



IX ENCONTRO BRASILEIRO DE ADMINISTRAÇÃO PÚBLICA

ISSN: 2594-5688

secretaria@sbap.org.br

Sociedade Brasileira de Administração Pública

ARTIGO

POSSIBILIDADES, DESAFIOS E O PAPEL DO ESTADO NO USO DE BLOCKCHAIN PARA O COMBATE ÀS FAKE NEWS E DESINFORMAÇÃO

ANDERSON RIBEIRO DE FREITAS, ERGON CUGLER DE MORAES SILVA, JOSÉ CARLOS VAZ,

**GRUPO TEMÁTICO: 04 Governança, Governo Eletrônico
e Transformação Digital**

IX Encontro Brasileiro de Administração Pública, São Paulo/SP, 5 a 7 de outubro de 2022.
Sociedade Brasileira de Administração Pública
Brasil

Disponível em: <https://sbap.org.br/>

Possibilidades, desafios e o papel do Estado no uso de Blockchain para o combate às Fake News e Desinformação

Resumo: Este trabalho se propõe a investigar uma nova possibilidade de aplicação tecnológica na Gestão Pública, respondendo à pergunta: “como a tecnologia blockchain pode contribuir no combate às *fake news* e à desinformação?”, partindo da premissa de que *fake news* e desinformação são um problema público no qual o Estado é um ator relevante. Para tal, realizou-se uma revisão de literatura sobre caminhos para uso da tecnologia, aproximando a discussão teórica do campo de políticas públicas e a discussão sobre *fake news* e desinformação. Como resultados, as categorias teóricas da desinformação foram relacionadas com as camadas de uso da tecnologia apontadas, resultando em um framework para organizar as abordagens no enfrentamento à desinformação utilizando da tecnologia blockchain.

Palavras-chave: Gestão Pública; Implementação; Blockchain; Desinformação; *Fake news*.

1. Introdução

Os estudos sobre desinformação e *fake news* (notícias falsas) avançaram após as eleições de Donald Trump nos Estados Unidos da América (2016), além do Brexit no Reino Unido (com referendo em 2016) e, no caso do Brasil, com a eleição de Jair Messias Bolsonaro à presidência (2018) (Recuero, 2019; Escossia, 2019). Ainda assim, autores como Abad (2018) e Volkoff (2004, p. 11) apontam que o termo ‘desinformação’ já era visto durante a Segunda Guerra Mundial e principalmente durante a Guerra Fria como estratégia na disputa geopolítica. Darnton (2017) inclusive localiza em documentos históricos o uso da desinformação no Império Bizantino (século VI). Assim sendo, é fundamental posicionar a desinformação como instrumento potencialmente consciente de distorção da realidade, existente antes mesmo das mais recentes tecnologias. Nesse sentido, Genesini (2018, p. 49) aponta que “o novo” são as plataformas e as tecnologias utilizadas para propagação massiva de desinformação, pois a “tentativa de falsificação política através da distorção de fatos e informações” é presente na história da humanidade.

Diversos autores (Castro & Ribeiro, 1997; Francisco, 2004; Wardle, 2016; Tandoc, Lim & Ling, 2017, apud Carvalho, 2019; Madrigal, 2017, apud Tsftati, Boomgaarden, Stromback, Viegenthart, Damstra & Lindgren, 2020; Benkler, Faris & Roberts, 2018; Carvalho & Mateus, 2018; Brisola & Romeiro, 2018; Alfonso, Galera & Calvo, 2019; Pinto & Zanetti, 2020), apontam para o crescimento do debate sobre a desinformação em diversas áreas e abordagens.

Em se tratando dos desafios tecnológicos ressaltados como instrumentos no debate sobre desinformação e notícias falsas, outra tecnologia, a chamada *blockchain*, pode se apresentar como uma aliada estratégica em diversas dimensões do Estado. A primeira prova de conceito desta tecnologia foi apresentada através do paper publicado de forma anônima a partir do pseudônimo Satoshi Nakamoto, em outubro de 2008, intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System”, onde Satoshi descreveu como as características centrais da rede, poderiam criar uma moeda capaz de ser transacionada dentro de uma rede de forma totalmente segura e descentralizada.

Portanto, o próprio sistema faz a gestão de transações sem a necessidade do estabelecimento de contratos e terceiros agentes intermediários como bancos e demais agentes financeiros.

Freitas e Vaz (2022) registram a existência e sistematizam diversas iniciativas de utilização de *blockchain* em diversos setores da administração pública, no Brasil e no mundo os mesmos autores apontam o potencial de criação de novas aplicações dessa tecnologia para outros problemas.

Nesse sentido, este trabalho se propõe a investigar uma nova possibilidade de aplicação, respondendo à pergunta: **como a tecnologia *blockchain* pode contribuir no combate às *fake news* e à desinformação?**, partindo da premissa de que este é um problema público no qual o Estado é um ator relevante. Para tal, realizou-se uma revisão de literatura para investigar caminhos já elaborados para uso da tecnologia, aproximando a discussão teórica do campo de políticas públicas e a discussão sobre *fake news* e desinformação.

2. Afinal, por que debater Desinformação e *Fake News* na Gestão Pública?

Em meio às disputas conceituais sobre desinformação e *fake news*, autores como Fallis (2015, apud Zattar, 2017) organizam quesitos para se classificar se algo seria uma desinformação, sendo estes: **1.)** Entender que a desinformação é uma informação; **2.)** Entender que esta informação é enganosa; e **3.)** Entender que esta informação enganosa tem como objetivo induzir ao erro - com dolo. Neste sentido, a “desinformação” não se trata de mera ausência da informação, mas de uma informação existente, enganosa e muitas vezes produzida com o objetivo induzir ao erro (Fallis, 2015; Zattar, 2017). Além disso, Wardle e Derakhshan (2017, p. 5) organizam a desinformação em três variações, sendo uma combinação de falsas e/ou potencialmente nocivas:

1.) “*Disinformation*”, na qual há o objetivo proposital em desinformar e prejudicar (informação falsa e nociva): Isto é, para muito além de um ‘tio do zap’ desavisado, existem “*Engenheiros do Caos*” (Da Empoli, 2019) que forjam padrões para simular inclusive a estética de memes bombásticos e artes supostamente amadoras, sem contar as *deep fakes*, com vídeos e áudios simulados; **2.) “*Misinformation*”**, na qual não há objetivo necessariamente de desinformar, mas ainda assim é um conteúdo enganoso (informação falsa e não necessariamente nociva): Neste caso um usuário desavisado pode cair no engano e replicar e/ou mesmo produzir uma informação enganosa sem necessariamente existir o dolo; **3.) “*Malinformation*”**, na qual há possível veracidade, porém há objetivo proposital em prejudicar com o vazamento ou com o discurso de ódio ou ataque (informação nociva e não necessariamente falsa): Quando um conteúdo verídico é retirado de contexto ou distorcido sem necessariamente demandar de edições, tal como um vídeo

real de bombardeios na Faixa de Gaza sendo veiculado como algo que ocorreu na Ucrânia¹ com o objetivo de disputar a opinião sobre o conflito com a Rússia.

