UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

ARTHUR NOGUEIRA GONÇALVES

Marca d'água em notícias online para prevenir *fake news*

Rio de Janeiro
2020

ARTHUR NOGUEIRA GONÇALVES

Marca d'água em notícias online para prevenir *fake news*

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Profa. Dra. Jonice de Oliveira Sampaio
Co-orientador: Prof. Dr. Cláudio Micelli de Farias

Rio de Janeiro
2020

Gonçalves, Arthur Nogueira
G635m Marca d'água em notícias online para prevenir fake news / Arthur Nogueira Gonçalves. - Rio de Janeiro, 2020.
91 f.

Orientadora: Jonice Oliveira Sampaio.
Coorientador: Claudio Micelli de Farias.

Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Instituto de Computação, Bacharel em Ciência da Computação, 2020.

1. Fake news. 2. Blockchain. I. Sampaio, Jonice Oliveira, (orient.). II. Farias, Claudio Micelli, (coorient.). III. Título.

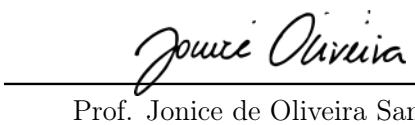
ARTHUR NOGUEIRA GONÇALVES

Marca d'água em notícias online para prevenir *fake news*

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 08 de março de 2022

BANCA EXAMINADORA:



Prof. Jonice de Oliveira Sampaio
D.Sc. (IC/UFRJ) - Orientadora

Participação por vídeo conferência

Prof. Claudio Miceli de Farias
D.Sc. (NCE/UFRJ) - Orientador

Participação por vídeo conferência

Prof. Valeria Menezes Bastos
D.Sc. (IC/UFRJ)

Participação por vídeo conferência

Prof. Jivago Medeiros Ribeiro
Msc. (IC/UFMT)

Gostaria de dedicar esse trabalho primeiramente a Deus, que sem ele nada disso seria possível, também aos meus pais que foram ao longo do curso e do desenvolvimento desse trabalho meus maiores apoiadores, dois anjos simples e humildes que me ensinaram tudo o que sou hoje. Gostaria também de dedicar essa jornada a minha irmã que durante toda a faculdade me impulsionou a atingir sonhos e objetivos maiores. Além do meu amigo Matheus Villaça no qual em uma carona para o estágio pensamos na ideia desse projeto. E por último gostaria de dedicar esse trabalho a minha família e amigos dentre eles destaco o Bel, o SIGA UFRJ, o LCI, o GRIS e meus demais amigos do Rio de Janeiro e da minha amada Carmo do Cajuru que me acompanharam e torceram por mim ao longo de todos esses anos.

AGRADECIMENTOS

Gostaria de agradecer a UFRJ (Universidade Federal do Rio de Janeiro) pela infraestrutra e oportunidade para desenvolver esse trabalho. E também aos professores Doutor Cláudio Micelli de Farias e Doutora Jonice Oliveira de Sampaio.

"There has been more new error propagated by the press in the last ten years than in an hundred years before 1798"

John Adams

RESUMO

O problema das *fake news* tem tido bastante foco da sociedade nos últimos anos. Depois das eleições americanas de 2016 no qual o presidente foi eleito com forte influência de notícias falsas propagada nas redes sociais, tratar esse problema ganhou caráter de destaque no debate público. Muitas abordagens tem sido sugeridas e uma delas que tem se demonstrado promissora é o uso de *Blockchain*, que é uma tecnologia de base de dados distribuída a prova de violação e resistente a mudanças. Até 2014 o uso de *Blockchain* era visto apenas para criptomoedas, desde então outros usos tem se demonstrado interessantes. Nesse trabalho será estudado a viabilidade dessa abordagem nas páginas Brasileiras e também quais metadados precisariam estar presentes para queum sistema se utilize dos dados salvos na *Blockchain*.

Palavras-chave: *fake news*; *blockchain*.

ABSTRACT

The problem of fake news has been the focus of society in recent years. After the 2016 US elections in which the president was elected with a strong influence of fake news propagated on social networks, dealing with this problem will gain prominence in the public debate. Many suggested solutions and one of them that has been promising is the use of Blockchain, which is a tamper-proof and change-resistant distributed database technology. Until 2014 the use of Blockchain was seen only for cryptocurrencies, since then other uses have been studied. This Conclusion Paper will study the feasibility of this approach in Brazilian pages and also which metadata would need to be present for a system to use data saved in the Blockchain.

Keywords: fake news; blockchain.

LISTA DE ILUSTRAÇÕES

LISTA DE CÓDIGOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
EUA	Estados Unidos da América
HTML5	Hypertext Markup Language version 5
IA	Inteligência Artificial
UFPB	Universidade Federal da Paraíba
WEB	Rede mundial de computadores
JSON	JavaScript Object Notation - Notação de Objetos JavaScript
UUIDv4	Universally Unique Identifier version 4 - Identificador Único Universal versão 4
SHA512	Secure Hash Algorithm 512 - Algoritimo de Hash Segura 512bits

SUMÁRIO

1 INTRODUÇÃO

Nos dias de hoje a população passa uma boa parte do dia em frente a internet, onde consome os mais diversos tipos de conteúdos. Esses podem se apresentar de diversas formas, sejam eles como imagens, vídeos, textos ou outras formas que em sua essência são uma mistura dessas mídias básicas.

O contato com essa diversidade de mídias eletrônicas trouxe um enorme avanço na forma como as pessoas se comunicam, onde mensageiros instantâneos, redes sociais, sites de vídeos e notícias trazem uma infinidade de conteúdo para seus usários. O porém é que com esse maior alcance das grandes massas partidos políticos, empresas e organizações tem se utilizado dessa nova fonte para espalhar conteúdos que são de origem duvidosas ou claramente falsas, as chamadas *fake news*.

Cada vez mais o público em geral tem sido expostos ao termo *fake news*. Segundo Junior, Lim e Ling (2018) que fizeram um levantamento entre os anos de 2003 e 2017 na literatura tiveram várias definições do que se trata essa expressão e segundo os mesmos suas definições podem ser divididas em seis diferentes grupos do que é uma *fake news*. Para esse trabalho o termo será utilizado para se referir à notícias fabricadas sejam em forma de texto ou mídia que buscam criar o sentimento de legitimidade do leitor, sem deixar claro que o conteúdo apresentado não apresenta cunho verídico.

De acordo com Allcott e Gentzkow (2017) nas eleições norte americanas de 2016 somente no *Facebook* 115 *fake news* pró-Donnald Trump (candidato vencedor) foram compartilhadas 30 milhões de vezes e 41 pró-Hilary Clinton (candidata derrotada) foram compartilhadas 7,6 milhões de vezes. Com esses números pode-se inferir a influência que esse tipo de conteúdo gerou na eleição da mais longeva democracia do mundo.

No Brasil Silva (2017) indica que dos 78% dos brasileiros que usam as redes sociais para se informar, pelo menos 42% deles admitem já ter compartilhado notícias falsas e segundo a mesma apenas 39% desses usuários que tem o hábito de checar a fonte da informação. Com o apresentado pode-se desprender o potencial de pessoas que nos dias de hoje espalham em seus meios sociais notícias sem cunho verídico, sejam elas intencionalmente ou não.

Ao pensar no quão latente é o problema de compartilhamento de *fake news*, tem-se a sensação de que é um fenômeno recente e causado pelas redes sociais, o que é um grande equívoco. O presidente norte americano John Adams esboçava preocupação com as *fake news* e falou: "Tem sido gerado mais notícias falsas propagadas pela imprensa nos últimos dez anos do que por todo o milênio anterior"(MANSKY, 2018 apud ADAMS, 1798 tradução nossa), isso na era dos jornais impressos. Nos dias de hoje o que ocorreu com a chegada das redes sociais, foi um aumento no volume da comunicação entre os usuários das redes sociais e assim um grande número de atores maliciosos viram nas mesmas uma

oportunidade de beneficiar a si próprio, sua empresa, partido político, grupo religioso, etc.

A disseminação de *fake news* causam impactos enormes na sociedade, ao ponto de ter um presidente eleito nos Estados Unidos da América com influências desse fenômeno. Além disso o efeito da alta exposição a notícias fabricadas tem sido estudado pelos mais diversos campos das ciências.

De acordo com Shu et al. (2017, tradução nossa) a disseminação de *fake news* ocorre não apenas por parte de atores maliciosos mas também por cidadãos neutros e outros até bem intencionados nesse quesito, daí surgem os conceitos sociais e psicológicos de como ocorrem por parte dos indivíduos o compartilhamento de conteúdo falso, e que para essas pessoas o que é divulgado é uma informação acertada e informativa. As razões para a disseminação desse tipo de conteúdo encontram bases em dois fundamentos que cercam as pessoas no seu dia-a-dia, eles são:

- **Fundamentos psicológicos:** os humanos não são bons em dicernir se o que lêem como informação é verídico ou não, dessa forma as *fake news* se aproveitam desse aspecto para explorar essa vulnerabilidade pessoal. As fraquezas que estão diretamente ligadas ao psicológico de uma pessoa podem ser divididas em dois fatores. A primeira está ligada a visão ingênua de mundo onde os consumidores tendem a acreditar que sua forma de ver é a única acertada e aqueles que não concordam com o que pensam são consideradas visões enviesadas, irracionais ou desinformadas. A segunda está ligada ao viés de confirmação, que diz que as pessoas gostam mais de ouvir aquilo que elas concordam do que aquilo que a contradiz. Uma vez que um cidadão forma sua opinião é difícil reverter esse erro e muitas vezes apenas apresentar o conteúdo verídico não tem o efeito de corrigí-lo e isso ocorre com mais intensidade quando se está frente a grupos ideológicos. (SHU et al., 2017, tradução nossa)

- **Fundamentos sociais:** ao considerar o processo de consumo de notícias, como um fenômeno social, algumas teorias contribuem para entender como essa dinâmica acontece. A teoria da prospecção diz que as pessoas tomam decisões baseadas em um processo de cálculo dos ganhos e perdas comparadas ao seu estado atual. Baseado nesse desejo de maximizar as recompensas sociais, as pessoas disseminam notícias mesmo que o material tenha cunho mentiroso. A teoria da identidade social diz que essa busca por aceitação social é essencial para que elas tenham auto-estima e uma identificação com os outros membros do seu grupo. Dessa forma os indivíduos tendem a tomar decisões que são mais seguras quando estão compartilhando informações, ao custo de que essa informação possa ser mesmo uma *fake news*. (SHU et al., 2017, tradução nossa)

  Essas teorias racionais possibilitam moldar o compartilhamento de uma *fake news* como parte da teoria dos jogos econômicos. Sendo dois atores principais: os produ-

> tores e os consumidores de conteúdo. O processo de criação de uma notícia, que a partir de um fato s e um viés tomado pelo produtor b leva em uma notícia a. O viés tomado pode ocupar valores que representam um grau de transformação que o ocorrido inicial passa, portanto $b = [-1, 0, 1]$, onde -1 representa um viés que inverte o fato, 0 procura mantê-lo como foi (imparcilidade) e 1 busca uma intensificação. A partir dessa análise os produtores de conteúdo se utilizam dela para terem seu retorno. Esse retorno pode ser: (I) *A curto prazo* maximixar o engajamento, que é positivo de acordo com o número de consumidores alcançados, (II) *a longo prazo* a reputação do produtor de conteúdo visto do quão autêntico é seu conteúdo. E por parte dos consumidores essa análise é feita para mostrar a utilidade do conteúdo ao público como: (I) *fonte informacional* obter notícias verdadeiras e impariciais, muitas vezes os consumidores podem pagar para ter acesso a esse tipo de informação e (II) *fonte social de informação* onde as notícias recebidas são vistas como reafirmação do seu ponto de vista e é utilizada para satisfazer as necessidades sociais e reafirmar o viés de seu grupo social. As partes envolvidas no fenômeno tentam sempre maximizar seus ganhos sociais como dito na teoria acima, portanto quando há a superposição do segundo modo de retorno/uso pelas partes, o ator passa a ser induzido ao fenomêno de divulgação de *fake news*. (SHU et al., 2017, tradução nossa)

Do que foi visto acima fica evidente a complexidade do que tange o assunto, se por um lado o público tende a assumir uma função de ator pouco confiável (já que são vulneráveis psico-socialmente), então o papel das fontes passam a ser cruciais (visto sua ligação com empresas e grupos que podem perdurar por muito tempo ativos na sociedade). São elas que devem buscar o ponto médio do viés, o fato de verdade, as várias visões de um ocorrido, mesmo que tenham que usar seus capitais políticos, econômicos e sociais.

Normalmente notícias com fontes mais apuradas, mais engajadas em levar bom conteúdo ao seu público alvo estão ligadas a grandes grupos que usam de seu capital para contratar os melhores repórters e também para que seus contratados consigam acesso as melhores fontes relacionadas ao tema que se busca noticiar. Porém com a liberdade de impressa, todas as pessoas interessadas em um certo tema pode noticiá-lo. Isso é bom, pois tornam mais democráticos a checagem de fatos e a divulgação de outras visões relacionadas aos acontecidos sociais, mas não se pode confundir esse livre acesso com a divulgação de conteúdo propositalmente sem qualidade. Portanto por parte das fontes a preocupação com a qualidade do que elas divulgam deve ser destaque, e ainda demonstrada aos seus cliente como forma de reafirmar o bom trabalho desenvolvido por seu corpo jornalístico ou mesmo como propaganda.

Apesar desse dever nem todas as fontes tem como objetivo buscar a imparcialidade, por uma série de motivos dentre eles público alvo, caixa e financiadores. Com isso se

mostra necessário mostrar ao público a origem do que eles tem consumido e se a fonte ao qual eles tem contato se mostram preocupadas com a qualidade do que publicam.

Somado então o problema de o cliente não ter o dicernimento necessário para retirar de circulação as *fake news* (e até agirem como atores de divulgação) mais o fato de que nem todos os meios estão engajados em divulgar as informações com boa qualidade, varias pesquisas com diferentes abordagens tem sido tomadas. Algumas na tentativa de entender como na fonte da fabricação da notícia se cria a *fake news*, outras no intuito de reconhecer o que o público tem tido acesso, ainda outras na intenção de julgar ou melhor reconhecer uma notícia como confiável ou não. Essas pesquisas se encontram com campo em várias áreas da academia como sociologia, filosofia, história, psicologia, pedagogia, jornalismo e ciência da computação. Essa última por sua vez em grande parte foca seus esforços nas modelagens estocásticas e reconhecimento de padrões para tentar modelar como ocorre o fenômeno de espalhamento de notícia falsas pelas redes sociais.

As abordagens mais famosas para as pesquisas no campo de *fake news* na Ciência da Computação encontram-se basicamente em duas áreas: identificação automática de fake news e simulação de propagação (como pode ser visto nas tabelas 1, 2 e 3 a seguir onde se compara a quantidade de citações entre cada abordagem de acordo com o número de citações no Google Acadêmico). A primeira tenta encontrar padrões que se repitam dentre as varias entradas e apartir dessas entradas, dada uma nova, o agoritmo vai tentar encontrar os padrões que existem e fazer uma aproximação com os grupos que tem formados e assim julgar como uma notícia confiável. Já a segunda a partir da propagação colocada como input para o algoritmo tenta-se correlacionar se eventuais novos compartilhamentos se dão como os já detectados e assim julgar que o novo conteúdo em cheque se trata de uma potencial *fake news*.

Trabalho	**Número de citações no Google Academics**
Zhao et al. (2020)	84
Ajao, Bhowmik e Zargari (2018)	182

Tabela 1 – Texto pesquisado: fake news identification and propagation

Trabalho	**Número de citações no Google Academics**
Liu e Wu (2018)	334
Shu et al. (2020)	73

Tabela 2 – Texto pesquisado: "propagation paths"fake news detection

Trabalho	Número de citações no Google Academics
Paul et al. (2019)	24
Qayyum et al. (2019)	65
Torky, Nabil e Said (2019)	8

Tabela 3 – Texto pesquisado: fake news blockchain detection

A falha das abordagens baseadas em reconhecimento de padrões está no fato de serem métodos probabilísticos, Menczer um cientista da Universidade de Indiana que estuda, desde o início do ano de 2005 o fenômeno de viralização de conteúdo na internet classifica as *fake news* como um "spam social"e diz que "você nunca terá um aprendizado de máquina com nenhum erro"(WALDROP, 2017 apud MENCZER 2010 tradução nossa). Essa característica coloca em risco qualquer tomada de decisão feita por esses algoritmos e por sua vez o que ocorre é que as redes sociais tomam medidas para contornar tal característica. A mais comum delas é relaxar o quociente de tomada de decisão do agorítmo quando se está frente a uma possível *fake news*, dessa forma as redes sociais preferem que notícias falsas passem para o consumidor final do que notícias verdadeiras sejam barradas, ou ainda colocam pessoas para analisar as saídas dos algorítmos que detectam as *fake news* e assim essa pessoa julga a característica de tal material.

1.1 OBJETIVOS

Dadas as limitações das soluções atuais ligadas a característica probabilistica, uma possível solução seria eliminar esse fator dos algoritmos de reconhecimento de padrão ou tentar contorná-los. Uma possível solução para o problema seria dar mais informações ao usuário de forma que ele consiga tomar as decisões por si próprio, e avisá-lo quando conteúdos tem origem duvidosa. Dessa forma o uso de *blockchain* para armazenar notícias tem se demonstrado uma boa alternativa de forma que os dados gravados na mesma (que são imutáveis, abertos e distribuídos) podem ser usado para consulta e enriquecer a experiência do usuário ao ter contato com um conteúdo qualquer, assim auxiliá-lo na tomada de decisão a respeito do conteúdo que ele está tendo contato.

Dessa forma um modelo teórico que se mostra promissor é a mudança de visão quando se tratar das notícias. Dado que são textos que visam passar a ideia de um fato, por uma certa pessoa ou empresa, pode-se pensar então que o autor do mesmo tem responsabilidade sobre o que é divulgado e cabe a empresa a certificação de que o conteúdo publicado passou pelo crivo de seus redatores. A partir de então começa-se a ver a notícia, texto noticiário ou mídia informativa como documentos, e ai pensar na aplicação de conceitos relacionados a segurança de documentos abertos como por exemplo a autenticidade das notícias que são espalhadas pela rede, disponiblidade, confiabilidade e integridade do documento.

Alinhado ao pensamento mencionado acima tem a ideia que motiva esse trabalho. Que parte do registro das mídias como forma de provar sua origem. Isso pode ser feito com diversos sitemas e abordagens já utilizadas pelo mercado (posteriormente esses sistemas serão chamados de autoridades certificadoras). Então basta que o conteúdo que se refere a notícia em questão tenha marcadores que possibilitem os sistemas WEB verificar seu registro nessas fontes de confiança. Também é necessário que o sistema consiga mostrar ao cliente se o que ele tem contato apresenta uma origem confiável e ainda pode possibilitá-lo acessar o conteúdo ao qual tal mídia se refere diretamente.

O principal objetivo desse trabalho é estruturar uma framework para marcar os conteúdos de notícias e possibilitar assim que os sistemas WEB possam verificar a autenticidade do conteúdo acessado pelo usuário. E depois como objetivo secundário esse trabalho se propõe a criar um sistema como prova dos conceitos aqui discutidos para analisar sua viabilidade.

A partir de então para pensar nesse modelo, primeiro vamos tentar entender em que pé estão os atores atuais de mercado e a partir daí criar uma prova de conceito de que o que será proposto é factível. No intuito de guiar o trabalho, algumas perguntas estão a seguir para serem respondidas até o final:

QP1 Quais são as abordagens utilizadas pelo mercado para fazer marcações em conteúdos da WEB através de metadados? Quais suas aplicações?

QP2 Como estão nos dias atuais os sites que divulgam notícias para os usuários finais? Sejam eles um portal de notícias ou uma rede social?

QP3 Como é possível com a menor quantidade de alterações nesses sites marcar que o conteúdo ali exibido se encontra autenticado?

- QP4 Quão difícil é montar um sistema que se utilize desses metadados?

A primeira pergunta vem no intuito de mapear as frameworks de metadado WEB disponíveis e quais as vantagens e desvantagens de se utilizá-los. Uma solução que parece viável a principio é o uso das *meta-tags* da linguagem HTML, que já prevê esse tipo de uso.

Depois de levantado os pontos relativos a onde colocar os dados de marcação de autenticidade da notícia, será feita uma avaliação a respeito de como estão os portais de divulgação. A principio os principais portais do país como Estadão, Folha de São Paulo, G1, Facebook e Google Notícias serão analisados e os dados levantados serão utilizados para desenvolver a framework.

Por último um protótipo que vai mostrar ao cliente a autenticidade da notícia que ele tem acesso. No qual, por motivos de simplicidade, deverá ser uma extensão para o navegador Google Chrome que avise qual o estado de autenticação de cada notícia

veiculada na página que o cliente acessa. Assim a viabilidade do que foi proposto será posto a prova e os prós e contras poderão ser levantados, uma oportunidade também para se colocar em prática conceitos aprendidos no decorrer do curso de Bacharelado em Ciência da Computação como modelagem e desenvolvimento de sistemas de informação, arquitetura cliente/servidor e responsabilidade social.

Com esse protótipo é esperado provar que não é difícil para os atores de mercado marcarem seus conteúdos de forma que seja viável fazer o rastreio através de sistemas de confiança voltado a esse intuito.

Como é quase impossível dizer se uma notícia apresentada é verídica ou não, a abordagem proposta nesse trabalho vem na ideia de apresentar uma alternativa aos sistemas probabilístico de detecção de *fake news*, uma vez que esses sitemas tem um erro difícil de ser eliminado. Esse trabalho fornece uma ferramenta mais discreta para que os sistemas terceiros possam tomar decisões a respeito de um conteúdo qualquer que está sendo compartilhado, ou seja, a partir de um dado se ele tem marcadores que apontam a uma notícia e/ou autor de conteúdo que fornece conteúdo de boa qualidade ele pode usar isso para autorizar a disseminação dessa mídia. Por outro lado se a mídia que chega para o sistema tem metadados que apontam a uma notícia, autor desconhecido, marcado como uma *fake news* ou um autor de conteúdo de má qualidade, ela pode penalizar o conteúdo e evitar que ele se espalhe.

