UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

CURSO DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

JOSE GABRIEL BERNARDES DE ALMEIDA

ANÁLISE COMPARATIVA DE ABORDAGENS BASEADAS EM *BLOCKCHAIN* PARA COMBATER *FAKE NEWS*

QUIXADÁ

2023

JOSE GABRIEL BERNARDES DE ALMEIDA

ANÁLISE COMPARATIVA DE ABORDAGENS BASEADAS EM *BLOCKCHAIN* PARA COMBATER *FAKE NEWS*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Ciência da Computação.

Orientador: Prof. Me. Roberto Cabral Rabêlo Filho.

QUIXADÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A448a Almeida, Jose Gabriel Bernardes de.
Análise comparativa de abordagens baseadas em blockchain para combater fake news / Jose Gabriel Bernardes de Almeida. – 2023.
56 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Ciência da Computação, Quixadá, 2023.
Orientação: Prof. Me. Roberto Cabral Rabêlo Filho.

1. blockchain. 2. fake news. 3. social media. 4. misinformation. I. Título.

CDD 004

JOSE GABRIEL BERNARDES DE ALMEIDA

ANÁLISE COMPARATIVA DE ABORDAGENS BASEADAS EM *BLOCKCHAIN* PARA COMBATER *FAKE NEWS*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Ciência da Computação.

Aprovada em: ____/____/____.

BANCA EXAMINADORA

Prof. Me. Roberto Cabral Rabêlo Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Antonio Rafael Braga
Universidade Federal do Ceará (UFC)

Prof. Dr. Sidartha Azevedo Lobo de Carvalho
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

À Deus, pela honra e glória da vida e por me dar a oportunidade de viver a realização do sonho de me formar. Me proporcionou vários momentos únicos, desafiadores e divertidos.

Agradeço aos meus pais, sem eles não estaria nesta etapa da minha vida. São minha base para tudo, sempre tirando deles para que eu pudesse avançar cada vez mais. Espero conseguir retribuir a fé que sempre depositaram em mim.

A UFC, pelo apoio e ensino, assim me ajudando no desenvolvimento profissional e pessoal.

Agradeço à minha esposa Erica, que desde o início dessa jornada esteve me apoiando em todos os momentos.

À minha filha Aurora, que me deu forças para continuar e persistir em frente.

À minha eterna vozinha Cleide que partiu no meio dessa caminhada, que esteve sempre presente na minha vida.

Agradeço aos meus amigos, que durante esses anos me ajudaram com conhecimento e vários momentos divertidos. Ao Alessandro, Claro, Lucas, Severo e Xavier, obrigado por todo auxílio que sem isso, talvez não conseguisse estar neste momento. Também aos demais amigos da nossa turma, em especial ao Diogo que me ajudou bastante.

Agradeço ao meu orientador, Prof. Roberto Cabral que me aceitou e teve bastante paciência, e claro me orientado da melhor maneira.

Aos professores participantes da banca examinadora Prof. Rafael e Prof. Sidartha pelo tempo, pelas valiosas colaborações e sugestões.

Por fim, gostaria de agradecer a todos aqueles que contribuíram direta ou indiretamente nessa caminhada da graduação.

RESUMO

A proliferação de fake news tornou-se um desafio significativo na era digital atual, resultando em desinformação e polarização social. Este trabalho tem como objetivo realizar uma análise comparativa das abordagens baseadas em *blockchain* para combater *fake news*. Foi realizada uma revisão sistemática, analisando cinco estratégias distintas do uso de *blockchain* para o combate às *fake news*. A metodologia envolveu uma pesquisa bibliográfica abrangente, extração de dados e análise comparativa dos artigos identificados. A análise considerou diversos fatores, incluindo a eficácia na detecção de *fake news*, escalabilidade, facilidade de implementação e impacto na redução da propagação de desinformação. Os resultados revelaram informações importantes sobre os pontos fortes e fracos de cada abordagem. O estudo de Balouchestani *et al.* (2019) demonstrou alta eficácia na detecção de *fake news* e facilidade de implementação, enquanto o estudo de Ochoa *et al.* (2019) apresentou alta escalabilidade e impacto na redução da desinformação. O estudo de Paul *et al.* (2019) exibiu a maior efetividade na detecção de *fake news*, enquanto o estudo de Sengupta *et al.* (2021) se destacou em termos de escalabilidade. O estudo Chakravorty e Rong (2017) demonstrou um impacto significativo na redução da propagação de desinformação. Considerando o estado atual do problema das *fake news*, esta pesquisa fornece uma visão abrangente sobre o potencial da tecnologia *blockchain* sobre o assunto. A análise comparativa destaca os pontos fortes e fracos de diferentes abordagens. No geral, este estudo contribui para o conhecimento existente, fornecendo *insights* valiosos sobre a aplicação de *blockchain* no enfrentamento do problema das *fake news*. Os resultados podem orientar futuras pesquisas e esforços de desenvolvimento no aproveitamento da tecnologia *blockchain* para aumentar a confiabilidade e a credibilidade das informações nas redes sociais.

Palavras-chave: *blockchain*; *fake news*; redes sociais; desinformação.

ABSTRACT

The proliferation of fake news has become a significant challenge in the current digital era, resulting in misinformation and social polarization. This study aims to conduct a comparative analysis of blockchain-based approaches to combat fake news. A systematic review was conducted, analyzing five distinct strategies of using blockchain for combating fake news. The methodology involved comprehensive literature research, data extraction, and comparative analysis of the identified articles. The analysis considered various factors, including the effectiveness in detecting fake news, scalability, ease of implementation, and impact on reducing the spread of misinformation. The results revealed important insights into the strengths and weaknesses of each approach. Balouchestani *et al.* (2019) demonstrated high effectiveness in detecting fake news and ease of implementation, while Ochoa *et al.* (2019) presented high scalability and impact on reducing misinformation. Paul *et al.* (2019) exhibited the highest effectiveness in detecting fake news, and Sengupta *et al.* (2021) stood out in terms of scalability. Chakravorty e Rong (2017) demonstrated a significant impact on reducing the spread of misinformation. Considering the current state of the fake news problem, this research provides a comprehensive insight into the potential of blockchain technology in addressing the issue. The comparative analysis highlights the strengths and weaknesses of different approaches. Overall, this study contributes to the existing knowledge by providing valuable insights into the application of blockchain in combating fake news. The results can guide future research and development efforts in leveraging blockchain technology to enhance the reliability and credibility of information in social networks.

