesmo precisava ser aplicado em um estudo de caso real para ser aplicado e ajustado caso necessário. Para Geisler (2000) uma tecnologia não pode de fato ser avaliada sem considerar seu contexto social e econômico. Segundo o autor, deve-se analisar a tecnologia em seu contexto de uso. Pois seu valor só será percebido quando for usado e assim o usuário pode avaliá-lo. E concluindo, argumenta que não se pode entender a tecnologia somente por sua existência, mas apenas no contexto de sua aplicação: pessoas, organizações e sociedade.

Portanto, de modo análogo ao exposto, o instrumento projetado precisava ser colocado em seu contexto de aplicação, executado na prática. Para isso foi utilizada uma PoC desenvolvida para a pesquisa, que será apresentada na Seção 5. Onde o instrumento metodológico foi aplicado para análise, avaliação e parecer da solução computacional baseada em blockchain construída.

4.2.1 Métricas do Instrumento de Avaliação

Em linhas gerais, o escopo deste estudo trata de um método de análise e avaliação de ciência e tecnologia, e este método foi concebido em forma de um instrumento técnico-científico. Portanto é necessário definir a maneira como este instrumento fará a medida.

Com relação a definição de métricas Müller (2008) reitera o conceito apresentado por Geisler (2000):

> Geisler (2000, p.48, 69) [...] define o termo métricas como um sistema de medidas que inclui o item objeto da medida, a unidade de medida e o valor da unidade. Geisler classifica as métricas como objetivas ou subjetivas. [...]. Ainda de acordo com a definição de Geisler, as métricas podem tomar vários formatos, por exemplo, uma medida única, uma razão (entre duas medidas), um índice, ou ainda uma medida integrada que combine várias métricas, até mesmo com atributos diferentes, objetivos e subjetivos (MUELLER, 2008, p. 27).

Rubenstein e Geisler (1989) definem indicadores de ciência e tecnologia como uma gama de medidas quantitativas e/ou qualitativas adotadas para medir processos, insumos e resultados da pesquisa, desenvolvimento e inovação.

Neste aspecto, o desenvolvimento do instrumento adotou métricas objetivas e subjetivas, com unidades de medida representadas por valores lógicos, quantitativos e qualitativos. Utilizando a definição de métricas apresentada por Geisler (2002), o sistema de medida da metodologia desenvolvida é composto por:

a) Indicador: Trata-se do item objeto da medida. A metodologia traz uma breve definição de cada indicador e os questionamentos que auxiliarão o especialista na avaliação do mesmo. Cada resposta obtém um valor métrico que é representado por uma categoria.
b) Categoria da Métrica: Trata-se na unidade de medida do indicador. No desenvolvimento da metodologia, estão sendo propostos três grupos de categoria, conforme apresentado no Quadro 14.
c) Valor da Métrica: Trata-se do valor da unidade de medida do indicador, também representado na no Quadro 14.

Quadro 14 – Sistema de medidas da metodologia.

Natureza	**Tipo da Métrica**	**Valor da métrica**
Objetiva	Binário	Sim/Não Probabilística/Determinística Permissionada/Não permissionada
Subjetiva	Texto	Aberta

Fonte: Elaborado pelo autor.

Além das métricas relacionais apresentadas no Quadro 13, o instrumento desenvolvido apresenta outras duas unidades de medida:

a) Não se aplica: esta opção pode ser utilizada para apontar que determinado indicador não deve ser considerado na análise do avaliador ou ainda que determinada pergunta pertinente ao indicador deve ser desconsiderada.
b) Parecer técnico: é um espaço reservado em cada indicador que o especialista deve utilizar para relatar sua análise e/ou avaliação a respeito daquele indicador.

4.2.2 Instrumento de Avaliação Técnico-Científico

Utilizando os indicadores, suas dimensões e subdimensões inferidos e identificados ao longo do progresso da pesquisa, esta equipe alcançou a metodologia pretendida sob a forma de um instrumento de análise e avaliação técnico-científico composto por três etapas. O instrumento metodológico completo encontra-se no Apêndice A deste documento e pode ser acessado em: https://github.com/main-dev/ methodology-to-evaluate-blockchain.

Para concepção do instrumento utilizou-se uma planilha eletrônica. Tal ferramenta oferece uma gama de recursos avançados e até de programação, permitindo que o instrumento possa ser atualizado ou aperfeiçoado. Com relação à distribuição, por utilizar uma planilha eletrônica inteiramente compatível com as ferramentas oferecidas por provedores de serviço em nuvem, pode ser disponibilizado de forma online ou offline. Com relação à estrutura o instrumento foi organizado e dividido com três abas, que representam as três etapas de execução do processo.

Quadro 15 – Metodologia computacional – Etapa I.

Instrumento de Análise e Avaliação Técnico-Científico – Etapa I		
Pergunta	**Resposta**	
	Sim	**Não**
Existem múltiplas partes envolvidas?	☑	
Existe déficit de confiança entre as partes?	☑	
Existe algum terceiro confiável?		☑
O registro da transação deve ser imutável?	☑	
A escalabilidade é um requisito crítico?		☑
Utilize Blockchain		
A verificabilidade é importante?		☑
Utilize Blockchain Privada.		
A durabilidade dos dados é importante?	☑	
Utilize armazenamento on-chain.		

Fonte: Adaptado de Chowdhury et al. (2018).

A primeira etapa a ser executada pelo especialista avalia se é adequado utilizar uma tecnologia blockchain em determinado caso de uso. Chowdhury et al. (2018) julgam que a blockchain não é uma tecnologia para propósitos gerais, porém se aplicada corretamente oferece diversos benefícios. Desta forma, adaptou-se a árvore de decisão proposta por Chowdhury et al. (2018) estruturando-a como um *checklist* dinâmico formatado em planilha

eletrônica. Tal formato tornou o processo de análise da árvore de decisão mais intuitivo. Esta etapa do instrumento permite ao especialista avaliar se a adoção da tecnologia blockchain foi uma escolha apropriada. Conforme Quadro 15.

Quadro 16 – Metodologia computacional – Etapa II.

Instrumento de Análise e Avaliação Técnico-Científico – Etapa II				
Nome:				
Data Realização:				
Assinatura:				
#	**Indicador**	**Não se aplica**	**Resposta**	
1	**Arquitetura**			
1.1	**Quantitativo**			
1.1.1	**Tamanho do bloco**			
	O tamanho do bloco atende a necessidade/demanda da aplicação?	▢	▢ Sim	▢ Não
	O tamanho do bloco é adequado ao tamanho da transação?	▢	▢ Sim	▢ Não
	O tamanho do bloco é adequado à rede?	▢	▢ Sim	▢ Não
	Quais são as vantagens e desvantagens para este tamanho de bloco para o sistema de modo geral?	▢	Aberta	
	O tamanho do bloco impacta a escalabilidade do tipo de Blockchain?	▢	▢ Sim	▢ Não
	O tamanho do bloco interfere na performance do sistema?	▢	▢ Sim	▢ Não
	Existe autonomia para configuração deste indicador na tecnologia avaliada?	▢	▢ Sim	▢ Não
	Parecer técnico:			
1.1.2	**Tamanho do *mempool***			
	O tamanho máximo do *mempool* atende à quantidade de transações previstas?	▢	▢ Sim	▢ Não
	O tamanho médio do *mempool* indica bom desempenho da aplicação?	▢	▢ Sim	▢ Não
	Existem requisitos de hardware mínimos devido ao tamanho do *mempool*?	▢	▢ Sim	▢ Não
	Parecer técnico:			

Fonte: Elaborado pelo autor.

A segunda etapa do instrumento desenvolvido contém a metodologia representada no formato de *checklist* com os indicadores agrupados por dimensões e subdimensões, seguindo o padrão definido no quadro de indicadores apresentada no Quadro 16. Segundo Fantin (2017) como guia no processo de avaliação, a utilização de *checklists* permite aos avaliadores, com diferentes níveis de conhecimento, determinar os aspectos relevantes a serem considerados no planejamento de uma avaliação. Para Silva (2002) embora limitados a aspectos da usabilidade da interação humano-computador, os *checklists* oferecem contribuições importantes em métodos de avaliação de software, quando implementados de forma objetiva e sistemática. Cabe também pontuar que instrumentos muito similares ao construído são desenvolvidos e utilizados por auditores em processo de obtenção de certificações do tipo ISO.

O Quadro 16 ilustra a caráter de exemplo um fragmento da segunda etapa do instrumento de análise e avaliação desenvolvido. Nela pode ser observado que para cada indicador foi elaborado um conjunto de perguntas que podem receber como resposta os valores apresentados na Seção 4.3.1. O instrumento conta com 143 perguntas, sendo 23 de resposta do tipo texto e 120 de resposta do tipo binária, agrupadas em 5 dimensões.

Além das opções de resultado definidas na coluna “Resposta”, cada indicador bem como as perguntas que o compõem podem receber a marcação “Não se aplica”. Cada indicador relacionado no instrumento ainda possui um campo “Parecer técnico”.

Como apresentado ao longo desta seção, alguns indicadores dependem de outros indicadores. Com o intuito de tornar o instrumento ainda mais assertivo e completo, construiu-se uma matriz de dependência listando todos os indicadores. Tal matriz constitui a terceira etapa do instrumento de análise e avaliação. Nesta etapa do processo de execução, o especialista pode registrar quais indicadores devem ser observados em conjunto e as relações de dependência existentes entre eles. A matriz de dependências pode ser observada na Figura 23. Embora sugeriu-se por uma questão de organização dispor a matriz de dependências na etapa 3, o especialista/avaliador poderá executá-la antes da etapa 2 se julgar conveniente.

Figura 23 – Metodologia computacional – Etapa III.

INSTRUMENTO DE ANÁLISE E AVALIAÇÃO TÉCNICO-CIENTÍFICO - ETAPA III

Matriz de dependência A (Elemento Ai,j => i depende de j)	1.2.1 Resiliência	1.2.2 Escalabilidade	1.2.3 Interoperabilidade	1.2.4 Alocação de recursos	1.2.5 Tipo de licenciamento	1.2.6 Algoritmo de consenso	1.2.7 Desempenho	1.2.8 Tolerância a faltas	1.2.9 Presença de banco de dados de estado	2.1.1 Aplicação	3.1.1 Documentação	3.1.2 Participação do fornecedor/comunidade	3.1.3 Tamanho do time de desenvolvimento	4.2.1 Segurança	4.2.2 Privacidade	4.2.3 Topologia da rede	4.2.4 Tipo de blockchain	4.2.5 Suporte a moeda ou token	1.1.1 Tamanho do bloco	1.1.2 Tamanho do mempool	1.1.3 Tamanho da transação	1.1.4 Latência da transação	1.1.5 Throughput	1.1.6 Tempo de finalidade	1.1.7 Tempo de espera da validação	1.1.8 Tempo de confirmação de bloco	4.1.1 Custo
1.2.1 Resiliência	■																										
1.2.2 Escalabilidade		■																									
1.2.3 Interoperabilidade			■																								
1.2.4 Alocação de recursos				■																							
1.2.5 Tipo de licenciamento					■																						
1.2.6 Algoritmo de consenso						■																					
1.2.7 Desempenho							■																				
1.2.8 Tolerância a faltas								■																			
1.2.9 Presença de banco de dados de estado									■																		
2.1.1 Aplicação										■																	
3.1.1 Documentação											■																
3.1.2 Participação do fornecedor/comunidade												■															
3.1.3 Tamanho do time de desenvolvimento													■														
4.2.1 Segurança														■													
4.2.2 Privacidade															■												
4.2.3 Topologia da rede																■											
4.2.4 Tipo de blockchain																	■										
4.2.5 Suporte a moeda ou token																		■									
1.1.1 Tamanho do bloco																			■								
1.1.2 Tamanho do mempool																				■							
1.1.3 Tamanho da transação																					■						
1.1.4 Latência da transação																						■					
1.1.5 Throughput																							■				
1.1.6 Tempo de finalidade																								■			
1.1.7 Tempo de espera da validação																									■		
1.1.8 Tempo de confirmação de bloco																										■	
4.1.1 Custo																											■

Fonte: Elaborado pelo autor.