Akers *et al.* (2018) apontam a carência de estudos voltados para identificar e sistematizar potenciais efeitos da desinformação, demonstrando-se mais recente a discussão sobre ‘desinformação e políticas públicas’ e ‘desinformação e administração pública’, tal como o papel do Estado. Entretanto, alguns autores alertam para os impactos negativos da desinformação sobre processos políticos, sobre a formação da opinião pública e sobre as políticas públicas. Tanto autores acadêmicos como atores relevantes no debate público caracterizam essa situação como a existência de um problema de interesse público, portanto passível de ação do Estado, sob a forma de políticas públicas e instrumentos legais de regulação.

3. Quais são os potenciais usos das tecnologias Blockchain na gestão pública?

Diversos estudos apontam para o uso das tecnologias *blockchain* como instrumentos para ação estatal e para a solução de problemas de natureza pública (Freitas & Vaz, 2022; Hang, 2016; Alketbi. et al, 2019; Olnes, 2017; Holbi et al, 2018; Janssens, 2019). Há experiências de uso na saúde para gestão de dados sobre tratamentos, em registros imobiliários para a garantia de dados imutáveis sobre propriedades imóveis, exemplos na utilização para prestação de contas, como o caso do anúncio do Termo de Cooperação entre TCU e BNDES para a construção da Rede Blockchain Brasil (RBB)². De modo geral, essas aplicações atendem a situações em que é necessário garantir a integridade, a imutabilidade e a rastreabilidade dos dados.

Para que a *blockchain* possa ser utilizada dessa maneira, é necessário que a rede tenha capacidade de processar uma grande quantidade de operações no menor tempo possível, com garantia de checagem e validação dos parâmetros definidos para essas transações. Essa garantia é produzida a partir de contratos inteligentes aprovados pelo protocolo de consenso da rede. Essa capacidade é determinada por um conjunto de características que permitem a construção de redes de dados imutáveis e altamente verificáveis (Freitas & Vaz, 2022):

a) Chaves de acesso público e privada: são o equivalente a autorizações necessárias para que a partir de encriptação e decriptação as informações sejam transportadas de maneira segura dentro da rede, possibilitando o processamento e validação desses dados pelos algoritmos sem que se tenha acesso ao conteúdo específico dessas informações (Hang, 2016). A chave privada é análoga a uma assinatura digital, que permite o acesso do usuário as suas informações, existindo apenas uma por

¹ Como exemplo, ver link: <https://www.aosfatos.org/noticias/video-misseis-faixa-de-gaza-ucrania/>

² Para mais informações, link do repositório oficial no GitHub da Rede Blockchain Brasil: <https://github.com/bndes/rbb>

usuário cadastrado na rede. A chave pública é utilizada pelos algoritmos da rede para ter acesso ao conteúdo e fazer a validação do conteúdo de determinada transação.

b) Blocos com criptografia hash encadeados: esta característica é a principal responsável por dar à rede *blockchain* as características ligadas a imutabilidade, pois a partir dela as informações na rede são armazenadas em uma sequência criptográfica onde o endereço do bloco anterior guarda estrita relação com o do bloco posterior e assim sucessivamente. Este processo é chamado de efeito cascata, uma vez que se tivermos uma cadeia de Blocos A, B e C, se alterarmos o conteúdo do primeiro bloco, ele altera o do segundo bloco, que altera o do terceiro bloco (Freitas & Vaz, 2022). O Hash, é um tipo de criptografia para representar um conjunto de dados, por uma numeração matematicamente constituída, o mais utilizado pelas redes *blockchain* ao redor do mundo é o SHA256, que resume a informação do bloco em um código de 64 caracteres, entre letras e números.

c) Contratos inteligentes e Protocolos de Consenso: podem ser explicados como as regras ou parâmetros em que os algoritmos validadores se baseiam para determinar a validade ou não das informações contidas em um determinado bloco. Os contratos inteligentes são essas listas de requisitos necessários em que o sistema vai se basear para legitimar uma informação e o protocolo de consenso consiste nos requisitos que os validadores devem atender para criar a sincronia algorítmica necessária para que uma informação seja aprovada como verdadeira na rede (Borges, et al, 2021). Alterações na rede só são permitidas a partir da aprovação de 50% + 1 dos membros validadores, o que pode ser centenas ou milhares de nós, ao depender do nível de descentralização da rede.

4. Metodologia

A partir da proposta de sistematização apresentada por Silva (2018), este trabalho adota uma revisão sistemática integrativa, que “*possibilita a síntese de vários estudos já publicados, permitindo a geração de novos conhecimentos, pautados nos resultados apresentados pelas pesquisas anteriores*” (Botelho, Cunha & Macedo, 2011; Silva, 2018). Deste modo, é possível explorar pontos em comum nos estudos acerca da *blockchain* e seus potenciais usos contra *fake news*. Em primeiro lugar, foi realizado um mapeamento geral da literatura através da seleção de palavras chaves relacionadas a avaliação em seis bancos de dados: Periódicos CAPES, Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), Proquest, Oasis Ibict, Scielo e Scielo Internacional. Em conjunto, elas abrangem tanto artigos de revistas acadêmicas quanto teses e dissertações não publicadas. A busca se limitou ao período de 2017 a 2022. O Quadro 1 a seguir mostra os primeiros achados da busca de acordo com cada termo e sua respectiva base de dados:

Quadro 1 – Resultados do Mapeamento Inicial

Palavras-chave	Per. Capes	BDTD	Proquest	Oasis Ibiect	SciELO
“Blockchain” + “Fake News”	346	2	291	5	0
“Blockchain” + “Desinformação”	9	0	4	0	0
“Blockchain” + “Disinformation”	144	0	109	0	0
“Combate” + “Fake News” + “Estado”	227	3	141	31	0
“Combate” + “Fake News” + “Políticas Públicas”	100	0	68	11	0

Fonte: Elaboração própria (2022)

O Quadro 2 resume os critérios para a seleção dos estudos neste mapeamento inicial:

Quadro 2 – Critério de Inclusão e Exclusão de Estudos

Critérios de Inclusão	Critérios de Exclusão
<ul style="list-style-type: none">- Documentos que apresentavam provas de conceitos de aplicação de blockchain para o combate às <i>Fake News</i>- Documentos que tiveram como foco de análise soluções implementadas na forma de redes e algoritmos- Documentos que discutiam o papel do blockchain como auxiliar do Estado no combate às <i>Fake News</i>	<ul style="list-style-type: none">- Documentos que apresentavam o uso de blockchain de forma geral e sem especificações técnicas de sua aplicação ao contexto- Duplicata, sob outro título, da mesma discussão;- Documento final inacessível.

Fonte: Elaboração própria (2022)

Os estudos identificados no mapeamento anterior foram submetidos a uma segunda triagem a partir da leitura de seus títulos e resumos.