Uma outra característica interessante que esse trabalho traz é quanto a mostrar ao cliente as fontes que foram utilizadas para basear um conteúdo que ele tem acesso. Dessa forma ele pode entrar no *link* anexo dentro do metadado e ter contato com o conteúdo referido. Isso também adiciona uma camada social de confiança ao leitor quando o publicador demonstra que ele tem responsabilidade de ligá-lo a metadados em boas fontes e sinalizar essa preocupação ao seu cliente.

1.2 METODOLOGIA

Foi utilizado ao longo do trabalho uma metodologia de pesquisa exploratória para entender a viabilidade do uso de um sistema de confiança baseado em metadados para tentar frear a disseminação de *fake news* em um ambiente virtual. Essa ideia vem junto a popularização dos uso de *blockchain* fora do contexto de *cripto moedas* como por exemplo nos ativos de *NFT* e nos cartórios virtuais. Essa pesquisa se difere das pesquisas mais comuns na área que estão ligadas ao campo de reconhecimento de padrões estatísticos como identificação automática de fake news e simulação de propagação, no momento em que se propões pesquisar uma abordagem menos probabilística, e que utilize dessa tecnologia que tem ganhado destaque.

O trabalho se baseou no estudo de Qayyum et al. (2019), Shang, Liu e Lin (2018), Torky, Nabil e Said (2019) and Paul et al. (2019) todos que utilizam *blockchain* na fina-

lidade de lidar com *fake news*. Esses trabalhos se focaram mais na forma como o banco de dados (*blockchain*) deveria ser montado para suportar esses sistemas e o trabalho aqui seguiu no intuito de entender como esses dados já salvos poderiam ser utilizados como metadados para expor ao cliente o que ele tem acesso.

Nessa ideia então o trabalho começa com uma investigação sobre como os padrões estabelecidos prevêm o uso de metadados, para isso foi investigado o *HTML5* mais precisamente a documentação disponibilizada pela *W3C* que é um dos órgãos que regulamentam o desenvolvimento da internet.

Logo após conhecer onde devem estar os metadados que ligam um texto a uma autoridade certificadora (ou blockchain) a pesquisa se direciona para entender quais são esses metadados que devem estar presentes nas páginas para simbolizar um registro de uma notícia. Ao final desse passo quais e onde devem estar os metadados são as saídas esperadas.

Então com os metadados e onde eles devem estar passa-se para o estudo da viabilidade de incorporação desses nos principais sistemas utilizados pelos brasileiros, aqui deve-se levar em consideração os principais portais de notícias e também os sistemas que redirecionam a esses conteúdos, como por exemplo agregadores, feeds RSS.

Com todas essas informações então um protótipo deve ser desenvolvido para se ter uma ideia da dificuldade que a adoção de um sistema como esse tem e no final o estudo dos pontos positivos e negativos ligados a tal abordagem que foram percebidos ao longo do trabalho.

2 CONCEITOS BÁSICOS

No decorrer desse capítulo será discutido os conceitos básicos que serão utilizados ao longo do trabalho para que quando citados sejam entendíveis e não deixe dúvidas. Será iniciado por conceitos mais gerais e no final conceitos mais técnicos serão abordados.

2.1 NOTÍCIA

Notícia é um termo utilizado para denominar um gênero literário que traz uma informação a respeito de um acontecido ou situação atual. Segundo o dicionário HOUAISS da língua portuguesa:

> Notícia (i) informação a respeito de acontecimento novo, de mudanças recentes em alguma situação, ou do estado em que se encontra algo; nova, novidade; (ii) conhecimento do paradeiro ou da situação de alguém; (iii) recordação, lembrança; (iv) nota, apontamento; (v) escrito sintético sobre um assunto qualquer; (vi) nota histórica; biografia; (vii) jornalismo relato de fatos e acontecimentos, recentes ou atuais, ocorridos no país ou no mundo, veiculado em jornal, televisão, revista etc. Houaiss (2020, tradução nossa)

Segundo Silva e Silva (2012, tradução nossa) com essa definição é possível perceber o caráter histórico e bibliográfico que a notícia tem para seus leitores no qual retrata acontecimentos ou pessoas ligados ao tempo atual ou remoto no corpo de sua redação. Segundo o mesmo autor a notícia tem uma função sociocomunicativa que é a de estabelecer a comunicação entre membros da comunidade discursiva jornalísitca e os leitores através dos fatos e acontecimentos e informa a população, dessa forma fica aparente o compromisso ético que os autores das notícias deveriam ter.

2.2 FAKE NEWS

O termo *fake news* foi usado de forma ampla ao longo da história. Hoje ele está associado a um conteúdo que tenha a intenção de se parecer com um conteúdo real e sério, mas que não se baseia em fatos reais para ser confeccionado. Dessa forma esse conteúdo ganha apelo entre os leitores e se espalha de forma rápida pelos meios de comunicação. Esse tipo de conteúdo tem dois fatores principais para serem produzidos: financeiro e político, que com elas conseguem angariar mais seguidores e adeptos as causas defendidas.

Segundo Junior, Lim e Ling (2018, tradução nossa) o termo *fake news* passou ao longo da história recente por uma mudança de significado. No inicio esse termo era relacionado a textos, ou melhor, conteúdos que faziam paródia, sátiras e propagandas,

depois ele tomou uma conotação voltada a descrever conteúdo falso e que tem um efeito de espalhamento que engane seus leitores. Um detalhe que se manteve na definição é quanto a sua alteração da realidade proposital para um fim específico.

2.3 WEB

A WEB é o nome pelo qual a internet é chamada. Segundo o dicionário Houaiss: "nome pelo qual a rede mundial de computadores internet se tornou conhecida a partir de 1991, quando se popularizou devido à criação de uma interface gráfica que facilitou o acesso e estendeu seu alcance ao público em geral."

2.4 PORTAL DE NOTÍCIAS

Segundo o G1 Definições 2008 um portal de notícias uma página na internet que serve como ponto de acesso a varios conteúdos. serviços e informações. O Imperial College 2020 oferece um complemento interessante sobre o que é um portal ao oferecer um divisão sobre os portais, nos quais eles podem ser:

- Empresariais - que se desinam a consolidar uma multiplicidade de origens em uma única página. Os usuários nessas páginas não costumam postar, no em tanto eles assumem a posição de consumidores das informações disponibilizadas pelo corpo da empresa.
- Com conteúdo gerenciado - são páginas que se destinam a oferecer uma experiência única de acesso. No qual os usuários são permitidos a publicar documentos ou conteúdos da web com outros usuários, e também ao mesmo tempo esses clientes tem contato com conteúdo publicado por outros membros do portal.

2.5 REDE SOCIAL

Rede social é o nome dado a sistemas computacionais que cujo foco é o auxilio na conexão entre pessoas e organizações sociais como por exemplo empresas, ONG's, grupos, etc (GARTON; HAYTHORNTHWAITE; WELLMAN, 1997, tradução nossa). Essas plataformas foram motivos de uma grande mudança na vida das pessoas nas últimas décadas cujas quais aproximaram e mudaram a dinâmica do contato cotidiano interpessoal, de forma que diminuiu a distância entre os membros de ciclos sociais e também criaram novos focados nos grupos de interesses entre seus membros. Por tanto a dinâmica cotidiana, o impacto no comportamento de seus usuários, a disseminação de informação por meio desses sistemas e a estrutura de poder nessas plataformas tem sido alvo de estudo em diversas áreas da ciência como sociologia, estatítica, filosofia e computação.

2.6 CONFIANÇA

A palavra confiança possui uma vasta quantidade de definições. Nesse trabalho ela será utilizada em dois contextos:

- No contexto de sistemas de informação confiança é uma palavra utilizada como sinônimo para "segurança", no qual a primeira é vista como uma conotação mais branda da segunda. Como por exemplo: no caso de salvar um arquivo no dispositivo o usuário confia naquele sistema, ou seja, ele acredita que o sistema é seguro (NGUYEN, 2003). Geralmente pode-se dizer que uma entidade é confiável dado que ela se comporte conforme se espera que ela deva se comportar (NOORDERGRAAF, 2002, tradução nossa).

- No contexto jornalístico confiança é uma palavra utilizada para designar aquelas notícias provenientes de meios de comunicação que seguem uma serie de princípios na sua redação como completude das informações apresentadas, assertividade dos fatos (checagem dos ocorridos), balanceamento do ponto de vista apresentado (não tomar um viés ao apresentar as novidades), transparência (prestar as devidas explicações quanto a forma de obtenção em quem obteve as informações apresentadas), apresentação (elegancia e beleza do meio de comunicação) e por último convencimento e entretenimento (os fatos são apresentados de forma interessante e que possa ser utilizado) (MIP, 2016, tradução nossa).

Ainda dentro do conceito de confiança um outro conceito deve ser apresentado, que é o de um sistema de confiança que está contido dentro do primeiro contexto, o de sistemas de informação).

2.6.1 Sistemas de confiança

Ainda segundo Noordergraaf (2002, tradução nossa) quando fala a respeito de modelagem de sistemas de confianças ainda o define como o conjunto de uma ou mais funcionalidades para garantir que o usuário devido utilize certas áreas de um sistema, ou obtenha acesso a certo tipo de informação. Esse sistema vem com um conjunto de atributos e regras que devem estar ligados a uma informação e quem a possui poderá criar uma relação de confiança no sistema para acessar o que precisa, logo os sistemas de confiança entregam então um conjunto de mecanismos de segurança para serem utilizados.

2.7 AUTORIDADE CERTIFICADORA

Segundo Moecke (2018) é

Uma autoridade certificadora é uma entidade responsável pela emissão dos certificados digitais. Popularmente, eles são conhecidos como a versão eletrônica de documentos importantes como o CPF ou o CNPJ, e têm a função de representar e verificar virtualmente a identidade de pessoas e empresas. Com eles, é possível assinar digitalmente diversos tipos de documentos.

2.8 *BLOCKCHAIN*

Segundo Yaga et al. (2018) *Blockchain* é um sistema que funciona como banco de dados para aplicações distribuídas. Ela é utilizada como base para todas criptomoedas que se tem, por apresentar duas características fundamentais, que são elas (i) à prova de violação e (ii) resistênte a mudanças, ou seja, a blockchain é resistente a mudanças, mas é possível que se possa desenvolver um sistema que necessite de atualizações nos valores salvos, porém as causas e consequências devem ser estudadas para se usar tal ferramenta. A mais famosa entre as criptomoedas é a *Bitcoin* e também aquela no qual em 2001 um pesquisador que se identificou como Satoshi Nakamoto (e que até hoje não se sabe ao certo quem é esse pesquisador) no artigo *"A Peer-to-Peer Electronic Cash System"*, descreve o que seria uma moeda descentralizada que se utiliza de criptografia para mantê-la sem influência de instituições locais.

Para ter esse comportamento descrito a *Blockchain* se baseia em uma estrutura de dados chamada *Ledger*, ou traduzido, livro razão que fica salvo de forma distribuída pela rede que compõe a *Blockchain*. Esse livro razão é composto de blocos dependentes, no qual cada bloco é composto de três partes: (i) cabeçalho, (ii) conteúdo e (iii) assinatura. No cabeçalho tem-se ao mínimo três campos no qual o primeiro (i) é a hash ligada ao bloco anterior, (ii) a data de criação do bloco e (iii) o *nonce* que é o resultado do desafio proposto pela rede para aceitar o bloco como próximo componente do livro razão (será explicado a posteriori como é feito e resolvido essa valor). Logo após o cabeçalho vem o conteúdo do bloco que tem aquilo que se deseja salvar no livro razão. E por último a hash do bloco que é tirada a partir do cabeçalho em conjunto com o conteúdo.

Como mencionado para que um bloco seja aceito no livro razão os nós (serviços que executam a *Blockchain*) precisam aceitá-lo como próxima entrada válida e essa validação é feita através de uma restrição no formato da hash que é gerada do bloco. Assim para adequar o formato da hash cada nó tenta de forma exaustiva iterar sobre o valor do *nonce* e gera para cada um desses valores hashes até que seja atingido o formato desejado e a partir daí esse bloco é propagado pela rede para que seja validado pelos outros nós e aceito como válido, a essa técnica de validação de nós é chamada de *prrof of work*, ou prova de trabalho e é o algoritmo de consenso mais utilizado.

Algumas dúvidas que surgem é e se em um dado momento dois blocos são considerados válidos e tentam ser propagados pela rede, qual deve ser escolhido? A escolha

na maioria das *blochains* é feita pelo bloco mais antigo, uma vez que ele está esperando durante mais tempo para ser processado, dessa forma deve ganhar prioridade, então após um nó ter sido aceito e outro chegar com uma data anterior válida o bloco é descartado e passa-se a aceitar o aquele como o verdadeiramente válido. Mas isso abriria margem para que um agente mal intencionado mude o valor por completo de uma *blockchain*, isso não acontece na prática, porque um bloco somente é considerado válido dentro da blockchain após um certo número de blocos posteriores terem sido adicionados a rede, e dessa forma esse bloco mais antigo passa a ser considerado mais estável, uma vez que vários nós o aceitam como válido e fonte para os próximos blocos. Pela sua forma descentralizada, a partir do momento que o nó percebe que o seu bloco não é estável ele volta os valores para a fila de processamento com maior prioridade para tentar criar nós validos com esses valores.

Como pode-se perceber a *blockchain* é um sistema que se utiliza de criptografia de forma intrínsica para funcionar, por isso as moedas digitais baseadas nela são chamadas de *"criptomoedas"*. A partir de 2008 o uso da *Blockchain* em contextos que não apenas esse tem sido estudado e sistemas que necessitam das características (resistência a alteração e a prova de violação) já citados a cima se mostraram promissores. Por exemplo nas NFTs (Non-fungible token) um código de computador que serve como autenticação de um arquivo como explicado por Lafratta (2021). Ela também tem sido estudado para ser usada em sistemas que precisam de confiança distribuídas como o necessário para o modelo apresentado nesse trabalho, ou mesmo sistemas de DNS (Domain Name Service), dentre outras aplicações.

2.9 METADADO

O termo metadado significa "dado que descreve um dado". Ele se relaciona a um ou mais dados utilizados para descrever outro dado, como por exemplo em um formulário que contenha dados relacionados a uma pessoa, o que cada campo significa é considerado um metadado, ou ainda dado um conjunto de dados relacionados ao balanço mensal de uma empresa, o valor final (lucro) é um metadado desprendido daquele conjunto. O termo metadado se tornou especialmente importante no contexto de sistemas informacionais, pois com isso é possível gerenciar, organizar, buscar, interpretar, selecionar e obter informações a partir de uma dada coleção de dados. Os metadados exercem um papel importante nos mecanismos de informação e permitem encontrar e fazer uso de uma propriedade para tirar certa informação, além de rotular, garantir a durabilidade e integridade dos recursos próprios da organização (AGNEW, 2020, tradução nossa).

Os metadados podem ser divididos em duas formas (i) intrínsecos e (ii) extrinsecos. Aqueles metadados intrínsecos são aquele incorporam informações a um dado, pode também ser chamado de rótulos. Os metadados extrínsecos são aqueles que abstraem

informações relacionados a um certo dado, como por exemplo os relatórios tirados em cima de uma balanço mensal de uma empresa.

Além da divisão anterior outra importante quase se fala de metadados é quanto a forma ao qual eles podem ser inferidos segundo Agnew (2020, tradução nossa) eles podem ser auto-gerados a partir de um conjunto de dados existentes, como por exemplo: dado um conjunto de dados que contém o valor das vendas de uma empresa em um mês, é possível gerar o valor arrecadado pela empresa a partir desses dados. Eles também pode ser formados de forma automatizada a partir dos dados existentes, como por exemplo: dado um conjunto de dados com a data de nascimento de pessoas, a partir desses dados é possível com a data atual inferir a idade das pessoas. E criados por humanos, como no caso da adição de endereço a uma base de dados de pessoas.

Gerir a informação ganhou nos últimos anos um grande foco por parte das empresas e entidades sociais, para dessa forma conhecer os dados aos quais tem acesso, ou seus usuários e cliente, e então oferecer produtos e serviços cada vez melhores para eles, tendo isso como base uma boa gestão de metadados passou a ter peça chave dentro das organizações passando a ter valor estratégico.

No trabalho aqui citado, os metadados entram na divisão de dados intrínsecos e auto-gerados, eles adquirem caráter importante dentro do contexto de notícias para agora guiar os leitores à fonte de informação e também a mais dados. Com isso quem acessa esse conteúdo tem a possibilidade de tomar melhores decisões.

2.10 *PLUGIN*

Pluging são *softwares* que adicionam funcionalidades a outros, ou mesmo personalizam-os com uma dada funcionalidade, eles são utilizados no intuito de melhorar a experiência que o usuário tem no seu uso do dia-a-dia com o programa (GEORGE, 2019, tradução nossa).

Os plugin mais famosos são os incorporados por navegadores web, que vão desde gerenciadores de senha, a otimizadores de conexão, ou mesmo gerenciadores de conteúdos.

3 TRABALHOS RELACIONADOS

Neste capítulo serão discutidos outros trabalhos presentes na literatura que tangem o assunto abordado nesse projeto que falam de soluções para o problema de *fake news* baseados no registro das notícias em bancos de dados, mais específicos nesses trabalhos o uso de *blockchain*'s que estão disponíveis para consultas públicas. É possível perceber a compatibilidade das propostas entre eles. Os trabalhos selecionados a serem estudados e que servirão de base para esse trabalho são *"Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News"* (QAYYUM et al., 2019), *"Tracing the Source of News Based on Blockchain"* (SHANG; LIU; LIN, 2018), *"Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks"* (TORKY; NABIL; SAID, 2019) e *"Fake News Detection in Social Media using Blockchain"* (PAUL et al., 2019).

Em todos os trabalhos o aumento do número de *fake news* foi atribuído a grande facilidade que os usuários de redes sociais tem em compartilhar conteúdo e também o uso de sistemas que fazem uso de técnicas como *machine learning* (aprendizado de máquina) e *bots* (robôs autônomos) que compartilham mídias no intuito de enviesar os sistemas de recomendação das redes sociais. E também concordam com os efeitos perversos das notícias falsas como por exemplo no artigo de Qayyum et al. (2019) quando os autores falam que: por meio desses conteúdos podem influenciar pessoas por propósitos políticos a apoiarem agendas que não-necessariamente tem cunhos sociais.

Nos trabalhos citados são discutidos sistemas para acompanhar a origem de notícias e dessa forma evitar a disseminação de *fake news* com o uso de persistência do conteúdo em bancos de dados que fazem uso da técnica de *blockchain*.

Uma *blockchain* de forma simplicada é um sistema distribuído com vários nós (unidades de processamento) que validam de forma criptográfica cada nova entrada, ou seja, a cada entrada nova é atribuído uma *hash* criptográfica gerada a partir de uma outra atribuída ao registro anterior. Dessa forma com o passar do tempo e o registro de novos blocos mais estáveis se tornam aqueles registrados anteriormente. Além de que com a disseminação dessa base de dados entre os vários nós da rede da *blockchain*, para uma possível ameaça o atacante teria que trocar um determinado bloco assim como também todos os posteriores de forma que a maioria dos nós da rede validem tais entradas como a válida na rede, ou seja, é quase impossível que isso aconteça numa rede bem distribuída.

3.1 USING BLOCKCHAIN TO REIN IN THE NEW POST-TRUTH WORLD AND CHECK THE SPREAD OF FAKE NEWS

Qayyum et al. (2019) em *"Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News"* ressalta o dinamismo que o uso de redes sociais e da internet trouxe para a distribuição de conteúdo, além disso ele cita a respeito da ameaça a verificação de fatos que tem as tecnologias de *deep learning* que é um modelo de inteligência artificial que cria áudios, imagens e até mesmo videos de forma realistica. O trabalho deles se utiliza de uma *blockchain Ethereum* para desenvolver o protótipo a que se propõe e a execução dos *smart contracts* para se realizar a veririficação da validade da mídia registrada. Um outro ponto importante para citar a respeito desse trabalho é quanto ao cuidado com quais os nós tem para escrever no livro razão da blockchain, no qual se sugere que apenas órgãos responsáveis ou grandes empresas recebam nós com o poder de adicionar conteúdo. Ainda eles adicionam a sua estrutura algumas características para se identificar a notícia como nome da publicadora do conteúdo, estado, uma chave pública atribuída para identificação e ainda uma cadeia de palavras para alimentar o algoritmo de verificação semântica.

Por outro lado o trabalho de Qayyum et al. (2019) apresenta algumas diferenças de abordagens ou focos como quanto a verificação de um determinado conteúdo que sugerem o uso de um veficador semântico de similaridade para correlacionar os conteúdos, enquanto no sistema aqui desenvolvido essa correlação fica a cargo do leitor que tem mais contexto para essa verificação de conteúdo. Além disso fica em aberto como será feito o consumo dos dados colocados nessa blockchain por outros sistemas, por exemplo o usuário deverá ter a chave identificadora da mídia apenas para chegar a notícia? E se o verificador semântico der falso, dado que é um algoritmo probabilistico, como proceder nesse caso? O foco do trabalho corrente é justamente identificar os aspectos relacionados ao consumo e a correlação entre a entrada no banco de dados e uma mídia, outro aspecto que se tem destaque é quanto a condução do cliente até a notícia fonte para que ele possa checar e ter mais informações para tomar a decisão a respeito da veracidade de um conteúdo.