5 ESTUDO DE CASO

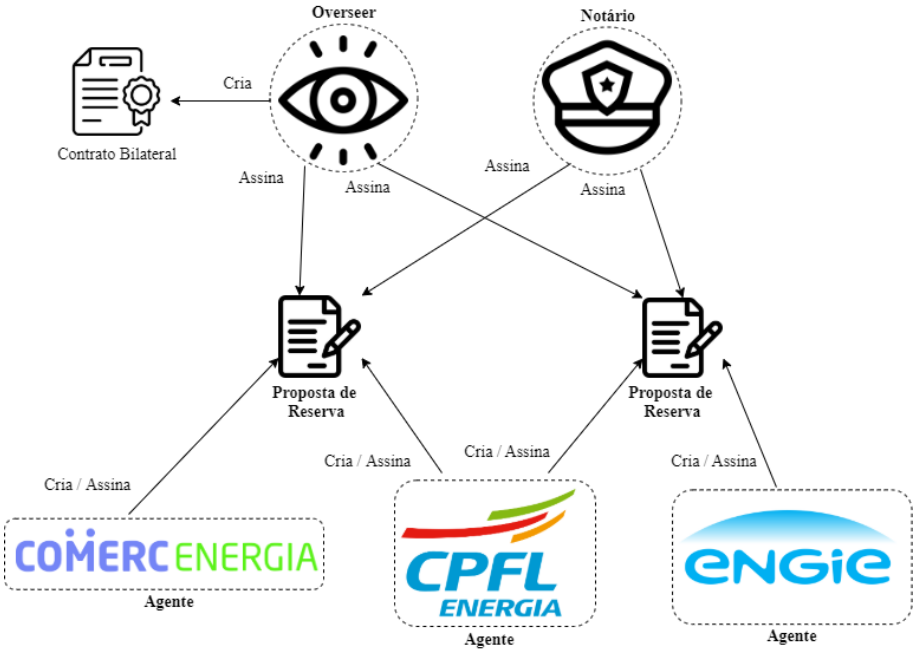
A comercialização de energia no Brasil é realizada em duas esferas de mercado: o Ambiente de Contratação Regulada (ACR) e o Ambiente de Contratação Livre (ACL). Todos os contratos, sejam do ACR ou do ACL, devem ser registrados na Câmara de Comercialização de Energia Elétrica (CCEE), e servem de base para a contabilização e liquidação das diferenças entre os montantes gerados, contratados e consumidos. No ACL, os geradores, comercializadores, importadores e exportadores de energia e consumidores livres e especiais têm liberdade para negociar e estabelecer em contratos os volumes de compra e venda de energia e seus respectivos preços a partir de contratos bilaterais entre os agentes envolvidos (CÂMARA BRASILEIRA DE COMERCIALIZAÇÃO DE ENERGIA ELÉTRICA, 2020).

Nos contratos de longo prazo, para entrega futura de energia elétrica, usualmente acordam-se contratualmente garantias financeiras entre os agentes (comprador e vendedor) junto à CCEE, durante o fornecimento de energia elétrica disposto no contrato (COMERC; CPFL; ENGIE, 2019). Estas garantias financeiras têm como finalidade proporcionar maior segurança às operações de compra e venda de energia elétrica na CCEE, tendo em vista que eventuais inadimplências podem comprometer a segurança das operações.

Com o objetivo de reduzir o impacto financeiro proveniente das garantias exigidas e pelo grande volume de contratos de compra e venda de energia transacionados no ACL entre os agentes CPFL Energia, Engie Energia e Comerc Energia, estas empresas encomendaram uma solução computacional na forma de uma prova de conceito de software (PoC). A PoC foi projetada e desenvolvida pela empresa contratada Orion Tech utilizando a tecnologia blockchain Corda *Open-Source*.

Na PoC os contratos de compra e venda são chamados de propostas de reserva, onde para cada contrato há um agente vendedor e um agente comprador. Mensalmente ocorre um processo de consolidação dessas propostas, onde o sistema realiza o balanço de compra e venda de energia entre cada par de agentes participantes do arranjo e gera os contratos bilaterais. Todas as propostas de reserva e os contratos bilaterais são registrados em blockchain. A Figura 24 apresenta uma abstração da arquitetura da PoC e os processos de criação e assinatura das propostas de reserva e dos contratos bilaterais.

Figura 24 – Arquitetura da PoC e ações básicas de cada nodo participante.



Fonte: Elaborado pelo autor.

A PoC foi desenvolvida utilizando a tecnologia Blockchain Corda com a seguinte arquitetura. A rede da PoC conta atualmente com 5 nós, sendo 3 nodos Agentes, 1 nodo Notário e 1 nodo Supervisor (Overseer), porém permite a possibilidade de posterior incremento de nodos, com a entrada de novos agentes caso necessário. Os nodos Agentes podem ser compreendidos como as entidades comercializadoras da rede, que operam na criação e interação com as propostas de reserva. O Overseer é considerado uma parte confiável e armazena todas as propostas de reserva entre nodos Agentes que posteriormente serão utilizadas na geração dos contratos bilaterais. O nodo notário é responsável em evitar o chamado “gasto duplo”, ou seja, que se reutilizem equivocadamente propostas de reservas já processadas (Figura 24).

Todo mês são lançadas diversas destas propostas de reserva que, no modelo tradicional de comercialização, exigiriam do agente comprador o aporte da garantia financeira ou seguro contratual, relativo ao mês vigente. No entanto, o ambiente da PoC permite que múltiplas operações comerciais sejam geradas e liquidadas intrinsecamente neste arranjo comercial entre os agentes. A redução de contratos bilaterais e consequentemente a diminuição dos aportes de garantia são o principal objetivo da PoC. Por outro lado,

privacidade dos dados, imutabilidade, segurança, dentre outros foram os fatores que levaram a escolha da tecnologia blockchain.

5.1 EXPERIMENTAÇÃO DA METODOLOGIA

Nesta fase da pesquisa, experimentou-se a metodologia computacional em um estudo de caso da PoC de comercialização de energia. Seguindo as etapas sequenciais do instrumento, pôde-se analisar e avaliar a PoC e observar quais os pontos positivos e negativos que a metodologia conseguiu auditar e extrair da solução desenvolvida.

Na execução da Etapa I da metodologia foram respondidos, com base nos dados coletados da PoC, aos questionamentos apresentados na etapa. Verificou-se que o método desenvolvido atendeu aos posicionamento esperado, podendo identificar se para a solução desenvolvida a utilização da tecnologia blockchain era a mais adequada, ante o modelo de negócio proposto. Observou-se também que a Etapa I da metodologia é um eficiente método de identificação de tecnologias alternativas ao uso da blockchain, que pode servir de norteador a especialistas e gestores em uma tomada de decisão mais ponderada e acurada para novos projetos.

Posteriormente, na realização da Etapa II da metodologia, de forma análoga à anterior, também foram respondidos aos questionamentos propostos no instrumento e constatou-se que de forma assertiva e consistente foi possível se inferir técnica e cientificamente, os pontos positivos, negativos e observações da aplicação examinada, utilizando o método fornecido pela metodologia computacional desenvolvida.

No processo de experimentação desta etapa os questionamentos propostos em cada indicador foram projetados no domínio da PoC e os resultados deste processo registrados no instrumento. Através da aplicação da metodologia pôde-se determinar que alguns dos indicadores não se aplicavam ao blockchain avaliado, sendo utilizado o espaço reservado ao parecer técnico para justificar esta característica. Entre estes indicadores estão o tamanho do bloco, tamanho do *mempool*, tempo de finalidade, tempo de confirmação do bloco, algoritmo de consenso e suporte a moeda ou token. Com relação aos indicadores do tamanho e tempo de confirmação do bloco, por exemplo, identificou-se que a implementação privada do blockchain Corda empregada na PoC utiliza o conceito de *estados* em vez de blocos,

justificando a descaracterização do indicador. Outro ponto observado foi que quando uma transação é criada neste modelo de negócio ela não fica aguardando para que seja processada pelos outros participantes desta transação. Ela é de imediato registrada no *ledger* e propagada na rede aos demais participantes da transação para ser analisada e validada, desta forma não se aplica a avaliação dos indicadores tamanho do *mempool* e tempo de finalidade da transação.

Utilizando os questionamentos – *O tempo de latência da transação atende as necessidades da aplicação? O canal de comunicação de dados utilizado atende a latência esperada da rede?* e *A latência se mantém adequada no pico de transações?* – oferecidos pela metodologia com relação ao indicador latência, pôde-se concluir que o indicador atende aos requisitos mínimos exigidos para o modelo de negócio. Observou-se também que não ele impacta o *throughput* e consequentemente o desempenho do sistema, representando pontos positivos extraídos pela metodologia na análise da PoC.

Outras vantagens observadas no emprego da metodologia foram referentes ao indicador tamanho da transação, onde os questionamentos – *O tamanho da transação atende a necessidade/demanda da aplicação? Quais são as vantagens e desvantagens para este tamanho da transação para o sistema de modo geral? Podem existir transações com tamanhos excessivos na aplicação que poderiam prejudicar o sistema?* e *Existe autonomia para configuração deste indicador na tecnologia avaliada?* – permitiram identificar que as transações processadas pela PoC possuem um tamanho e variação de tamanho adequados ao tipo de processo, otimizando o desempenho, e que a tecnologia avaliada oferece suporte à configuração deste indicador.

Por outro lado, no indicador segurança, a metodologia permitiu aos pesquisadores identificar, por meio dos questionamentos – *A solução desenvolvida garante a confidencialidade ou sigilo dos dados, auditabilidade e não repúdio das operações ou a utilização de algoritmos de assinatura digital exigidos ou recomendados pelo sistema brasileiro de certificação digital, quando necessário? A solução desenvolvida sofre de alguma vulnerabilidade conhecida e crítica?* e *Todo dado sigiloso trafega somente por canais de comunicação protegidos?* – que a solução desenvolvida não garante o sigilo e integridade dos dados, não utiliza algoritmos de assinatura digital recomendados que visam garantir a autenticidade e não repúdio das transações, possui vulnerabilidades críticas de

segurança e que dados sigilosos trafegam por canais de comunicação não protegidos. Na análise e avaliação deste indicador a metodologia possibilitou a equipe de pesquisa identificar as condições de inflexão ou de falha do sistema, apurando vários pontos negativos no quesito segurança. Cabe citar que, de acordo com o posicionamento da equipe de desenvolvimento, por se tratar de uma PoC não foram adotadas as boas práticas de segurança na construção da solução, e que tais inconsistências seriam tratadas em um posterior MVP (*Minimum Viable Product)*.

O Quadro 17 traz um fragmento do instrumento que apresenta uma amostra do resultado da aplicação da metodologia no indicador desempenho da PoC.

Quadro 17 – Fragmento de exemplo da aplicação do instrumento da metodologia computacional aplicada a PoC.
continua

Indicador	**Não se aplica**	**Resposta**			
Desempenho	☐				
A tecnologia blockchain dispõe de algum recurso que permita o monitoramento de desempenho?	☐	☑	Sim	☐	Não
O número de nodos blockchain contribui ou prejudica o desempenho da solução?	☐	O número de nodos do atual ambiente é de apenas 5 nodos. Mesmo acrescentando 5 nodos agentes ainda seria insignificante para as tecnologias utilizadas. O número de nodos contribui para o desempenho.			
O desempenho computacional de soluções blockchain podem ser menos eficazes que soluções centralizadas. Para a solução proposta o desempenho pode ser limitante para o modelo de negócio?	☐	☐	Sim	☑	Não
A escolha do banco de dados de estado contribui para o desempenho da solução?	☐	Por padrão, os nós Corda utilizam o banco de dados H2. Este banco de dados é o mais otimizado considerando a implementação padrão da tecnologia, como utilizado na PoC. Cabe destacar que o Corda oferece uma API de persistência compatível *Java Database Connectivity* (JDBC). Desta forma qualquer banco de dados com um driver JDBC é um candidato e pode ser consumido por um nó Corda, o que torna o mapeamento objeto-relacional amplamente interoperável.			