5. Resultado da revisão sobre o uso de redes blockchain para combate às Fake News

Considerando o crescimento das discussões sobre *Fake News* a partir de 2017 e a ascendente mais recente sobre o uso de tecnologia *blockchain* em proximidade com a Gestão Pública, esta revisão sistemática selecionou um total de 13 artigos considerando os critérios descritos acima, e deles puderam-se extrair algumas semelhanças em suas teses, que foram agrupadas e tratadas, de modo a oferecer um entendimento do estado de arte sobre a utilização de sistemas *blockchain* para combate a *Fake News*. Neste mesmo sentido, buscou-se perceber as diferenças de posições dos autores em suas propostas de solução, considerando também o papel do Estado nessa função, que também foi levado em conta na criação das categorias nas quais se dividiram os textos analisados.

Procurou-se também ao longo do trabalho perceber o papel que os autores atribuem a própria tecnologia *blockchain*, no combate às *fake news*, uma vez que há aqueles que defendem que seu uso só pode ser eficaz nesse contexto se as suas características e protocolos forem alterados de acordo com as determinadas necessidades ou apenas com amparo de outras tecnologias como

algoritmos de Inteligência Artificial com parâmetros dinâmicos e Machine Learning para o devido processamento e validação das informações. Neste sentido, as principais características destas obras, bem como as suas classificações serão discutidas no Quadro 3 e parágrafos seguintes:

Quadro 3 – Características dos Estudos sobre Blockchain e Fake News

Autor, Ano	Objetivo	Principais resultados
Redes blockchain baseadas em validação organizada pela rede e parâmetros determinados por autoridades midiáticas		
Muhammad Saad, Ashar Ahmad e Aziz, Mohaisen, 2019	Este trabalho busca discutir os principais desafios para a utilização de tecnologias blockchain no combate a notícias falsas. Levando em consideração as necessidades de processamento para gerar escalabilidade nesta aplicação e propondo alterações no modelo tradicional da rede, para tornar possível esta solução	A ideia central é que um sistema blockchain tenha um design construído para comportar os principais stakeholders do processo de construção e disseminação de notícias que são as mídias tradicionais e as empresas gestoras das redes sociais. Portanto, constitui-se um sistema de validação das notícias, onde os algoritmos comparam o conteúdo compartilhado nas redes, ao conteúdo compartilhado pelos veículos tradicionais, gerando uma espécie de banco de dados de notícias verdadeiras. Essa verificação funciona como um selo de autenticidade, validado por diferentes contratos inteligentes gerados por autoridades midiáticas altamente rastreáveis.
Panayiotis Christodoulou, Klitos Christodoul, 2021	Propor uma prova de conceito de aplicação de blockchain onde a partir do registro das organizações de notícias na rede blockchain Ethereum, onde será possível que os próprios usuários façam as pesquisas e comparações das notícias publicadas, com os parâmetros das fake news, a partir das identificações ID das organizações	A proposição de um aplicativo descentralizado programado em solidity e hospedado na rede blockchain Ethereum para apoiar as autoridades públicas no combate às notícias falsas. De forma mais específica, é proposto um modelo de governança a partir da tecnologia blockchain e de seus contratos inteligentes para registro de notícias confiáveis.
Shovon Paul, Jubair Islam Joy, Shaila Sarker et al., 2019	Propor uma hipótese sobre utilização de tecnologias blockchain em redes sociais para aumentar a capacidade de detecção de notícias falsas e legitimação de notícias verdadeiras	Sistematização de uma proposta de utilização de tecnologia blockchain nos bancos de dados de publicações de redes sociais onde a validação é feita de forma anônima por jornalistas e organizações midiáticas. Também se propõe a utilização do algoritmo chamado de Breadth First Search (BFS), responsável por organizar as distintas avaliações em um sistema de pontos que define o potencial grau de falsidade ou veracidade de determinada notícia.
Adnan Qayyum, Muhammad Umar Janjua, Junaid Qadir, 2022	Apresentar de maneira geral, os principais desafios e potencialidades na criação de uma infraestrutura de rede baseada em blockchain para combater as Fake News, a partir de um protocolo de consenso e métodos de agrupamento semântico para categorização das informações de forma específicas	Este artigo apresenta um modelo de blockchain onde os validadores são jornalistas e agentes de notícias, e se utiliza um sistema de reputação para classificação de mensagens, que são classificadas em uma espécie de árvore de similaridade semânticas (merkle), para determinar o potencial de falsidade de uma notícia. O texto também apresenta, de maneira superficial, o uso de Inteligência Artificial, sobretudo de métodos de processamento de linguagem natural para definir a confiabilidade de notícias em uma base de dados. O processamento em escala dessas informações é o principal desafio.
Mohamed Torky, Emad Nabil e Wael Said, 2019	Este artigo busca apresentar um novo protocolo de consenso para uma rede blockchain com foco em combater notícias falsas chamado de Proof of Credibility (PoC). A prova de conceito deste protocolo, foi aplicada a base de dados do Twitter, coletando e classificando suas publicações e notícias a partir da tecnologia, e seus resultados são positivos no que diz respeito à identificação e interceptação de notícias falsas.	A prova de Credibilidade (PoC), é um protocolo de consenso que agrupa notícias de uma mesma fonte, ou de fontes cruzadas um grande número de vezes, e os classifica a partir do seu conteúdo como mais ou menos suscetível a ser Fake News. Esse agrupamento cria na rede, uma espécie de reputação para aquele grupo produtor de notícias, uma vez que cada registro definido como falso, é isolado das demais e utilizado como parâmetro, identificação de outras notícias falsas em potencial.
Paula Fraga-Lamas and Tiago M. Fernandez-Carriales, 2020	O texto introduz uma crítica à literatura que apresenta as características de rastreabilidade do blockchain como principais no combate a Fake News, e coloca considerações sobre caminhos importantes para aprimoramento da tecnologia para aplicação ao contexto.	Deve-se buscar o agrupamento de hashes de identificação, a partir de índices de similaridade de um conteúdo, para que esses grupos tenham facilidade de identificação pela rede, diminuindo o processamento. O nível de descentralização é moderado, e a validação fica a cargo das organizações que têm autoridade midiática. A rede em si não é capaz de identificar contextos, apenas de comparar conteúdos e a partir disso definir sua autenticidade, portanto, é necessário integrar essa ideia com sistemas de PLN e Machine Learning.
Ronaldo Borges do Val, Thamirys Dias Viana e Luis Borges Gouveia, 2021	Estudar e descrever as iniciativas de algoritmos de combate a notícias falsas que utilizam ou podem se beneficiar da tecnologia blockchain para suas bases de dados.	Há uma série de iniciativas para a construção de ferramentas de combate a Fake e News que utilizam ou poderiam utilizar blockchain, porém, como o perfil das organizações desenvolvedoras dessas ferramentas está ligado a grandes a corporações do mercado de tecnologia como instagram e facebook, o que por um lado assegura a credibilidade das informações geradas pelos seus algoritmos, mas por outro restringe o acesso a essas iniciativas.