Keywords: blockchain; fake news; social media; misinformation.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BFS	*Breadth First Search*
DAPP	Aplicativo Descentralizado
FN	*Fake News*
FNDSM	Detecção de Fake News em mídias sociais usando Blockchain
IoT	*Internet of Things*
NLP	Processamento de Linguagem Natural
PCA	Autoridade de Certificação Pessoal
PoS	*Proof of Stake*
PoT	*Proof of Trust*
PSC	*Propagator Smart Contract*

SUMÁRIO

1 INTRODUÇÃO

Diante de uma sociedade onde as trocas de informação se tornaram meios práticos e de fácil acesso, o uso de notícias falsas vem gerando diferentes problemas, como influências politicas, sociais, etc (ALLCOTT; GENTZKOW, 2017).

De acordo com Marchi (2012), a população mais jovem atualmente tende a consumir menos os meios de comunicação mais antigos, como jornais, rádio e TV, pois acreditam que, além de serem desinteressantes, são repetitivos.

A internet por ser um ambiente dinâmico, descentralizado e adaptativo, impulsionado por inovações constantes. Ela democratiza a liberdade de expressão, permitindo que os usuários criem e compartilhem instantaneamente seu próprio conteúdo. No entanto, é crucial estabelecer uma distinção clara entre liberdade de expressão nas redes sociais e irresponsabilidade. Embora todos tenham o direito de se expressar livremente, não se deve usar esse direito como justificativa para praticar abusos ou disseminar informações falsas (GOMES, 2018).

As notícias publicadas em redes sociais e aplicativos de troca de mensagens possuem um baixo nível de confiabilidade (NEWMAN *et al.*, 2017), causado principalmente pela falta de filtragem de notícias falsas, mais conhecidas como *Fake News* (FN). As FN são definidas como artigos de notícias que contêm informações errôneas ou criadas com a intenção de enganar e influenciar os leitores (SHU *et al.*, 2017).

A construção de uma FN é realizada com o intuito de atingir algum objetivo. Seja para manipular o leitor, ou seja para desconstruir uma informação verdadeira. No que é certo ela traz consequências reais, como prejuízos financeiros, exposição da vida particular das pessoas e afeta empresas e organizações. Além disso, a desinformação causa também certa fragilidade no convívio social, criando um ambiente polarizado e hostil entre os cidadãos (CARNEIRO, 2018).

Com o surgimento de novas tecnologias torna-se cada vez mais fácil não só falsificar textos, como também áudios e vídeos, levando as FN para um novo e mais preocupante estágio. Com a facilidade e usabilidade no acesso a essas tecnologias, os usuários mal intencionados tendem a criar conteúdos que aparentam ser reais e geram uma credibilidade maior para os leitores desse conteúdo enganoso. O problema é que, a detecção e prevenção de FN nas mídias sociais apresenta desafios únicos que exigem novos algoritmos (NETO *et al.*,).

Existem algumas propostas para detecção de FN em uma notícia online, como procurar pelas fontes de imagens e verificar em quais sites elas também foram utilizadas. Outra alternativa é modificar o algoritmo de busca da *Google*, o *PageRank*, levando em consideração

não apenas a quantidade de referências de sites citados, mas também sua relevância, como sua importância e confiança (MARUMO, 2018). Além disso, é também viável utilizar a fonte, título, texto e vídeos das notícias como dados para classificação de FN (SHU *et al.*, 2017).

A rastreabilidade das FN até sua fonte é um desafio crucial no combate à desinformação. A capacidade de rastrear é essencial para proteger a integridade da informação na era digital. Através do rastreamento, é possível identificar os responsáveis pela criação e disseminação das notícias falsas, bem como entender as estratégias e motivações por trás dessas ações. Essas informações são fundamentais para desenvolver estratégias eficazes de combate à desinformação e promover um ambiente informacional mais confiável e preciso (SMITH; GARCIA, 2020).

Obviamente, só podemos rastrear uma FN após sua publicação e não podemos eliminá-las. Neste sentido, uma referência para avaliar notícias são as próprias pessoas que estão em um ambiente descentralizado. Portanto, dado a presença de um núcleo descentralizado, a fim de evitar as FN (BALOUCHESTANI *et al.*, 2019).

Considerando o cenário de rastreio de FN, a tecnologia *Blockchain* tem chamado a atenção dos pesquisadores por garantir a integridade e confiabilidade das informações armazenadas em sua estrutura de blocos. As características de descentralização e imutabilidade dos dados da *Blockchain* podem ser efetivas. Devido a essas características é possível rastrear a quantidade de informações sobre um determinado tema que está sendo disseminado na rede e identificar os responsáveis pela sua disseminação (NETO *et al.*,).

Outras tecnologias como a inteligência artificial são capazes de treinar algoritmos computacionais para detectar informações falsas e com o uso da *Blockchain* pode ser um lugar adequado para publicar notícias sem interferência de terceiros e uma solução para o problema de confiança em sistemas distribuídos (LI *et al.*, 2020).

Neste estudo, realizaremos uma análise comparativa de diferentes abordagens baseadas em *blockchain* para combater *fake news*. Nosso objetivo é examinar diferentes propostas e metodologias apresentadas na literatura, destacando seus pontos fortes, limitações e contribuições para o enfrentamento desse problema. Para isso, foram selecionado cinco artigos relevantes sobre o tema, que exploram o uso de *blockchain* no contexto da detecção e prevenção de *fake news*.

Os artigos selecionados incluem "*SANUB: A new method for Sharing and Analyzing News Using Blockchain*", "*FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks*", *"ProBlock: a novel approach for fake news detection*", "*Ushare: user*

controlled social media based on Blockchain"e "*Fake News Detection in Social Media using Blockchain*". Essas pesquisas abordam diferentes aspectos da utilização de *Blockchain*, como compartilhamento e análise de notícias, arquiteturas confiáveis em redes sociais e detecção de *fake news*.