3.2 TRACING THE SOURCE OF NEWS BASED ON BLOCKCHAIN

No trabalho de Shang, Liu e Lin (2018) *"Tracing the Source of News Based on Blockchain"* ele faz uma discussão a partir de um nível de abstração mais elevado quando o assunto tange a *Blockchain*, ele começa definindo que o sistema para rastrear a fonte de notícias está diretamente relacionado com as pesquisas na área de rastreio de dados e se baseiam em três pilares: (i) transmissão dos dados, (ii) aquisição e (iii) persistência dos dados. E que de acordo com esse modelo básico a tecnologia de *Blockchain* se encaixaria muito bem por ser um banco de dados baseado na distribuição, tempo e criptografia quando vai aceitar e persistir qualquer bloco. Além disso um outro ponto importante

que ele traz para a discussão é quanto a categorização que a literatura traz para se fazer o rastreio dos dados que são eles (i) métodos anotados e (ii) métodos sem anotação. A primeira categoria (anotação) no momento de criação de um determinado dado é anexado junto a ele metadados para identificação, no momento que ele é transmitido e alterado, os adendos feitos são adicionados e marcados com quem/quando os fizeram. No final esses dados anexos identificam o processo de transformação sofrido e pode ser usado no contexto de *fake news* para idenficar onde pontos de erro foram introduzidos. Na segunda categoria (dados não anotados) para toda alteração feita nos dados são feitos envios dessas alterações para serem persistidas nos sistemas de rastreio de dados, com isso no final pode-se fazer uma função inversa na última versão do dado e se obter informações das alterações de quem/quando alterou os dados. Essa segunda é do ponto de vista de armazenamento mais eficiente, pois não necessita de salvar nenhuma informação a mais, porém ela reside sua corretude na função inversa que muitas vezes é impossível de ser feita.

No que tange a como os dados estarão dispostos o trabalho de Shang, Liu e Lin (2018) ele apenas se resume a dizer que toda notícia deve ser salva para no futuro ser utilizada por sistemas de rastreio de dados. Ainda sobre esse tema ele discorre que os sistemas baseados em *Blockchain* se parecem com uma evolução da forma de persistência de notícias que a indústria utiliza na atualidade, onde cada empresa persiste suas matérias em infraestruturas próprias na forma de ilhas de informação que do ponto de vista mais amplo são pouco úteis, enquanto no modelo que tem uma *Blockchain* essas publicações são compartilhadas e podem ser utilizadas por terceiros para futuras análises.

Quando comparado o trabalho de Shang, Liu e Lin (2018) com o trabalho corrente foi usada uma abordagem no rastreio de notícias anotado, no qual precisa-se da presença dos metadados na páginas para funcionar de motor aos sistemas que vão se utilizar desses dados como no caso do protótipo desenvolvido. Por outro lado no que tange a composição do bloco de identificação da notícia esse trabalho confia na idoneidade da infraestrutura original da publicadora da notícia para referenciá-la e deixar com que o cliente decida a veracidade/qualidade do conteúdo que tem contato versus ter no banco de dados todo os dados para prova. Além disso no corrente trabalho o foco fica em como será feito uso dos dados da *Blockchain*, com o pressuposto de que ela é uma boa base de dados para um sistema que faz o rastreio de notícias, enquanto no trabalho de Shang, Liu e Lin (2018) ele estuda a viabilidade do uso de uma *Blockchain* para solucionar o problema de disseminação de *fake news*, ou seja, esse trabalho pode ser considerado como um enfoque dentro do outro.

3.3 PROOF OF CREDIBILITY: A BLOCKCHAIN APPROACH FOR DETECTING AND BLOCKING FAKE NEWS IN SOCIAL NETWORKS

O trabalho de Torky, Nabil e Said (2019) *"Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks"* está pautado no uso da ferramenta de *Blockchain* como motor primário para um modelo de rede social descentralizada e com essa um modelo inteligente de detecção de *fake news*. No qual toda mensagem posta a essa rede seria propagada no modelo *peer-to-peer* e esses nós componentes da rede social teriam uma cópia do livro razão da *Blockchain* em sua propriedade. Dessa forma ao invés de utilizar o modelo padrão de desafio, ou seja, *Proof of work* (que é usado pelas cripto moedas como o *Bitcoin*), ocuparia o espaço o *PoC (Proof of credibility)* criado ao longo do artigo. Esse *PoC* executa um algoritmo sobre os dados que já estão inputados na rede social e os dividem entre aceitáveis e rumores. Os dados considerados aceitáveis são propagados e salvos nos bancos de dados de cada nó componente da rede, enquanto os rumores são adicionados a *Blockchain* de rumores e será usado como entrada na validação dos próximos nós que é feito através do algoritmo de *Best Match technique (BM25F) metric* para julgar um conteúdo como *fake news*.

Ao comparar o trabalho desenvolvido por Torky, Nabil e Said (2019) e o Trabalho corrente uma diferença considerável está presente, enquanto a *Blockchain* no corrente trabalho foi utilizada como banco de dados fonte de dados "aceitáveis"ela faz frente ao uso por parte de Torky, Nabil e Said (2019) como fonte de dados ruins para serem utilizados no decrécimo da nota de um futuro dado candidato a integrar a *Blockchain*. Além disso o trabalho aqui se concentra em discutir uma forma de se chegar ao uso desses dados salvos na *Blockchain* enquanto o outro se pauta mais em sugerir um modelo alternativo ao *Proof of Work* como modelo para um sistema de detecção de *fake news* que pode ser até mesmo uma rede social.

3.4 FAKE NEWS DETECTION IN SOCIAL MEDIA USING BLOCKCHAIN

No trabalho de Paul et al. (2019) *"Fake News Detection in Social Media using Blockchain"* é discutido o uso de uma blockchain baseada na *Ethereum* que é uma blockchain capaz de executar scripts sobre os dados presentes nela, os chamados *smart contracts* no qual a execução pode ser replicada por qualquer nó da rede da blockchain que deve produzir o mesmo resultado, no qual ele pode ser uma saída, uma troca de moedas por exemplo. No modelo proposto eles se utilizam dessa *blockchain* como fonte de dados para alimentar um sistema colaborativo de pontuação de uma notícia qualquer. Nesse caso três grupos de usuários da *blockchain* são selecionados quando uma notícia chega a um número expressivo de compartilhamentos. Esses usuários são divididos em três grupos: outros jornais (que não o publicador da notícia), um grupo de usuários que esteja fisicamente perto do "assunto"e outro grupo de usuários aleatórios. Cada um desses usuários

atribui uma nota que será usada no final para pontuar a nota da notícia. Segundo o artigo ainda cada um desses usuários terá uma diferenciação no cálculo do peso da sua nota, uma vez que usuários com notas mais baixas podem "mentir"a respeito dos assuntos ao qual ele foi questionado, ou mesmo, um grupo jornalistico que vem sempre atribuindo boas notas deve ser recompensado por isso.

Esse trabalho dentre todos os lidos até aqui é o que mais se aproxima do uso da *blockchain* que esse trabalho tem, uma vez que ele usa a blockchain como fonte de confiabilidade e deixa aos usuários o julgamento da qualidade do conteúdo. Incorporar uma nota dada pelos usuários seria benéfica para o sistema como um todo e poderia agregar valor ao uso do sistema de verificação de notícias além daquele já feito com o apontamento para a notícia original como foi implementado no protótipo. Além disso o texto de Paul et al. (2019) cita que esse modelo baseado em verificações externas traz um problema de sob pressão os usuários selecionados para pontuar uma notícia podem apresentar comportamentos enviesados, e dessa forma o sistema se torna sucetível a governos autoritários que por ventura venham a interferir nos meios jornalísticos, porém apesar disso o sistema apresenta uma vantagem de uso visto a forma livre de publicação de notícias que tem gerados os problemas sociais das *fake news*.

3.5 COMPARAÇÃO

Como pôde ser observado esses textos focam suas discussões na *blockchain*, na arquitetura dos sistemas que às envolucram e também naqueles que publicam notícias na *blockchain*. Uma característica que é possível perceber em comum do trabalho aqui desenvolvido e os citados é o cuidado com o registro de documentos nesses bancos de dados (como pode ser visto na Tabela 4), uma vez que eles são imutáveis e eventuais *fake news* publicadas na base ficarão para sempre face a possibilidade de revogação da confiança a uma determinada autoridade certificadora ao qual esse trabalho sugere.

Um aspecto que é importantes de ser discutido é quanto a diferença entre os trabalhos quando se fala de quais dados devem estar presentes na autoridade certificadora. Nesse quesito as abordagens vão desde salvar apenas textos considerados *fake news*, à referencia ao conteúdo em um portal externo ou mesmo que tudo deve ficar salvo, como pode ser visto na Tabela 6. Além disso os trabalhos apresentam previsões diferentes quanto ao uso de mais de uma blockchain como autoridade certificadora, a Tabela 7 mostra como cada um dos trabalhos abordam esse aspecto.

Um outro aspecto interessante de se comprar é quanto a forma de checagem do conteúdo que é feito no sistema. Alguns dos trabalhos citam que é possível usar algoritmos de identificação automática para entregar uma conclusão ao usuário. Essa comparação pode ser visto na Tabela 5.

Entre tanto fica em aberto nesses trabalhos como seria o consumo por parte dos

clientes, as vantagens que um publicador de conteúdo teria ao integrar suas publicações com tal tecnologia e as dificuldades para os atuais portais e redes sociais de se usar os dados da blockchain.

Nas tabelas abaixo é possível ver o comparativo entre os principais aspectos que os trabalhos apresentam e o trabalho que aqui é desenvolvido. O Qayyum et al. (2019) refere-se à *"Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News"* (QAYYUM et al., 2019), Shang, Liu e Lin (2018) *"Tracing the Source of News Based on Blockchain"* (SHANG; LIU; LIN, 2018), Torky, Nabil e Said (2019) *"Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks"* (TORKY; NABIL; SAID, 2019) e Paul et al. (2019) *"Fake News Detection in Social Media using Blockchain"* (PAUL et al., 2019).

Trabalho \Aspecto abordado	**Previsão de segurança no acesso a blockchain**
Qayyum et al. (2019)	Não, uma vez que usa a Ethereum
Shang, Liu e Lin (2018)	Sim, publicadores são os responsáveis
Torky, Nabil e Said (2019)	Sim, uma vez que ela armazena os conteúdos ruins
Paul et al. (2019)	Não, uma vez que usa a Ethereum
Trabalho corrente	**Cada blockchain é responsável por seus dados**

Tabela 4 – Comparativo da previsão de segurança no acesso a blockchain

Trabalho \Aspecto abordado	**Forma de checagem do conteúdo**
Qayyum et al. (2019)	Utilização de um algoritmo de verificação semântica
Shang, Liu e Lin (2018)	Feito por parte do leitor
Torky, Nabil e Said (2019)	Através de um algoritmo de Best Match Technique
Paul et al. (2019)	Feito por parte do leitor
Trabalho corrente	**Feito por parte do leitor**

Tabela 5 – Comparativo forma de checagem de conteúdo

Trabalho \Aspecto abordado	**Armazenagem de dados**
Qayyum et al. (2019)	Todos dados são armazenados
Shang, Liu e Lin (2018)	Armazenam apenas referências no caso de metadados anotados e todo os dados no caso sem anotação
Torky, Nabil e Said (2019)	Todos os dados que são considerados rumores e podem ser fontes de "fake news"
Paul et al. (2019)	Não houve menção
Trabalho corrente	**Armazena apenas referências**

Tabela 6 – Comparativo armazenagem de dados

Trabalho \Aspecto abordado	**Previsão do uso de mais de uma autoridade certificadora**
Qayyum et al. (2019)	Não, usa apenas a Ethereum
Shang, Liu e Lin (2018)	Não há menção
Torky, Nabil e Said (2019)	Não há menção
Paul et al. (2019)	Não há menção
Trabalho corrente	**Sim, de acordo com quem utiliza o sistema**

Tabela 7 – Comparativo da previsão do uso de mais de uma autoridade certificadora

No intuito de esclarecer as lacunas citadas acima deixadas por esses trabalhos será discutido e desenvolvido um sistema prova de conceito e um estudo nos principais portais e redes sociais mais utilizados no Brasil ao longo dos próximos capítulos como já mencionado.

4 PROPOSTAS

Este trabalho busca desenvolver um protótipo de um sistema verificador de notícias baseados numa modelagem de confiança com respaldo nos metadados marcados no conteúdo da página WEB. Tal protótipo deve se mostrar promissor na coibição da divulgação de *fake news* uma vez que busca uma abordagem que dá ao usuário o ator mais proprício a tomada de decisão a confiar ou não no conteído versus as abordagens probabilísticas como identificação automática de fake news e simulação de propagação que tentam tomar essa decisão pelo cliente. Para que esse tipo de abordagem funcione o órgão que publica tal conteúdo toma o cuidado (para mostrar ao leitor que o conteúdo é verídico) com o registro dele em uma unididade certificadora, que pode ser qualquer sistema imutável com uma certa confiança pelo mercado, e assim esse ator armazena os metadados passados e os sistemas clientes podem consultar para exercer suas funções.

Para melhor origanizar o estudo de como fazer um sistema de consumo de autenticidade de notícias, esse capítulo será organizado em quatro partes. (i) a primeira vai buscar quais as possibilidades existem para a incoporação desses metadados em uma página *WEB* (segundo a norma da W3C que é órgão que regulamenta a internet) na intenção de responder , (ii) depois será visto como estão os principais atores de mercados visto frente com o que está previsto no item anterior, (iii) a seguir virá um estudo de quais os metadados são essenciais para que se faça um protótipo e (iv) por último será discutido a arquitetura que o sistema deve ter para funcionar em sua essência.

4.1 LOCALIZAÇÃO MAIS EFICIENTE DOS METADADOS

A linguagem de marcação padrão da internet o HTML e mais especificamente a sua quinta versão prevê uma marcação de metadados mais semânticos no intuito de facilitar o trabalho do desenvolvedor e de sistemas autônomos que eventualmente vão processar os dados que estão na página construída, este padrão foi estudado para entender quais ferramentas são oferecidas e que sirvam para o framework ao qual esse trabalho se propõe, dessa forma ao final dessa sessão espera-se ter uma conclusão que responda a QP1 "Quais são as abordagens utilizadas pelo mercado para fazer marcações em conteúdos da WEB através de metadados? Quais suas aplicações?".

A partir de então quatro elementos de marcação se mostraram promissores para uso, são elas as tags *meta* e *data*, o atributo *data-** e a funcionalidade de *microdata* prevista pela linguagem[1].

[1] Para se aprofundar ou saber mais sobre os elementos do HTML5 aqui citados é recomendado a leitura da documentação da linguaguem que se encontra na bibliografia (2019).

4.1.1 Tag *meta*

Essa tag existe no intuito de disponibilizar um espaço para a disposição de diferentes tipos de metadados referentes a página WEB como um todo. Ela vem acompanhada de dois atributos o *name* e *content* no qual seu conteúdo representa uma tupla de chave-valor e pode ser utilizada para extender os metadados. Algumas chaves são padronizados pela W3C como *author* para autor e *description* para a descrição da página. Exemplo de uso:

.

Código 4.1 – Exemplo contendo a tag *meta*

```
<html>
    <head>
        <meta name="author" content="John Doe">
        <meta name="description" content="some description">
    </head>
    <body>
    </body>
</html>
```

4.1.2 Tag *data*

Tal tag existe para ter a disposição uma tradução do conteúdo que se apresenta legível para humanos e máquinas. Um exemplo de uso é a presença de uma conta matemática que um humano consegue entender o significado, e o resultado da mesma se encontra no atributo *value* da tag para que uma máquina consiga processar. A seguir tem um código com exemplo de uso onde o *value* da tag *data* representa o id da propriedade escrita para humanos.

.

Código 4.2 – Exemplo contendo a tag *data*

```
<html>
    <head>
    </head>
    <body>
        <ul>
            <li><data value="21053">Cherry Tomato</data></li>
            <li><data value="21054">Beef Tomato</data></li>
        </ul>
    </body>
</html>
```

4.1.3 Atributo data-*

É um atributo global da linguagem HTML para disponibilizar a scripts próprios a página dados não visuais que sejam importantes para o processamento de um certo elemento presente. Esse atributo vem com uma restrição no qual ele deve ser utilizado apenas por scripts internos a página para ser processado a não ser que nenhuma outra ferramenta seja apropriada para uso. Se a última condição for apropriada então a W3C recomenda que um nome bem descritivo e que tenha pouca chance de coincidir com nomes utilizados em scripts de terceiros seja escolhido na intenção de evitar quebra das lógicas das páginas WEB. Exemplo:

.

Código 4.3 – Exemplo contendo o argumento global do HTML *data-**

```
<html>
    <head>
    </head>
    <body>
        <ul>
          <li data-animal-type="bird">Owl</li>
          <li data-animal-type="fish">Salmon</li>
        </ul>
    </body>
</html>
```

4.1.4 Microdata

É uma funcionalidade não normativa prevista na documentação da última versão da linguagem HTML para se marcar dados importantes que sejam úteis para softwares terceiros a página WEB. Onde os atributos *itemscope* demarcam elementos semânticos, *itemprop* um atributo do elemento em questão e o conteúdo ao qual as tags estão ligadas fazem o papel do respectivo valor nas tuplas que compõe os elementos.

.

Código 4.4 – Exemplo de uso da funcionalidade *Microdata*

```
<html>
    <head>
    </head>
    <body>
```

```
        <div itemscope itemtype="http://schema.org/
            SoftwareApplication">
             <span itemprop="name">Angry Birds</span>
        </div>
    </body>
</html>
```

Visto as aplicações desses elementos e suas restrições dois dentre os citados elementos foram selecionados para o uso na framework desse trabalho. Onde o primeiro deles é a tag *meta* para ser usado no caso de uma página inteira dedicada a uma mesma notícia. E o segundo elemento é o o atributo global *data-** que segundo a documentação da linguagem HTML foi feito para disponibilizar a scripts da página dados não visuais que sejam importantes para o processamento de um certo elemento presente. Esse elemento será usado para identificar uma notícia que esteja atrelada a um elemento da página, como um link, uma chamada para notícia em um feed como *Facebook*, *RSS feed* ou na página inicial de um portal de notícias. O atributo global em questão vem com uma recomendação para se evitar o uso em caso de scripts de terceiros e se esse for escolhido para uso que sejam escolhidas as chaves mais descritivas possíveis para que se evite a colisão durante seu processamento. Como a funcionalidade *microdata* é bem específica para marcação de elementos que se encontram em tags diferentes e visuais e o atributo *data-** é mais voltado para a declaração de metadados, ele foi escolhido para uso na framework mesmo com as já referidas recomendações.

Com a ideia de onde posicionar os metadados para fazer referencia de um registro de uma notícia, a seguir será relatado como estão os portais mais famosos da internet brasileira e se em seu HTML seria difícil a incorporação dessas marcações em suas páginas.

4.2 ESTADO DOS PORTAIS MAIS ACESSADOS PELOS BRASILEIROS

Os portais de notícias mais acessados do Brasil segundo Nascimento (2018) são em ordem G1, Estadão, Gazeta do Povo, Folha de São Paulo e UOL. Além dos portais, o Facebook e o Google Notícias serão pesquisados também pela sua relevância e volume de acessos que redirecionam por dia para outros portais. Esses sites serão estudados no intuito de saber se os elementos selecionados na sessão anterior são de difícil incorporação a sua estrutura e ao final dessa sessão espera-se responder a QP2 "Como estão nos dias atuais os sites que divulgam notícias para os usuários finais? Sejam eles um portal de notícias ou uma rede social?".

Nas páginas iniciais desses portais foram observado que toda matéria está atrelada a tag *a* que é a tag de *link* ou âncora entre as páginas. Nesse caso ela especifica a respectiva matéria a ser redirecionada. O que varia no estilo entre os portais é no caso do G1 e da Folha de São Paulo que apresentam um *link* para o título, outro para a imagem

e outros para as informações extras (data, hora e local, por exemplo), enquanto os outros como o Estadão, Gazeta do Povo e UOL apresentam um único *link* para cada chamada de matéria. Dessa forma nenhum impeditivo para a incorporação do elemento *data-** apareceu.

No Facebook e no Google Notícias, ambos se utilizam de uma tag *div* que circunda seus links para as matérias que eles fazem referência, como o atributo *data-** pode ser colocado na referida tag, nesses divulgadores de notícia tal marcação também tem a possibilidade de ser utilizada.

Já nas páginas das respectivas notícias os parâmetros da tag *meta* que de acordo com a W3C deveriam conter os metadados (dentre eles alguns normatizados) com os dados das páginas estão presentes e com padrões bem distintos entre eles. Por exemplo o título da matéria no G1 está conforme fala a W3C (com *name="title"*), já a Gazeta do Povo coloca os seus dados de forma específica para uso dos robôs autônomos os chamados *crwalers* de outras empresas como por exemplo *Facebook*, *Twitter* e *Google*. Mesmo com essas diferenças entre os portais não há nenhum impeditivo para que se adicione outras tags *meta* com os metadados a serem utilizados pelos sistemas de rastreio de notícias.

Dado a abordagem escolhida para ser aplicada às páginas foi constatada que os pré-selecionados items durante o estudo são aplicáveis as páginas. É importante então discriminar quais são os metadados a serem marcados para que o sistema protótipo seja desenvolvido.

4.3 OS METADADOS A SEREM DISCRIMINADOS PARA USO PELO SISTEMA DE AUTENTICIDADE DE UMA NOTÍCIA

Depois do estudo relacionado a quais metadados deveriam estar presentes em uma página web para que um autenticador de metadados funcione, varias possibilidades surgiram como por exemplo data e hora de publicação, data e hora da última alteração, CNPJ da empresa que publicou, CPF do jornalista, mas ou essas informações são mutáveis, ou pessoais o suficientes para não serem divulgadas ao longo da *WEB*.

Tendo isso, duas variáveis foram definidas como chaves para o acesso mínimo a um registro de uma notícia e são elas (i) um valor identificador (*ID*) único para a notícia e (ii) a autoridade que certifica os dados (apartir de agora vamos nos referir como autoridade certificadora) com esses dois metadados espera-se responder a QP3 "Como é possível com a menor quantidade de alterações nesses sites marcar que o conteúdo ali exibido se encontra autenticado?".