Parecer técnico: Os indicadores latência da transação e throughput são parâmetros que colaboram na análise do desempenho do sistema. Ambos os resultados destes indicadores mostraram que a solução desenvolvida atende plenamente o modelo de negócio. Consequentemente, o desempenho também é adequado à proposta. Importante lembrar que o sistema está hospedado em nuvem e para o improvável caso de problemas de desempenho, bastaria aumentar os recursos de CPU e/ou principalmente memória. A equipe UFSC acredita que não seria necessário este aumento, mesmo com uma possível inclusão de mais 5 agentes. Um dado importante para análise do desempenho é a baixa quantidade de transações/dia (15 transações), considerando 3 agentes. Esta quantidade é muito baixa para sistemas computacionais e não compromete o desempenho do sistema. Nos testes efetuados pela equipe UFSC no ambiente da PoC, todos os tempos ficaram inferiores aos limites definidos pela CPFL, comprovando que o desempenho atende plenamente ao modelo de negócio.

Fonte: Elaborado pelo autor.

Por fim, na Etapa III da metodologia construiu-se a matriz de dependências dos indicadores para a PoC estudada. O método disposto nesta etapa permitiu identificar quais indicadores dependem e se relacionam entre si e que devem ser observados em conjunto, retratando a visão do todo, mais alto nível. No estudo de caso da PoC, a metodologia mostrou que a maioria dos indicadores (13 de 21) depende do indicador “Aplicação”. Portanto, caso futuras modificações neste indicador sejam necessárias (por exemplo, mudança de regras de negócio), deve-se atentar para os efeitos nos demais indicadores. O indicador “Desempenho” depende significativamente de outros indicadores (8 no total), sendo portanto provavelmente sensível a futuras mudanças na PoC. Adicionalmente, ficou evidente a correlação esperada entre os indicadores “Desempenho”, “Escalabilidade” e “Alocação de Recursos”, dado que eles têm a ver com a agilidade da PoC em executar seu trabalho. Assim, é importante analisar “Desempenho”, “Escalabilidade” e “Alocação de Recursos” em conjunto em futuras modificações da PoC.

6 CONSIDERAÇÕES FINAIS

Este trabalho apresentou uma metodologia na forma de um instrumento de análise e avaliação técnico-científica para tecnologias blockchains. Adicionalmente, aplicou-se a metodologia desenvolvida para avaliar a tecnologia Corda *Open-Source* aplicada a uma prova de conceito que calcula a diferença entre as compras e vendas de energia elétrica de no Ambiente de Comercialização Livre de energia elétrica no Brasil. Até onde se explorou, não há trabalho anterior na literatura que se assemelhe à metodologia apresentada.

Dentre os resultados obtidos, este estudo apresentou a compilação dos principais indicadores técnicos e científicos que devem ser considerados ao se analisar ou avaliar qualquer solução computacional blockchain, disposto no Quadro 3. Os indicadores foram agrupados por similaridade em 4 dimensões: Arquitetura, Objetivo, Suporte e Governança. Baseado neste *cluster* de indicadores, amplamente explorados e fundamentados, determinou-se o conjunto de perguntas mais holistas e relevantes ao se estudar cada um dos indicadores até o momento. Tal conjunto de perguntas foi então organizado e estruturado sistematicamente em um instrumento de três etapas, compondo a metodologia desenvolvida.

Concerne destacar que a metodologia computacional foi idealizada e construída ampla e genérica, abstraindo-se plataformas e suas aplicações, permitindo ser utilizada em qualquer solução blockchain encontrada atualmente.

Utilizando os questionamentos instigados pelo instrumento, o especialista é projetado a refletir e inferir suas próprias considerações a respeito da solução observada. E assim obter respostas para indagações como – *Será que realmente era necessária a utilização da tecnologia blockchain? Como a solução desenvolvida atende cada um destes indicadores? e Qual a relação encontrada entre os indicadores?* – sendo estes apenas fragmentos do conhecimento formado e exercitado pela metodologia desenvolvida.

Cabe também evidenciar o ineditismo na concepção da metodologia uma vez que ficou comprovado no levantamento do estado da arte não haver estudos ou propostas equivalentes ou similares ao trabalho desenvolvido nesta pesquisa.

O instrumento foi aplicado e homologado em uma prova de conceito de comercialização de energia elétrica baseada na tecnologia blockchain Corda. Nesta etapa de experimentação pôde-se verificar que a metodologia contribuiu de forma consistente e

assertiva na análise e avaliação da solução desenvolvida, uma vez que permitiu se observar e refletir sobre muitos aspectos que poderiam passar despercebidos. No caso da PoC, pontos positivos e negativos foram identificados e destacados pelo uso da metodologia.

Em relação a problemática o instrumento se mostrou um consistente método de análise e avaliação de soluções computacionais *blockchain-based* e que pode ser utilizado como modelo por outros pesquisadores e novos estudos. Em relação às hipóteses todas foram validadas, pois construiu-se com esta pesquisa um instrumento de análise e avaliação técnico-científico (*hipótese a*) genérico (*hipótese b*) composto por indicadores encontrados na literatura atualmente (*hipótese c*).

Compete apontar que devido à imaturidade e a grande velocidade da tecnologia blockchain, seus recursos ainda estão em desenvolvimento e suas aplicações estão cada vez mais em expansão. Desta forma, embora esta pesquisa não medisse esforços para construir uma lista completa e abrangente de indicadores e questionamentos técnicos e científicos de análise e avaliação da tecnologia, os recursos alcançados nesta pesquisa são os resultados do estudo do estado atual da tecnologia. Sendo assim, é necessário que esta metodologia seja atualizada e evolua gradualmente ao longo do tempo, devido às mudanças cada vez maiores nas tecnologias baseadas em blockchain e suas evoluções.

Como trabalhos futuros são esperados novos estudos descrevendo a utilização da metodologia aqui desenvolvida em outras provas de conceito e aplicações existentes. Também pode-se esperar a transformação do instrumento em um *framework* ainda mais automatizado, sendo possível sua disponibilização on-line.

REFERÊNCIAS

ABDELLA, Juhar; SHUAIB, Khaled. Peer to Peer Distributed Energy Trading in Smart Grids: a survey. **Energies**, [S.L.], v. 11, n. 6, p. 1560-1582, 14 jun. 2018. MDPI AG. http://dx.doi.org/10.3390/en11061560.

AHL, Amanda *et al*. Exploring blockchain for the energy transition: opportunities and challenges based on a case study in japan. : Opportunities and challenges based on a case study in Japan. **Renewable And Sustainable Energy Reviews**, [s.l.], v. 117, [s.p.], jan. 2020.

ALDWEESH, Amjad *et al*. OpBench: a cpu performance benchmark for ethereum smart contract operation code. **2019 Ieee International Conference On Blockchain (blockchain)**, [s.l.], p. 274-281, jul. 2019. IEEE. http://dx.doi.org/10.1109/blockchain.2019.00043.

ALGORAND. **ALGORAND'S IMMEDIATE TRANSACTION FINALITY**. 2019. Disponível em: https://www.algorand.com/what-we-do/technology/immediate-transaction-finality. Acesso em: 22 jun. 2020.

AMSDEN, Ryan; SCHWEIZER, Denis. Are Blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings. **Ssrn Electronic Journal**, [s.l.], p. 1-66, abr. 2018. Elsevier BV. http://dx.doi.org/10.2139/ssrn.3163849.

ANTE, Lennart; SANDNER, Philipp; FIEDLER, Ingo. Blockchain-Based ICOs: pure hype or the dawn of a new era of startup financing?. : Pure Hype or the Dawn of a New Era of Startup Financing?. **Journal Of Risk And Financial Management**, [s.l.], v. 11, n. 4, p. 80-99, 21 nov. 2018. MDPI AG. http://dx.doi.org/10.3390/jrfm11040080.

BAIRD Leemon. **The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance**, White Paper, 2016. Blockchain Association. Disponível em: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf. Acesso em 17 nov. 2020.

BALIGA, Arati *et al*. **Performance Evaluation of the Quorum Blockchain Platform**. 2018. Disponível em: https://arxiv.org/pdf/1809.03421.pdf. Acesso em: 08 maio 2020.

BARINOV, Igor; BARANOV, Viktor; KHAHULIN, Pavel. **POA network, White paper**. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper, 2018.

BENAHMED, Sofiane *et al.*. A Comparative Analysis of Distributed Ledger Technologies for Smart Contract Development. **2019 Ieee 30th Annual International Symposium On Personal, Indoor And Mobile Radio Communications (pimrc)**, [s.l.], p. 1-6, set. 2019. IEEE. http://dx.doi.org/10.1109/pimrc.2019.8904256.

BINANCE ACADEMY. **Confirmation Time**. Community Submission – Author: John Ma. Disponível em: https://www.binance.vision/glossary/confirmation-time. Acesso em: 05 maio 2020.

BJÖRCK, Fredrik *et al.*. Cyber Resilience – Fundamentals for a Definition. **New Contributions In Information Systems And Technologies**, [s.l.], p. 311-316, 2015. Springer International Publishing. http://dx.doi.org/10.1007/978-3-319-16486-1_31.

BLOCKCHAIN COUNCIL. **PERMISSIONED AND PERMISSIONLESS BLOCKCHAINS**: A COMPREHENSIVE GUIDE. 2019. By Toshendra Kumar Sharma. Disponível em: https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/. Acesso em: 13 maio 2020.

BLOCKCHAIN COUNCIL. **TYPES OF BLOCKCHAIN IN THE MARKET**: WHICH ONE IS BETTER?. 2019. By Toshendra Kumar Sharma. Disponível em: https://www.blockchain-council.org/blockchain/types-of-blockchain-in-the-market-which-one-is-better/. Acesso em: 13 maio 2020.

BLOCKCHAIN.COM. **Tamanho do Mempool (Bytes)**. 2020. Disponível em: https://www.blockchain.com/pt/charts/mempool-size. Acesso em: 05 maio 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. ESTABELECE PRINCÍPIOS, GARANTIAS, DIREITOS E DEVERES PARA O USO DA INTERNET NO BRASIL. [S. l.], 24 abr. 2014. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 13 jul. 2020.

BRILLIANTOVA, Vlada; THURNER, Thomas Wolfgang. Blockchain and the future of energy. **Technology In Society**, [S.L.], v. 57, p. 38-45, maio 2019. Elsevier BV. http://dx.doi.org/10.1016/j.techsoc.2018.11.001.

BROOKS, Harvey. The relationship between science and technology. **Research Policy**, [S. l.], ano 1994, v. 23, n. 5, p. 477-486, set. 1994. DOI 10.1016/0048-7333(94)01001-3. Disponível em: http://www.sciencedirect.com/science/article/pii/0048733394010013. Acesso em: 22 ago. 2020.

BROUSMICHC, Kei-leo *et al*. Blockchain Energy Market Place Evaluation: an agent-based approach. : An Agent-Based Approach. **2018 Ieee 9th Annual Information Technology, Electronics And Mobile Communication Conference (iemcon)**, [s.l.], p. 321-327, nov. 2018. IEEE. http://dx.doi.org/10.1109/iemcon.2018.8614924.

BUCHMANN, Johannes. **Introduction to Cryptography**. 2. ed. [s.l.]: Springer, 2004. 356 p.

BUENROSTRO, Erick D. *et al*. Evaluating Usability of Permissioned Blockchain for Internet-of-Battlefield Things Security. **Milcom 2019 – 2019 Ieee Military Communications Conference (milcom)**, [s.l.], p. 841-846, nov. 2019. IEEE. http://dx.doi.org/10.1109/milcom47813.2019.9020736.