Ao realizar a análise comparativa, como resultado foi possível identificar as contribuições principais de cada trabalho, avaliar a eficácia das soluções propostas e discutir o potencial do uso do *Blockchain* no combate às *fake news*. Além disso, também abordaremos as considerações éticas relacionadas ao compartilhamento de informações e a importância de rastrear e verificar a origem das notícias.

Espera-se que o estudo contribua com o avanço do conhecimento nessa área e forneça *insights* valiosos para pesquisadores, profissionais e tomadores de decisão interessados em lidar com o desafio das *fake news*.

1.1 Objetivos

Nesta seção, são apresentados o objetivo geral e os objetivos específicos deste trabalho.

1.1.1 Objetivo geral

- O objetivo principal deste trabalho é realizar uma análise comparativa das abordagens baseadas em *Blockchain* para combater *fake news*, investigando suas características, metodologias e resultados, a fim de identificar suas contribuições e limitações.

1.1.2 Objetivos específicos

- Revisar a literatura acadêmica sobre o uso de *Blockchain* no combate às *fake news*, compreendendo os conceitos, impactos e desafios relacionados a esse fenômeno.
- Comparar as abordagens utilizadas em cada artigo, destacando suas principais características, pontos fortes e limitações.
- Avaliar a eficácia das soluções propostas em relação à detecção, prevenção e mitigação de *fake news*.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão apresentados os conceitos importantes presentes neste trabalho.

2.1 O problema com o compartilhamento de *Fake News* na internet

A Internet, por meio de suas variadas aplicações, é considerada como um dos principais meios de comunicação. Desde o seu surgimento, até os dias atuais, ela tem provocado grandes impactos e influências positivas e negativas na sociedade (NEVES; BORGES, 2020).

O termo *Fake News* (FN) ganhou força mundialmente em 2016 nos Estados Unidos com a corrida presidencial, em que conteúdos falsos sobre a candidata Hillary Clinton foram compartilhados de forma intensa pelos eleitores de Donald Trump. Apesar do recente uso do termo FN, seu significado pode ser compreendido de maneira simples pelo sentido literal da palavra, notícias falsas. (MARUMO, 2018).

APRÁ (2017) identificou algumas características comuns em sites de FN que são registrados com domínio ".com"ou ".org", dificultando a identificação dos responsáveis com a mesma transparência que acontecem com os domínios registrados no Brasil, que terminam com ".br". Além disso, seus nomes são semelhantes a outros de jornais e de blogs autorais.

Segundo Victor (2017), O ato de espalhar FN já ocorre desde o século VI, quando um historiador bizantino difamou o imperador da época, entre outras pessoas. Também ocorreram casos de disseminação de FN durante eventos históricos, como na eleição do presidente Trump nos Estados Unidos e nas vésperas da Revolução Francesa na França, mesmo com a presença de censura à imprensa na época. No entanto, se compararmos os dias atuais com alguns anos atrás, é evidente que a capacidade de difusão das FN era significativamente menor, assim como o volume de notícias verdadeiras disponíveis.

No cenário de pós-verdade, as FN ganham espaço nas redes sociais e preocupam a grande mídia no Brasil, gerando impacto negativo às instituições jornalísticas no país. O quartel general das notícias falsas durante a eleição americana foi a Macedônia, lar de dezenas de operadores de sites que criaram FN projetadas para atrair a atenção dos americanos durante as eleições. Cada clique adicionava dinheiro às suas contas bancárias, o que tornou o negócio lucrativo para os jovens da região (SOARES; DAVEY-ATTLEE, 2017).

Segundo o estudo de BALLOUSSIER (2016) as notícias falsas que mais viralizaram nas eleições de 2016 nos EUA foram “*Wikileaks* confirma que Hillary Clinton vendeu armas

para o Estado Islâmico" e "Papa Francisco choca o mundo e apoia Donald Trump". Outro caso de destaque foi de um homem de 28 anos que entrou atirando em uma pizzaria da Carolina do Norte para "investigar por conta própria uma teoria da conspiração fictícia de que o restaurante mantinha um cativeiro de tráfico sexual de crianças, financiado pelo partido democrata".

Em meio a pandemia do Covid-19, conhecido como coronavírus, que se iniciou no começo de 2020, fez-se presente na realidade dos brasileiros o amplo compartilhamento de FN sobre o Covid-19. Conforme a doença foi se espalhando ao redor do mundo, também foram crescendo o número de pesquisas feitas para entender esse novo vírus e até mesmo encontrar uma vacina, contudo, mesmo nesse momento de crise, as notícias falsas ganharam força, e aqui no Brasil não foi diferente (BALLOUSSIER, 2016).

Notícias verificadas e carimbadas ou outras de interesse da população devem ser difundidas para mitigar os efeitos danosos das FN. Da mesma forma que as redes sociais e o *WhatsApp* são empregados como impulsionadores de conteúdo falso, devem ser utilizadas como ferramentas para informar seus cidadãos corretamente (BALLOUSSIER, 2016).

2.2 *BlockChain*

Blockchain significa cadeia de blocos. De forma simplificada, pode ser definido como uma sequência de blocos conectados entre si por meio de resumos criptográficos, formando assim uma cadeia contínua. Esses blocos contêm informações relevantes para a rede. O surgimento do *Blockchain* veio com a proposta de Nakamoto *et al.* (2008), onde foi criada uma nova moeda criptográfica, o *bitcoin*.

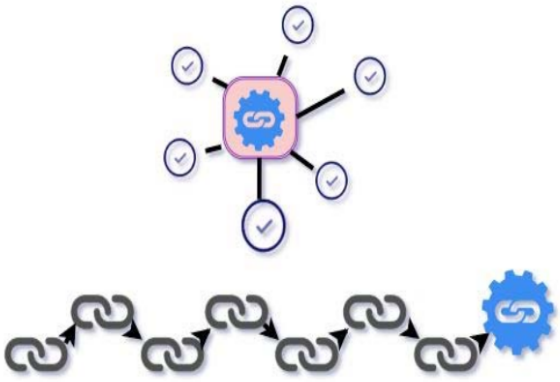
Essa moeda atraiu muito interesse e por conta dessa nova tecnologia, empregada na sua concepção. Tal inovação permite que o *bitcoin* funcione sem nenhuma dependência com instituições bancárias ou qualquer entidade (YANO *et al.*, 2018).