Com a autoridade certificadora fica a responsabilidade de aceitar os documentos vindos de boas fontes de notícias para seus usuários. Assim um sistema qualquer que se utilize dos dados salvos na certificadora pode aceitar os registros considerados de boa origem. Ou se caso achar que ela confia em registros de má qualidade pode revogar

sua confiança e a partir daí outra unidade precisará ser citadas na matéria para que a autenticação seja feita. Com essa unidade também fica a responsabilidade de possíveis erratas ou alterações nos dados que simbolizam a notícia para que ela sempre entregue o mais fidedígno e atual registro ao sistema. Além de possíveis cancelamentos e o mais importante que são os dados que fazem referencia a matéria registrada.

Já com o ID fica a ligação direta ao registro que os sistemas vão usar para obter as informações, ou seja, é um valor salvo no banco de dados da autoridade certificadora (esse banco, por sua vez, pode ser de qualquer tecnologia). Com esse ID também ficam todas as responsabilidade referentes a um atributo identificador seguro como número de atributos criados por tempo, relacionamento entre o identificador e o dado difícil de se ligar e a não sequenciabilidade. Esse atributo identificador pode ser de qualquer tipo dentre os usados no mercado como, por exemplo, UUIDv4, SHA512, etc.

No sistema a ser desenvolvido a discriminação desses metadados será feita com três chaves:

- *news-origin-base-path* que terá a URL para o acesso a base de notícias certificadas, nessa URL o domínio será referente a autoridade certificadora, portanto ela deverá estar dentre as confiáveis pelo cliente e a URI será o path com o ID da notícia registrada;
- *news-record-id* que terá o *ID* de acesso a notícia especificada, como já discutido acima;
- *news-origin-url* que será a composição do *URL* de acesso a base de notícias.

Um outro metadado será adicionado no protótipo a ser desenvolvido para controlar o elemento ligado ao argumento *data-**, uma vez que apenas com a chave do mesmo não é possível identificar o que está sendo referido, portanto foi adicionado o *data-type="news"* para assim adicionar os métodos que trabalharão com os elementos marcados.

Dessa forma então é preciso formalizar a construção da framework aqui idealizada, nela destacaremos os atores e a forma de apresentação dos dados para que qualquer sistema consiga utilizá-lo.

4.4 FRAMEWORK PARA O SISTEMA DE RECONHECIMENTO DE NOTÍCIAS

Nessa seção vamos formalizar o framework ao qual o trabalho aqui precisa para poder funcionar da forma correta e fazer a detecção das notícias. Para isso vamos dividí-lo em três partes (i) a unidade certificadora, (ii) a página web e (iii) o sistema que fará o reconhecimento dos metadados (plugin).

4.4.1 Unidade certificadora

A unidade certificadora deverá receber requisições GET em uma rota que possibilite a consulta dos dados relacionados a uma notícia e depois retornar um json com os dados relacionados a ela quando encontrada. Em caso de erros relacionados a notícias não encontradas retornar um 404. Dessa forma os sistemas clientes podem interpretar esses resultados.

4.4.2 Página Web

Na página web devem estar contidos os metadados para serem processados pelo sistema que fará o reconhecimento dos metadados. Essas páginas podem apresentar de duas formas, na qual a primeira é uma página ligada a uma notícia, ou não é apenas uma página que contém âncoras para outras páginas que contém notícia. Uma observação importante é quanto a páginas de notícias elas podem conter também âncoras para outras notícias. Na página que contém uma notícia ela deve ter meta tags que direcione a um registro na unidade certificadora. Ela pode aparecer nas formas:

- *<meta name="newsOriginUrl"content="some-value»*
- *<meta name="newsOriginBasePath"content="some-value»*
- *<meta name="newsRecordId"content="some-value»*

Nota que a primeira forma *newsOriginUrl* substitui por completo as duas seguintes que devem aparecer juntas *newsOriginBasPath* e *newRecordId*.

Outra forma é na página web ter itens que referencie a uma outra notícia e para isso deve-se ter no componente o argumento *data-**. Esse arugmento deve ter um *data-type="news"* e também uma das duas formas (i) *data-news-origin-url="some-value"* ou (ii) *data-news-origin-base-path="some-value"* e *data-news-record-id="some-value"* para possibilitar a busca pelo dado na unidade certificadora.

4.4.2.1 Sistema de reconhecimento de notícia - plugin

Com o sistema de reconhecimento de notícias fica a responsabilidade de reconhecer ou não uma unidade certificadora válida, de atribuí-la tempo de expiração para que se evite que unidades certificadoras que tenham sua qualidade decaída com o passar do tempo parmaneçam na lista daquelas aceitáveis pelo sistema. Além disso fica a cargo dessa peça processar a página WEB a procura da meta tag e dos argumentos *data-** que façam referência a uma notícia e ainda e não menos importante fazer as requisições a unidade certificadora a procura dos dados relativos a essa notícia.

A partir da framework formalizada acima, um protótipo será desenvolvido de forma a conseguir mostrar os detalhes que esse tipo de aplicação tem e também mensurar se

tal tipo de 'abordagem pode de forma fácil ser adotados pelas empresas que criam e intermediam notícias para o grande público.

Os sistemas que seguem esse modelo em sua base funcionarão de maneira parecida e será descrito a seguir como podem ser. Além disso a dificuldade de desenvolvimento desse sistema procura responder a QP4 "Quão difícil é montar um sistema que se utilize desses metadados?".

4.5 A ARQUITETURA DE UM SISTEMA DE RECONHECIMENTO DE AUTENTICIDADE DE UMA NOTÍCIA

O sistema desenvolvido foi inspirado no modelo de confiabilidade utilizado pelo protocolo HTTPS (*Hyper Text Transport Protocol Security*). Esse sistema utiliza-se de uma arquitetura híbrida entre cliente/cliente e cliente/servidor para a marcação de segurança. E a ideia básica será relatada de forma mais didática a seguir. Que será posteriormente aprofundada na parte relevante ao sistema a ser desenvolvido.[2]

Dado um ator X que respeita o modelo de confiança restrito, ele a princípio não confia na assinatura de nenhum outro ator, ou seja, qualquer troca de mensagem que se queira fazer esse cliente não irá realizá-la dado que ele não confia em ninguém. A partir de um certo momento, X tem na sua lista de confiança adicionado a assinatura de um certo ator Y, portanto agora assinaturas de outros atores que não Y continuarão sem ter por parte de X mensagens aceitas, uma vez que ao consultar sua lista de confiança esses atores não estarão presentes nessa lista. Mas dado que Y queira se comunicar com X, antes de receber uma mensagem X vai verificar se Y é um ator confiável na sua lista de confiança e se sim ele receberá sem bloqueios as mensagens de Y.

A partir de um momento que falamos a respeito de vários atores confiáveis habilitados a trocar mensagem entre si, a gestão de confiança passa a ser uma atividade muito honerosa a um certo cliente ter que fazer a adição de ator por ator na sua lista de confiança. Então uma solução para esse problema foi criada que são as chamadas **unidades certificadoras**. Basicamente elas funcionam como um cartório de registro de assinaturas confiáveis e apartir de então os clientes podem usar seu banco de confiança como fonte de pesquisa de atores confiáveis, uma vez que esses clientes confiem nessa autoridade certificadora como uma boa fonte de dados.

A partir do momento que um dado cliente não confia mais nos dados providos por uma dada autoridade certificadora, esse cliente apenas devem remover da sua lista de confiança os dados providos e a referida à autoridade certificadora. Esse modelo é complementar ao narrado no exemplo acima, portanto registros de confiança tanto vindos de uma autoridade certificadora quanto adicionadas manualmente podem coexistir em um dado ator.

[2] Para se aprofundar ou saber mais sobre o protocolo HTTPS aqui citados é recomendado a leitura da RFC 2660 Rescorla e Schiffman (1999).

Nas listas de confiança o que ocorre é a marcação de cada entrada. Se ela refere a um outro ator ou uma autoridade certificadora, e além disso dado que é um cliente qual unidade que o certificou como confiável. No exemplo a seguir de maneira mais didática será apresentado a forma como esse protocolo trabalha para os casos que envolvem uma autoridade certificadora.

O mesmo cliente X do exemplo anterior, começou a aumentar seu ciclo de confiança e a ter uma lista muito extensa de atores que ele confia, mas ao mesmo tempo, atores que ele antes confiava passaram a atores com informação duvidosa e no seu modelo restrito de confiança esses atores não estão mais aptos a trocar mensagem com X. Só que fazer essa gestão se tornou algo muito complexo, dado o número de entradas que são adicionadas e removidas. No intuito de melhorar a gestão de X, um outro dado ator C, se propôs a compartilhar sua lista de confiança com X, uma vez que ele tem um modelo de confiança igualmente bom como o de X. Dessa forma ao invés de X ter que gerir quem ele confia unitariamente, um novo dado ator Z que ele ainda não conhece, basta que pergunte a C se tem Z na sua lista de confiança. Uma vez presente ele adiciona Z mas refere C como o ator que indicou Z como confiável. Qualquer outro ator que não esteja na lista de confiança de X e C, não conseguirá trocar mensagens com X, dado o seu modelo de confiança agora é semi-restrito, que agora ele confia em pessoas que C confia. Após um certo momento, X passa a perceber que C tem adicionado em sua lista de confiança atores de mais e que X não os julga como atores confiáveis, então a partir desse momento X remove C de sua lista de confiança e todos os atores que C o indicou. Dessa foram ele volta a melhorar seu ciclo de confiança.

Com o modelo de confiança descrito anteriormente para o sistema de rastreio de notícias será igual. Essas unidades certificadoras terão os dados relevantes relacionados as notícias que foram registradas nelas disponíveis a consultas externas. Já um sistema cliente a partir de uma página que tenha marcadores encontrados, eles poderão estar com os metadados de duas formas: (i) com uma autoridade certificadora inválida, ou desconhecida pelo cliente, e (ii) com uma autoridade certificadora válida. Para (i) se o sistema não reconhece a autoridade certificadora, ele retorna ao usuário com o alerta de que a unidade citada não está dentre as aceitas pelo sistema. Já em (ii) o sistema aceita que os dados podem referir a uma notícia confiável e prosseguirá com a requisição a unidade cerficadora.

Então com o retorno da autoridade certificadora a resposta pode marcar uma notícia em três situações diferentes. Em (i) que a nototícia se encontra válida e exibe os dados da mesma para o cliente validar os dados do corpo da notítica como autor, publicadora, data de publicação, título, descrição e link para a matéria original, (ii) que a notícia não foi encontrada na autoridade certificadora e portanto pode ser um conteúdo forjado e (iii) que a notícia marcada foi referida como uma notícia invalidada, uma vez que a mesma pôde conter dados erronêos sobre o fato relatado, ou mesmo por algum outro

motivo foi retirada de circulação. Na Figura 1 encontra-se o diagrama de atividades pelo qual o sistema a ser desenvolvido pode passar.

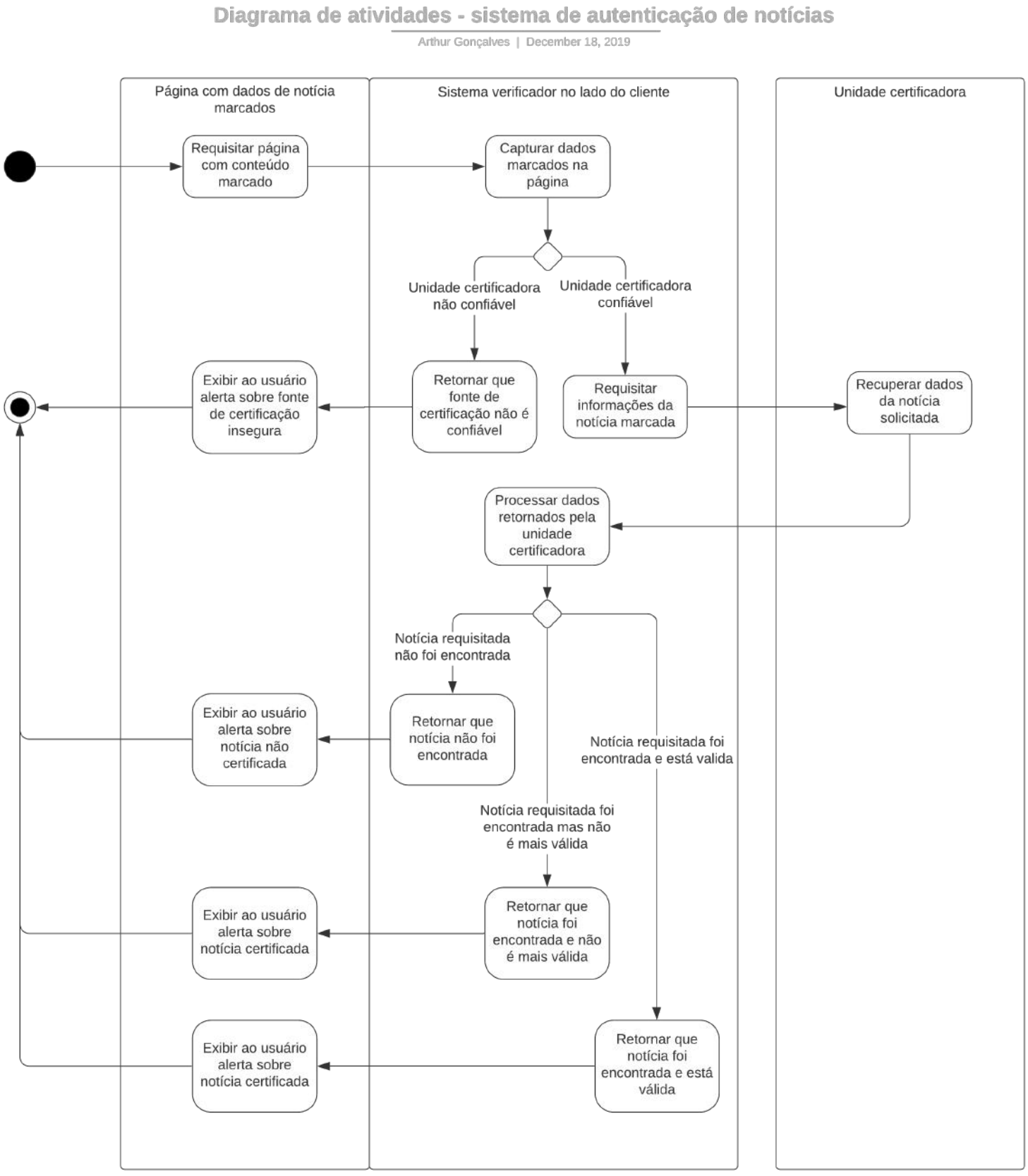


Figura 1 – Diagrama de Atividades UML

Com essa arquitetura e os detalhes importantes dela discutidos, o sistema a ser desenvolvido será um extensão do Google Chrome, que a partir de uma lista de unidades certificadoras e de metadados vindos no HTML da página mostrará ao cliente o estado que uma certa página ou elemento referente a uma notícia se encontra. A partir de agora a eficácia, as dificuldades relacionadas a sua implementação, a diferença de percepção por parte de um usário qualquer para os dados marcados e não marcados, e também eventuais vulnerabilidades que esse sistema tenha terá espaço para ser aprofundado.

5 IMPLEMENTAÇÃO E CASOS DE USO

Esse capítulo será dedicado a discussão a respeito do protótipo desenvolvido para o rastreio de notícias. Ele será dividido em quatro partes onde na primeira delas os componentes do protótipo serão estudados, na segunda parte as dificuldades que o desenvolvimento do projeto passou, na terceira as vantagens que logo a principio aparecem, os possíveis ataques pelos quais a solução está sujeita e por último as possíveis soluções de contorno.

O protótipo foi desenvolvido e nomeado de *News Origin Verify* e para futuras referências será chamado assim.

5.1 DESCRIÇÃO DOS COMPONENTES DA EXTENSÃO CRIADA

A *News Origin Verify* será composta de dois elementos visuais. O *popup* que exibirá a informação relacionados aos metadados ligados a página (tag *meta*) e o modal que aparecerá flutuando sobre os elementos marcados que façam referência a outra notícia. Com isso a extensão será descrita a partir da visão tecnológica para construí-la.

Os desenvolvedores do navegador Google Chrome, quando pensaram na criação de extensões para o navegador tiveram um grande foco na segurança de seus usários, não apenas por causas deles, mas também pela responsabilidade na qual pode ser atribuída a empresa por ter a distribuição dos mesmos elementos na sua loja online a *Chrome Web Store* que é focada na venda e distribuição dessas ferramentas e também de temas para a personalização dos mesmos. Para cuidar dessa segurança as extensões tem um arquivo que trata da autorização de cada componente, o arquivo *Manifet* que será descrito a posteriori.

Além do arquivo *Manifest*, no protótipo desenvolvido foram incorporados quatro outros arquivos contendo *scripts*: o *background.js* que é como se fosse o "coração da extensão", o *popup.js* que controla o comportamento da página do *popup*, responsável por mostrar o estado dos metadados inscritos em uma página inteira dedicada a uma notícia, o *content_script.js* que adicionará o código que controlará o *modal* e por último o *fill_metadata_info_script.js* que é o validador e executor das chamadas as autoridades certificadoras. A seguir são apresentados primeiro a Figura 3 com o diagrama de componentes e seus contratos de forma que o sistema funcione da forma esperada e em segundo a Figura 2 com o diagrama de sequência de como cada componente do sistema interage para dar a extensão criada o funcionamento esperado em cada fluxo de execução que o sistema tem.

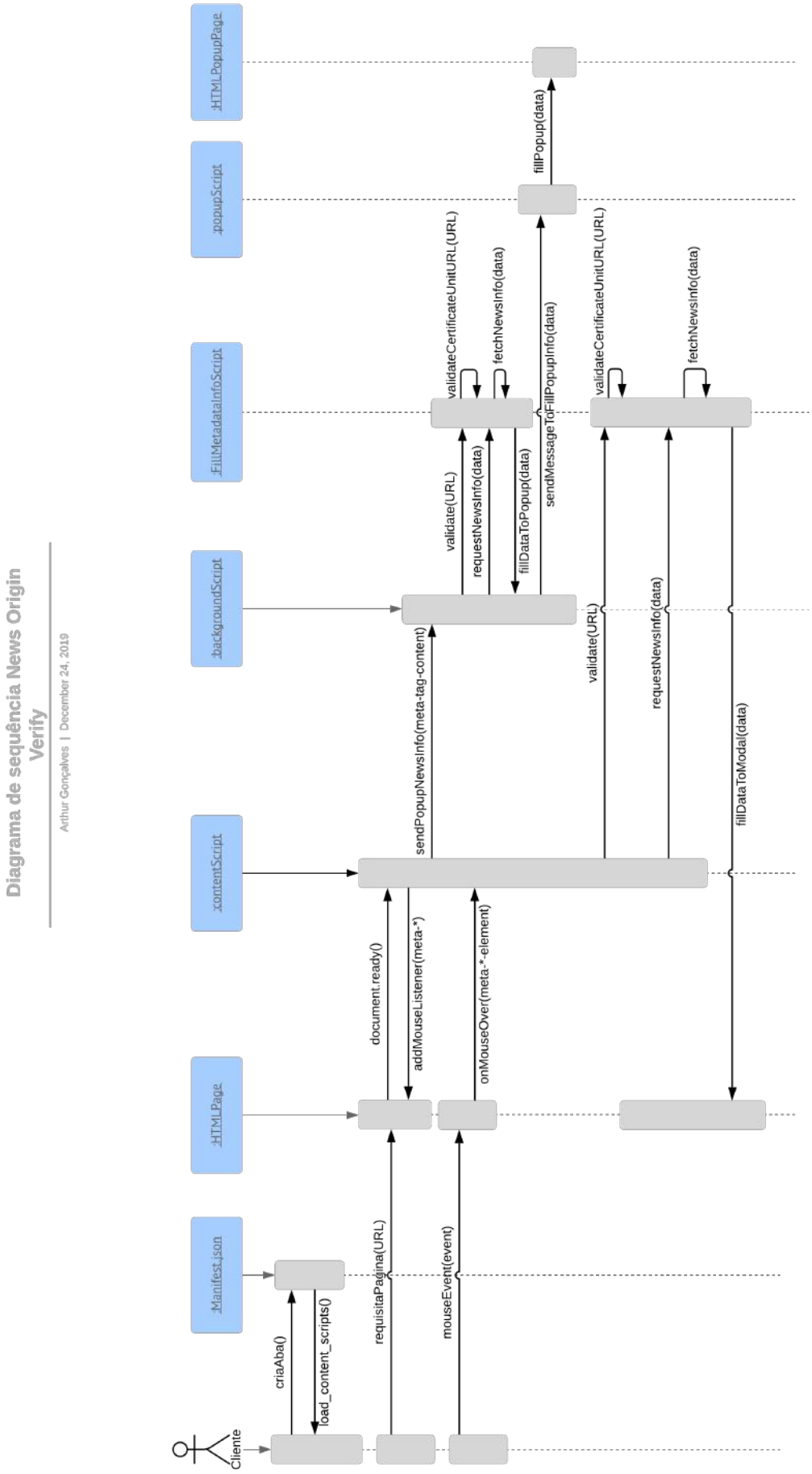


Figura 2 – Diagrama de Sequência News Origin Verify

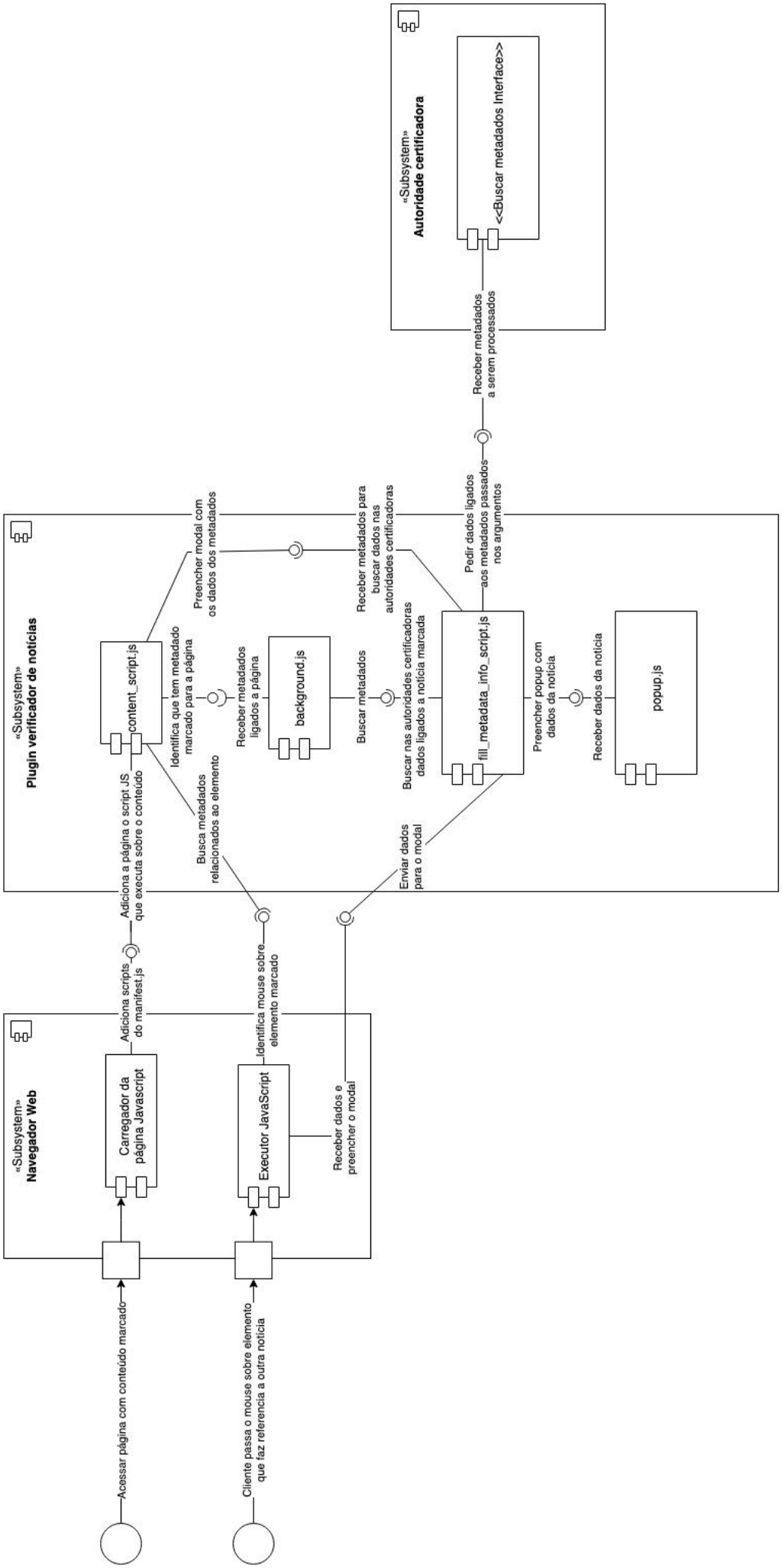


Figura 3 – Diagrama de Componentes News Origin Verify

A seguir todos os componentes citados nessa sessão terão seus detalhes explicados mais a fundo na busca de um melhor entendimento de cada um deles.