Eishvak Sengupta, Renuka Nagpall, Deepti Mehrotra e Gautam Srivastava, 2021	Considerando o impacto que as notícias falsas tem atualmente, este estudo se preocupa em apresentar um modelo dinâmico com um protocolo de consenso e tomadas de decisões seguras e anonimizadas para que os revisores de notícias possam fornecer feedbacks sobre grupos de notícias e a partir de um modelo matemático probabilístico, possa se usar esses feedbacks para prever a potencial veracidade de notícias. O nome deste modelo de sistema proposto baseado em blockchain é ProBlock	O artigo fornece um modelo que busca ampliar a capacidade de reconhecimento de notícias falsas para arquivos de áudio, imagem e vídeo. A legitimidade das decisões é baseada no conhecimento especializado dos revisores de notícia que a partir de votações dinâmicas e com pesos diferenciados com base em sua credibilidade determina e classifica as informações como falsas ou genuínas, de forma simultânea, para que não se tenha problemas relacionados a escalabilidade no processo de validação das informações.
Redes blockchain baseadas em validação organizada pela rede e parâmetros determinados por algoritmos internos		
Zeinab Shahbazi, Yung-Cheol Byun, 2021	O objetivo deste artigo, consiste na apresentação de uma solução integrada que reúne características da tecnologia blockchain e de Inteligência Artificial com processamento de linguagem natural e Machine Learning, para facilitar a detecção de notícias falsas em redes sociais.	Apresenta-se uma estratégia de combate a <i>fake news</i> que emprega em uma mesma rede de identificação e processamento diferentes tecnologias, que são: blockchain, com seus contratos inteligentes e protocolos de consenso combinado com um sistema de decisão estruturado em algoritmos de machine learning, para se criar uma rede de confiabilidade capaz de validar as notícias e identificar <i>Fake News</i>
Yonggang Xiao , Yanbing Liu and Tun Li, 2020	Neste texto, os autores propõe uma estrutura de sistema em rede chamada Quick <i>Fake News</i> Detection (QcFND), construída a partir de tecnologias de rede por software (SND), computação de borda e blockchain, com o objetivo de validar as notícias disponibilizadas em aplicativos de trânsito, uma vez que informações falsas ou imprecisas veiculadas em redes de mapas de trânsito como o Easy ou maps, pode gerar ineficiências no tráfego e até mesmo acidentes.	Criação de um algoritmo para balanceamento da carga de tráfego interconectados. O resultado deste processamento, hospedado em um blockchain com protocolo de consenso baseado em autoridade (PoA), acoplado a um algoritmo de rede Bayesiana para calcular a probabilidade posterior de um evento de tráfego levando em consideração os acontecimentos anteriores e a duração desses eventos.
Redes blockchain baseadas em validação organizada pela rede e com foco em rastreabilidade		
Ashutosh Dhar Dwivedi, Rajani Singh, Sakshi Dhall, Gautam Srivastava and Saibal K. Pal, 2020.	Neste artigo, uma estrutura de mídia social baseada em blockchain e marca d'água ingênua é proposta para controlar a propagação de notícias falsas. Postulamos um novo modelo de blockchain para mitigar os desafios existentes neste campo. Além disso, a nova solução pode ajudar a reduzir a disseminação de notícias falsas, rastreando a raiz ou a origem das notícias falsas nas mídias sociais. Por meio de nossos resultados experimentais, mostramos que nossa solução baseada em blockchain é capaz de transmitir dados imediatamente por meio de um servidor blockXroute que pode propagar dados até 100 vezes mais rápido que as soluções conven	A principal contribuição deste texto ao debate sobre blockchain e <i>Fake News</i> é uma abordagem com foco em escalabilidade, se utilizando um algoritmo de difusão de informações na rede com potencial para aumentar a capacidade de transmissão de dezenas de vezes chamado blockchain Distributed Network (BDN). Esse alto grau de escalabilidade junto a um sistema de marcas d'água permite o rastreamento quase que instantâneo de focos propagadores de notícias falsas, uma vez que foi selecionado um algoritmo de criptografia e troca de informações leve e eficiente.
Imran Ush Shahid, Tanbir Anjum, Shafayet Hossain Miah, Rahanuma Tasnim, Al-Amin, 2021	Os autores se propõem a apresentar uma estratégia de eliminação de notícias falsas das mídias sociais, a partir da utilização de redes blockchain para desenvolver aplicações descentralizadas e bancos de dados imutáveis, capazes de classificar notícias de acordo com seus conteúdos e rastrear com facilidade os agentes produtores de notícias falsas.	Determinado autor emite uma informação a rede, essa informação é registrada com informações sobre a notícia e sobre o autor (nome do autor, endereço, e-mail, hora de publicação). Se ocorrer alguma situação indesejada, pode-se facilmente identificar e rastrear o autor da notícia A validação de todas as notícias acontecerá com na popularidade dos perfis, geradas a partir do histórico de avaliações de suas publicações anteriores
Akshada Babar, a Nalini Jagtap, Akshata Mithari, Aakash Shukla, Prachi Chaudhari, 2020	Propõe um modelo de utilização de tecnologia blockchain com foco na rastreabilidade das notícias falsas, com contratos inteligentes utilizando PoC, para agrupar os conteúdos e as fontes, permitindo uma rápida identificação de perfis que produção e compartilhamento massivo e profissionalizado de notícias falsas	Proposta de um sistema que pode ajudar as agências de notícias na propagação de artigos autênticos, uma vez que será identificada pela rede os compartilhamentos de notícias verdadeiras com conteúdos adulterados. Ainda neste sentido, esta proposta também contribuirá para que os stakeholders do processo compreendam as incidências de falsas notícias, para incorporarem em suas estratégias de comunicação e produção de artigos autênticos. Da mesma forma, a rastreabilidade pode contribuir para que as autoridades identifiquem focos produtores de conteúdos falsos.

Fonte: Elaboração própria (2022)

Foi identificado, na literatura analisada, um padrão de proposição de redes *blockchain*, que se baseia em duas necessidades distintas. A primeira necessidade é a de **validar, ou seja, analisar os grupos de informações**, para que a partir de seus resultados se possa constituir uma base de parâmetros a serem adotados para a validação dos próximos blocos de informações. Há dentro deste primeiro grupo de propostas duas visões, aquela que aposta em grupos de autoridades midiáticas para definição desses parâmetros e uma outra que aposta em algoritmos ligados à rede para fazer

essa identificação de forma automática. A segunda necessidade é a de **rastrear as notícias, possibilitando que sejam identificados focos de produção e propagação de Fake News**, possibilitando a identificação de organizações profissionais que investem massivamente nessas notícias falsas como modelo de negócio e também aqueles que se utilizam de notícias verdadeira, mas que alteram o contexto para seus determinados fins. Pensando nesta necessidade estabeleceu-se 3 grupos de categorias de redes *blockchain* para combate às *Fake News*, os dois primeiros ligados às necessidades de validação e atribuição de parâmetros e o segundo ligado a rastreabilidade, sendo:

a) Redes blockchain baseadas em validação organizada pela rede com parâmetros determinados por autoridades internas a rede: neste grupo, se concentra a maioria das propostas já em algum grau de funcionamento e também as provas de conceitos mais elaboradas. Consiste em se construir mecanismos de validação que considerem as opiniões emitidas, ou parâmetros, por autoridades internas à rede (agentes validadores) que representam segmentos oficiais de agentes de comunicação, como universidades, os grupos de jornais, revistas e televisão, e outros órgãos públicos e privados. Há neste grupo aqueles que, conforme destacado no primeiro grupo da tabela proposta acima, defendem a criação desta rede em cima de infraestruturas de *blockchain* já existentes com a da Ethereum, (Panayiotis Christodoulou, Klitos Christodoul, 2021) por ser uma rede que opera contratos inteligentes em grande escala, outros dependem da criação de infraestruturas para integrar sistemas *blockchain* a bases de dados das redes sociais, onde circulam de forma massiva as notícias falsas (Shovon Paul, Jubair Islam Joy, 2019). Alguns tipos de protocolo de consenso, com destaque ao chamado *proof of credibility* (PoC), onde se estabelece análises comparativas entre o conteúdo dos feedbacks dos validadores com o agrupamento por similaridade semântica, para classificação, para que então se determine níveis de popularidade entre os validadores e agentes emissores, e esse níveis vão se tornando parâmetros para agrupamento e identificação de redes de notícias com potencial verdadeiro ou falso (Mohamed Torky, Emad Nabil e Wael Said, 2019).