BUTERIN, Vitalik. **A next-generation smart contract and decentralized application platform.** 2014. White Paper. Disponível em: https://github.com/ethereum/wiki/wiki/White-Paper.. Acesso em: 25 maio 2020.

BUTERIN, Vitalik. **On Slow and Fast Block Times.** 2015. Disponível em: https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/. Acesso em: 22 jun. 2020.

CÂMARA BRASILEIRA DE COMERCIALIZAÇÃO DE ENERGIA ELÉTRICA. 2020. **Regras de comercialização**: Contratos (CCEE, ed.). Disponível em: https://www.ccee.org.br/portal/faces/oquefazemos_menu_lateral/liquidacao?_adf.ctrl-state=ejaejfbdk_74&_afrLoop=2548173813516612#!. Acesso em: 12 jun. 2020.

CAO, Bin et al. Performance analysis and comparison of PoW, PoS and DAG based blockchains. **Digital Communications And Networks**, [s.l.], [s.p.], jan. 2020. Elsevier BV. http://dx.doi.org/10.1016/j.dcan.2019.12.001.

CARSON, Brant; ROMANELLI, Giulio; WALSH, Patricia; ZHUMAEV, Askhat. **Blockchain beyond the hype**: What is the strategic business value?. 2018. Artigo da revista McKinsey. Disponível em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. Acesso em: 13 abr. 2020.

CASTRO, Miguel; LISKOV, Barbara. **Practical byzantine fault tolerance, in: Proceedings of the Third Symposium on Operating Systems Design and Implementation**, New Orleans, USA, February 1999. Disponível em: http://pmg.csail.mit.edu/papers/osdi99.pdf. Acesso em 21 out. 2020.

CHASE; Brad, MACBROUGH, Ethan. **Analysis of the XRP Ledger Consensus Protocol**. 2018. Disponível em: https://www.researchgate.net/publication/323302411_Analysis_of_the_XRP_Ledger_Consensus_Protocol. Acesso em: 20 jun 2020.

CHAVDA, Sagarkumar Kantilal. **RELATIONSHIP BETWEEN SCIENCE, TECHNOLOGY AND SOCIETY**. In: SWP, 2012, Rajkot. Rajkot: Kotak Institute Of Science, 2012. v. 1, p. 179-180.

CHE, Zheng *et al*.. A Distributed Energy Trading Authentication Mechanism Based on a Consortium Blockchain. **Energies**, [s.l.], v. 12, n. 15, p. 2878-2899, 26 jul. 2019. MDPI AG. http://dx.doi.org/10.3390/en12152878.

CHENG, Sui; LIN, Sian-Jheng. A Memory-Hard Blockchain Protocol. **2018 Ieee International Conference On Smart Energy Grid Engineering (Sege)**, [S.L.], p. 284-287, ago. 2018. IEEE. http://dx.doi.org/10.1109/sege.2018.8499411.

CHOWDHURY, Mohammad Jabed Morshed *et al*. A Comparative Analysis of Distributed Ledger Technology Platforms. **Ieee Access**, [s.l.], v. 7, p. 167930-167943, 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2019.2953729.

CHOWDHURY, Mohammad Jabed Morshed *et al*. Blockchain Versus Database: a critical analysis. **2018 17th Ieee International Conference On Trust, Security And Privacy In Computing And Communications/ 12th Ieee International Conference On Big Data Science And Engineering (trustcom/bigdatase)**, [s.l.], p. 1348-1353, ago. 2018. IEEE. http://dx.doi.org/10.1109/trustcom/bigdatase.2018.00186.

COMERC; CPFL; ENGIE. **RFP (Request for Proposal)**: Blockchain nas operações entre Comerc, CPFL e Engie. [S.L.]: [S.N.], 2019. 13 p.

CORDA. **Corda Top Ten Facts #8**: pluggable consensus. Pluggable Consensus. 2018. Disponível em: https://www.corda.net/blog/corda-top-ten-facts-8-pluggable-consensus/. Acesso em: 22 jun. 2020.

CORDA. **Notaries**. 2020. Disponível em: https://docs.corda.net/docs/corda-os/4.7/key-concepts-notaries.html. Acesso em: 22 jun. 2020.

DARIN, Luiz Eduardo da Cunha; ASSUMPÇÃO, Mariana Baptista de. O NOVO PERFIL DA ADVOCACIA EMPRESARIAL: como a tecnologia de blockchain irá complementar de maneira positiva o compliance. **Percurso**, [S.L.], v. 1, n. 28, p. 325-340, 28 jan. 2019.

International Journal of Professional Business Review. http://dx.doi.org/10.21902/revpercurso.2316-7521.v1i28.3432.

DATAFLAIR TEAM. **Types of Blockchains:** Decide which one is better for your Investment Needs. 2019. Disponível em: https://data-flair.training/blogs/types-of-blockchain/. Acesso em: 13 maio 2020.

SCHWARTZ, David; YOUNGS, Noah; BRITTO Arthur. **The Ripple protocol consensus algorithm**. Ripple Labs Inc White Paper, 2014. Disponível em: https://ripple.com/files/ripple_consensus_whitepaper.pdf. Acesso em: 13 maio 2020.

DEMIR, Mehmet; TURETKEN, Ozgur; FERWORN, Alexander. A Financial Evaluation Framework for Blockchain Implementations. **2019 Ieee 10th Annual Information Technology, Electronics And Mobile Communication Conference (iemcon)**, [s.l.], p. 0715-0722, out. 2019. IEEE. http://dx.doi.org/10.1109/iemcon.2019.8936297.

DI SILVESTRE, Maria Luisa *et al*. Blockchain for power systems: current trends and future applications. **Renewable And Sustainable Energy Reviews**, [S.L.], v. 119, 109585, mar. 2020. Elsevier BV. http://dx.doi.org/10.1016/j.rser.2019.109585.

DINH, Tien Tuan Anh *et al*.. BLOCKBENCH: a framework for analyzing private blockchains. : A Framework for Analyzing Private Blockchains. **Proceedings Of The 2017 Acm International Conference On Management Of Data - Sigmod '17**, [s.l.], p. 1085-1100, mai. 2017. ACM Press. http://dx.doi.org/10.1145/3035918.3064033.

DORRI, Ali et al. Peer-to-Peer EnergyTrade: a distributed private energy trading platform. : A Distributed Private Energy Trading Platform. **2019 Ieee International Conference On Blockchain And Cryptocurrency (icbc)**, [s.l.], p. 61-64, maio 2019b. IEEE. http://dx.doi.org/10.1109/bloc.2019.8751268.

DORRI, Ali *et al*. SPB: a secure private blockchain-based solution for distributed energy trading. : A Secure Private Blockchain-Based Solution for Distributed Energy Trading. **Ieee Communications Magazine**, [s.l.], v. 57, n. 7, p. 120-126, jul. 2019a. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mcom.2019.1800577.

DUAN, Xuheng *et al*.. BBB: make benchmarking blockchains configurable and extensible. : Make Benchmarking Blockchains Configurable and Extensible. **2019 Ieee 24th Pacific Rim International Symposium On Dependable Computing (prdc)**, [s.l.], p. 61-611, dez. 2019. IEEE. http://dx.doi.org/10.1109/prdc47002.2019.00026.

ECOINOMIC. **WHAT IS THE BITCOIN MEMPOOL AND WHY DOES IT MATTER?** 2018. Disponível em: https://medium.com/ecoinomic/what-is-the-bitcoin-mempool-and-why-does-it-matter-c7a9ed2859ff. Acesso em: 05 maio 2020.

EHMKE, Christopher; WESSLING, Florian; FRIEDRICH, Christoph M.. Proof-of-Property – A Lightweight and Scalable Blockchain Protocol. **2018 IEEE/ACM 1St International Workshop On Emerging Trends In Software Engineering For Blockchain (WETSEB)**, Gothenburg, Sweden, p. 48-51. Disponível em: https://ieeexplore.ieee.org/document/8445059. Acesso em: 22 mar. 2020.

ETH GAS STATION BLOG. **What's the Maximum Ethereum Block Size?** 2019. Disponível em: https://ethgasstation.info/blog/ethereum-block-size/. Acesso em: 15 jun. 2020.

ETHEREUM. **Ethereum for Enterprise**. 2020. Disponível em: https://ethereum.org/enterprise/. Acesso em: 24 maio 2020.

FANTIN, Kátia. **Metodologia de Avaliação de Software Educacional**. 2017. 21 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade de Caxias do Sul, Caxias do Sul, 2017. Disponível em: https://repositorio.ucs.br/handle/11338/3080. Acesso em: 24 ago. 2020.

FERRETTI, Stefano; D'ANGELO, Gabriele. On the Ethereum blockchain structure: a complex networks theory perspective. **Concurrency And Computation**: Practice and Experience, [s.l.], [s.p.], 22 ago. 2019. Wiley. http://dx.doi.org/10.1002/cpe.5493.

GALVAO, Tais; PANSANI, Thais de Souza Andrade; HARRAD, David. Principais itens para relatar Revisões sistemáticas e Meta-análises: a recomendação prisma. : A recomendação PRISMA. **Epidemiologia e Serviços de Saúde**, [s.l.], v. 24, n. 2, p. 335-342, jun. 2015. Instituto Evandro Chagas. http://dx.doi.org/10.5123/s1679-49742015000200017.

GEISLER, Eliezer. **The Metrics of Science and Technology**. [S.L.]: Quorum Books, 2000. 400 p.

GEISLER, Eliezer. The metrics of technology evaluation: where we stand and where we should go from here. **International Journal Of Technology Management**, [S.L.], v. 24, n. 4, p. 341, 2002. Inderscience Publishers. http://dx.doi.org/10.1504/ijtm.2002.003060.

GEISSLER, Stefan *et al*. Discrete-Time Analysis of the Blockchain Distributed Ledger Technology. **2019 31st International Teletraffic Congress (itc 31)**, [s.l.], p. 130-137, ago. 2019. IEEE. http://dx.doi.org/10.1109/itc31.2019.00029.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Atlas, 2017. 192 p.

GOBEL, J.; KRZESINSKI, A.e.. Increased block size and Bitcoin blockchain dynamics. **2017 27th International Telecommunication Networks And Applications Conference (ITNAC)**, [s.l.], p. 1-6, nov. 2017. IEEE. http://dx.doi.org/10.1109/atnac.2017.8215367.

GRAKOV, Alexey. **A blockchain platforms comparison**. 2018. Disponível em: https://vironit.com/a-blockchain-platforms-comparison/. Acesso em: 13 abr. 2020.

GUO, Yi-Ming *et al*. A bibliometric analysis and visualization of blockchain. **Future Generation Computer Systems**, [S.L.], v. 116, p. 316-332, mar. 2021. Elsevier BV. http://dx.doi.org/10.1016/j.future.2020.10.023.

HADZILACOS, Vassos; TOUEG, Sam. **A modular approach to the specification and implementation of fault-tolerant broadcasts**. [s.l.]: Ep. Of Computer Science, Cornell Univ, 1994. 86 p.

HALL, John; HOFER, Charles W.. Venture capitalists' decision criteria in new venture evaluation. **Journal Of Business Venturing**, [S.L.], v. 8, n. 1, p. 25-42, jan. 1993. Elsevier BV. http://dx.doi.org/10.1016/0883-9026(93)90009-t.

HASSAN, Naveed Ul; YUEN, Chau; NIYATO, Dusit. Blockchain Technologies for Smart Energy Systems: fundamentals, challenges, and solutions. : Fundamentals, Challenges, and Solutions. **Ieee Industrial Electronics Magazine**, [s.l.], v. 13, n. 4, p. 106-118, dez. 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mie.2019.2940335.

HEARN, M. **Corda**: a distributed ledger. A Distributed Ledger. 2016. Disponível em: https://docs.corda.net/_static/corda-technical-whitepaper.pdf. Acesso em: 3 nov. 2019.

HENRY, Ryan; HERZBERG, Amir; KATE, Aniket. Blockchain Access Privacy: challenges and directions. : Challenges and Directions. **Ieee Security & Privacy**, [s.l.], v. 16, n. 4, p. 38-45, jul. 2018. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/msp.2018.3111245.