5.1.1 Arquivo *Manifest*

Para a criação de uma extensão toda ferramenta disponível pelo navegador como câmera, *bluetooth*, sistema de arquivos, arquivos e pastas da extensão devem ser registrado no *Manifest* que tem o papel de controlador de permissões da extensão. Dessa forma evita-se que os scripts criados pela extensão tenham acesso a mais ferramentas do que deveriam dentro do navegador e também do ponto de vista de segurança evita que em um possível compromentimento da extensão, o navegador dê plenos poderes ao atacante, dessa forma se uma extensão for corrompida apenas os recursos disponíveis a ela estarão sucetíveis de serem usados pelo executor do ataque.[1]

No anexo A.1 tem-se o *Manifest* desenvolvido para o protótipo, nele é possível ver a adição dos scripts de plano de fundo *background.js* e *fill_plugin_info.js*, como também a adição dos scripts que serão executados sobre o conteúdo da página carregada *jquery.js*, *fill_modal_info.js* e *contentScript.js* e a permissão para que esses scripts sejam adicionados em todas as páginas (que é possível ser visto no atributo "*matches*"que contém uma expressão regular que casa com todo tipo de URL que o navegador vier a acessar), além da permissão de acesso ao arquivo *server.json* que será usado para consultar o status das autoridades certificadoras que o sistema considera confiáveis e também a definição da página do *popup* presente no atributo "*page_action*"do *JSON*.

5.1.2 *Scripts* que executam sobre a página

Os *scripts* que são incorporados a página do cliente são três, (i) *jQuery.js* que é uma biblioteca com uma série de métodos para trabalhar com os buscadores do *JavaScript* de forma mais fácil e intuitiva, (ii) *content_script.js* que é o arquivo contendo o coração da busca pelos metadados marcados pela página cliente e por último (iii) o arquivo *fill_metadata_info_script.js* que é um arquivo contendo métodos auxiliares para trabalhar com as requisições as autoridades certificadoras que vierem a ser mencionadas nos metadados do atributo global *data-**. Junto a esses scripts está o arquivo *servers.json* que contém a lista de autoridades certificadoras e a validade de sua certificação de segurança.

O *jQuery* é um framework desenvolvido para a linguagem *JavaScript* que segue a filosofia *write less* que traduzido na sua forma literal é "ecreva menos". Ela tem o intuito de facilitar o código necessário a um desenvolvedor para acessar os elementos de uma página HTML. Para a extensão criada, ela foi utilizada na versão *v3.4.1* no intuito de facilitar o acesso ao conteúdo das tags *meta* e dos atributos *data-** e também para

[1] Para se aprofundar ou saber mais sobre o arquivo *Manifest* aqui explorado é recomendado a leitura da documentação referente ao arquivo Manifest 2.0 2019.

facilitar a alteração do código que aparece no *modal* além de facilitar a construção das requisições a autoridade certificadora.

O arquivo *content_ script.js* que se encontra no anexo B.1 tem duas atribuições (i) quando a página é carregada, ele deve buscar pela presença da tag *meta* que tenha os metadados *name=news-origin-url*, *name=news-origin-base-path* e *name=news-record-id* e assim alertar para o script em *background.js* quais são esses dados; (ii) controlar como funciona o modal que aparece quando algum elemento que contenha o atributo global *data-type=news* exista, dessa forma ele deve buscar se a autoridade certificadora citada é válida e o estado da notícia nela marcada; além disso esse script configura para quando se sair do modal que o mesmo seja removido da visão do cliente e não atrapalhe sua experiência de uso.

O último arquivo de scripts *fill_ metadata_ info_ script.js* que se encontra no anexo C.1 tem três responsabilidades: (i) fazer a validação da URL da autoridade certificadora, (ii) verificar se a mesma se encontra na lista dentro do arquivo *servers.json* com informações válidas como por exemplo prazo de validade que a mesma foi certificada para avaliar notícias como confiáveis e ainda (iii) requisita a autoridade certificadora os dados referentes ao status da notícia que o usuário está com o mouse sobre.

O arquivo *servers.json* existe para de forma estática destacar quais são as autoridades certificadoras confiáveis a discriminar o estado de uma notícias. Ele tem três metadatados *url*, *path* e *expiration_ date* que servem para discriminar o caminho a se requisitar as informações referentes a uma notícia e o tempo pelo o qual aquela entrada está apta a discriminar o estado de uma notícia.

5.1.3 *Scripts* de plano de fundo

Os *scripts* que executam no contexto de plano de fundo da extensão são três, (i) *jQuery.js* que é uma biblioteca com uma série de metodos para criar de forma mais fácil a requisição as autoridades certificadoras vistas como confiáveis pela extensão (já citado na sessão anterior), (ii) *backsgroud.js* que é o arquivo contendo o coração da execução da extensão e por último (iii) o arquivo *fill_ metadata_ info_ script.js* que é o mesmo arquivo citado na seção anterior, porém nesse caso ele trabalha com os metadados da tag *meta* e também o arquivo citado preenche os dados do *popup*. Junto a esses scripts está também o arquivo *servers.json* também já descrito acima.

O script *background.js* apresentado no anexo D.1 existe para alterar o ícone da extensão. Para que essa alteração ocorra então uma requisição a autoridade certificadora é feita. Com o dado retornado é aproveitado para preencher o *popup*, esse processo não é feito no script que controla o *popup* uma vez que apenas nesse ambiente a extensão é autorizada a alterar o ícone que aparece na barra de favoritos do navegador. No processo de desenvolver a extensão a possibilidade de fazer duas requisições foi abordada, uma para adequar o ícone da extensão e outro para preencher o *popup*, mas na ideia de se manter

a integridade dos dados ao máximo possível, o retorno da autoridade certificadora foi aproveitado. O ícone da extensão pode variar então de três formas: (i) quando a notícia está com metadados corretamente preenchidos um ícone verde aparece, (ii) a autoridade certificadora não está dentre as reconhecidas um ícone vermelho e (iv) em uma página que não representa uma notícia, ou seja, não tem metadados marcados um ícone padrão é configurado para a extensão. Essas cores foram inspiradas em um semáforo de trânsito, com o verde representado que a informação está certa e portanto o leitor pode continuar seu acesso, e o vermelho de alerta para o conteúdo na qual ele deve "parar"e refletir a respeito do que lê.

5.1.4 *Popup*

A partir de agora o elemento visual *popup* será estudado, assim como os estados que ele pode aparecer. De acordo com a documentação do Google Chrome para a construção de extensões o *popup* é uma página HTML exibida em um janela especial logo após a barra de ferramentas do navegador. Nessa página o desenvolvedor pode colocar itens de interação ou mesmo mensagens a serem passadas ao usuário que utilizá-la. A exposição de uma mensagem ao usuário é o uso que será dado ao popup.

A extensão criada foi desenvolvida em cima de dois elementos visuais, o *popup* e o *modal* o primeiro está diretamente ligado ao estado na notícia marcada para a página como um todo, a seguir na Figura 4 apresenta um exemplo tirado do *G1* desse tipo de página que deverá vir marcada com metadados a serem exibidos no referido elemento visual.

Figura 4 – Exemplo de página dedicada a uma notícia

O *popup* pode apresentar três possíveis estados, onde (i) reflete o caso de uma notícia com os metadados marcados e válidos, (ii) é exibido no caso de uma notícia com os metadados marcados inválidos e (iii) quando não tem metadado marcado referente a toda a página, em outras palavras, não tem a presença das *meta* tags para notícia na página.

Na Figura 5 a seguir, tem a imagem que representa como o *popup* fica caso seja validado que a unidade certficadora citada pela página está correta, que nela a notícia está com o *ID* gravado e quais são os dados a respeito dessa notícia. Esse dado gravado na autoridade certificadora é de extrema importância, dado que ele terá o papel de segunda verificação por parte do cliente e o link salvo poderá ser utilizado para ascender a página dedicada a tal notícia se essa já não for a página atribuida na autoridade certificadora.

Figura 5 – Exemplo de popup com metadados validados pela autoridade certificadora

Por outro lado se alguma falha ocorrer na validação dos metadados marcados na

página, no *popup* terá o motivo da falha de validação e o ícone ficará vermelho como mostra a Figura 6. As falhas da validação podem ocorrer em três situações, (i) a autoridade certificadora citada é inválida, (ii) dado que é valida o registro pode não estar salvo na mesma ou ainda (iii) que o registro foi revogado como ocorre em caso de informação divulgada de forma errônea ou que ainda apresente uma errata.

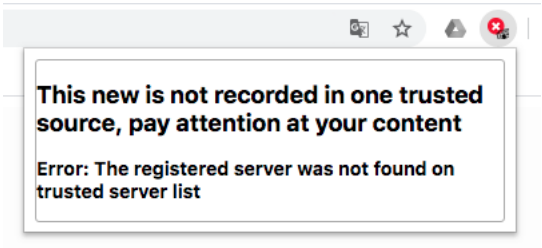


Figura 6 – Exemplo de popup com metadados inválidados

De acordo com a documentação do Google Chrome caso a página contexto para a execução da extensão não se aplique, um ícone em escala de cinza deve ser colocado para simbolizar tal comportamento. E no caso de páginas que não são dedicadas a uma notícia, ou seja, sem os metadados na tag *meta*, que é o onde o *popup* perde a utilidade esse ícone é configurado conforme pode ser visto na Figura 7.

Figura 7 – Exemplo de popup com desabilitado

5.1.5 Modal

O modal no "*News Origin Verify*"é o elemento gráfico ligado aos componentes do HTML que fazem referência a notícias que se encontram em outra página, em outras palavras, é o item gráfico que aparece quando se tem marcado o atributo global *data-type="news"* em um elemento.

Abaixo estão dois exemplos de páginas que podem conter esse tipo de marcação, a Figura 8 mostra o feed do Facebook que referencia várias notícias, já a Figura 9 é o rodapé do portal UOL com apontadores para outras notícias. Nelas podem incluir os marcadores para a autencidade do conteúdo que essas páginas fazem a divulgação e se valerem desse elemento para mostrar que o que tem ali é confiável.

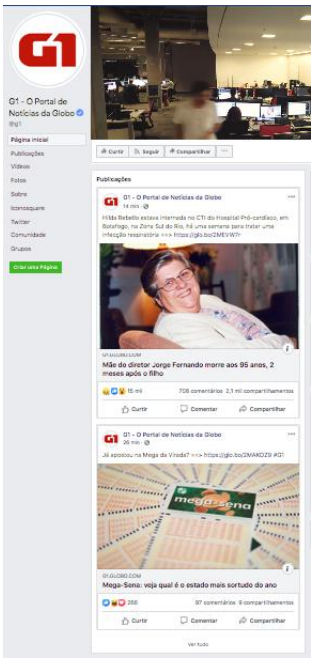


Figura 8 – Feed do Facebook

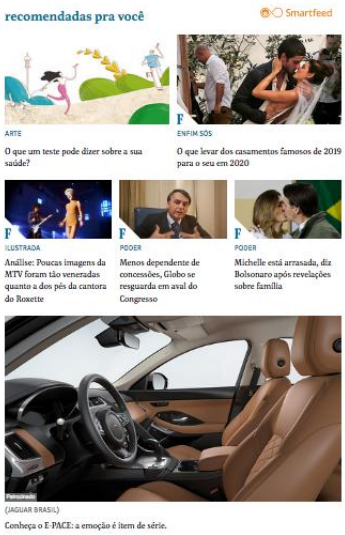


Figura 9 – Rodapé do portal UOL

Dessa forma quando o cliente arrasta o mouse sobre um item que tem o argumento *data-**, aparecerá o modal com o estado dos dados registrados na autoridade certificadora. Como já foi dito esses dados podem se encontrar de três formas (i) com autoridade certificadora e dados válidos, (ii) com autoridade certificadora inválida e (iii) autoridade certificadora válida mas dados inválidos ou não encontrados. No primeiro estado o *popup* mostrará os dados salvos na autoridade certificadora (Figura 10 para a checagem pelo usuário do que foi referido e para os outros dois estados o erro encontrado será exibido (Figura 11 e Figura 12.

Figura 10 – Exemplo de modal com dados validados

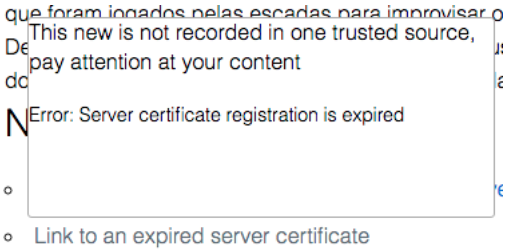


Figura 11 – Exemplo de modal com autoridade certificadora inválida

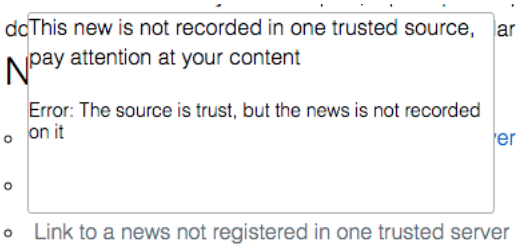


Figura 12 – Exemplo de modal com dado não registrado na autoridade certificadora marcada

5.2 DESCRIÇÃO DAS DIFICULDADES ENCONTRADAS

Durante a produção do protótipo *News Origin Verify* uma serie de problemas apareceram. Alguns dos quais foram separados e serão discutidos a seguir, como problemas ligados a resposta do servidor da autoridade certificadora, o uso do *popup*, a biblioteca para facilitar o desenvolvimento em *JavaScript* o *jQuery*, o banco de dados de autoridades certificadoras e o design visual da extensão.

5.2.1 Servidor não responde

A extensão foi construída na ideia do melhor caminho possível, que todo o aparato tecnológico estaria disponível para consultas e interações. Durante o desenvolvimento, a possibilidade desse cenário não ser real e ter a situação da autoridade certificadora não responder ocorreu.

Uma vez com a autoridade certificadora fora significa que do ponto da extensão ela não sabe como está os dados referidos e para tal o navegador deve estourar um erro no *console javascript* para sinalizar tal ocorrido, e para o cliente nada deve ser exibido nem o *popup* e nem mesmo o modal deve aparecer sobre os elementos que estiverem marcados, que assim se espera passar ao usuário a ideia de que a extensão apenas exibe a informação que ela tem disponível, na busca de atingir mais confiabilidade e também que não atrapalhe a experiencia de uso do cliente no dia-a-dia.

5.2.2 Popup

Quanto ao *popup* o problema enfrentado foi com a comunicação com os outros elementos da extensão. Uma vez que ele reage dado os metadados marcados no conteúdo da página HTML do cliente e esse script ligado ao conteúdo da página tem permissão somente para se comunicar com o script de plano de fundo. Um segundo problema é que o script do *popup* precisaria se comunicar com o script de plano de fundo para alterar o ícone que aparece na extensão.

O primeiro problema foi contornado com o envio de uma mensagem do script adicionado ao conteúdo da página cliente *content_script.js* para o script de plano de fundo *background.js* e dessa forma o script de plano de fundo armazena os metadados capturados.

Se for pensar na distribuição de responsabilidades o script do *popup* que deveria ter os dados para sua exibição. Uma vez que o dado já está salvo no script de plano de fundo (*background.js*) e é esse que altera o ícone da extensão, foi então movido o preenchimento do *popup* para o *background.js* e apenas os dados já processados serão enviados ao script do *popup* para preenchê-lo.

Ainda assim com essa redistribuição de responsabilidades o *popup* apresentava um problema. Pois sua carga é feita posterior a execução do *background.js* e a mensagem contendo o dado processado era perdida. A solução de contorno foi intuitiva, onde o plano de fundo processa e não faz o envio do dado, uma vez o *popup* pronto para a recepção dos dados ele faz a requisição para o script de plano de fundo.

5.2.3 Uso da lib *jQuery*

O uso da biblioteca *jQuery* a principio se mostrou muito promissor e permitiu que o protótipo fosse desenvolvido bem mais rápido do que se esperava. Porém um problema apareceu nas baterias de testes com um dos vários portais que divulgam notícia no Brasil, o Google Notícias.

Em suma o problema que apareceu foi relacionado ao principal operador do *jQuery* o "*$*"que funciona para iniciar a execução de qualquer código que vá usar a biblioteca. Todos os portais relacionados ao Google utilizam esse mesmo operador em seus códigos

JavaScript para métodos próprios e com seus comportamentos espcíficos. Quando tem o *jQuery* carregado nas páginas do Google, a biblioteca não funciona, e como toda extensão se baseia em procurar os dados na página HTML do cliente a extensão falha.

Como o comportamento citado não influencia nos objetivos do trabalho, tal problema foi deixado para ser corrigido em um trabalho futuro e assim o foco se manteve no desenvolvimento de funcionalidades para a ferramenta.

5.2.4 Banco de dados de autoridades certificadoras

O Google Chrome oferece dois métodos de armazenamento de dados para uma determinada extensão, são elas o *storage.local* e o *storage.sync* a primeira das duas salva o dado em um banco de dados local e a segunda sincroniza essa informação com a nuvem e todos os navegadores que ligados a mesma conta Google terão acesso a esses dados desde que ligados a internet. O porém desse banco de dados é que eles são compartilhados com todos os aplicativos no navegador, ou seja, uma outra APP pode se passar pela extensão criada e injetar novas autoridades certificadoras na lista de unidades autorizadas, sem que o cliente tenha consciência desse comportamento. Isso foi cosiderado fraco para a segurança da extensão, e outra abordagem precisou ser criada.

A solução de contorno tomada foi engessar a confiança do protótipo a apenas autorizar a consulta em autoridades certificadoras presentes em uma lista estática o *servers.json* que já foi descrito na seção "Descrição dos componentes da extesão criada". Dessa forma apenas os servidores descritos no momento do empacotamento da extensão estarão autorizados a discriminar o estado de uma dada notícia.

5.2.5 Design visual

A criação de uma identidade visual é um grande problema da extensão. Apesar de os componentes funcionais serem mostrados da mesma forma e exibirem os dados iguais e terem uma coesão entre os elementos que estão presentes a extensão exibe apenas texto limpo no *modal* e no *popup* e isso o deixa com um aspecto pouco profissional e ainda perde um pouco da confiabilidade que é o desejo de um sistema que busca ter a ideia de atestar confiança.

Porém como o sistema desenvolvido se trata de um protótipo, e o funcionamento correto do mesmo é o maior desejo a ser alcançado esse desafio da interface visual da extensão foi deixado para posteriori.

5.3 EXEMPLO DE USO

Nessa seção será mostrado como o protótipo desenvolvido funciona. Para isso cada situação será enumerada e descrita como e porque se encontra dessa forma. De forma básica existem dois momentos que o protótipo reage que é (i) quando tem metadado

marcado que referencia a página toda (dentro da tag *meta*) e (ii) quando tem alguma âncora que aponte para outra página que referência um conteúdo (dentro do argumento *data*).

No caso de referência a toda a página pode-se ter as situações de (i) quando é uma referência reconhecida por uma autoridade certificadora e essa autoridade certificadora é válida, (ii) é uma referência a uma autoridade certificadora com validade expirada, (iii) referencia a uma notícia que não se encontra em uma determindade autoridade certificadora válida ou (iv) quando os metadados referenciam a uma autoridade certificadora inválida.