Blockchain são bases de registros e de dados distribuídos e compartilhados que têm a função de criar um índice global para todas as transações que ocorrem em um determinado mercado. Por causa dessa origem, a unidade de informação no *Blockchain* é chamada de transação, embora não esteja necessariamente relacionada a ativos financeiros (GREVE *et al.*, 2018).

Os registros são imutáveis devido ao tipo de encadeamento que é feito com os blocos, em que o ponteiro para o bloco anterior é feito com resumos criptográficos com regras específicas. De maneira que para alterar esse resumo deve-se dedicar grande poder computacional, que na

maioria dos casos, torna-se inviável. Como é um protocolo distribuído, todas as informações não estão armazenadas em um servidor central e não há um nó mestre que coordene a rede. Justamente o oposto disso, o *Blockchain* está replicado em todos os nós participantes da rede, que podem estar espalhados pelo mundo inteiro. Além de ser um esquema distribuído, o referido também é público, pois não há como censurar uma parte de participar da rede, basta o interessado ter acesso a internet que ele poderá realizar a sua cópia da base de dados (UNDERWOOD, 2016).

Figura 1 – Ilustração de uma *Blockchain*



Fonte: Adaptado de Paul *et al.* (2019).

A imutabilidade do *Blockchain* reduz significativamente as chances de ataques à rede, pois os elementos centrais são os principais pontos de um possível ataque. O *Blockchain* é uma tecnologia de alta disponibilidade, pois o sistema estará disponível mesmo que alguns dos nós computacionais não estejam ativos (YAGA *et al.*, 2019).

Uma das principais vantagens desta tecnologia, é sua capacidade de criar uma plataforma descentralizada, ou seja, sistema confiável com base no consenso que vem sem a necessidade de um núcleo centralizado e qualquer indivíduo da rede pode ter acesso e verificar os blocos (CHRISTIDIS; DEVETSIKIOTIS, 2016).

2.2.1 Estrutura dos blocos

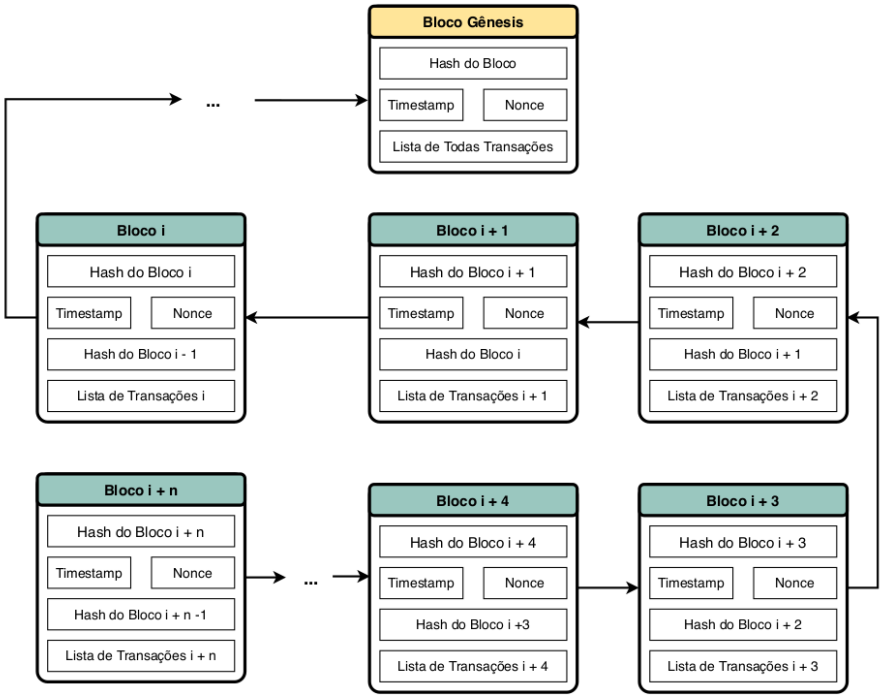
O *Blockchain* é composto por um conjunto de blocos conectados por meio de ponteiros chamados *hash* até o bloco gênesis, que é o primeiro bloco da estrutura (VANCE; VANCE, 2019). Além do *hash* raiz, são armazenadas as transações geradas e um número aleatório chamado *nonce* usado para validar o *hash* (SENRA, 2017). A estrutura de dados do *Blockchain* pode ser visualizada na Figura 2.

- O *hash* do bloco: O *hash* do bloco é uma assinatura digital única gerada a partir

dos dados do bloco, incluindo o cabeçalho e as transações;

- O *hash* do bloco anterior: funciona como uma ligação entre os blocos da cadeia, de modo que se um bloco for alterado seu *hash* vai mudar e ele fica incompatível com o resto do *Blockchain*;
- O *nonce*: um número único que identifica os blocos e é crescente ao longo da cadeia;
- O *timestamp*: armazena um carimbo de data/hora da criação de um bloco.

Figura 2 – Estrutura de blocos do *Blockchain*



Fonte: Adaptado de Neto *et al.* ().

2.2.2 Tipos de Blockchains

Segundo Massessi (2018), as *Blockchain* podem ser classificadas quanto às restrições impostas tanto na leitura quanto na escrita dos dados, existindo, então, *Blockchain* **públicas** e **privadas**.

2.2.2.1 Blockchain pública:

As características deste tipo de *Blockchain* de acordo com (MASSESSI, 2018) são:

- Sem restrições para leitura e escrita de dados: qualquer um pode participar da rede, enviar transações e visualizar as transações que já foram inseridas.

- As informações são replicadas em todos os nós, tornando a rede mais resistente contra adulteração e contra indisponibilidade de serviço. Como não há restrições de acesso e todos os participantes são tratados da mesma forma, pode-se dizer que a *Blockchain* pública é democrática e transparente.
- Na maioria das *Blockchains* públicas, novos blocos são inseridos pelos chamados mineradores. Segundo Tschorsch e Scheuermann (2016), qualquer nó de uma rede pública pode ser um minerador e competir com os demais em uma tarefa computacional difícil conhecida como prova de trabalho. Assim, a habilidade de inserir transações na *Blockchain* depende do poder computacional, e não apenas do número de nós na rede, onde a maioria seria mais facilmente obtida em caso de ataque.