HINTZMAN, Zane. **Comparing Blockchain Implementations**. [s.l.]: Scte/isbe, 2017.

HORCH, John W.. **Practical Guide to Software Quality Management**. [s.l.]: Artech House, 2003. 286 p.

HYPERLEDGER FAQ. **Chaincode (Smart Contracts and Digital Assets)**. 2017. Disponível em: https://hyperledger-fabric.readthedocs.io/en/v0.6/FAQ/chaincode_FAQ.html Acesso em: 22 jun. 2020.

HYPERLEDGER WIKI. **Hyperledger.** 2020. Disponível em: https://pt.wikipedia.org/wiki/Hyperledger. Acesso em: 04 mar. 2019.

HYPERLEDGER. **Hyperledger: What is Hyperledger?**. 2020a. Disponível em: https://www.hyperledger.org/about. Acesso em: 15 jun. 2020.

HYPERLEDGER. **Blockchain**. 2020b. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/blockchain.html. Acesso em: 04 maio 2020.

HYPERLEDGER. **Smart Contracts and Chaincode**. 2020c. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/blockchain.html. Acesso em: 04 maio 2020.

HYPERLEDGER. **Endorsement Policies**. 2020d. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/endorsement-policies.html. Acesso em: 12 maio 2020.

HYPERLEDGER. **Channels**. 2020e. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/channels.html. Acesso em: 14 maio 2020.

HYPERLEDGER. **The Ordering Service**. 2020f. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html. Acesso em: 22 jun. 2020.

HYPERLEDGER. **CouchDB as the State Database**. 2020g. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/couchdb_as_state_database.html. Acesso em: 22 jun. 2020.

HYRYNSALMI, Sami *et al*. **Software Business**: 10th international conference, icsob 2019, jyväskylä, finland, november 18-20, 2019, proceedings. [s.l.]: Springer, 2019. 443 p.

IBM. **IBM® Informix® 12.10**. 2019. Disponível em: https://www.ibm.com/support/knowledgecenter/SSGU8G_12.1.0/com.ibm.perf.doc/ids_prf_042.htm. Acesso em: 15 jun. 2020.

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **ICP-01.01**: PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL. [s.l.]: [s.n.], 2019. 14 p. Disponível em: https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/01.1/DOC-ICP-01.01_-_v.4.2_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL_copy.pdf. Acesso em: 09 jul. 2020.

JAMES, K. L.. **SOFTWARE ENGINEERING**. [s.l.]: Phi Learning Pvt. Ltd, 2008. 388 p.

JANSSEN, Marijn et al. A framework for analysing blockchain technology adoption: integrating institutional, market and technical factors. : Integrating institutional, market and technical factors. **International Journal Of Information Management**, [s.l.], v. 20, p. 302-309, fev. 2020.

JERSIN, John. **What's really going to happen with Blockchain in HR & Recruiting**. 2018. Disponível em: https://www.linkedin.com/pulse/whats-really-going-happen-blockchain-hr-recruiting-john-jersin/. Acesso em: 14 abr. 2020.

KANG, Qi *et al*. A Collaborative Resource Allocation Strategy for Decomposition-Based Multiobjective Evolutionary Algorithms. **Ieee Transactions On Systems, Man, And Cybernetics**: Systems, [s.l.], v. 49, n. 12, p. 2416-2423, dez. 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/tsmc.2018.2818175.

KENYON, Tony. **High Performance Data Network Design**: design techniques and tools. [s.l.]: Digital Press, 2002. 623 p.

KOSTAREV, Gleb. **Review of blockchain consensus mechanisms**. 2017. Disponível em: https://medium.com/wavesprotocol/review-of-blockchain-consensus-mechanisms-f575afae38f2. Acesso em: 15 jun. 2020.

KOSTOFF, Ronald N. The metrics of science and technology. **Scientometrics** , [S. l.], v. 50, p. 353-361, 2001. DOI 10.1023/A:1010590111245. Disponível em: https://link.springer.com/article/10.1023/A:1010590111245. Acesso em: 19 ago. 2020.

KOUVELIOTIS-LYSIKATOS, Iasonas *et al*. Blockchain-Powered Applications for Smart Transactive Grids. **2019 Ieee Pes Innovative Smart Grid Technologies Europe (isgt-europe)**, [s.l.], p. 1-5, set. 2019. IEEE. http://dx.doi.org/10.1109/isgteurope.2019.8905482.

KSHETRI, Nir. 1 Blockchain's roles in meeting key supply chain management objectives. **International Journal Of Information Management**, [s.l.], v. 39, p. 80-89, abr. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.ijinfomgt.2017.12.005.

KUVSHINOV, Kirill et al. **Disciplina:** blockchain for education. Blockchain for Education. 2017. Disponível em: https://disciplina.io/yellowpaper.pdf.. Acesso em: 03 mar. 2018.

KUZLU, Murat *et al*. Performance Analysis of a Hyperledger Fabric Blockchain Framework: throughput, latency and scalability. : Throughput, Latency and Scalability. **2019 Ieee International Conference On Blockchain (blockchain)**, [s.l.], p. 536-540, jul. 2019. IEEE. http://dx.doi.org/10.1109/blockchain.2019.00003.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. **The Byzantine Generals Problem**. [s.l.]: Acm, 1982. 20 p. ACM Transactions on Programming Languages and Systems (TOPLAS).

LIU, Yinqiu *et al.*. **Effective Scaling of Blockchain Beyond Consensus Innovations and Moore's Law**. 2020. Disponível em: https://arxiv.org/pdf/2001.01865.pdf. Acesso em: 05 maio 2020.

LO, Sin Kuang et al. Evaluating Suitability of Applying Blockchain. **2017 22nd International Conference On Engineering Of Complex Computer Systems (iceccs)**, [s.l.], p. 158-161, nov. 2017. IEEE. http://dx.doi.org/10.1109/iceccs.2017.26.

MASLIN, Madeleine; WATT, Millicent; YONG, Christopher. Research Methodologies to Supportthe Development of Blockchain Standards. **Journal Of Ict Standardization**, [S.L.], v. 7, n. 3, p. 249-268, 2019. River Publishers. http://dx.doi.org/10.13052/jicts2245-800x.734.

MACDONALD, M; LIU-THORROLD, Lisa; JULIEN, R. **The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin**. 2017. 17 p. Pesquisa (Advanced Computer and Network Security) - The University of Queensland, [S. l.], 2017.

MACEDO, Victor Gabriel Reyes; ROSALES, Moises Salinas; GARCIA, Gina Gallegos. A Method for Blockchain Transactions Analysis. **Ieee Latin America Transactions**, [s.l.], v. 17, n. 07, p. 1080-1087, jul. 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/tla.2019.8931194.

MAESA, Damiano di Francesco; MORI, Paolo. **Blockchain 3.0 applications survey.** Journal Of Parallel And Distributed Computing, [s.l.], v. 138, p. 99-114, abr. 2020. Elsevier BV. http://dx.doi.org/10.1016/j.jpdc.2019.12.019.

MAULL, Roger *et al*. Distributed ledger technology: applications and implications. **Strategic Change**, [S.L.], v. 26, n. 5, p. 481-489, set. 2017. Wiley. http://dx.doi.org/10.1002/jsc.2148.

MECHKAROSKA, Daniela; DIMITROVA, Vesna; POPOVSKA-MITROVIKJ, Aleksandra. Analysis of the Possibilities for Improvement of BlockChain Technology. **2018 26Th Telecommunications Forum (Telfor)**, [S.L.], p. 1-4, nov. 2018. IEEE. http://dx.doi.org/10.1109/telfor.2018.8612034.

MEMORIA, Francisco. **700 Million Stuck in 115,000 Unconfirmed Bitcoin Transactions.**. 2017. Disponível em: https://www.ccn.com/700-million-stuck-115000-unconfirmed-bitcoin-transactions/. Acesso em: 16 junho 2020.

MIAO, Guowang et al. Fundamentals of Mobile Data Networks. [s.l.]: Cambridge University Press, 2016. 322 p. https://doi.org/10.1017/CBO9781316534298.

MOEZKARIMI, Zahra; ABDOLLAHEI, Fatemeh; ARABSORKHI, Abuzar. Proposing a Framework for Evaluating the Blockchain Platform. **2019 5th International Conference On Web Research (ICWR)**, [s.l.], p. 152-160, abr. 2019. IEEE. http://dx.doi.org/10.1109/icwr.2019.8765280.

MÜLLER, Suzana Pinheiro Machado. Métricas para a ciência e tecnologia e o financiamento da pesquisa: algumas reflexões. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, Florianópolis, p. 24-35, abr. 2008. ISSN 1518-2924. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2008v13nesp1p24>. Acesso em: 24 ago. 2020. doi:https://doi.org/10.5007/1518-2924.2008v13nesp1p24.

MUZYKA, Dan; BIRLEY, Sue; LELEUX, Benoit. Trade-offs in the investment decisons of European venture capitalists. **Journal Of Business Venturing**, [S.L.], v. 11, n. 4, p. 273-287, jul. 1996. Elsevier BV. http://dx.doi.org/10.1016/0883-9026(95)00126-3.

NADIR, Rana M.. Comparative study of permissioned blockchain solutions for enterprises. 2019 International Conference On Innovative Computing (ICIC), Lahore, p. 1-6, nov. 2019. IEEE. http://dx.doi.org/10.1109/icic48496.2019.8966735.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. 2009. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 25 maio 2020.

NARAYANAN, Arvind *et al*.. **Bitcoin and Cryptocurrency Technologies**: a comprehensive introduction. [s.l.]: [s.n.], 2016. 336 p.

NATARAJAN, Harish; KRAUSE, Solvej; GRADSTEIN, Helen. Distributed Ledger Technology and Blockchain. **World Bank**, [s.l.], [s.p.], jan. 2017. World Bank. http://dx.doi.org/10.1596/29053.

NIELES, Michael; DEMPSEY, Kelley; PILLITTERI, Victoria Yan. An introduction to information security. **Nist - National Institute Of Standards And Technology**, [S.L.], p. 1-101, jun. 2017. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-12r1.

O'NEAL, Stephen. **Blockchain Interoperability, Explained**. 2019. Disponível em: https://cointelegraph.com/explained/blockchain-interoperability-explained. Acesso em: 04 maio 2020.

OLIVEIRA, Marcela T. *et al*. Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload. **2019 22nd Conference On Innovation In Clouds, Internet And Networks And Workshops (icin)**, [s.l.], p. 180-187, fev. 2019. IEEE. http://dx.doi.org/10.1109/icin.2019.8685888.

PACKT. Types of blockchain. 2017. Disponível em: https://subscription.packtpub.com/book/big_data_and_business_intelligence/9781787125445/1/ch01lvl1sec10/types-of-blockchain. Acesso em: 13 maio 2020.

PALMA, Lucas M.; VIGIL, Martín A. G.; PEREIRA, Fernando L.; MARTINA, Jean E.. Blockchain and smart contracts for higher education registry in Brazil. **International Journal Of Network Management**, [s.l.], v. 29, n. 3, [s.p.], 21 jan. 2019. Wiley. http://dx.doi.org/10.1002/nem.2061.

PONGNUMKUL, Suporn; SIRIPANPORNCHANA, Chaiyaphum; THAJCHAYAPONG, Suttipong. Performance Analysis of Private Blockchain Platforms in Varying Workloads. **2017 26Th International Conference On Computer Communication And Networks (Icccn)**, [S.L.], p. 1-6, jul. 2017. IEEE. http://dx.doi.org/10.1109/icccn.2017.8038517.

POPOV, Serguei. **The tangle**. cit. on, p. 131, 2016.

PORRU, Simone *et al*. Blockchain-Oriented Software Engineering: challenges and new directions. : Challenges and New Directions. **2017 Ieee/acm 39th International Conference On Software Engineering Companion (icse-c)**, [s.l.], p. 169-171, maio 2017. IEEE. http://dx.doi.org/10.1109/icse-c.2017.142.