No caso de referência a outra página todas as situações listadas no parágrafo anterior se fazem válidas.

5.3.1 Metadados referentes a página corrente

Nessa parte do trabalho será demonstrado como o protótipo desenvolvido se comporta quando há a presença de metadados na tag *meta*, ou seja, que refencia ao conteúdo da página atual.

5.3.1.1 O metadado é reconhecido e está em uma autoridade certificadora válida

Ao acessar a página que tiver os metadados na tag *meta* (como pode ser visto na Figura 13, o ícone do plugin mudará para verde e ao clicar sobre ele será mostrado os dados salvos na autoridade certificadora para dar ao usuário informações e possibilitar ao mesmo checar a correspondência dos dados como é visto na Figura 14.

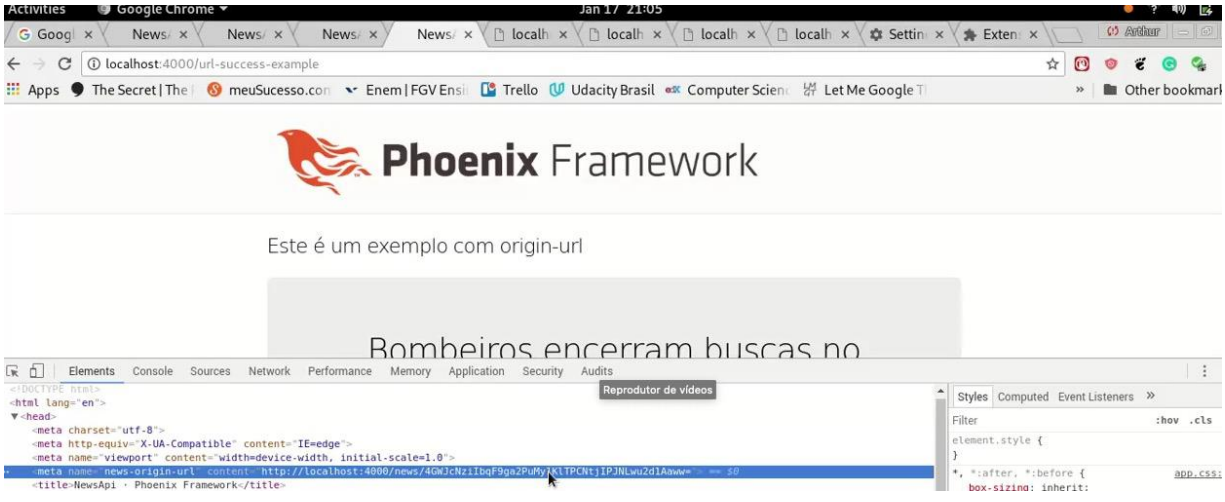


Figura 13 – Exemplo de página com metadados validados pela autoridade certificadora

Figura 14 – Exemplo de popup com metadados validados pela autoridade certificadora

5.3.1.2 O metadado faz referência a uma autoridade certificadora expirada

Quando acessar a página e os metadados na tag *meta* referenciam uma unidade certifcadora com certificado expirado, o ícode do plugin se apresentará como amarelo e ao clicar sobre ele será exibido a justificativa para tal comportamento. Como é possível ver na Figura 15 a seguir.

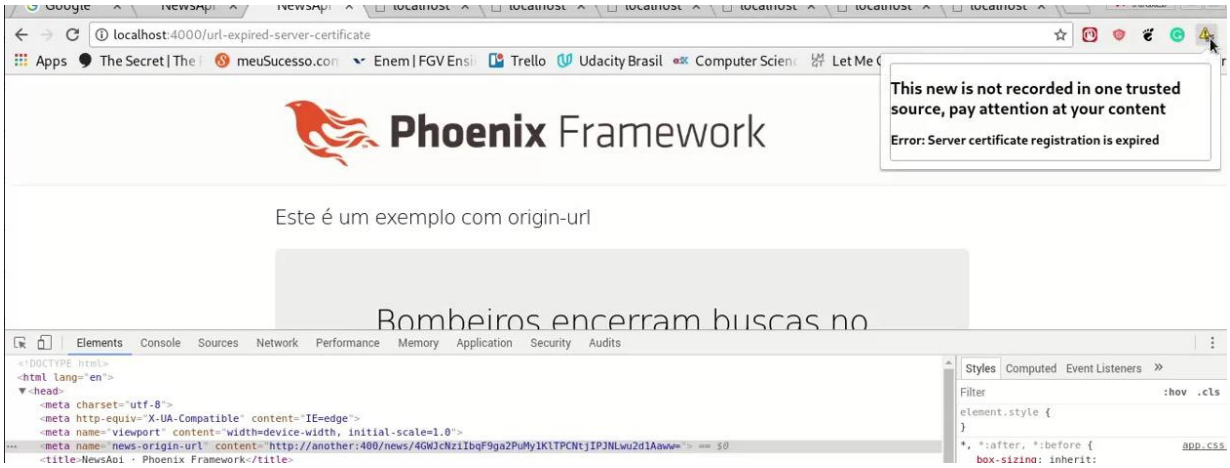


Figura 15 – Exemplo de página com metadados referentes a uma autoridade certificadora expirada

5.3.1.3 O metadado faz referência a uma autoridade certificadora sem o registro

Quando acessar a página e os metadados na tag *meta* referenciam uma unidade certifcadora com certificado válida porém sem referência ao registro, o ícode do plugin se apresentará como amarelo e ao clicar sobre ele será exibido a justificativa para o comportamento. Como é possível ver na Figura 16 e a tag *meta* da mesma página referente a um registro não encontrado (Figura 17).

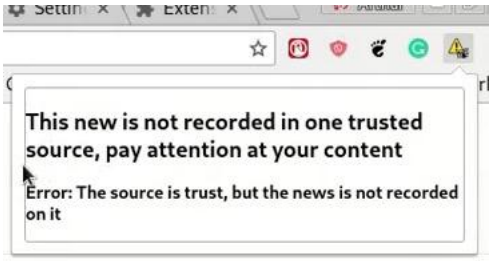


Figura 16 – Exemplo do comportamento do plugin em caso da autoridade certificadora ser válida, porém sem a referência ao registro na mesma

Figura 17 – Exemplo do HTML com a tag meta que referencia a um registro não encontrado na autoridade certificadora

5.3.1.4 O metadado faz referência a uma autoridade certificadora não reconhecida

Quando acessar a página e os metadados na tag *meta* referenciam uma unidade certifcadora inválida, o ícode do plugin se apresentará como vermelho e ao clicar sobre ele será exibido a justificativa para o comportamento. Como é possível ver na Figura 18 e a tag *meta* da mesma página referente a um registro não encontrado (Figura 18).

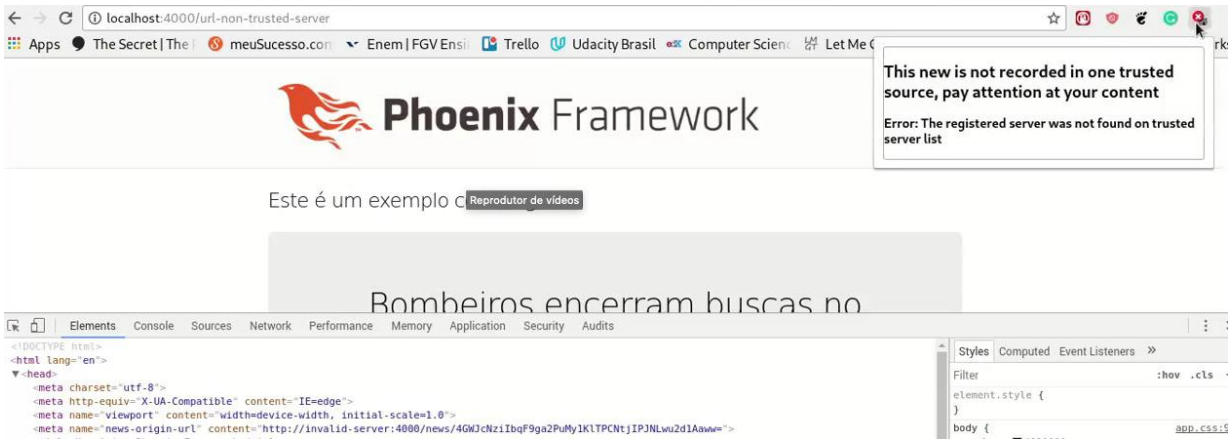


Figura 18 – Exemplo do comportamento do plugin em caso da autoridade certificadora ser inválida

5.3.2 Metadados que referenciam outra página

Os metadados quando presentes no argumento de tag *data* são referentes a outras páginas e apresentam uma forma de registro. Nesse caso o plugin reage a essa presença e apresenta um modal próximo com o estado daqueles metadados e suas referências. Nessa seção será mostrado cada caso e como o modal se apresenta na página.

5.3.2.1 O metadado é reconhecido e está em uma autoridade certificadora válida

Nesse caso o modal aparecerá quando o *mouse* estiver sobre o conteúdo e mostrará os dados salvos na autoridade certificadora referente a esse dado, como pode ser visto na Figura 19 a seguir.

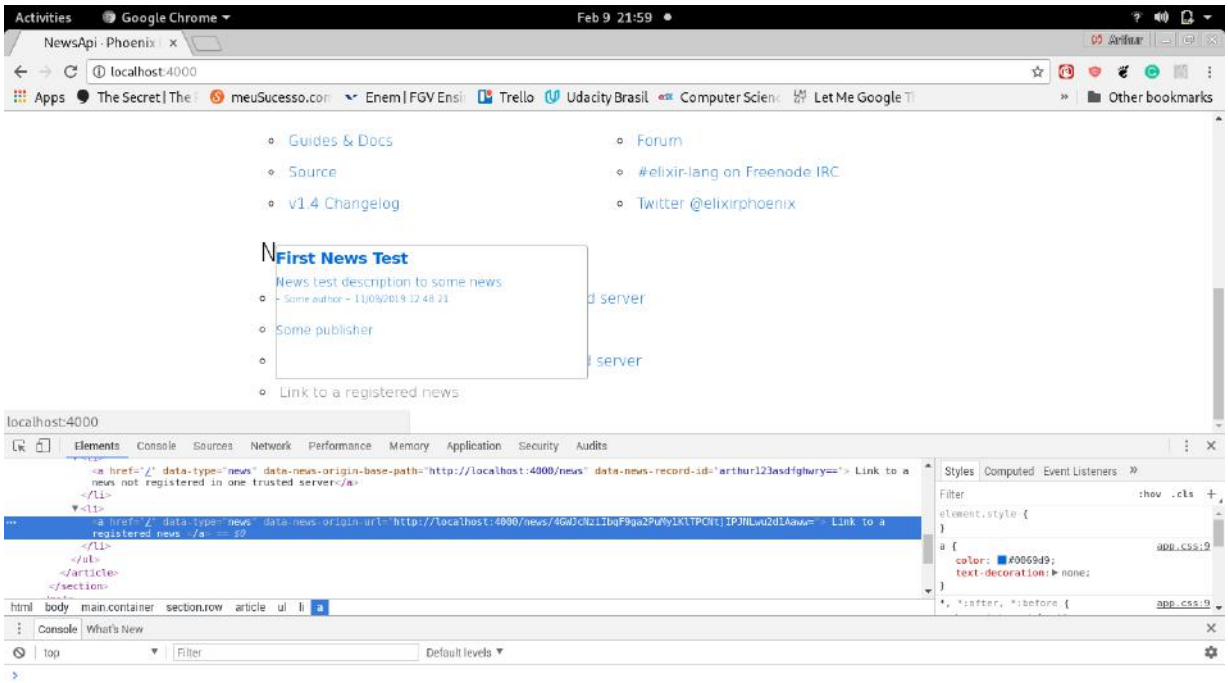


Figura 19 – Exemplo do comportamento do modal em caso da autoridade certificadora e notícia válida

5.3.2.2 O metadado é reconhecido e está em uma autoridade certificadora expirada

Nesse caso o modal aparecerá quando o *mouse* estiver sobre o conteúdo e mostrará uma informação de alerta para o cliente com a motivação para esse alerta como mostra a Figura 20 a seguir.

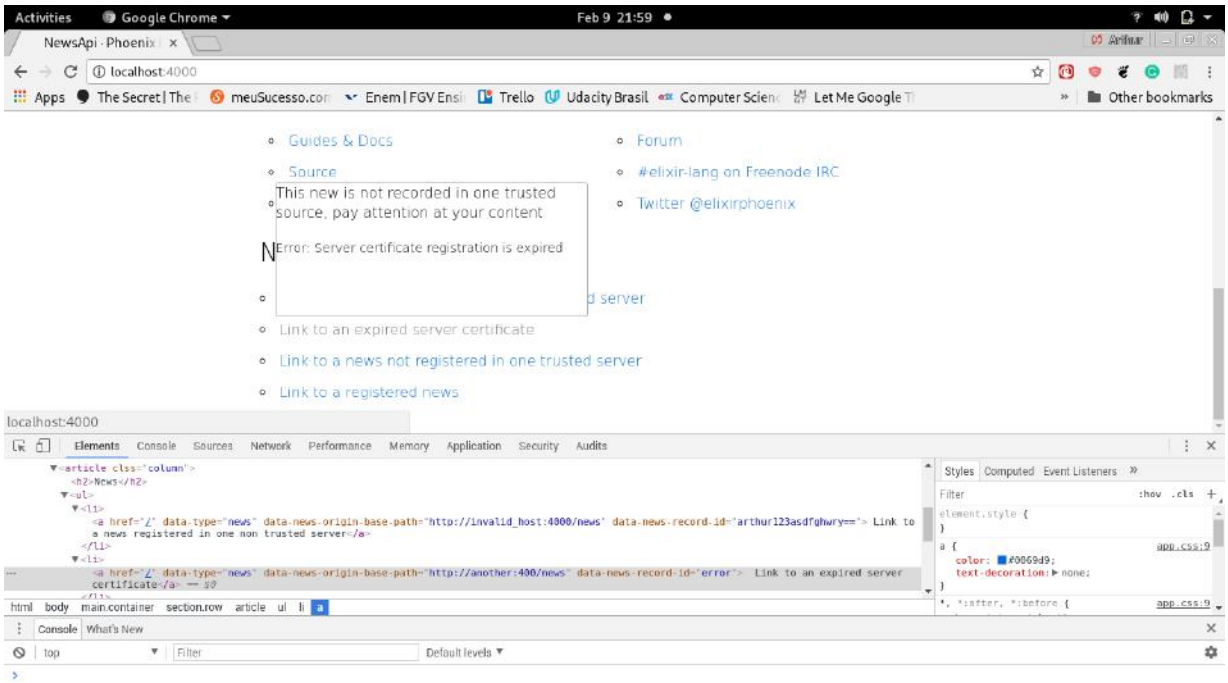


Figura 20 – Exemplo do comportamento do modal em caso da autoridade certificadora expirada

5.3.2.3 O metadado não é reconhecido em uma autoridade certificadora válida

Nesse caso o modal aparecerá quando o *mouse* estiver sobre o conteúdo e mostrará uma informação de alerta para o cliente com a motivação para o mesmo como mostra a Figura 21 a seguir.

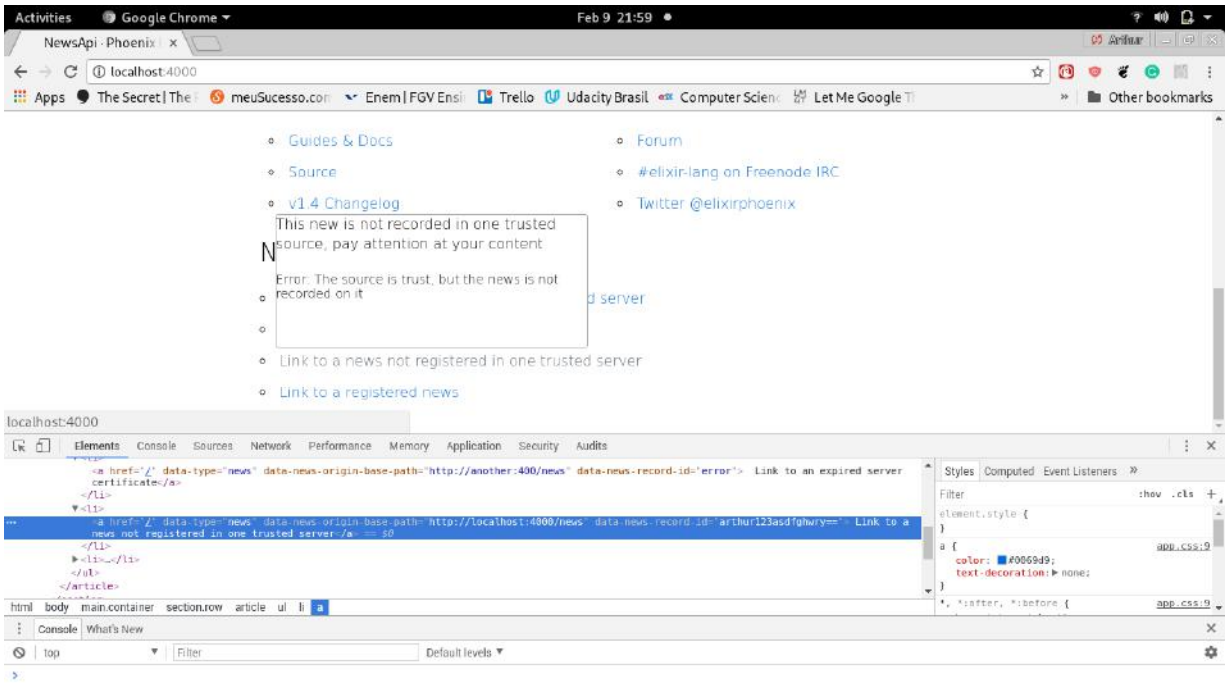


Figura 21 – Exemplo com o modal em caso de notícia sem registro em uma autoridade certificadora válida

5.3.2.4 O metadado e autoridade certificadora não reconhecidos

Nesse caso o modal aparecerá quando o *mouse* estiver sobre o conteúdo e mostrará uma informação de erro para o cliente com a motivação para o mesmo como mostra a Figura 22 a seguir.

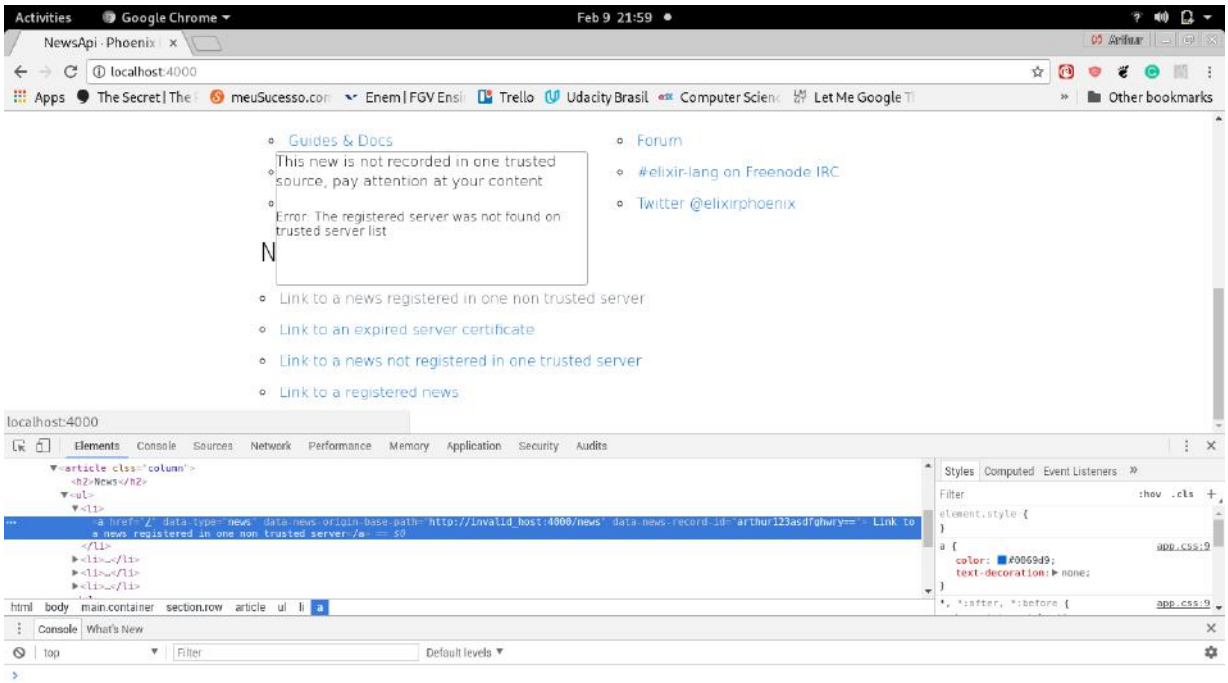


Figura 22 – Exemplo com o modal em caso de notícia e autoridade certificadora não reconhecidos

5.4 TENTATIVAS DE ATAQUE

A abordagem aqui proposta pode sofrer com atores maliciosos, essa seção será dedicada a discutir esses possíveis ataques e algumas soluções para os problemas citados. A primeira parte será a subversão do texto ao qual a notícia está associada, a segunda é o apontamento para uma página diferente na blockchain e a terceira será como trabalhar com uma autoridade certificadora de baixa qualidade.

5.4.1 Mudança de sentido do texto

A primeira ideia que vem quando se pensa em um ataque a esse modelo de metadados é colocar um título diferente do que se trata aquele referido texto nas marcações. Para isso a presença do plugin no navegador tende a dar a oportunidade do leitor de averiguar o que se tem salvo na blockchain ou mesmo acessar o texto original e a partir de então tirar a conclusão sobre a veracidade, ou melhor, o sentido da citação que é feita.

Se partir de um cenário onde não tem o plugin no navegador do usário o que ocorreria é a incorporação de uma citação a um texto que não condiz com a informação a ser transmitida, que é a definição de uma *fake news*. Dessa forma a presença do *"News Origin Verify"* por si só se mostra vantajosa.