b) Redes blockchain baseadas em validação organizada pela rede com parâmetros determinados por algoritmos internos: este se caracteriza pelo grupo com menor índice de produções, uma vez que as suas propostas exigem um novo nível de apropriação desta tecnologia, sobretudo no que diz respeito a criação de capacidades para processamento, uma vez que a estruturação das decisões necessárias para se definir os parâmetros são mais complexas. Também pode-se atribuir o baixo nível de produção pelo fato que em muitas vezes será necessário o emprego de outras tecnologias, sobretudo as ligadas à inteligência artificial, mais especificamente o Machine Learning e o Deep Learning, que agregam um nível a mais ao desafio técnico de se debater a viabilidade deste arranjo para identificação e combate às *fake news* (Zeinab Shahbazi, Yung-Cheol

Byun, 2021). A idéia de atribuir ao sistema a autoridade necessária para decidir de forma autônoma sobre estas classificações, está relacionada diretamente com: I) O nível de estruturação desta base de dados de notícias falsas e sua categorização; II) O nível de governança sobre a transparência dos algoritmos das IA's.

c) Redes blockchain baseadas em validação organizada pela rede e com foco em rastreabilidade: este grupo de propostas está ligado às funções rastreadoras da rede *blockchain*, onde o foco não é a identificação semântica, mas sim a identificação de padrões de disseminação para que se encontre redes e agentes propagadores de *Fake News* (Akshada Babar, a Nalini Jagtap, Akshata Mithari, et al, 2020). Aqui, também se busca identificar as notícias que são verdadeiras, porém tiveram o seu contexto alterado no sentido de produzir desinformação. Neste grupo, as informações objetivas da publicação como nome do autor, endereço *web* e hora de publicação são registrados junto ao bloco. Cada vez que essas informações são compartilhadas, são registrados automaticamente os dados de quem as compartilhou, o que permite identificar padrões de compartilhamento por usuários e também as redes de impulsionamento de notícias falsas.

6. O uso da Blockchain pelo Estado como ator no combate à Desinformação

Pode-se considerar o Estado não apenas como agente organizador de políticas de combate às notícias falsas, mas também como representante dos interesses da população na fiscalização dos caminhos adotados por organizações e por sistemas feitos por essas, para a execução de protocolos diversos. Em outras palavras, pode-se dizer que o Estado não deve apenas coordenar as estratégias de combate às *fake news*, mas fiscalizar a execução de forma a garantir os direitos e interesses da população em todo o processo. Para tanto, é necessário que se tenha uma percepção estratégica sobre onde o Estado pode atuar na formulação, implantação e fiscalização dos processos de validação e estabelecimento de requisitos a serem empregados em redes *blockchain* para identificar ações de desinformação e disseminação de notícias falsas.

O estabelecimento de requisitos pode ocorrer em duas camadas tecnológicas para o uso da blockchain, neste caso específico: Camada de Parâmetros Externos (CPE); Camada de Parâmetros Internos (CPI).

- a) **Camada de Parâmetros Externos (CPE):** As propostas de redes *blockchain* com os parâmetros definidos a partir da incidência dos *feedbacks* de autoridades internas à rede (agentes validadores) sobre determinada matéria e aquelas com foco em detecção de padrões de disseminação são perfeitamente comportadas por esta primeira camada de propostas de utilização das tecnologias *blockchain*. Isto ocorre

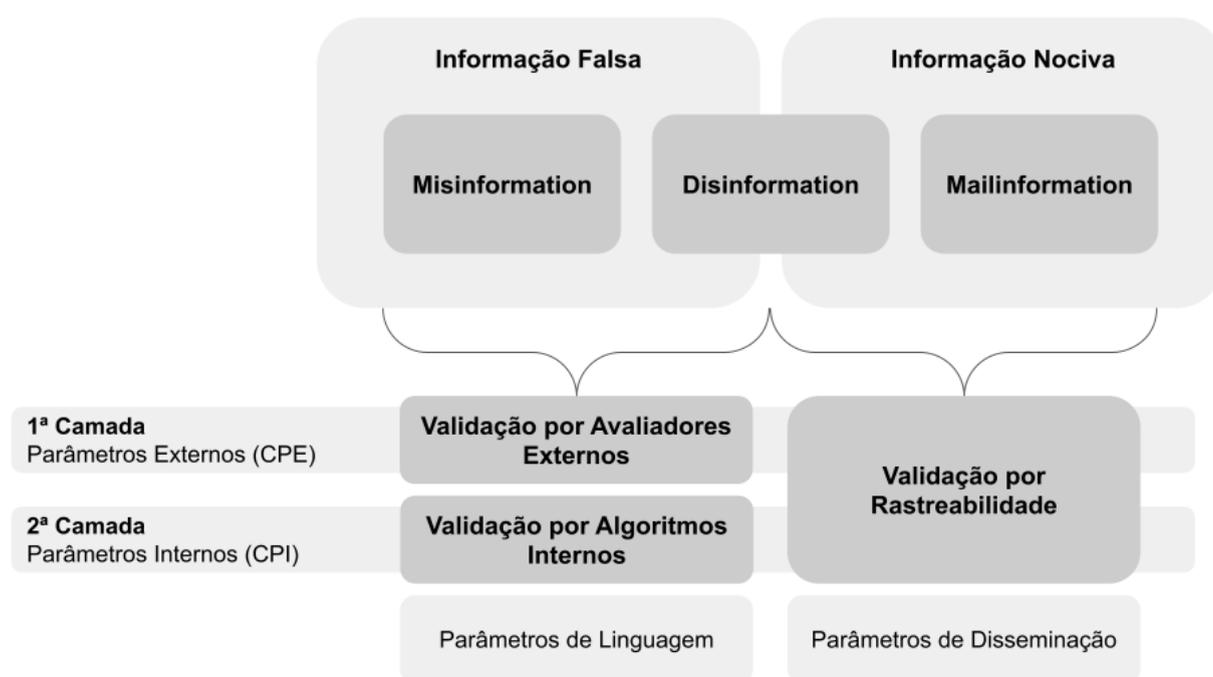
porque a interpretação dos dados é feita não pelo sistema em si, mas corresponde ao resultado de uma opinião emitida e registrada na rede por uma autoridade da área correlata, devidamente registrada na rede. Nesse caso, a maior preocupação está na devida qualificação e acompanhamento dos *feedbacks* emitidos pelas autoridades internas à rede (agentes validadores). O sistema de protocolo de credibilidade é um bom aliado para isso, uma vez que atribui credibilidade também aos avaliadores, por meio de um mecanismo de estabelecimento de reputação que estabelece o peso da avaliação de um dado agente para uma matéria conforme seu grau de concordância com a maioria dos demais avaliadores. A ação do Estado pode se dar na regulamentação, organização e fiscalização do processo de mobilização de atores sociais para ingressarem na rede como autoridades participantes do processo de criação de parâmetros validadores. Isto pode ocorrer com graus diferentes de profundidade da intervenção estatal, adotando-se tanto modelos de intervenção leve, basicamente regulatória, como a regulação de iniciativas de consórcios e redes da sociedade civil ou propostas de autorregulação, até iniciativas de maior presença estatal, como redes de colaboração público-privado de avaliação.