PPGTIC. **Linhas de Pesquisa do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação**. 2018. Disponível em: https://ppgtic.ufsc.br/linhas-de-pesquisa. Acesso em: 22 fev. 2020.

PURBO, Onno et al. **Benchmark and comparison between hyperledger and MySQL. Telkomnika** (telecommunication Computing Electronics And Control), [s.l.], v. 18, n. 2, p. 705-715, 1 abr. 2020. Universitas Ahmad Dahlan. http://dx.doi.org/10.12928/telkomnika.v18i2.13743.

QUORUM. **Quorum Whitepaper**. 2018. Disponível em: https://github.com/ConsenSys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf. Acesso em: 02 jun 2020.

R3. **Corda Enterprise–a next-gen blockchain platform**. Disponível em: https://www.r3.com/corda-platform/. Acesso em: 24 maio 2020.

RAJPUT, Dharmendra Singh; THAKUR, Ramjeevan Singh; BASHA, Syed Muzamil. **Transforming Businesses With Bitcoin Mining and Blockchain Applications**. [s.l.]: Business Science Reference, 2019. 282 p.

RASCHENDORFER, Alexander *et al*. **On IOTA as a potential enabler for an M2M economy in manufacturing.** Procedia CIRP, v. 79, p. 379-384, 2019.

REYNA, Ana *et al*. On blockchain and its integration with IoT. Challenges and opportunities. **Future Generation Computer Systems**, [S.L.], v. 88, p. 173-190, nov. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.future.2018.05.046.

RIPPLE. **Technical FAQ**. Disponível em: https://xrpl.org/technical-faq.html. Acesso em: 24 maio 2020.

ROSA, Reginaldo José da. **Modelo de logística reversa baseado em contabilidade distribuída – Blockchain**. 2019. 136 f. Dissertação (Mestrado) - Curso de Tecnologias da Informação e Comunicação, Centro de Ciências, Tecnologias e Saúde – Campus Araranguá, Universidade Federal de Santa Catarina, Araranguá, 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/215093. Acesso em: 07 jun. 2021.

RUBENSTEIN, Albert H.; GEISLER, Eliezer. The Use of Indicators and Measures of the R & D Process in Evaluating Science and Technology Programmes. **Government Innovation Policy**, London, p. 185-203, 1989. DOI 10.1007/978-1-349-08882-9_14. Disponível em: https://doi.org/10.1007/978-1-349-08882-9_14. Acesso em: 19 ago. 2020.

RYDZI, Filipi; TRUONG, Hong-linh. Sharing Blockchain Performance Knowledge for Edge Service Development. **2019 Ieee 5th International Conference On Collaboration And Internet Computing (cic)**, Los Angeles, p. 20-29, dez. 2019. IEEE. http://dx.doi.org/10.1109/cic48465.2019.00012.

SAMANIEGO, Mayra; DETERS, Ralph. Internet of Smart Things - IoST: using blockchain and clips to make things autonomous. **2017 Ieee International Conference On Cognitive Computing (Iccc)**, [S.L.], p. 9-16, jun. 2017. IEEE. http://dx.doi.org/10.1109/ieee.iccc.2017.9.

SANKAR, Lakshmi Siva et al. Survey of consensus protocols on blockchain applications. **2017 4th International Conference On Advanced Computing And Communication Systems (icaccs)**, [s.l.], p. 1-5, jan. 2017. IEEE. http://dx.doi.org/10.1109/icaccs.2017.8014672.

SARAF, Chinmay; SABADRA, Siddharth. Blockchain platforms: a compendium. : A compendium. **2018 Ieee International Conference On Innovative Research And**

Development (icird), [s.l.], p. 1-6, maio 2018. IEEE. http://dx.doi.org/10.1109/icird.2018.8376323.

SARFRAZ, Umair et al. **Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions.** Computer Networks, v. 148, p. 361-372, 2019.

SCHNEIER, Bruce. **Opinion: Cryptanalysis of MD5 and SHA: Time for a new standard**. Crypto researchers report weaknesses in common hash functions. 2004. Disponível em: https://www.computerworld.com/article/2566208/opinion--cryptanalysis-of-md5-and-sha--time-for-a-new-standard.html. Acesso em: 25 mar. 2020.

SCHWENTKER, R.; LINUXFOUNDATIONX. **Blockchain for Business - An Introduction to Hyperledger Technologies**. Curso LFS171x – EDX. Disponível em: https://courses.edx.org/ courses/course-v1:LinuxFoundationX+LFS171x+3T2017/course/. Acesso em: 20 set. 2018.

SHEPHERD, Dean A.; ZACHARAKIS, Andrew. Conjoint analysis: a new methodological approach for researching the decision policies of venture capitalists. **Venture Capital**, [S.L.], v. 1, n. 3, p. 197-217, jul. 1999. Informa UK Limited. http://dx.doi.org/10.1080/136910699295866.

SHI, Zeshun *et al*. Operating Permissioned Blockchain in Clouds: a performance study of hyperledger sawtooth. : A Performance Study of Hyperledger Sawtooth. **2019 18th International Symposium On Parallel And Distributed Computing (ispdc)**, [s.l.], p. 50-57, jun. 2019. IEEE. http://dx.doi.org/10.1109/ispdc.2019.00010.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005. 138 p. Disponível em: https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf. Acesso em: 26 mai. 2020.

SILVA, Erivaldo Cabral da. **Determinação do nível de sistematização e proposta de revisão da técnica de inspeção de conformidade ergonômica para software educacional.** 2002. 102 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2002. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/84487. Acesso em: 24 ago. 2020.

SILVA, Erivaldo Cabral da. **Determinação do nível de sistematização e proposta de revisão da técnica de inspeção de conformidade ergonômica para software educacional.** 2002. 102 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2002. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/84487. Acesso em: 24 ago. 2020.

SILVA, Marcelo Ribeiro Xavier da. **Tolerância a faltas bizantinas através de hibridização do sistema distribuído**. 2013. 123 f. Monografia (Especialização) - Curso de Engenharia de Automação e Sistemas, Universidade Federal de Santa Catarina, Florianópolis, 2013.

STALLINGS, William; BROWN, Lawrie. **Computer Security**: principles and practice. 3. ed. [s.l.]: Pearson, 2015. 848 p.

SILVANO, Wellington Fernandes; MARCELINO, Roderval. **Iota Tangle: a cryptocurrency to communicate Internet-of-Things data**. Future Generation Computer Systems, [S.L.], v. 112, p. 307-319, nov. 2020. Elsevier BV. http://dx.doi.org/10.1016/j.future.2020.05.047.

STINSON, Douglas Robert. **Cryptography: theory and practice**. 2006. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=cat07205a&AN=uls.301778&lang=pt-br&site=eds-live&scope=site. Acesso em: 25 mar. 2020.

SUKHWANI, Harish *et al*. Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). **2018 Ieee 17th International Symposium On Network Computing And Applications (NCA)**, [s.l.], p. 1-8, nov. 2018. IEEE. http://dx.doi.org/10.1109/nca.2018.8548070.

SUN, Yao et al. Blockchain-Enabled Wireless Internet of Things: performance analysis and optimal communication node deployment. : Performance Analysis and Optimal Communication Node Deployment. **Ieee Internet Of Things Journal**, [s.l.], v. 6, n. 3, p. 5791-5802, jun. 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jiot.2019.2905743.

SYED, Toqeer Ali *et al*. A Comparative Analysis of Blockchain Architecture and its Applications: problems and recommendations. : Problems and Recommendations. **Ieee Access**, [s.l.], v. 7, p. 176838-176869, dez. 2019. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2019.2957660.

SZABO, N. Formalizing and Securing Relationships on Public Networks. **First Monday**, v. 2, n. 9, 1 Sep. 1997

THAKKAR, Parth; NATHAN, Senthil; VISWANATHAN, Balaji. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. **2018 Ieee 26th International Symposium On Modeling, Analysis, And Simulation Of Computer And Telecommunication Systems (mascots)**, [s.l.], p. 264-276, set. 2018. IEEE. http://dx.doi.org/10.1109/mascots.2018.00034.

TSCHORSCH, Florian; SCHEUERMANN, Bjorn. Bitcoin and Beyond: a technical survey on decentralized digital currencies. : A Technical Survey on Decentralized Digital Currencies. **Ieee Communications Surveys & Tutorials**, [s.l.], v. 18, n. 3, p. 2084-2123, 2016. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/comst.2016.2535718.

URMILA, M S; HARIHARAN, Balaji; PRABHA, Rekha. A Comparitive Study of Blockchain Applications for Enhancing Internet of Things Security. **2019 10th International Conference On Computing, Communication And Networking Technologies (icccnt)**, Kanpur, p. 1-7, jul. 2019. IEEE. http://dx.doi.org/10.1109/icccnt45670.2019.8944446.

VALKENBURGH, Peter Van. **What is “open source” and why is it important for cryptocurrency and open blockchain projects?** 2017. Disponível em: https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects. Acesso em: 01 maio 2020.

VANGULICK, David; CORNELUSSE, Bertrand; ERNST, Damien. Blockchain for Peer-to-Peer Energy Exchanges: design and recommendations. : Design and Recommendations. **2018 Power Systems Computation Conference (pscc)**, Dublin, p. 1-7, jun. 2018. IEEE. http://dx.doi.org/10.23919/pscc.2018.8443042.

WALDMAN, Jonathan. **Blockchain – Conceitos básicos do Blockchain.** 2018. Disponível em: https://docs.microsoft.com/pt-br/archive/msdn-magazine/2018/march/blockchain-blockchain-fundamentals. Acesso em: 15 jun. 2020.

WALPORT Mark, **Distributed ledger technology: Beyond block chain**, Government Office for Science, p. 1–88, 2015. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Acesso em 10 mai. 2020.

WANG, Xiaonan *et al*. Blockchain-based smart contract for energy demand management. **Energy Procedia**, [S.L.], v. 158, p. 2719-2724, fev. 2019. Elsevier BV. http://dx.doi.org/10.1016/j.egypro.2019.02.028.

WOOD, G. **Ethereum**: a secure decentralised generalised transaction ledger. A secure decentralised generalised transaction ledger. 2014. Disponível em: http://gavwood.com/paper.pdf. Acesso em: 25 maio 2020.

XU, Xiwei et al. A Taxonomy of Blockchain-Based Systems for Architecture Design. **2017 Ieee International Conference On Software Architecture (icsa)**, [s.l.], p. 243-252, abr. 2017. IEEE. http://dx.doi.org/10.1109/icsa.2017.33.

XU, Xiwei *et al*. Designing blockchain-based applications a case study for imported product traceability. **Future Generation Computer Systems**, [S.L.], v. 92, p. 399-406, mar. 2019. Elsevier BV. http://dx.doi.org/10.1016/j.future.2018.10.010.

YASAWEERASINGHELAGE, Rajitha; STAPLES, Mark; WEBER, Ingo. Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation. **2017 Ieee International Conference On Software Architecture (icsa)**, [s.l.], p. 0-0, abr. 2017. IEEE. http://dx.doi.org/10.1109/icsa.2017.22.

YOSHIDA, Hirotaka; BIRYUKOV, Alex. Analysis of a SHA-256 Variant. **Selected Areas In Cryptography**, [s.l.], p. 245-260, ago. 2006. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11693383_17.

ZHANG, Dongpo *et al*. Blockchain Technology Hyperledger Framework in the Internet of Energy. **Iop Conference Series**: Earth and Environmental Science, [s.l.], v. 168, p. 012043-012047, jun. 2018. IOP Publishing. http://dx.doi.org/10.1088/1755-1315/168/1/012043.

ZHANG, Laney. **China: Rules on Blockchain-Based Information Services Issued Requiring Authentication of Users' Real Identities**. 2019. Disponível em: https://www.loc.gov/law/foreign-news/article/china-rules-on-blockchain-based-information-services-issued-requiring-authentication-of-users-real-identities/. Acesso em: 21 maio 2020.