2.2.2.2 Blockchain privada:

Destacam-se três características principais de *Blockchain* privada de acordo com (MASSESSI, 2018), onde:

- Há controle sobre quem pode participar da rede, enviar transações e visualizar as informações que foram inseridas.
- Costumam ser utilizadas por empresas que precisam proteger informações confidenciais.
- Maior performance: como todos os participantes são identificados e confiáveis, esse tipo de *Blockchain* permite a utilização de algoritmos de consenso mais rápidos, como a prova de autoridade, onde o grupo de validadores é pré-fixado e 2/3 destes devem votar para validar uma transação (ANGELIS, 2018).

2.2.3 Smart Contracts (contratos inteligentes)

Outra vantagem do uso de *blockchain* são os contratos inteligentes, que são definidos por um protocolo de transação computadorizado capaz de executar automaticamente os termos de um contrato (ZHENG *et al.*, 2018), onde os usuários podem trocar dados entre si sem a presença de um terceiro confiável (ISLAM *et al.*, 2020).

Os contratos inteligentes são programas autônomos executados em *blockchain* que automatizam a execução e o cumprimento de acordos digitais, da mesma forma que um contrato tradicional faria. Entretanto, ao contrário do tradicional, pode também obter informação como

input e processá-la de acordo com as regras nele estabelecidas e assim determinar o cumprimento ou não das obrigações contraídas pelas partes sem a intervenção constante de terceiros (RAMÍREZ, 2019).

A verificação formal de contratos inteligentes também desempenha um papel importante na garantia da corretude e segurança. Através de métodos formais, é possível verificar matematicamente se o contrato atende a certas propriedades desejadas, evitando vulnerabilidades e falhas (NIKITIN *et al.*, 2021).

Diversos estudos têm explorado o uso de contratos inteligentes no combate às FN. O artigo de Smith e Johnson (2022) propõe um sistema baseado em contratos inteligentes para verificação de notícias, onde as informações são rastreadas e verificadas em tempo real.

Além disso, a identificação de identidades digitais confiáveis é essencial para a eficácia dos contratos inteligentes no combate às FN. Outro aspecto importante é o rastreamento de fontes de informação. O trabalho de Wang *et al.* (2021) propõe um sistema de rastreamento de notícias baseado em *blockchain*, onde cada notícia é registrada em uma *blockchain* pública, permitindo a verificação de sua origem e autenticidade.

Em resumo, os contratos inteligentes são uma tecnologia promissora no combate às FN, oferecendo transparência, segurança e automação na verificação e autenticação de informações. O uso de identidades digitais confiáveis e o rastreamento de fontes de informação são aspectos essenciais para garantir a eficácia dessas soluções

2.3 Aplicações de *Blockchain* no Combate às *Fake News*

No combate às FN, o *blockchain* pode ser aplicado de várias maneiras. Sua utilização tem sido objeto de estudo e desenvolvimento por pesquisadores e especialistas. Esta tecnologia emergente oferece várias possibilidades para abordar esse problema complexo, proporcionando maior transparência, confiança e rastreabilidade das informações.

Uma das principais aplicações é a verificação de identidade e autenticidade das fontes de informação. Através do uso de contratos inteligentes e registros imutáveis, é possível verificar a autenticidade das notícias e garantir que foram publicadas por fontes confiáveis (LEE *et al.*, 2019). Isso ajuda a reduzir a disseminação de informações falsas, uma vez que apenas as fontes verificadas e autenticadas são consideradas confiáveis.

Além disso, o uso de *blockchain* permite o rastreamento das informações, desde a sua origem até a sua disseminação. Isso é essencial para identificar a propagação de FN e

as fontes responsáveis por sua criação e divulgação, tornando possível rastrear a trajetória das notícias e identificar os responsáveis por sua disseminação (OUYANG *et al.*, 2020).

Outra aplicação relevante é a criação de plataformas de compartilhamento de notícias baseadas em *blockchain*, onde os usuários têm maior controle sobre o conteúdo compartilhado. Através de contratos inteligentes, é possível estabelecer regras e critérios para a publicação de notícias, garantindo a veracidade e qualidade das informações compartilhadas (PÉREZ-SOLÀ *et al.*, 2020). Isso permite uma maior participação dos usuários na seleção e verificação das notícias, reduzindo a propagação de FN.

É importante destacar que o uso de *blockchain* no combate às FN também apresenta desafios e limitações. Questões relacionadas à privacidade e segurança dos dados podem surgir devido à natureza pública e imutável dos registros em *blockchain*. Além disso, a centralização versus descentralização da tecnologia também deve ser considerada, uma vez que uma abordagem excessivamente centralizada pode comprometer a confiança e a imparcialidade das informações (JOHNSTON, 2018).

As aplicações que usam *blockchain* no combate às FN oferecem soluções promissoras para enfrentar esse desafio global. A verificação de identidade e autenticidade das fontes, o rastreamento das informações e a criação de plataformas descentralizadas são abordagens que podem contribuir para reduzir sua disseminação e promover um ambiente de informação mais confiável e seguro.

2.4 Aspectos Éticos e Desafios

No contexto ético o *blockchain* traz consigo implicações que devem ser consideradas. Essas questões envolvem preocupações relacionadas à privacidade, segurança dos dados, centralização versus descentralização, efeitos colaterais indesejados e possíveis impactos na liberdade de expressão.

2.4.1 Privacidade

O *blockchain*, por sua natureza imutável e transparente, pode representar um desafio para a privacidade dos usuários. As informações compartilhadas podem ser acessadas por todos os participantes da rede, o que pode levantar preocupações sobre a exposição de dados sensíveis. É importante garantir que as medidas adequadas sejam tomadas para proteger a privacidade dos

usuários, como a pseudonimização dos dados ou o uso de técnicas de criptografia (JOHNSTON, 2018).