- b) **Camada de Parâmetros Internos (CPI):** Esta camada demanda uma expansão dos recursos tecnológicos em relação ao seu nível atual, em que pese algumas iniciativas já estejam em desenvolvimento nesse sentido. Para se criar sistemas para definição de parâmetros totalmente automatizados, devem ser mobilizadas outras tecnologias com recursos voltados para o tipo de análise necessária, incorporando seus recursos aos sistemas baseados em *blockchain*. As principais possibilidades que podem preencher essa segunda camada são aquelas que se utilizam de tecnologias de inteligência artificial, especialmente aprendizado de máquina (*Machine Learning*) e redes neurais profundas (*Deep Learning*). Podem ser aplicadas ao processamento de linguagem natural, para, a partir da própria construção semântica, comparada em um histórico de análises, definir e classificar o grau de probabilidade de informações não serem verdadeiras ou terem sido colocadas fora de contexto. As principais limitações desta camada estão ligadas ao alto nível de processamento necessário para manter essas cadeias de algoritmos validadores de informação em circulação para validação de toda a rede, considerados aspectos como capacidade computacional e tempo de processamento, que pode variar de acordo com o número de parâmetros a serem validados e de informações alocadas na rede em um determinado intervalo de

tempo. A intervenção estatal neste contexto, deve seguir no sentido de criar mecanismos de transparência algorítmica, para que se fiscalize a execução de protocolos e a definição de parâmetros feitos pelos sistemas de compreensão mais avançados. Da mesma forma que no caso anterior, esta intervenção estatal pode ter diferentes graus de profundidade.

Ao associar os achados da revisão de literatura sobre práticas de enfrentamento à desinformação por meio da tecnologia *blockchain* de acordo com as categorias teóricas da desinformação e com as camadas de uso da tecnologia apontadas acima, é possível construir um *framework* para organizar as abordagens no enfrentamento da desinformação, como apresentado na Figura 1 e descrito a seguir:

Figura 1 - FrameWork de Possibilidades de uso da Blockchain no Combate à Desinformação



Fonte: Elaboração própria (2022)

Como observado na Figura 1, as chamadas *Disinformation*, *Misinformation* e *Malinformation* podem ser organizadas em informações falsas e/ou nocivas. Uma informação falsa pode ser validada por parâmetros de linguagem ao ter seu conteúdo comparado com a base de dados referencial. Por outro lado, uma informação nociva e não necessariamente falsa demanda uma análise de elementos, tal como o seu contexto, exigindo uma validação por parâmetros de disseminação, isto é, uma informação massivamente circulada na rede pode alertar para a possibilidade de ser algo nocivo.

Neste contexto, as duas camadas (CPE e CPI) são relevantes, pois no caso do parâmetro de linguagem, até que a rede contenha referenciais suficientes para utilizar os próprios parâmetros internos em uma validação por algoritmos internos, serão necessários avaliadores externos para observar tais informações com base nestes parâmetros externos, isto é, uma rede de checagem das informações em circulação. No caso da informação nociva que demande parâmetros de disseminação, uma validação por rastreabilidade conta com as duas camadas, uma vez que parâmetros internos podem apontar para padrões anormais de disseminação, mas ainda parâmetros externos podem ser utilizados para complementar tal análise. Isto é, na fronteira tecnológica, o desafio está em estabelecer tais parâmetros internos, avançando em uma validação por algoritmos internos tanto por padrões de linguagem, mas pela otimização da validação de rastreabilidade dos parâmetros de disseminação.

Tais usos da tecnologia são tecnicamente adequados às suas características mais estabelecidas e consolidadas, baseadas em parâmetros externos registrados nas redes, o que corresponde à Primeira Camada. Novos desenvolvimentos, com a integração de recursos de Inteligência Artificial ao processamento interno das redes *blockchain* podem ampliar seu potencial de uso para o combate à desinformação para a segunda camada.

7. Considerações Finais

Este Trabalho se propôs a responder a seguinte questão: **como a tecnologia blockchain pode contribuir no combate às *fake news* e à desinformação?**. Para tal, realizou-se uma revisão de literatura para investigar caminhos já elaborados para uso da tecnologia, aproximando a discussão teórica do campo de políticas públicas e a discussão sobre *fake news* e desinformação. Além de posicionar a tecnologia *blockchain* como potencial instrumento no cotidiano da Gestão Pública, este trabalho também aponta para a necessidade de que a desinformação seja observada enquanto agenda de pesquisa e posicionada como problema em políticas públicas.

Percebeu-se que há uma correlação entre capacidade de validação e legitimidade do processo de estabelecimento de parâmetros. Quando a rede tem capacidade total de compreender os dados fornecidos e validá-los de acordo com o parâmetro determinado, há a necessidade de legitimação do caminho empregado para se formar tal juízo, em outras palavras, transparência algorítmica para se entender como se chegou em tal definição. Quando a rede não é capaz de definir de maneira autônoma os parâmetros necessários, e portanto se mobiliza agentes externos para produzir tais parâmetros, a necessidade central consiste na produção de protocolos transparentes e adequados para habilitação dos agentes para serem nós validadores da rede. O Estado, quer do ponto de vista do estabelecimento de regulações, quer do ponto de vista da sua implementação e

fiscalização, pode assumir funções importantes nas duas camadas de uso da tecnologia blockchain para combate às *Fake News*.

A partir dos resultados do presente estudo é possível antever alguns caminhos para uma agenda de pesquisa na temática:

Do ponto de vista institucional, há necessidade de estudos futuros sobre os processos políticos e sociais para a implantação de soluções como as exploradas neste artigo. Instrumentos de políticas públicas e instâncias de governança voltadas ao combate à desinformação podem ter sua implantação ou as dificuldades para sua materialização tomadas como objeto de estudo. A utilização de recursos de *blockchain* no combate à desinformação demanda a construção de soluções institucionais das quais o Estado não pode estar apartado. Quanto mais responsabilidades as organizações estatais assumirem nesse campo, maior será a demanda pelo domínio das tecnologias requeridas. A aplicação da *blockchain* demanda, portanto, a mobilização de novas capacidades tecnológicas no âmbito estatal. Compreender os processos em que tal tecnologia é adotada, mesmo que para outros fins, por agentes estatais, pode auxiliar no desenvolvimento de iniciativas de mobilização dessas capacidades.