5.4.2 Metadados para outra página

Outro problema que pode ocorrer quando se tem o plugin incorporado no navegador é a exploração da falta de visibilidade inicial quanto aos dados marcados que representam a página inteira. Pois esses dados por definição são exibidos no modal do plugin e este por sua vez muda a forma do ícone que o exibe.

A tal prática o plugin é vulnerável, mas se partir do ponto onde antes nem essa segunda verificação era possível, já tem-se uma abordagem capaz de diferenciar uma página de notícia marcada ou não com bons dados. Se o cliente desconfiar do texto apresentado, pode ir no modal e verificar quais são os dados marcados na autoridade certificadora, ou mesmo acender a página que originou tal metadado e fazer a verificação direta.

5.4.3 Autoridade Certificadora com notícias de baixa qualidade

Dado uma autoridade certificadora que está presente na lista das que o plugin confia, em um determinado momento por questões quaisquer ela pode passar a aceitar notícias que de maneira geral os clientes não consideram como boas, ou melhor, aquelas cujas aprensentam notícias duvidosas e que não são confiáveis. Esse problema da forma como o plugin está para corrigí-lo deve ser lançado uma nova versão na qual a tal autoridade certificadora não consta entre as confiáveis pelo sistema.

Ainda na mesma linha desse problema que está em discussão foi adicionado um tempo de expiração para toda autoridade certificadora, no qual após esse tempo os desenvolvedores, ou atores que cuidam do plugin devem se certificar a respeito da satisfação dos usuários e também da qualidade das notícias.

5.5 DESCRIÇÃO DAS VANTAGENS DA SOLUÇÃO

Ao concluir o desenvolvimento do protótipo e tê-lo em execução, alguns diferenciais interessantes para um usuário interessado na qualidade do conteúdo que consome e faz uso do sistema apareceram. Será discutido as vantagens dessa abordagem correlacionada com os trabalhos que serviram de base para o projeto e como dito no Capítulo 1 um usuário está sujeito a compartilhar *fake news* por dois fatores: sociais e psicológicos. A partir daí serão discutidos os diferenciais baseadas nesses dois quesitos, também da parte tecnológica será analisado os potenciais usos dessa abordagem sugerida e a comparação com os demais trabalhos.

5.5.1 Diferenciais sociais

Segundo Shu et al. (2017, tradução nossa) baseado na teoria da prospecção o processo de tomada de decisão de um indivíduo é feito baseado nos ganhos e perdas

relativos ao estado atual da pessoa dentro de seu ciclo social. Elas tendem a sempre querer maximizar seus ganhos sociais e ter mais aceitação pelos outros membros de sua rede.

Tal aspecto citado no parágrafo anterior é um dos fatores que contribuem para a disseminação de *fake news*, pois os indivíduos tendem a não se importar com a origem do que é compartilhado em troca de serem mais visíveis em sua rede social.

A extensão tende a se aproveitar da teoria da prospecção para coibir a disseminação de *fake news*, uma vez que a abordagem sugerida pela extensão tenha tido aderência na rede social do indivíduo exemplo, ele tenderá a ser penalizado ao compartilhar conteúdo sem certificação de seu conteúdo. Sobre o mesmo processo de penalização para explicar melhor pode-se analisar do ponto de vista de quem recebe uma página que não seja validada e os marcadores da extensão mostrarão o estado que ela se encontra, a partir de então todo conteúdo que vier da pessoa que compartilhou pode ser visto com receio, por poder apresentar ou querer confundir o leitor, e assim os perfis que compartilham muito desse tipo de conteúdo terão dificuldades para encontrar apelo nas redes sociais.

Um outro aspecto ligado a parte social do uso do sistema apresentado vem junto as produtoras de conteúdo. Que podem usar dessa preocupação com a certificação de seu conteúdo como forma de reafirmar sua atenção com o que entrega aos seus consumidores. Os ganhos de publicação de notícias apelativas ou hoje também chamadas de *click baits* geram um grande engajamento inicial, mas a longo prazo conforme os consumidores percebem como funciona tal publicador de notícias os mesmos tendem a se afastar, o registro do que é publicado entra como mais um forma da busca pela aceitação que esses meios passarão.

5.5.2 Diferenciais psicológicos

Quando na presença da extensão, o usuário do navegador preocupado com o que consome estará frente a algumas questões no momento em que recebe um certo conteúdo, como por exemplo em uma dada notícia que a extensão alerte que o conteúdo não é registrado em uma autoridade certificadora confiável levará o leitor a duvidar e refletir sobre a veracidade do que é exposto, ou mesmo o quanto de crédito ele deve dar ao texto ou *link* que ele tenha contato.

Ainda pautado na teoria da prospecção a abordagem sugerida de marcação e exibição do estado de confiança de uma notícia influencia uma pessoa quando na tomada de decisão a respeito do compartilhamento de um conteúdo duvidoso e ainda sem registro. Dessa forma o cálculo de ganhos sociais dessa pessoa a leva a tomar mais cuidado com o que tem repassado aos outros membros da suas redes sociais dado a má aceitação que pode ter quando não tem o atestado de confiança da mesma.

Um outros aspecto que a abordagem oferece aos seus usuário é ter nos dados salvos na autoridade certificadora o apontador para a matéria original. Uma vez que a notícia

refenciada e o texto atrelado apresenta qualquer motivo para a dúvida, então com esse link a notícia original pode ser acessada e uma segunda checagem do conteúdo seria feito a critério de interesse do leitor.

5.5.3 Diferenciais técnológicos

Do ponto de vista tecnológico o uso desses metadados marcados nas páginas da internet dão uma série de potenciais usos, além da extensão criada. Eles podem ser utilizados para melhorar a qualidade dos algoritmos de recomendação nas redes sociais, onde a qualidade da autoridade certificadora citada no conteúdo pode ser ordenada e posto como critério em seus algoritmos de recomendação. Além disso os metadados podem ser utilizados para alertar aos clientes no momento em que compartilham uma determinada página que não tenha os dados válidados por uma autoridade certificadora que a rede social confia.

Além disso as autoridades certificadoras podem fazer a coleta dos dados de acesso a elas e gerar materiais para ser estudado e melhorar as formas como as aplicações consomem seus dados. Que assim se tornarão mais efetivas e úteis no combate a disseminação de notícias *fake*.

Uma outra aplicação que essa estrutura fornece é por parte da autoridade certificadora disponibilizar os dados de acesso as empresas que registram seu conteúdo nela. E assim as mesmas podem direcionar seus investimentos e serem mais efetivas na conquista de consumidores de seus conteúdos.

5.5.3.1 Diferencias comparativos aos demais trabalhos

Quando comparado esse trabalho com os outros algumas vantagens aparecem. Nessa seção vamos discutir cada um deles e suas implicações.

Comparado com o trabalho de Qayyum et al. (2019) em *"Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News"* no qual se apresenta a ideia de usar um algortimo de verificação semântica. O sistema aqui desenvolvido prefere dar mais informações ao usuário que tem mais conhecimento para tomar uma decisão que um algoritmo probabilistico. Além disso os dois trabalhos concordam no controle de escrita na *blockchain* que vai ditar a qualidade dos dados na mesma. O trabalho aqui desenvolvido prevê a possibilidade de revogação e substituição de uma *blockchain por outra*, o que seria um bom acréscimo ao trabalho de Qayyum et al. (2019).

Quanto ao trabalho de Shang, Liu e Lin (2018) *Tracing the Source of News Based on Blockchain"* esse trabalho se mostra com um enfoque dentro do outro, no qual o anterior olha a abordagem de um ponto de vista mais amplo e esse se especializa em como o consumo dos dados da *blockchain* pode ser feito. No entando a diferença entre eles se dá quanto ao conteúdo da blockchain no caso o trabalho daqui confia na idoniedade dos

links na blockchain enquanto o de Shang, Liu e Lin (2018) traz para dentro da *blockchain* todo o conteúdo.

No trabalho de Torky, Nabil e Said (2019) *Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks"* ele prevê a criação de uma rede social que se baseia em *blockchain's* no caso do trabalho aqui o banco de dados é usado para alimentar outros sistemas que queiram se utilizar desses dados. Uma diferença crucial entre os dois trabalho é quanto ao que se salva, no trabalho de Torky, Nabil e Said (2019) salva-se conteúdo mentiroso e no aqui se referencia conteúdo de boa qualidade.

Já no trabalho de Paul et al. (2019) *"Fake News Detection in Social Media using Blockchain"* utiliza-se um sistema colaborativo para atribuir uma nota ao conteúdo do que é publicado. Na *blockchain* são salvos os dados de forma bem parecida com o proposto nesse trabalho com a adição da nota que esse registro tem, ou seja, os dois trabalhos coadunam em sua essência e no final deixam ao usuário a responsabilidade de julgar a qualidade do conteúdo que tem contato.

6 CONCLUSÃO

No decorrer do trabalho procurou-se desenvolver e conceituar uma ideia alternativa para o longevo problema das *fake news*. As principais abordagens em estudo nos dias de hoje estão ligadas a algoritmos probabilisticos e como todo problema resolvido por esse meio tem a possibilidade de retornar respostas inexatas, então uma outra abordagem foi discutida em busca de evitar tal característica por parte do sistema computacional. Para que essa alternativa fosse desenvolvida uma pequena mudança relacionada a como são vistas as notícias publicadas foi necessária. As notícias passaram então a serem olhadas como documentos, no qual suas características como data de publicação, autor e veículo de publicação por exemplo reforçam a validade dessa mudança. Com essa nova visão pode-se pensar na segurança de notícias conforme hoje é visto a segurança de sistemas que trabalham com documentos como (i) disponibilidade, (ii) autenticidade e (iii) integridade da informação contida nelas. Com esse conceito foi pensado uma abordagem que liga uma notícia qualquer a um sistema de confiança, esse sistema trabalha para atestar as informações básicas de uma notícia e também para apontar a narrativa original que serviu de base para o dado compartilhado. Ou seja, as mídias noticiárias viriam com metadados e os sistemas que tiverem implementado essa abordagem terão a capacidade de mostrar ao leitor mais informações relacionadas ao conteúdo e o leitor em posse dessas informações pode tomar a decisão se o que tem contato é uma notícia verídica.

A partir do que foi falado acima percebe-se que os maiores interessados na segurança do que é publicado são os próprios autores e/ou entidades publicadoras como os jornais e para isso eles podem acrescentar em seus conteúdos os metadados ligados ao conteúdo e assim outros sistemas podem consumir esses dados de forma que o usuário confira o que foi publicado, uma espécie de segunda fator de checagem do texto. Então para estudar essa viabilidade o trabalho se focou no desenvolvimento de um protótipo que se utilize desses metadados guardados em uma autoridade certificadora como base para alimentação do sistema que funciona semelhante a um semáforo ligado a qualidade do dado disponiblizado, no qual dados marcados ligados a uma notícia reconhecida por uma autoridade certificadora tem mais relevância e/ou segurança do que aquela marcada mas não reconhecida ou ainda uma marcada mas invalidada. Esse sistema vai demonstrar ao cliente que a empresa na qual ele está consumindo o conteúdo tem a preocupação da validade do que é disponiblizado, dessa forma, cria-se um ambiente benéfico para quem publica e quem lê.

Neste trabalho foi desenvolvido o *"News Origin Verify"* um *plugin* que tem como objetivo verificar a procedência a partir de alguns marcadores semânticos em uma página que representa uma notícia. Ele verifica se essas marcações fazem referência a um dado registrado em uma autoridade certificadora confiável.

A presença desse sistema permite que um usuário acesse a notícia original referida e veja seus dados principais como data de publicação, autor e veículo de publicação. Também no momento que acessar uma página que é origem da referencia uma notícia o sistema verifica se a mesma tem metadados refenciados a alguma autoridade certificadora que o *plugin* confia e dessa forma muda a apresentação dele para passar a mensagem de confiança no conteúdo que ele tem contato.

6.1 LIMITAÇÕES

No decorrer do trabalho a abordagem escolhida apresenta algumas limitações. Que precisam ser esclarecidas para que possam ser estudadas ou mesmo afastar a ideia de uma solução perfeita, ao qual é muito difícil que apareça dado o fenômeno social que as *fake news* apresentam.

A primeira limitação que a abordagem aqui desenvolvida apresenta é quanto a interface do usuário, ela não foi bem desenvolvida por falta de conhecimento e com isso diminui a confiança que o usuário coloca sobre o sistema. Outro ponto ligado a isso é quanto a forma de apresentação dos erros, eles se apresentam como textos em inglês que deveriam ser traduzidos de acordo com a preferência de linguagem do navegador do usuário.

Outra limitação é quanto a gestão de autoridades certificadoras reconhecidas pelo plugin, da forma feita ela é uma lista estática e que deve ser atualizada a cada intervalo de tempo para refletir a evolução das várias autoridades certificadoras que ela aceita. Um modelo mais fluído deve ser estudado mas ele precisa ser construído de uma forma a evitar a confiança em um ator que em um dado momento possa ser imposto certas regras por algum governo ou outro órgão. Além disso outro detalhe importante é quanto ao tráfego dos dados, nenhuma checagem de segurança com o uso de protocolos criptografados foram feitos, inclusive no exemplo utilizado ao longo do trabalho em vários momentos são feitas chamadas com o protocolo *http*, para evitar ataques como *man in the middle* ou mesmo *snnifing* por atores maliciosos esse sistema deve utilizar protocolos que criptografem os dados transitados como por exemplo *https*.

Uma outra questão que esse trabalho não trata é quanto a como utilizar dessa abordagem em sistemas mobile, uma vez que os navegadores apresentam caráter secundário nesses sistemas, um modelo de consumo deve ser pensado. A princípio se os dados tiverem esses marcadores padrões eles podem ser pegos pelos sistemas mobile e utilizado para dar ao cliente mais informações de forma a auxiliá-lo na tomada de decisão a cerca do conteúdo em questão.

Por ultimo e não menos importante outra limitação a cerca do trabalho aqui desenvolvido é que o mesmo indivíduo que são sucetíveis ao viés social e psicológico é dado o papel de julgar quanto a veracidade de um conteúdo, porém isso continua como uma

abordagem sujeita a erros no qual os indivíduos comprometidos se manterão no mesmo posicionamento, mesmo com os alertas dados pelo sistema. Uma solução para isso passa pela forma de apresentação dos sistemas que utilizam essa ferramenta ao qual o trabalho desenvolvido aqui não discute.

6.2 LIÇÕES APRENDIDAS

Ao longo do trabalho varias lições puderam ser tiradas de proveito, tanto relacionadas a abordagem escolhida, como a tecnologia e a implementação feita. Para isso essa sessão vai discutir os principais aspectos percebidos.

O primeiro ponto é quanto a uma solução ideal que não deixe nenhuma *fake news* ser julgada como válida. Essa ideia é muito difícil de se alcançar uma vez que as *fake news* permeiam conceitos como verdade, fato, ponto de vista e opinião, que não são aspectos discretisáveis, dessa forma torna-se muito difícil uma solução ótima para esse problema.

A partir de então começa-se a pensar na solução apresentada, sobre ela o que vale ser ressaltado é que a tecnologia utilizada não soluciona por completo o problema. Nessa técnica ela busca melhorar os sistemas que tentam julgar uma notícia. Para que essa melhora seja atingida essa tecnica busca tirar do sistema computacional a carga de julgar a veracidade, ou a factualidade de um certo conteúdo. Assim o sistema passa a dar mais informação ao cliente para que ele (persona com maior habilidade para tomar uma decisão a respeito da factualidade) faça tal tipo de julgamento por si mesmo, ou seja, o sistema apresentado muda sua posição quando comparado aos sistemas que utilizam das tecnias de inteligência artificial, no qual esses sistemas tentam através da entrada dada apresentar um veredito a respeito da mídia em questão. A tecnica discutida ao longo do trabalho basea-se em marcadores semânticos e autoridades certificadoras e age como um sistema de suporte a tomada de decisão, oferecendo mais conteúdo para que o usuário tenha maior acertividade na sua decisão. Esse aspecto se demonstrou importante a respeito do protótipo desenvolvido uma vez que durante o uso ele não cria a ideia de veredito a respeito do conteúdo, ele apenas adiciona informações que o usuário poderá usar para agregar a sua navegação.

Um outro aspecto que vale ser discutido é quanto a influência do design na percepção de confiança de um usário, esse aspecto foi deixado de lado durante o desenvolvimento do trabalho, por falta de conhecimento de tecnicas de design e interfaces gráficas de uso para o cliente. E nesse quesito o sistema desenvolvido ficou com um aspecto bem aquém de qualquer outro plugin encontrado no mercado.O problema desse aspecto é que por várias vezes quando o modal aparece para o cliente na sua navegação ele acaba tirando um pouco da credibilidade da mensagem passada.

Mas esse papel do sistema de confiança atuar como apoio a tomada de decisão deixa ainda em aberto algumas questões sobre como previnir a rede de tentativas na

alteração do sentido de uma notícia quando feita a referência, pois agora as páginas que fazem citação podem utilizar-se dessa rede para referir outras matérias e assim melhorar a qualidade da experiência do leitor, oferecendo-lhe formas de checar o conteúdo. Para o problema da mudança de contexto do referido fica a cargo do cliente perceber tal tipo de mal uso e reportar a autoridade certificadora que isso está acontecendo e ela por sua vez toma as medidas cabíveis, o máximo que o sistema pode fazer é se o conteúdo atual que refere a uma notícia e altera seu sentido está registrado na autoridade certificadora esse conteúdo pode ser marcado como inválido, e os próximos clientes ao entrar em contat ocom esse conteúdo terá o aviso a respeito.

Outro problema encontrado na abordagem é também quanto a incorporação de metadados referentes a outra notícia confiável numa página qualquer. E as soluções apresentadas no parágrafo anterio se aplicam também a esse problema.

Mesmo com os problemas citados acima, a incorporação de metadados junto ao conteúdo de mídias online quando comparadas a um cenário sem a presença de nenhum sistema apresenta uma forma para que tais informações sejam conferidas e adiciona uma ferramenta para que o cliente tire suas dúvidas e melhore seu julgamento sobre o que é apresentado. Além disso ainda ficam em aberto muitas questões sobre a efetividade do sistema construído cujo qual é uma oportunidade para o desenvolvimento de outros trabalhos.

6.3 TRABALHOS FUTUROS

O tema desenvolvido nesse trabalho é bem amplo e rico, ele tange áreas como design de interfaces com o usuário, sociologia, filosofia, computação, jornalismo dentre outras. Dessa forma várias lacunas ficaram abertas e que oferecem oportunidades para o desenvolvimento de trabalhos bem interessantes. Para melhor organizar a sessão vamos dividir esses trabalho futuros em cinco sub-áreas: (i) efetividade do sistema desenvolvido, (ii) pesquisa de mercado, (iii) design da interface com o usuário, (iv) integração com redes orientadas a conteúdo e (v) autoridades certificadoras.

6.3.1 Efetividade do sistema desenvolvido

O *News Origin Verify* apresenta um sistema de suporte a tomada de decisão interessante, no qual nutre o cliente com a citação original para que ele consiga embasar melhor sua leitura e tire as melhores conclusões dela. Entretanto vários pontos relacionados a sua efetividade ainda ficaram em aberto como a adaptabilidade desse sistema para outras plataformas como o mobile, seria interessante conhecer quais ferramentas ela oferece as redes sociais já existentes nesse mundo como o *Whats App*, *Telegram* e *Instagram*. Além disso o plugin foi feito para o *Google Chrome* na sua versão *desktop* e como seria sua adaptação para ser usado no navegador em outras plataformas que ele se encontra como

por exemplo o *Android*, *iOS* e *Smart TVs*. Essas pesquisas são importantes para enteder o quão adaptável é abordagem de sistemas que se baseiam metadados para os diversos universos das plataformas comercializadas.

Além dessa parte das plataformas ficou em aberto uma questão a respeito de qual o melhor banco de dados para salvar as credenciais dentro dos plugins dos usuários uma vez que o disponibilizado pelo *Google Chrome* compartilha esses dados com os outros plugins de dentro do navegador, o que demonstra um possível alvo fácil de ataques por outras aplicações maliciosas. Tais pesquisas servem para desenvolver um sistema com a menor probabilidade de erro e de vulnerabilidades para o cliente, de forma que ele não passe a ter contato com conteúdo de baixa qualidade marcado como confiável pelo sistema.

6.3.2 Pesquisa de mercado

Uma outra área que o trabalho deixa em aberto é quanto a uma possível adesão pelos agentes de mercado. Toda a premissa para o sistema funcionar é baseado na ideia de que os publicadores de conteúdo vão registrar suas mídias em uma autoridade certificadora. O porém é se eles tem interesse em se integrar com esse tipo de sistema e se existe tal vontade, quais dados eles efetivamente estariam dispostos a colocar para alimentar o sistema, tudo isso soma-se a domínios próprios de funcionamento dos dias de hoje das empresas de conteúdo, como quais operações elas teriam com as autoridades certificadoras de forma a mapear qual é a melhor interação entre as partes alimentadoras do sistema de forma que essa relação seja benéfica para ambos os lados.

6.3.3 *Design* da interface com o usuário

A forma como se comunica com o usuário é muito importante para que se crie o sentimento esperado do mesmo durante sua interação com o sistema. Como o protótipo desenvolvido ao longo do trabalho se preocupou em entender como seria um sistema que se utilize de metadados e não com a forma como o usuário receberia a mensagem passada por ele, fica uma lacula em aberta a se criar uma interface que crie o sentimento de segurança e confiança no usuário. Uma parte fundamental para que se consiga atingir o objetivo que é ter o usuário em contato com conteúdos de melhor qualidade. Se esse sentimento não for gerado o cliente pode passar a ignorar tais informações e a seguir ao modelo de ausência do sistema.

6.3.4 Integração com redes orientadas a conteúdo

As redes orientadas a conteúdo são um novo paradigma de internet que surgiu, no qual partes do núcleo da rede participam ativamente do armazenamento e entrega dos conteúdos multimídias e seus dados associados. A principal vantagem das redes orientadas a conteúdo é a melhor eficiência na entrega de seus conteúdos e metadados sem importar

a localização desse dados originalmente além disso ela apresenta melhorias na segurança e trafego ao longo da rede. Para atingir tal ideal mecanismos como nomeação (no qual atribui-se nomes únicos aos conteúdos para orientar seu armazenamento), cache (salvar dados mais acessados para serem retornados com maior velocidade) e roteamento de conteúdo (os nós tem acesso a uma tabela de roteamento dos conteúdos que elas tem disponíveis) são utilizados conforme disse Brito, Velloso e Moraes (2012).