2.4.2 Segurança dos dados

A segurança dos dados é fundamental no contexto do combate às FN. Embora o *blockchain* seja conhecido por sua resistência a ataques e alterações de dados, ainda é importante garantir a proteção adequada das informações armazenadas. Contudo. Vulnerabilidades na implementação do *blockchain* ou na infraestrutura subjacente podem ser exploradas por adversários maliciosos. Medidas de segurança robustas, como criptografia e autenticação adequada, devem ser adotadas para proteger os dados armazenados (SWAN, 2015).

2.4.3 Centralização versus descentralização

O debate entre centralização e descentralização é relevante no contexto do uso de *blockchain* no combate às FN. Embora a descentralização possa oferecer maior transparência e resistência à censura, também pode apresentar desafios, como a governança e coordenação de uma rede descentralizada. É importante encontrar um equilíbrio entre a descentralização e a capacidade de tomar medidas rápidas e efetivas contra a disseminação de FN (LEE *et al.*, 2019).

2.4.4 Efeitos colaterais indesejados

O uso de *blockchain* no combate às FN pode ter efeitos colaterais indesejados. Como por exemplo, a adoção em larga escala de uma abordagem baseada em *blockchain* pode levar à sobrecarga de recursos computacionais e ao aumento do consumo de energia. Além disso, a confiabilidade das informações armazenadas pode ser afetada por eventos externos, como ataques de 51% ou falhas nos nós da rede (OUYANG *et al.*, 2020).

2.4.5 Impactos na liberdade de expressão

Embora o objetivo seja combater a disseminação de informações falsas, é importante garantir que o uso de *blockchain* não resulte em cenários de censura ou restrição injustificada da liberdade de expressão. Mecanismos adequados de verificação e moderação devem ser implementados para evitar abusos (PÉREZ-SOLÀ *et al.*, 2020).

3 METODOLOGIA

A metodologia adotada neste trabalho consistiu em uma pesquisa bibliográfica e comparativa com o objetivo de coletar e analisar o estado da arte. O processo de pesquisa foi conduzido em etapas distintas, conforme descrito a seguir:

3.1 Seleção dos Artigos

Inicialmente, foi realizada uma busca sistemática em bases de dados acadêmicas, como *IEEE Xplore* [1], *ACM Digital Library* [2] e *Google Scholar* [3], utilizando termos de pesquisa relevantes, como "*blockchain*", "*fake news*", "*trust*", "*verification*" e suas variações. A busca foi limitada a artigos publicados nos últimos cinco anos para garantir a relevância e atualidade das informações.

Os critérios de inclusão para seleção dos artigos foram estabelecidos, levando em consideração a temática central do trabalho. Foram considerados apenas artigos que abordassem o uso do *blockchain* no contexto das *fake news*, com foco em soluções, arquiteturas, algoritmos e técnicas relacionadas à verificação e autenticidade de informações.

3.1.1 Critérios de Inclusão:

1. **Relevância do tópico:** Abordar diretamente o uso do *blockchain* para detecção e combate às FN.
2. **Qualidade do conteúdo:** Revisados por pares e publicados em conferências ou revistas científicas de renome.
3. **Atualidade:** Ser publicados nos últimos seis anos para garantir a inclusão das abordagens mais recentes e relevantes.
4. **Metodologia:** Apresentar uma metodologia clara e robusta para lidar com a detecção e combate às FN usando *blockchain*.
5. **Contribuições:** Contribuições significativas para o campo, como novos algoritmos, arquiteturas e etc.
6. **Resultados:** Relatar resultados ou análises quantitativas que evidenciam a eficácia e a eficiência das abordagens propostas.

[1] https://ieeexplore.ieee.org/Xplore/home.jsp
[2] https://dl.acm.org/
[3] https://scholar.google.com.br/

3.1.2 Artigos Selecionados:

- **"*SANUB: A new method for Sharing and Analyzing News Using Blockchain*"**
- **"*FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks*"**
- **"*ProBlock: A novel approach for fake news detection*"**
- **"*Ushare: User controlled social media based on blockchain*"**
- **"*Fake News Detection in Social Media using Blockchain*"**

3.2 Análise dos Artigos

Após a seleção dos artigos, foi realizada uma leitura criteriosa e detalhada de cada um. Os artigos foram analisados quanto ao seu conteúdo, metodologia utilizada, resultados obtidos e contribuições para o campo de estudo.

Durante a análise, foram estabelecidas categorias e temas relevantes para agrupar os artigos de acordo com suas abordagens e contribuições. Essas categorias foram definidas com base em similaridades de conceitos e métodos utilizados pelos autores, permitindo uma comparação mais efetiva entre os estudos revisados.

O Quadro 1 apresenta um resumo das principais contribuições, metodologia adotada e resultados obtidos na análise dos artigos selecionados para o trabalho.

Quadro 1 – Quadro de Principais Contribuições, Metodologia e Resultados

Artigo	**Principais Contribuições**	**Metodologia Utilizada**	**Resultados Obtidos**
SANUB	Novo método para compartilhar e analisar notícias usando *blockchain*	Desenvolvimento de uma plataforma baseada em *blockchain* para compartilhamento de notícias	Melhor rastreabilidade e autenticidade das notícias
FakeChain	Arquitetura *blockchain* para garantir confiança em redes sociais	Utilização de contratos inteligentes para verificação da autenticidade das informações compartilhadas	Aumento da transparência e integridade dos dados em redes sociais
ProBlock	Abordagem inovadora para detecção de FN	Aplicação de técnicas de NLP e aprendizado de máquina para identificação de padrões de desinformação	Melhor detecção de FN com base em verificação de fontes e contexto
Ushare	Plataforma de mídia social baseada em *blockchain* com controle do usuário	Implementação de uma plataforma de mídia social descentralizada baseada em *blockchain*	Maior privacidade e segurança do usuário, redução da disseminação de informações falsas
FNDSM	Detecção de FN em mídias sociais usando *blockchain*	Utilização de análise de sentimentos e NLP para identificação de conteúdo enganoso	Colaboração de usuários na detecção de FN, aumento da transparência através do uso de *blockchain*

Fonte: elaborado pelo autor.

3.3 Síntese dos Resultados

Após a análise individual de cada artigo, os resultados foram sintetizados e organizados em uma visão geral dos principais aspectos discutidos. Foram identificadas tendências, lacunas de pesquisa e desafios comuns mencionados pelos autores. Essa síntese dos resultados serviu como base para a elaboração das seções de revisão da literatura e discussão do trabalho.