Do ponto de vista tecnológico, a adoção de aplicações que integrem recursos de Inteligência Artificial a redes *blockchain* para a validação de informações e rastreamento de emissores também requer estudos para seu uso em larga escala. Por fim, sugere-se que próximos estudos possam observar em perspectiva comparada e até mesmo em meta-análise a implementação de outras tecnologias complementares ou não à *blockchain*, ampliando a compreensão acerca dos possíveis métodos e práticas no enfrentamento à desinformação.

8. Referências Bibliográficas

ABAD, Ana Carolina Ciattei. **Uma revisão de literatura sobre desinformação**. Monografia de Conclusão de Curso, Faculdade de Administração e Ciências Contábeis, Universidade Federal do Rio de Janeiro. Rio de Janeiro, Rio de Janeiro, Brasil. 2018. Disponível em: <https://pantheon.ufrj.br/handle/11422/11856>. Acesso em: 25 jun. 2022.

AKERS, John; BANSAL, Gagan; CADAMURO, Gabriel; CHEN, Christine; CHEN, Quanze; LIN, Lucy; MULCAIRE, Phoebe; NANDAKUMAR, Rajalakshmi; ROCKETT, Matthew; SIMKO, Lucy; TOMAN, John; WU, Tongshuang; ZENG, Eric; ZORN, Bill; ROESNER, Franziska. **Technology-Enabled Disinformation: Summary, Lessons, and Recommendations**. Cornell University: Computer and Society, arXiv:1812.09383. Ithaca, Nova York, United States of America. 2019. Disponível em: <https://arxiv.org/abs/1812.09383>. Acesso em: 25 jun. 2022.

ALFONSO, Ignacio Blanco Alfonso; GALERA, Carmen García; CALVO, Santiago Tejedor. **El impacto de las fake news en la investigación en Ciencias Sociales**. Revisión bibliográfica sistematizada. Periodico Historia y comunicación social 24 (2), 449-469.. España. 2019. Disponível em: https://www.researchgate.net/profile/Ignacio_Blanco_Alfonso/publication/339292278_El_impacto_de_las_fake_news_en_la_investigacion_en_Ciencias_Sociales_Revison_bibliografica_sistemat/links/5e484c2792851c7f7f3ddb32/El-impacto-de-las-fake-news-en-la-investigacion-en-Ciencias-Sociales-Revison-bibliografica-sistemat.pdf. Acesso em: 25 jun. 2022.

- ALKETBI, a. NASIR; et al, "**Blockchain for government services — Use cases, security benefits and challenges,**" 2018 15th Learning and Technology Conference (L&T), 2018, pp. 112-119. Disponível em: <https://doi.org/10.1109/LT.2018.8368494>. Acesso em: 25 jun. 2022.
- BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.** Oxford University Press. Oxford, England, United Kingdom. 2018.
- BORGES, Ronaldo. DIAS, Thamirys. BORGES, Luis. O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação. Brazilian Journals of Business. 2021. Acesso em: 25 jun. 2022. Disponível em: https://www.researchgate.net/publication/354367207_O_uso_de_Blockchain_na_identificacao_de_Fake_News_ferramentas_de_apoio_tecnologico_para_o_combate_a_desinformacao_The_use_of_Blockchain_in_the_identification_of_Fake_News_technological_support_tools_t. Acesso em: 25 jun. 2022.
- BOTELHO, Louise Lira Roedel; CUNHA, Cristiano Castro de Almeida; MACEDO, Marcelo. **O método da revisão sistemática integrativa nos estudos organizacionais.** Revista Gestão & Sociedade, v. 5, n. 11, p. 121-136. Belo Horizonte, Minas Gerais, Brasil. 2011. Disponível em: <https://www.gestaosociedade.org/gestaosociedade/article/view/1220>. Acesso em: 25 jun. 2022.
- BRISOLA, Anna Cristina; ROMEIRO, Nathália Lima. **A competência crítica em informação como resistência: uma análise sobre o uso da informação na atualidade.** Revista Brasileira de Biblioteconomia e Documentação, São Paulo, Online First, 20 p.. São Paulo, São Paulo, Brasil. 2018. Disponível em: <https://rbbd.febab.org.br/rbbd/article/view/1054>. Acesso em: 25 jun. 2022.
- CARVALHO, Rafiza Luziani Varão R.. **Notícias falsas ou propaganda?: Uma análise do estado da arte do conceito fake news.** Revista de Epistemologias da Comunicação, Questão Transversais. ISSN 2313-6372. v. 7, n. 13. Brasil. 2019. Disponível em: <http://www.revistas.unisinos.br/index.php/questoes/article/view/19177>. Acesso em: 25 jun. 2022.
- CARVALHO, Mariana Freitas Caniello de; MATEUS, Cristielle Andrade. **FAKE NEWS E DESINFORMAÇÃO NO MEIO DIGITAL: análise da produção científica sobre o tema na área de Ciência da Informação.** in: V Encontro Regional dos Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação das Regiões Sudeste, Centro-Oeste e Sul. Belo Horizonte, Minas Gerais, Brasil. 2018. Disponível em: <https://periodicos.ufmg.br/index.php/moci/article/view/16901>. Acesso em: 25 jun. 2022.
- CASTRO, César Augusto; RIBEIRO, Maria Solange Pereira. **Sociedade da informação: dilema para o Bibliotecário.** Transinformação, v. 9, n.1. Campinas, São Paulo, Brasil. 1997. Disponível em: <http://periodicos.puc-campinas.edu.br/seer/index.php/transinfo/article/view/1589>. Acesso em: 25 jun. 2022.
- CHRISTODOULOU, Panayiotis et al. **Developing more Reliable News Sources by utilizing the Blockchain technology to combat Fake News,**" 2020 Second International Conference on Blockchain Computing and Applications (BCCA), 2020, pp. 135-139. Disponível em: <https://doi.org/10.1109/BCCA50787.2020.9274460>. Acesso em: 25 jun. 2022.
- DA EMPOLI, Giuliano. **Os Engenheiros do Caos.** Vestígio; 1ª edição. Italia. 2019. Disponível em: Vestígio; 1ª edição.
- DARNTON, Robert. **A verdadeira história das notícias falsas: séculos antes das redes sociais, os boatos e as mentiras alimentavam pasquins e gazetas na Europa.** El País Brasil, [S.l.]. Brasil. 2017. Disponível em: https://brasil.elpais.com/brasil/2017/04/28/cultura/1493389536_863123.html. Acesso em: 25 jun. 2022.
- DWIVEDI, Ashutosh. et al, "**Tracing the Source of Fake News using a Scalable Blockchain Distributed Network,**" 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2020, pp. 38-43. Disponível em: <https://doi.org/10.1109/MASS50613.2020.00015>. Acesso em: 25 jun. 2022
- FALLIS, Don. **What Is Disinformation?.** Johns Hopkins University Press. Volume 63, Number 3, Winter 2015. pp. 401-426. 10.1353/lib.2015.0014. Baltimore, Maryland, United States of America. 2015. Disponível em: <https://muse.jhu.edu/article/579342>. Acesso em: 25 jun. 2022.
- FRACISCO, Severino. **Sociedade da desinformação.** Artigo publicado no Observatório da Sociedade da Informação, de responsabilidade do Setor de Comunicação e Informação da UNESCO no Brasil. Brasília, Distrito Federal, Brasil. 2004. Disponível em: <http://unesdoc.unesco.org/images/0015/001540/154058por.pdf>. Acesso em: 25 jun. 2022.
- FRAGA-LAMAS, Paula. et al. "**Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,**" in IT Professional, vol. 22, no. 2, pp. 53-59, 1 March-April 2020. Disponível em: <https://doi.org/10.1109/MITP.2020.2977589>. Acesso em: 25 jun. 2022.
- FREITAS, Anderson Ribeiro de, VAZ, José Carlos. **Potenciais aplicações e benefícios na utilização de sistemas blockchain para a gestão pública.** Boletim de Políticas Públicas/OIPP, n.20, março/2022. Disponível em: <https://sites.usp.br/boletimoipp/marco-de-2022/>. Acesso em: 25 jun. 2022.
- GENESINI, Silvio. **A pós-verdade é uma notícia falsa.** Revista USP. N 116 (2018): Dossiê Pós-Verdade e Jornalismo. São Paulo, São Paulo, Brasil. 2018. Disponível em: <https://www.revistas.usp.br/revusp/article/view/146577>. Acesso em: 25 jun. 2022.