Como os conteúdos noticiários são uma forma de mídia que trafega na internet, a presença desses metadados associados as notícias podem ser utilizados nas redes orientadas a conteúdo para nomear e melhorar o acesso aqueles dados que são marcados como confiáveis/verificados por uma autoridade certificadora. E ao olhar por outro lado esses metadados podem ser usados para dificultar que os usuários sejam expostos a conteúdos de baixa qualidade. Tal tecnologia promissora deve ser estudada para criar formas positivas de integração entre esses agentes da rede e os sistemas que consumirão os dados trafegados, onde no final o objetivo será a melhoria na qualidade da experiência do usuário.

6.3.5 Autoridades certificadoras

Esse trabalho foi focado no estudo dos metadados ao longo de um conteúdo multimídia e de todo o ambiente que envolve o uso desses dados na WEB, porém uma parte importante para a composição dessa tecnologia não ganhou espaço e que é parte fundamental para que todo ele funcione, a composição de uma autoridade certificadora. Para compor tem-se alguns requsitos: esse sistema precisa-se de uma autoridade certificadora que seja aberta para consulta pública, os dados devem ser imutáveis (uma vez que uma notícia não muda, apenas são feitas correções após sua publicação) e os dados devem estar disponíveis a todo momento.

Muitas tecnologias se fazem candidatas para serem usadas como base de dados para a autoridade certificadora, como vários dos bancos de dados disponíveis no mercado e um api rest para dispor tais informações. Outro exemplo de banco de dados é o Datomic usado por vários sistemas que precisam da propriedade de imutabilidade (COGNITEC, 2021). Uma outra alternativa que tem se demonstrado muito interessante é o uso de *blockchain*, cujo tal banco entrega as três propriedades requeridas pelo sistema e ainda distribui os dados na rede de forma a evitar um único ponto de falha. Além disso a *blockchain* tem os chamados *smart contracts* que permitem a execução de código sobre os dados que a mesma tem, isso pode ser usado para aplicar as alterações que são feitas sobre o texto original publicado e com isso melhorar a qualidade do dado disponibilizado pelas autoridades certificadoras.

Fora o banco de dados a ser usado nas unidades certificadoras fica de trabalho futuro também estudar como seria para os diversos jornais integrar com a tecnologia mais benéfica para esse sistema, por exemplo, como integrar um editorial de um jornal com

uma *blockchain*. E as rotas que devem ser criadas pela API da blockchain para dar vida ao sistema como um todo.

Outro ponto que fica em aberto é quanto a qualidade das notícias que estarão dentro de uma autoridade certificadora, de alguma forma, conteúdo de baixa qualidade deve ser penalizado para não ser veiculado da mesma forma daqueles advindos de boas fontes de conteúdo. E dessa forma evitar que a qualidade da blockchain como um todo decaia com o passar do tempo e tenha que ser limpa a cada intervalo de tempo para manter apenas conteúdos de melhor qualidade.

REFERÊNCIAS

AGNEW, G. **Understanding Metadata**. 2020. Disponível em: https://www.researchgate.net/publication/228822133_Understanding_Metadata. Acesso em: 03 mai. 2020.

AJAO, O.; BHOWMIK, D.; ZARGARI, S. A. Fake news propagates differently from real news even at early stages of spreading. 2018. Disponível em: https://dl.acm.org/doi/abs/10.1145/3217804.3217917#sec-terms. Acesso em: 08 may 2022.

ALLCOTT, H.; GENTZKOW, M. Social media and fake news in the 2016 election. **Journal of Economic Perspective**, v. 31, n. 2, p. 211–236, 2017.

BRITO, G. M. de; VELLOSO, P. B.; MORAES, I. M. Redes orientadas a conteúdo:um novo paradigma para a internet. **XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC 2012**, v. 30, p. 211–264, 2012. Disponível em: http://www2.ic.uff.br/~igor/cursos/files/BVM12.pdf. Acesso em: 03 mar. 2021.

COGNITEC. **Datomic Customers**. 2021. Disponível em: https://www.datomic.com/customers.html. Acesso em: 04 mar. 2021.

CONSORTIUM, W. W. W. **HTML: The Living Standard**. 2019. Disponível em: https://html.spec.whatwg.org/. Acesso em: 25 ago. 2019.

ESTADÃO. 2019. Disponível em: https://www.estadao.com.br/. Acesso em: 27 jul. 2019.

FACEBOOK. 2019. Disponível em: https://www.facebook.com/. Acesso em: 27 jul. 2019.

FOLHA de São Paulo. 2019. Disponível em: https://www.folha.uol.com.br/. Acesso em: 27 jul. 2019.

G1. 2019. Disponível em: https://g1.globo.com/. Acesso em: 27 jul. 2019.

G1, E. editorial. **O que é: Portal**. 2008. Disponível em: http://g1.globo.com/Noticias/0,,MUL414442-15524,00-O+QUE+E+PORTAL.html. Acesso em: 22 abr. 2020.

GARTON, L.; HAYTHORNTHWAITE, C.; WELLMAN, B. Studying online social networks. **Journal of Computer-Mediated Communication**, v. 3, n. 2, 1997. Disponível em: https://academic.oup.com/jcmc/article/3/1/JCMC313/4584354. Acesso em: 23 abr. 2020.

GAZETA do Povo. 2019. Disponível em: https://www.gazetadopovo.com.br/. Acesso em: 27 jul. 2019.

GEORGE, A. **What Are Plugins And How Do They Work?** 2019. Disponível em: https://www.lifewire.com/what-are-plugins-4582189. Acesso em: 17 mai. 2020.

GOOGLE Notícias. 2019. Disponível em: https://news.google.com/. Acesso em: 27 jul. 2019.

HOUAISS, A. **HOUAISS, Grande dicionário**. 2020. Disponível em: https://houaiss.uol.com.br/pub/apps/www/v5-2/html/index.php. Acesso em: 22 abr. 2020.

JUNIOR, E. C. T.; LIM, Z. W.; LING, R. Defining "fake news". **Digital Journalism**, v. 6, n. 2, p. 137–153, 2018.

LAFRATTA, C. **O que é NFT? Conheça a tecnologia que permite comprar um meme**. 2021. Disponível em: https://blog.nubank.com.br/o-que-e-nft/. Acesso em: 25 jul. 2021.

LIU, Y.; WU, Y.-F. Early detection of fake news on social media through propagation path classification with recurrent and convolutional networks. 2018. Disponível em: https://ojs.aaai.org/index.php/AAAI/article/view/11268. Acesso em: 08 may 2022.

MANIFEST File Format. 2019. Disponível em: https://developer.chrome.com/extensions/manifest. Acesso em: 24 dez. 2019.

MANSKY, J. **The Age-Old Problem of "Fake News"**. 2018. Disponível em: https://www.smithsonianmag.com/history/age-old-problem-fake-news-180968945/.

MIP, M. I. P. The meaning of trust in news. **A New Understanding: What Makes People Trust and Rely on News**, p. 4–8, 2016. Disponível em: https://www.americanpressinstitute.org/wp-content/uploads/2016/04/What-Makes-People-Trust-and-Rely-on-News-Media-Insight-Project.pdf. Acesso em: 02 mai. 2020.

MOECKE, C. T. **O que é uma autoridade certificadora e quais são confiáveis?** 2018. Disponível em: https://www.bry.com.br/blog/o-que-e-uma-autoridade-certificadora/. Acesso em: 03 mai. 2020.

NASCIMENTO, M. **Conheça os 5 sites de notícias mais acessados do Brasil**. 2018. Disponível em: https://imperatriznoticias.ufma.br/noticias/cinco-maiores-sites-de-noticias/. Acesso em: 27 jul. 2019.

NGUYEN, B. **Linux Dictionary**. 0.16. ed. Linux Documentation Project, 2003. Disponível em: https://www.tldp.org/LDP/Linux-Dictionary/Linux-Dictionary.pdf. Acesso em: 23 abr. 2020.

NOORDERGRAAF, A. Trust modeling for security architecture development. **Enterprise Security: Solaris Operating Environment, Security Journal, Solaris OEv2.51, 2.6, 7, and 8**, n. 1, 2002. Disponível em: https://www.informit.com/articles/article.aspx?p=31546&seqNum=5. Acesso em: 02 mai. 2020.

O que é um portal? 2020. Disponível em: http://www3.imperial.ac.uk/portalHelp2/ohw/topics/welchelp_hs_BR/welcport.htm?tp=true&locale=pt_BR. Acesso em: 22 abr. 2020.

PAUL, S. et al. Fake news detection in social media using blockchain. p. 1–5, 2019. Disponível em: https://ieeexplore.ieee.org/document/8843597. Acesso em: 01 ago. 2021.

QAYYUM, A. et al. Using blockchain to rein in the new post-truth world and check the spread of fake news. **IT Professiona**, v. 21, n. 4, p. 16–24, 2019.

RESCORLA, E.; SCHIFFMAN, A. M. **The Secure HyperText Transfer Protocol**. 1999. Disponível em: https://tools.ietf.org/html/rfc2660.

SHANG, W.; LIU, M.; LIN, W. Tracing the source of news based on blockchain. **IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore**, p. 377–381, 2018.

SHU, K. et al. Hierarchical propagation networks for fake news detection: Investigation and exploitation. 2020. Disponível em: https://ojs.aaai.org/index.php/ICWSM/article/view/7329. Acesso em: 08 may 2022.

SHU, K. et al. Fake news detection on social media: A data mining perspective. **ACM SIGKDD Explorations Newsletter**, v. 19, n. 1, p. 22–36, 2017.

SILVA, N. M. R. da. Fake news: the revitalization of the newspaper and the effects fact-checking and crosscheck in the digital news. **Temática**, v. 13, n. 08, 2017.

SILVA, P. H.; SILVA, M. B. d. N. Notícia: A fluidez de um gênero. **Anais do SIELP**, Uberlândia, v. 2, n. 1, 2012. Disponível em: http://www.ileel.ufu.br/anaisdosielp/wp-content/uploads/2014/07/volume_2_artigo_249.pdf. Acesso em: 22 apr. 2020.

TORKY, M.; NABIL, E.; SAID, W. 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, p. 321–327, 01 2019.

UOL. 2019. Disponível em: https://www.uol.com.br/. Acesso em: 27 jul. 2019.

WALDROP, M. M. The genuine problem of fake news. **PNAS - Proceedings of the National Academy of Sciences of the United States of America**, v. 114, n. 52, p. 12631–12634, 2017.

YAGA, D. et al. Blockchain technology overview. **NISTIR**, p. 66, 2018.

ZHAO, Z. et al. Fake news propagates differently from real news even at early stages of spreading. 2020. Disponível em: https://epjds.epj.org/articles/epjdata/abs/2020/01/13688_2020_Article_224/13688_2020_Article_224.html. Acesso em: 08 may 2022.

ANEXOS

ANEXO A – MANIFEST.JSON

Código A.1 – manifest.json

```
{
  "name": "News Origin Verify",
  "version": "0.1",
  "description": "From meta-* and meta tag it will find for origin of
     news based on reliable database",
  "permissions": ["activeTab", "storage", "declarativeContent"],
  "background": {
    "scripts": ["node_modules/jquery/dist/jquery.min.js", "
       fill_metadata_info_script.js", "background.js"],
    "persistent": false
  },
  "content_scripts": [
    {
        "matches": ["*://*/*"],
        "js": ["node_modules/jquery/dist/jquery.min.js", "
           fill_metadata_info_script.js", "content_script.js"],
        "file": ["servers.json"]
    }
  ],
  "web_accessible_resources": [
    "servers.json"
  ],
  "page_action": {
    "default_popup": "popup.html",
    "default_icon": {
      "16": "images/get_started16.png",
      "32": "images/get_started32.png",
      "48": "images/get_started48.png",
      "128": "images/get_started128.png"
    }
  },
  "manifest_version": 2
}
```

ANEXO B – CONTENT_SCRIPT.JSON

Código B.1 – content_script.json

```
$(window).on('focus', function(){
    send_popup_news_info();
});

$(document).ready(function(){
    document.body.innerHTML += modal
    var timer;
    $('[data-type="news"]').mouseenter(function(){
        current_object = $(this)
        timer = setTimeout(function(){
            let news_metadata = getNewsMetadataFromGlobalAttributeData(
               current_object)
            fillNewsModal(news_metadata)
            positionModal(current_object)
        }, 1000);
    }).mouseleave(function(){
        clearTimeout(timer);
        if(is_modal_visible()) {
            timer = setTimeout(function(){
                hideModal()
            }, 300);
        }
    });
    $('#news-block').mouseenter(function(){
        clearTimeout(timer);
    }).mouseleave(function(){
        clearTimeout(timer);
        timer = setTimeout(function(){
            hideModal()
        }, 300);
    });
    send_popup_news_info();
});

function send_popup_news_info(){
    let news_metadata = getNewsMetadataFromMetaTag()
    console.dir(news_metadata)
    chrome.runtime.sendMessage({"popup_data": news_metadata}, function(
       response) {})
}
```

```
function getNewsMetadataFromMetaTag(){
    let news_info = {}
    news_info["newsOriginUrl"] = $("meta[name=news-origin-url]").attr("
        content")
    news_info["newsOriginBasePath"] = $("meta[name=news-origin-base-path
        ]").attr("content")
    news_info["newsRecordId"] = $("meta[name=news-record-id]").attr("
        content")
    return news_info;
}

function getNewsMetadataFromGlobalAttributeData(current_object){
    let news_info = {}
    news_info["newsOriginUrl"] = current_object.data("newsOriginUrl")
    news_info["newsOriginBasePath"] = current_object.data("
        newsOriginBasePath")
    news_info["newsRecordId"] = current_object.data("newsRecordId")
    return news_info
}

function fillNewsModal(news_metadata){
    if (!FillMetadataInfoScript.validate(news_metadata)){
        console.log("Error: some news metadata is missing")
        return;
    }
    FillMetadataInfoScript.fetch(news_metadata);
}

function putErrorInfo(error){
    $("#news-block").html(modalWithoutNews(error));
}

function putSuccessInfo(news_info){
    $("#news-block").html(modalWithNews(news_info));
}
function is_modal_visible(){
    if($("#news-block").css("display") == "block"){
        return true;
    }else{
        return false;
    }
}

function hideModal(){
    $("#news-block").css("display","none")
}
```

```
function showModal(){
    $("#news-block").css("display","block")
}

function positionModal(current_object){
    $("#news-block").css("left", leftPosition(current_object))
    $("#news-block").css("top", topPosition(current_object))

}

function leftPosition(element){
    right = element.offset().left + 350
    if (right > $(document).width()){
        return element.offset().left - 345
    }else{
        return element.offset().left - 5
    }
}

function topPosition(element){
    top = element.offset().top - 155
    if (top < 0){
        return element.offset().top + element.height() + 5
    }else{
        return element.offset().top - 155
    }
}

let modal = "\
␣␣␣␣<div␣style='display:␣none;␣border:␣1px␣solid;␣border-color:␣#AAAAAA;
    ␣border-radius:␣3px;␣background-color:␣white;␣␣overflow-y:auto;␣width
    :␣350px;␣height:␣150px;␣position:␣absolute;␣top:␣100px'␣tabindex=-1␣
    id='news-block'>\
␣␣␣␣</div>\
";

function modalWithNews(news_info) {
    return "\
␣␣␣␣␣␣␣␣<a␣href=""+ news_info["url"] + "'␣id='news-url'>\
␣␣␣␣␣␣␣␣␣␣␣␣<h4␣id='news-title'␣style='margin-bottom:␣5px;␣font-weight:␣
    bold;'>"+ news_info["title"] + "</h4>␣\
␣␣␣␣␣␣␣␣␣␣␣␣<h6␣id='news-subtitle'␣style='margin-bottom:␣2px'>"+
    news_info["subtitle"] + "</h6>␣\
␣␣␣␣␣␣␣␣␣␣␣␣<h6>-␣<span␣id='news-author'␣style='font-size:␣10px'␣>"+
    news_info["author"] + "</span>␣-␣<span␣id='news-released-date-time'␣
    style='font-size:␣10px'␣>"+ new Date(news_info["publication_date"]).
    toLocaleString("pt-BR") + "</span></h6>\
```

```
␣␣␣␣␣␣␣␣␣␣␣␣\
␣␣␣␣␣␣␣␣␣␣␣␣<h6␣id='news-publisher'>"+ news_info["publisher"] + "</h6>\
␣␣␣␣␣␣␣␣</a>\
␣␣␣␣";
}

function modalWithoutNews(error){
    return "\
␣␣␣␣<h5>␣This␣new␣is␣not␣recorded␣in␣one␣trusted␣source,␣pay␣attention␣
   at␣your␣content␣</h5>\
␣␣␣␣<h6>Error:␣"+error+"</h6>\
";
}
```

ANEXO C – FILL_METADATA_INFO_SCRIPT.JSON

Código C.1 – fill_metadata_info_script.json

```
class FillMetadataInfoScript {
    static validate(news_metadata) {
        if(news_metadata["newsOriginUrl"] != undefined ||
            (news_metadata["newsRecordId"] != undefined &&
                news_metadata["newsOriginBasePath"] != undefined)
        ){
            return true;
        }
        return false;
    }

    static fetch(news_metadata, sender=null){
        if (news_metadata["newsOriginUrl"] != null) {
            news_metadata = this.parse_url(news_metadata)
        }
        news_metadata = this.ensure_no_slash_on_end(news_metadata)
        this.validate_origin_base_path(news_metadata, sender);
    }

    static ensure_no_slash_on_end(news_metadata){
        if(typeof(news_metadata["newsOriginUrl"]) == "string" &&
           news_metadata["newsOriginUrl"].substr(-1) == '/'){
            news_metadata["newsOriginUrl"] = news_metadata["
               newsOriginUrl"].slice(0,-1)
        }

        if(typeof(news_metadata["newsOriginBasePath"]) == "string" &&
           news_metadata["newsOriginBasePath"].substr(-1) == '/'){
            news_metadata["newsOriginBasePath"] = news_metadata["
               newsOriginBasePath"].slice(0,-1)
        }
        return news_metadata
    }

    static parse_url(news_metadata) {
        let url = news_metadata["newsOriginUrl"].split("/")
        news_metadata["newsRecordId"] = url.pop()
        news_metadata["newsOriginBasePath"] = url.join("/")
        return news_metadata
    }
```

```
    static validate_origin_base_path(news_metadata, sender){
        $.getJSON(chrome.runtime.getURL("servers.json")).done(function(
            servers){
            for(let server_name in servers){
                let origin_base_path = news_metadata["newsOriginBasePath
                    "]
                let server = servers[server_name]
                if(origin_base_path == server["url"].concat(server["path
                    "])){
                    if(new Date(server["expiration_date"]) > new Date())
                        {
                        FillMetadataInfoScript.request_news_info(
                            news_metadata, sender)
                        return
                    }else{
                        if (sender != null) {
                            putErrorInfo("Server␣certificate␣
                                registration␣is␣expired", sender)
                            showPageAction(sender)
                        }else{
                            putErrorInfo("Server␣certificate␣
                                registration␣is␣expired")
                            showModal()
                        }
                        return
                    }
                }
            }
            if(sender != null){
                putErrorInfo("The␣registered␣server␣was␣not␣found␣on␣
                    trusted␣server␣list", sender)
                showPageAction(sender)
            }else{
                putErrorInfo("The␣registered␣server␣was␣not␣found␣on␣
                    trusted␣server␣list")
                showModal()
            }
        })
    }

    static request_news_info(news_metadata, sender){
        $.ajax({
            url: [news_metadata["newsOriginBasePath"], news_metadata["
                newsRecordId"]].join("/"),
            method: "GET",
            statusCode: {
                204: function(){
```

```
                    if (sender != null){
                        putErrorInfo("The source is trust, but the news
                            is not recorded on it", sender);
                        showPageAction(sender)
                    }else{
                        putErrorInfo("The source is trust, but the news
                            is not recorded on it");
                        showModal()
                    }
                },
                200: function(news_info){
                    if (sender != null) {
                        putSuccessInfo(news_info, sender)
                        showPageAction(sender)
                    }else{
                        putSuccessInfo(news_info)
                        showModal()
                    }
                }
            }
        });
    }
}
```

ANEXO D – BACKGROUND.JSON

Código D.1 – background.json

```
'use␣strict';

chrome.runtime.onInstalled.addListener(function() {
});
var data = null;

chrome.runtime.onMessage.addListener(
    function(message, sender, sendResponse){
        if(message == "from_popup"){
            sendResponse(data);
        }else if(message.constructor == Object && message["popup_data"])
           { // Message comming from content_script
            sendResponse();
            data = message["popup_data"];
            fillNewsPopup(data,sender)
        }
    }
);

function fillNewsPopup(news_metadata, sender){
    if (!FillMetadataInfoScript.validate(news_metadata)){
        console.log("Error:␣some␣news␣metadata␣is␣missing")
        putInfoNotFound(sender)
        return;
    }
    FillMetadataInfoScript.fetch(news_metadata, sender);
}

function putInfoNotFound(sender){
    chrome.pageAction.setIcon({
        tabId: sender.tab.id,
        path : "images/news.png"
    })
}


function putErrorInfo(error_message, sender){
    data = {
        msg: "news_error",
        data: error_message
    }
```

```
        chrome.pageAction.setIcon({
            tabId: sender.tab.id,
            path : "images/error-icon-4.png"
        })
    }

    function putSuccessInfo(news_info, sender){
        data = {
            msg: "news_success",
            data: news_info
        }
        chrome.pageAction.setIcon({
            tabId: sender.tab.id,
            path : "images/successful-icon-10.png"
        })
    }

    function showPageAction(sender){
        chrome.pageAction.show(sender.tab.id);
    }
```