3.4 Limitações

É importante ressaltar que a presente pesquisa bibliográfica e comparativa possui algumas limitações. A busca foi restrita a bases de dados acadêmicas específicas, o que pode ter excluído potenciais artigos relevantes em outras fontes. Além disso, a análise dos artigos foi realizada de forma subjetiva, levando em consideração a interpretação dos pesquisadores.

3.5 Considerações Éticas

Durante o processo de pesquisa, foram seguidas as diretrizes éticas de uso e citação de materiais acadêmicos. Todos os artigos selecionados e referenciados neste trabalho foram devidamente atribuídos aos seus autores originais, respeitando os direitos autorais e intelectuais.

4 ANÁLISE DOS ARTIGOS

Foram identificados e registrados os principais conceitos, abordagens, desafios e resultados apresentados em cada artigo. Estes estudos são apresentados nesta seção, assim como suas principais contribuições e relações com o presente trabalho.

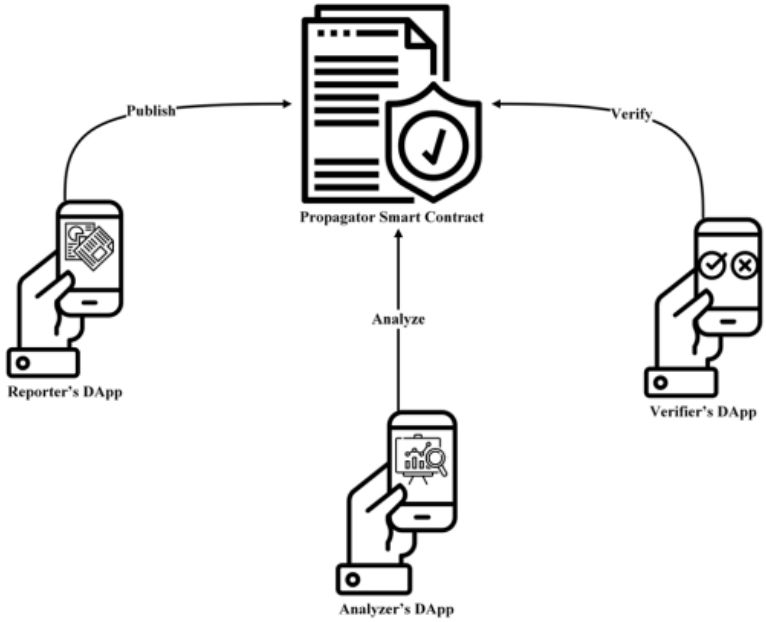
4.1 SANUB: *A new method for Sharing and Analyzing News Using Blockchain*

4.1.1 Motivação

A tecnologia *Blockchain* fornece uma plataforma para que as pessoas transmitam notícias anonimamente, no entanto, pode levar à criação de FN. Existem inúmeros desafios para implementar o *Blockchain* para avaliação de notícias, como um sistema baseado em *Blockchain* com detecção de FN. No entanto, a melhor maneira de evitar FN é avaliá-las pelas próprias pessoas.

Com esse pensamento. Balouchestani *et al.* (2019) propuseram um aplicativo descentralizado baseado em *Blockchain* onde cada pessoa pode compartilhar notícias como um repórter anônimo. No qual analistas podem verificar notícias para sua precisão e compartilhar seus resultados com o público. Repórteres e analistas têm crédito no sistema e a validade de suas notícias e análises determinam seu crédito. A Figura 3 mostra a estrutura do **SANUB**.

Figura 3 – Modelo SANUB



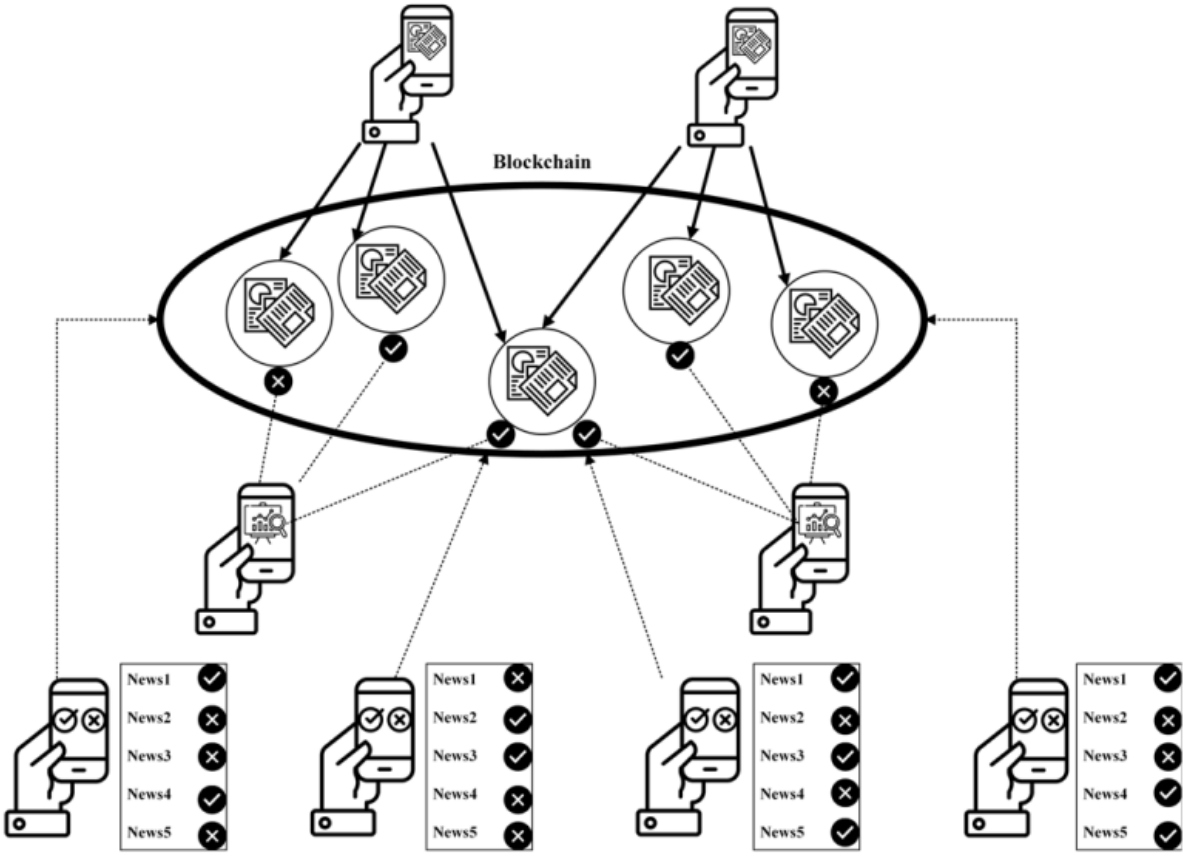
Fonte: Adaptado de Balouchestani *et al.* (2019).