- HOLBI, M. et al. **A systematic Review of the use of blockchain in Healthcare.** Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor 2018. Disponível em: https://www.researchgate.net/publication/328208535_A_Systematic_Review_of_the_Use_of_Blockchain_in_Healthcare#:~:text=The%20findings%20indicate%20that%20blockchain,of%20frameworks%2C%20architectures%20or%20models. Acesso em: 25 jun. 2022.
- MADRIGAL, Alexis C.. **What Facebook Did to American Democracy.** The Atlantic. 2017. Disponível em: <http://www.cs.yale.edu/homes/jf/MadrigalFeb2018-2.pdf>. Acesso em: 25 jun. 2022.
- OLNES, S. et al. **Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.** ScienceDirect. 2017. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X17303155>. Acesso em: 25 jun. 2022.
- PAULI, J. I. JOY, S. Sarker, A. -. A. -. H. Shakib, S. Ahmed and A. K. Das, **"Fake News Detection in Social Media using Blockchain,"** 2019 7th International Conference on Smart Computing & Communications (ICSCC), 2019, pp. 1-5. Disponível em: <https://doi.org/10.1109/ICSCC.2019.8843597>. Acesso em: 25 jun. 2022.
- PINTO, Thamara Machado; ZANETTI, Daniela. **DESINFORMAÇÃO E FAKE NEWS: UMA REVISÃO DE LITERATURA.** in: 6º Seminário Comunicação e Territorialidades: Caminhos da comunicação no mundo em crise. v. 1 n. 6 (2020). Espírito Santo, Brasil. 2020. Disponível em: <https://periodicos.ufes.br/poscom/article/view/32568>. Acesso em: 25 jun. 2022.
- QAYYUM Adnan, et al. **"Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News,"** in IT Professional, vol. 21, no. 4, pp. 16-24, 1 July-Aug. 2019. Disponível em: <https://doi.org/10.1109/MITP.2019.2910503>. Acesso em: 25 jun. 2022.
- RECUERO, Raquel da Cunha. **Disputas discursivas, legitimação e desinformação: o caso Veja x Bolsonaro nas eleições brasileiras de 2018.** Revista Comunicação, Mídia e Consumo. v. 16, n. 47. Brasil. 2019. Disponível em: <http://revistacmc.espm.br/index.php/revistacmc/article/view/2013>. Acesso em: 25 jun. 2022.
- SAAD, Muhammed et al. **"Fighting Fake News Propagation with Blockchains,"** 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1-4. Disponível em: <https://doi.org/10.1109/CNS.2019.8802670>. Acesso em: 25 jun. 2022.
- SENGRUPTA, e, NAGPAL, R., MEKHORTA, D. et al. **ProBlock: a novel approach for fake news detection.** Cluster Comput 24, 3779–3795 (2021). Disponível em: <https://doi.org/10.1007/s10586-021-03361-w>. Acesso em: 25 jun. 2022.
- SHAHID, ush et al. **Authentic Facts: A Blockchain Based Solution for Reducing Fake News in Social Media.** In 2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021). Association for Computing Machinery, New York, NY, USA, 121–127. Disponível em: <https://doi.org/10.1145/3510487.3510505>. Acesso em: 25 jun. 2022.
- TANDOC JR., Edson C.; LIM, Zheng Wei; LING, Richard. **Defining “Fake News: A typology of scholarly definitions.** Digital Journalism. vol. 6, 2018 - Issue 2: Trust, Credibility, Fake News. International. 2017. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/21670811.2017.1360143>. Acesso em: 25 jun. 2022.
- TORKY, Mohamed; NABIL, Emad; SAID, Wael. **Proof of credibility: A blockchain approach for detecting and blocking fake news in social networks.** International Journal of Advanced Computer Science and Applications, v. 10, n. 12, 2019. Disponível em: https://www.researchgate.net/profile/Mohamed-Torky-6/publication/338282589_Proof_of_Credibility_A_Blockchain_Approach_for_Detecting_and_Blocking_Fake_News_in_Social_Networks/links/5e0bd974a6fdcc28374d33de/Proof-of-Credibility-A-Blockchain-Approach-for-Detecting-and-Blocking-Fake-News-in-Social-Networks.pdf. Acesso em: 25 jun. 2022.
- VOLKOFF, Vladimir. **Pequena história da desinformação: do cavalo de Tróia à internet.** Editorial Notícias. Coleção: Média sociedade, 10. ISBN: 972-46-1155-8.. Lisboa, Portugal. 2004. Disponível em: Ed. Vila do Príncipe.
- XIAO, et al. **Edge Computing and Blockchain for Quick Fake News Detection in IoV.** Sensors 2020, 20, 4360. Disponível em: <https://doi.org/10.3390/s20164360>. Acesso em: 25 jun. 2022.
- WARDLE, Claire. **6 types of misinformation circulated this election season.** Columbia Journalism Review. New York, New York, United States of America. 2016. Disponível em: https://www.cjr.org/tow_center/6_types_election_fake_news.php. Acesso em: 25 jun. 2022.
- ZATTAR, Marianna. **Competência em informação e desinformação: critérios de avaliação do conteúdo das fontes de informação.** Liinc em Revista, Rio de Janeiro, v.13, n.2, p. 285-293. Rio de Janeiro, Rio de Janeiro, Brasil. 2017. Disponível em: <http://revista.ibict.br/liinc/article/view/4075>. Acesso em: 25 jun. 2022.
- ZEINAB, Shahbazi et al. **Fake Media Detection Based on Natural Language Processing and Blockchain Approaches,** in IEEE Access, vol. 9, pp. 128442-128453, 2021. Disponível em: <https://doi.org/10.1109/ACCESS.2021.3112607>. Acesso em: 25 jun. 2022.