ZHANG, Peng; WHITE, Jules; SCHMIDT, Douglas C.; LENZ, Gunther. Design of blockchain-based apps using familiar software patterns with a healthcare focus. **Proceedings Of The 24th Conference On Pattern Languages Of Programs**, [s.l.], p. 1-14, out. 2017.

ZHENG, Peilin *et al*. A detailed and real-time performance monitoring framework for blockchain systems. **Proceedings Of The 40th International Conference On Software Engineering In Practice – Icse-seip '18**, [s.l.], p. 134-143, maio 2018. ACM Press. http://dx.doi.org/10.1145/3183519.3183546.

ZHENG, Xiaoying; ZHU, Yongxin; SI, Xueming. A Survey on Challenges and Progresses in Blockchain Technologies: a performance and security perspective. : A Performance and Security Perspective. **Applied Sciences**, [s.l.], v. 9, n. 22, [s.p.], 6 nov. 2019. MDPI AG. http://dx.doi.org/10.3390/app9224731.

APÊNDICE A – Metodologia Computacional

INSTRUMENTO DE ANÁLISE E AVALIAÇÃO TÉCNICO-CIENTÍFICO – ETAPA I		
Pergunta	Resposta	
	Sim	Não
Existem múltiplas partes envolvidas?	☑	☐
Existe déficit de confiança entre as partes?	☑	☐
Existe algum terceiro confiável?	☐	☐
O registro da transação deve ser imutável?	☑	☐
Escalabilidade é um requisito crítico?	☐	☐
Utilize Blockchain		
Verificabilidade é importante?	☐	☑
Utilize Blockchain Privada.		
Durabilidade dos dados é importante?	☐	☑
Utilize armazenamento *off-chain*.		

INSTRUMENTO DE ANÁLISE E AVALIAÇÃO TÉCNICO-CIENTÍFICO – ETAPA II						
Nome:						
Data Realização:						
Assinatura:						
	Indicador	**Não se aplica**	**Resposta**			
1	**ARQUITETURA**					
1.1	**Quantitativo**					
1.1.1	**Tamanho do bloco**	☐				
	O tamanho do bloco atende a necessidade/demanda da aplicação?	☐	☐	Sim	☐	Não
	O tamanho do bloco é adequado ao tamanho da transação?	☐	☐	Sim	☐	Não
	O tamanho do bloco é adequado à rede?	☐	☐	Sim	☐	Não
	Quais são as vantagens e desvantagens para este tamanho de bloco para o sistema de modo geral?	☐	Aberta			
	O tamanho do bloco impacta a escalabilidade do tipo de Blockchain?	☐	☐	Sim	☐	Não
	O tamanho do bloco interfere na performance do sistema?	☐	☐	Sim	☐	Não
	Existe autonomia para configuração deste indicador na tecnologia avaliada?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.2	**Tamanho do *mempool***	☐				
	O tamanho máximo da *mempool* atende à quantidade de transações previstas?	☐	☐	Sim	☐	Não
	O tamanho médio da *mempool* indica bom desempenho da aplicação?	☐	☐	Sim	☐	Não
	Existem requisitos de hardware mínimos devido ao tamanho da *mempool*?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.3	**Tamanho da transação**	☐				
	O tamanho da transação atende a necessidade/demanda da aplicação?	☐	☐	Sim	☐	Não
	O tamanho da transação é adequado ao tamanho do bloco?	☐	☐	Sim	☐	Não

	O tamanho do bloco é adequado à rede?	☐	☐	Sim	☐	Não
	Quais são as vantagens e desvantagens para este tamanho da transação para o sistema de modo geral?	☐	Aberta			
	Podem existir transações com tamanhos excessivos na aplicação que poderiam prejudicar o sistema?	☐	☐	Sim	☐	Não
	Existe autonomia para configuração deste indicador na tecnologia avaliada?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.4	**Latência da transação**	☐				
	O tempo de latência da transação atende as necessidades da aplicação?	☐	☐	Sim	☐	Não
	O canal de comunicação de dados utilizado atende a latência esperada da rede?	☐	☐	Sim	☐	Não
	A latência se mantém adequada no pico de transações?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.5	***Throughput***	☐				
	O *throughput* da tecnologia blockchain atende o volume de transações da aplicação?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.6	**Tempo de finalidade**	☐				
	A tecnologia blockchain adotada para o projeto utiliza-se de algoritmos de consenso com finalidade probabilística ou determinística?	☐	☐	Probabilística	☐	Determinística
	O tempo de finalidade recomendado da tecnologia blockchain oferece segurança e é viável à aplicação?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.1.7	**Tempo de espera da validação**	☐				
	O tempo de espera da validação atende as necessidades da aplicação?	☐	☐	Sim	☐	Não
	O tempo de espera da validação se mantém adequado no pico de	☐	☐	Sim	☐	Não

	transações?					
	Parecer técnico:					
1.1.8	**Tempo de confirmação de bloco**	☐				
	O tempo de confirmação de bloco atende às necessidades da aplicação?	☐	☐	Sim	☐	Não
	O tempo de confirmação de bloco é adequado aos usuários com menor prioridade?	☐	☐	Sim	☐	Não
	Existe algum gargalo de hardware que pode prejudicar o tempo de confirmação do bloco?	☐	☐	Sim	☐	Não
	Existe autonomia para configuração deste indicador na tecnologia avaliada?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.2	**Qualitativo**					
1.2.1	**Resiliência**	☐				
	A solução desenvolvida mantêm-se operacional frente a eventos adversos? (e.g., ataques ou acidentes)	☐	☐	Sim	☐	Não
	A solução desenvolvida possui algum mecanismo para autodetecção e autocorreção de problemas?	☐	☐	Sim	☐	Não
	Qual a autonomia do desenvolvedor da aplicação para adaptar a tecnologia blockchain utilizada na solução desenvolvida?	☐	Aberta			
	As possíveis indisponibilidades da solução desenvolvida são aceitáveis para a aplicação?	☐	☐	Sim	☐	Não
	Com relação a demanda de acesso, capacidade de armazenamento, tipos variados de dados entre outras características técnicas, a solução desenvolvida possui a capacidade de acompanhar o crescimento e a complexidade dos sistemas atuais?	☐	Aberta			
	Parecer técnico:					
1.2.2	**Escalabilidade**	☐				
	A solução desenvolvida mantêm desempenho aceitável quando a carga de trabalho ou número de nodos aumentam?	☐	☐	Sim	☐	Não

	A solução desenvolvida mantém estabilidade com o aumento de cargas de trabalho concorrente?	☐	☐	Sim	☐	Não
	O algoritmo de consenso ajuda na escalabilidade?	☐	☐	Sim	☐	Não
	O banco de dados contribui na escalabilidade?	☐	☐	Sim	☐	Não
	A distribuição geográfica dos usuários ou nodos contribui na escalabilidade?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.2.3	**Interoperabilidade**	☐				
	Há necessidade de integrar a tecnologia blockchain utilizada com outras tecnologias blockchain?	☐	☐	Sim	☐	Não
	A tecnologia blockchain utilizada é interoperável com outras tecnologias blockchain?	☐	☐	Sim	☐	Não
	Usaram-se padrões de projeto que facilitam a adaptação da solução? Por exemplo, *Publish-Subscriber*.	☐	☐	Sim	☐	Não
	A tecnologia blockchain dispõe de bibliotecas, *frameworks* ou SDKs para integração com outras tecnologias? Possuem um nível de maturidade considerado aceitável?	☐	Aberta			
	A solução desenvolvida é multiplataforma?	☐	Aberta			
	Parecer técnico:					
1.2.4	**Alocação de recursos**	☐				
	A alocação de recursos é suficiente para a estratégia proposta no modelo de negócio?	☐	Aberta			
	Há recursos suficientes para a solução desenvolvida ser executada em todos os nodos?	☐	Aberta			
	Quais são os recursos mínimos para a solução desenvolvida funcionar?	☐	Aberta			
	Parecer técnico:					
1.2.5	**Tipo de licenciamento**	☐				
	A tecnologia blockchain utilizada no projeto é *open-source*?	☐	☐	Sim	☐	Não

	Existem custos relacionados ao licenciamento das tecnologias utilizadas?	☐	☐	Sim	☐	Não
	Respeita-se o licenciamento da tecnologia blockchain e da aplicação?	☐	☐	Sim	☐	Não
	O licenciamento promove sustentabilidade e manutenabilidade da tecnologia blockchain usada?	☐	☐	Sim	☐	Não
	As tecnologias blockchain fornecem uma versão de suporte de longo prazo (LTS)?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.2.6	**Algoritmo de consenso**	☐				
	O algoritmo de consenso utilizado atende a necessidade de escalabilidade do projeto?	☐	☐	Sim	☐	Não
	O algoritmo de consenso utilizado atende a necessidade de transações por segundo do projeto?	☐	☐	Sim	☐	Não
	O algoritmo de consenso utilizado atende a necessidade de velocidade de verificação do projeto?	☐	☐	Sim	☐	Não
	Existe limitação acerca da utilização de recursos computacionais?	☐	☐	Sim	☐	Não
	É possível trocar ou configurar o algoritmo de consenso?	☐	☐	Sim	☐	Não
	O algoritmo de consenso utilizado é adequado à tecnologia blockchain utilizada?	☐	☐	Sim	☐	Não
	A política de consenso adotada permite a definição de papéis ou regras diferentes entre participantes da rede?	☐	☐	Sim	☐	Não
	A política de consenso adotada permite a definição de tipos de transações diferentes entre participantes da rede?	☐	☐	Sim	☐	Não
	Parecer técnico:					
1.2.7	**Desempenho**	☐				
	A tecnologia blockchain dispõe de algum recurso que permita o monitoramento de desempenho?	☐	☐	Sim	☐	Não
	O número de nodos blockchain contribui ou prejudica o desempenho da solução?	☐	Aberta			

	O desempenho computacional de soluções blockchain podem ser menos eficazes que soluções centralizadas. Para a solução proposta o desempenho pode ser limitante para o modelo de negócio?	☐	☐	Sim	☐	Não
	A escolha do banco de dados de estado contribui para o desempenho da solução?	☐	Aberta			
	Parecer técnico:					
1.2.8	**Tolerância a faltas**	☐				
	A solução desenvolvida tolera faltas:					
	a) de hardware?	☐	☐	Sim	☐	Não
	b) de software?	☐	☐	Sim	☐	Não
	c) bizantinas?	☐	☐	Sim	☐	Não
	Quais meios a tecnologia blockchain oferece para contingenciar faltas?	☐	Aberta			
	Como a solução monitora faltas em tempo real?	☐	Aberta			
	Parecer técnico:					
1.2.9	**Presença de banco de dados de estado**	☐				
	O banco de dados utilizado contribui para escalabilidade e desempenho da solução desenvolvida?	☐	☐	Sim	☐	Não
	O banco de dados utilizado contribui para o desempenho da solução desenvolvida?	☐	☐	Sim	☐	Não
	De que maneira os dados são armazenados? Por exemplo, on-chain ou off-chain.	☐	Aberta			
	O banco de dados utilizado atende as regras de negócio da solução?	☐	☐	Sim	☐	Não
	A tecnologia blockchain permite utilizar de mais de um tipo de banco de dados de estado?	☐	☐	Sim	☐	Não
	Parecer técnico:					
2	**OBJETIVO**					

2.1	**Qualitativo**					
2.1.1	**Aplicação**	☐				
	A solução desenvolvida cumpre os requisitos esperados?	☐	☐	Sim	☐	Não
	A solução desenvolvida utiliza contratos inteligentes para atender o modelo de negócio?	☐	☐	Sim	☐	Não
	Quais benefícios a solução desenvolvida traz para o negócio (financeiro, produtividade, inovação)?	☐	Aberta.			
	A tecnologia blockchain oferece uma linguagem de programação Turing-completa para desenvolver aplicações?	☐	☐	Sim	☐	Não
	A tecnologia blockchain utilizada é a mais apropriada ao modelo de negócio proposto? Por quê?	☐	Aberta			
	Utilizou-se ferramenta(s) de gerenciamento de projeto durante o desenvolvimento da aplicação? Se sim, quais?	☐	Aberta			
	Evitou-se alterar características originais da tecnologia blockchain para atender ao modelo de negócio?	☐	☐	Sim	☐	Não
	Parecer técnico:					
3	**SUPORTE**					
3.1	**Qualitativo**					
3.1.1	**Documentação**	☐				
	A aplicação desenvolvida:					
	a) oferece documentação de desenvolvimento comunicando requisitos, projeto e implementação da aplicação? Por exemplo, documento de requisitos e diagramas UML (modelos conceitual, lógico e físico).	☐	Aberta			
	b) oferece documentação de infraestrutura comunicando como implantar a aplicação? Por exemplo, criar usuários.	☐	Aberta			
	c) oferece documentação de utilização comunicando de como usar a aplicação? Por exemplo, casos de testes e tutoriais de usuário.	☐	Aberta			
	A tecnologia blockchain utilizada na solução desenvolvida:					

	a) oferece tutorial de utilização e/ou recursos para testes?	☐	☐	Sim	☐	Não
	b) oferece tutoriais de implantação?	☐	☐	Sim	☐	Não
	c) oferece tutorias de codificação dos contratos inteligentes?	☐	☐	Sim	☐	Não
	d) recebe atualização frequente da documentação?	☐	☐	Sim	☐	Não
	e) atende diferentes tipos de usuários?	☐	☐	Sim	☐	Não
	f) conta com documentação (em forma de materiais) da comunidade para resolução de problemas? Por exemplo, Stackoverflow e Github.	☐	☐	Sim	☐	Não
	Parecer técnico:					
3.1.2	**Participação do fornecedor/comunidade**	☐				
	O mantimento da tecnologia blockchain utilizada conta com a participação do fornecedor e/ou da comunidade?	☐	☐	Sim	☐	Não
	Os mantenedores da tecnologia blockchain utilizada são consistentes e ativos?	☐	☐	Sim	☐	Não
	Questões relacionadas à tecnologia blockchain utilizada possuem volume de atividade frequente nas comunidades de desenvolvimento? Por exemplo, Stackoverflow e Github.	☐	☐	Sim	☐	Não
	Parecer técnico:					
3.1.3	**Tamanho do time de desenvolvimento**	☐				
	O tamanho time de desenvolvimento é adequado para continuidade e evolução da tecnologia blockchain?	☐	☐	Sim	☐	Não
	Qual o nível de conhecimento e habilidade do time?	☐	Aberta			
	O volume de atividade do time de desenvolvimento é consistente?	☐	☐	Sim	☐	Não
	A frequência de contribuições do time é consistente?	☐	☐	Sim	☐	Não
	Parecer técnico:					
4	**GOVERNANÇA**					

4.1	**Quantitativo**					
4.1.1	**Custo**	☐				
	São adequados os custos de:					
	a) infraestrutura (e.g., *datacenter*, energia elétrica e mão de obra)?	☐	☐	Sim	☐	Não
	b) taxas de transação pagas à rede blockchain?	☐	☐	Sim	☐	Não
	c) profissionais especializados na tecnologia blockchain?	☐	☐	Sim	☐	Não
	O custo da solução desenvolvida justifica as vantagens da sua implantação?	☐	☐	Sim	☐	Não
	Existem custos relacionados ao licenciamento da tecnologia blockchain?	☐	☐	Sim	☐	Não
	Parecer técnico:					
4.2	**Qualitativo**					
4.2.1	**Segurança**	☐				
	A solução desenvolvida garante à aplicação:					
	a) uso de algoritmos e parâmetros criptográficos considerados seguros?	☐	☐	Sim	☐	Não
	b) integridade dos dados?	☐	☐	Sim	☐	Não
	c) funcionamento conforme especificação?	☐	☐	Sim	☐	Não
	d) disponibilidade?	☐	☐	Sim	☐	Não
	f) confidencialidade ou sigilo dos dados, quando necessário?	☐	☐	Sim	☐	Não
	e) autenticação dos participantes?	☐	☐	Sim	☐	Não
	f) autorização dos participantes?	☐	☐	Sim	☐	Não
	g) auditabilidade das operações?	☐	☐	Sim	☐	Não
	h) não repúdio das operações, quando necessário?	☐	☐	Sim	☐	Não
	A solução desenvolvida utiliza:					
	a) somente algoritmos de resumo criptográfico exigidos ou recomendados por (ICP-BRASIL, 2019)?	☐	☐	Sim	☐	Não
	b) somente algoritmos de assinatura digital exigidos ou recomendados por (ICP-BRASIL, 2019)?	☐	☐	Sim	☐	Não
	c) somente tamanhos de chave maiores ou iguais ao tamanho mínimo exigido ou recomendado por (ICP-BRASIL, 2019)?	☐	☐	Sim	☐	Não

	É viável executar ataques conhecidos contra tecnologia blockchain? Por exemplo, ataque de 51%?	☐	Aberta			
	A solução desenvolvida sofre de alguma vulnerabilidade conhecida e crítica? Por exemplo, uma vulnerabilidade listada na *Common Vulnerabilities and Exposures* e avaliada com nota igual ou superior a 7 seguindo a metodologia CVSSv3.1?	☐	Aberta			
	A solução desenvolvida atende às políticas de segurança das informações adotadas pela instituição que usará a solução?	☐	☐	Sim	☐	Não
	A solução desenvolvida oferece sigilo em nível de transação entre um subconjunto dos participantes?	☐	☐	Sim	☐	Não
	A solução usa banco de dados dedicado? Por exemplo, para evitar acesso não autorizado de terceiros.	☐	☐	Sim	☐	Não
	A solução desenvolvida armazena senhas no formato usando hash e salt?	☐	☐	Sim	☐	Não
	Existe procedimento periódico para criar backup da solução desenvolvida?	☐	☐	Sim	☐	Não
	Existe procedimento periódico para restaurar backup da solução desenvolvida?	☐	☐	Sim	☐	Não
	Todo dado sigiloso trafega somente por canais de comunicação protegidos?	☐	☐	Sim	☐	Não
	Todo dado sigiloso é armazenado de modo cifrado?	☐	☐	Sim	☐	Não
	Toda comunicação entre APIs e as camadas de infraestrutura ocorre de forma segura?	☐	Aberta			
	As sessões de acesso à solução desenvolvida expiram?	☐	☐	Sim	☐	Não
	A solução desenvolvida atende às políticas de segurança das informações adotadas pela instituição que usará a solução?	☐	Aberta			
	A solução desenvolvida atende aos requisitos de sigilo do modelo de negócio?	☐	Aberta			
	Parecer técnico:					
4.2.2	**Privacidade**	☐				

	Aplica-se um processo irreversível de anonimidade de dados pessoais garantindo privacidade?	☐	☐	Sim	☐	Não
	A solução desenvolvida permite aos indivíduos controlar:					
	a) quais dados pessoais são coletados e armazenados?	☐	☐	Sim	☐	Não
	b) quem fornece e para quem fornece os dados pessoais?	☐	☐	Sim	☐	Não
	Atende-se à Lei Geral de Proteção de Dados (LGPD, Lei nº 12.965/2014) quanto:					
	a) Utilizam-se dados pessoais não anonimizados, isto é, informação relacionada a pessoa natural identificada ou identificável conforme as finalidades prescritas Art. 7?	☐	☐	Sim	☐	Não
	b) Utilizam-se dados pessoais sensíveis não anonimizados, isto é, aqueles que determinam "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" de uma pessoa natural conforme finalidade prescritas no Art 11?	☐	☐	Sim	☐	Não
	c) Adotaram-se medidas de segurança da informação contra situações acidentais ou ilícitas para promover confidencialidade, integridade e disponibilidade dos dados (pessoais ou pessoais sensíveis) desde a concepção da solução desenvolvida?	☐	☐	Sim	☐	Não
	d) Cessa-se a utilização de dados quando alguma das hipóteses elencadas no Art 15 forem verificadas?	☐	☐	Sim	☐	Não
	e) Cessada a utilização dos dados, estes são eliminados conforme prescreve o Art 16?	☐	☐	Sim	☐	Não
	Parecer técnico:					
4.2.3	**Topologia da rede**	☐				

	A topologia da rede segue o padrão do tipo de blockchain escolhido?	☐	☐	Sim	☐	Não
	A topologia da rede contribui para a escalabilidade da solução desenvolvida?	☐	☐	Sim	☐	Não
	A topologia da rede contribui para o desempenho da solução desenvolvida?	☐	☐	Sim	☐	Não
	Parecer técnico:					
4.2.4	**Tipo de blockchain**	☐				
	Qual o tipo da tecnologia blockchain escolhida? Por exemplo, pública, privada, híbrida ou consórcio?	☐	Aberta			
	O tipo de tecnologia blockchain escolhido é adequado às regras de negócio? (Ver a árvore de decisão)	☐	☐	Sim	☐	Não
	A blockchain é permissionada ou não permissionada?	☐	☐	Permissionada	☐	Não permissionada
	Parecer técnico:					
4.2.5	**Suporte a moeda ou token**	☐				
	O modelo de negócio proposto exige suporte da tecnologia blockchain para moeda ou token?	☐	☐	Sim	☐	Não
	A moeda ou token apresenta suficiente lastro para o modelo de negócio proposto?	☐	☐	Sim	☐	Não
	A volatidade da moeda ou token é aceitável para o modelo de negócio proposto?	☐	☐	Sim	☐	Não
	Parecer técnico:					

INSTRUMENTO DE ANÁLISE E AVALIAÇÃO TÉCNICO-CIENTÍFICO
ETAPA III

Matriz de dependência A (Elemento Ai,j => i depende de j)	1.2.1 Resiliência	1.2.2 Escalabilidade	1.2.3 Interoperabilidade	1.2.4 Alocação de recursos	1.2.5 Tipo de licenciamento	1.2.6 Algoritmo de consenso	1.2.7 Desempenho	1.2.8 Tolerância a faltas	1.2.9 Presença de banco de dados de estado	2.1.1 Aplicação	3.1.1 Documentação	3.1.2 Participação do fornecedor/comunidade	3.1.3 Tamanho do time de desenvolvimento	4.2.1 Segurança	4.2.2 Privacidade	4.2.3 Topologia da rede	4.2.4 Tipo de blockchain	4.2.5 Suporte a moeda ou token	1.1.1 Tamanho do bloco	1.1.2 Tamanho do *mempool*	1.1.3 Tamanho da transação	1.1.4 Latência da transação	1.1.5 *Throughput*	1.1.6 Tempo de finalidade	1.1.7 Tempo de espera da validação	1.1.8 Tempo de confirmação de bloco	4.1.1 Custo
1.2.1 Resiliência																											
1.2.2 Escalabilidade																											
1.2.3 Interoperabilidade																											
1.2.4 Alocação de recursos																											
1.2.5 Tipo de licenciamento																											
1.2.6 Algoritmo de consenso																											
1.2.7 Desempenho																											
1.2.8 Tolerância a faltas																											
1.2.9 Presença de banco de dados de estado																											
2.1.1 Aplicação																											
3.1.1 Documentação																											
3.1.2 Participação do fornecedor/comunidade																											
3.1.3 Tamanho do time de desenvolvimento																											
4.2.1 Segurança																											
4.2.2 Privacidade																											
4.2.3 Topologia da rede																											
4.2.4 Tipo de blockchain																											
4.2.5 Suporte a moeda ou token																											
1.1.1 Tamanho do bloco																											
1.1.2 Tamanho do *mempool*																											
1.1.3 Tamanho da transação																											
1.1.4 Latência da transação																											
1.1.5 *Throughput*																											
1.1.6 Tempo de finalidade																											
1.1.7 Tempo de espera da validação																											
1.1.8 Tempo de confirmação de bloco																											
4.1.1 Custo																											