Os repórteres devem enviar as notícias para o *Propagator Smart Contract* (PSC) com seu Aplicativo Descentralizado (DAPP) quando eles pretendem transmitir algumas notícias. O PSC é responsável por analisar e avaliar notícias para transmiti-las. Existem 2 tipos de entidades no modelo **SANUB**, usuários do sistema e o PSC.

A principal tarefa do PSC é publicar notícias na rede. Os usuários enviarão a notícia para o contrato inteligente quando pretendem publicá-la. O PSC mantém uma lista de repórteres e seus créditos, lista de análises de cada pessoa sobre as notícias, lista de notícias e suas *tags*.

Na Figura 4 fornece a estrutura da comunicação entre usuários do DAPP.

Figura 4 – Comunicação de usuários



Fonte: Adaptado de Balouchestani *et al.* (2019).

4.1.2 Contrato inteligente do propagador (Propagator Smart Contract)

A principal tarefa do PSC é publicar notícias na rede. Os usuários enviarão a notícia para o contrato inteligente quando pretendem publicá-la. O PSC está mantendo uma lista de repórteres e seus créditos, lista de análises de cada pessoa sobre as notícias, lista de notícias e suas *tags*. Além disso, gerencia a análise e avaliação das notícias.

4.1.3 Usuários do sistema

Os usuários no **SANUB** podem aceitar 3 funções diferentes e dois tipos de crédito são definidos no sistema para eles:

1) **Repórter**: Cada usuário pode publicar notícias anonimamente e todas as suas fontes e evidências que apoiam as notícias com a ajuda de seu DAPP. Os usuários podem definir *tags* diferentes para suas notícias. Com base na avaliação, cada notícia publicada leva crédito de 0 a 1.

2) **Analisador**: Cada usuário pode pesquisar *tags* e rastrear notícias relacionadas com a ajuda de seu DAPP. Então, eles podem analisar as notícias publicadas e comentar sobre suas análises. Essas notícias são válidas ou não. A validade de cada analista representará a crença pública sobre a validade da análise dos analisadores.

3) **Verificador**: Os usuários podem ler as notícias publicadas e suas análises para validá-las. Eles podem dar nota um ou zero a cada notícia. A média das pontuações dos usuários mostrará a crença do público sobre a notícia e sua análise. São as pessoas normais que leem as notícias junto com suas análises e pontuam com base no fato de acreditarem ou não nas notícias.

4.1.4 Transmissão de notícias

Qualquer pessoa pode compartilhar as notícias com as outras anonimamente como um repórter. Os repórteres usam os DAPPs para enviar o texto das notícias ao PSC junto com as fontes e evidências.

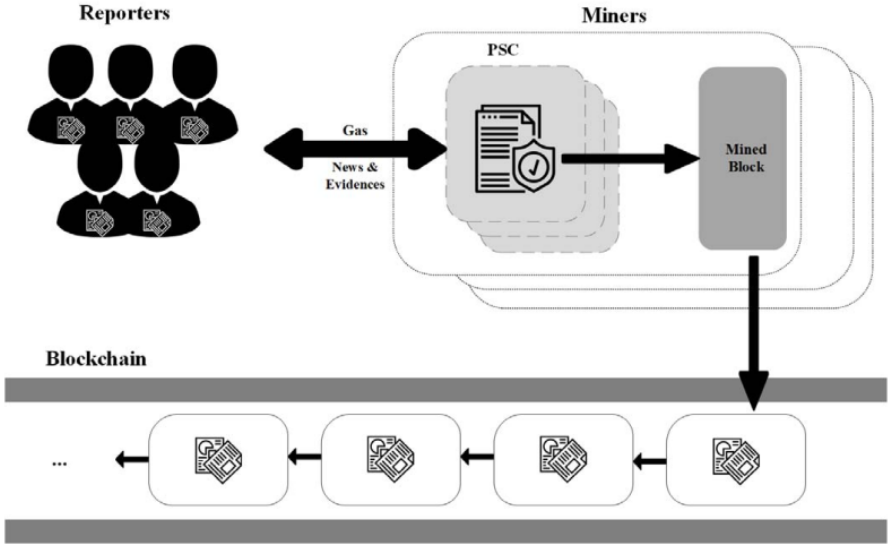
O PSC mantém uma lista de repórteres com seus créditos, uma lista de notícias com suas *tags*, o status de cada notícia e a validade de qualquer notícia depois de identificada. Quando a notícia é publicada no sistema, seu status é de análise. Cada notícia no sistema tem 2 status: analisando e verificando. De acordo com a Figura 5.

4.1.5 Avaliação de notícias

Quando um repórter publica uma notícia, o analista tem um tempo para submeter suas análises. Se não houver evidências suficientes para provar a notícia ou se as evidências forem falsas, os analistas colocam isso como uma análise no PSC.

Os analistas também podem fornecer evidências adicionais para apoiar essa notícia. Passado algum tempo, o limite de tempo de análise para analistas vai acabar e o PSC não

Figura 5 – Transmissão de notícias do SANUB



Fonte: Adaptado de Balouchestani *et al.* (2019).

permitirá outras análises para esta notícia. O status da notícia muda neste momento para o status de verificação. Em seguida, outros usuários podem pontuar estas notícias com base em fontes de repórteres, evidências e comentários de analistas.

Cada usuário atribui pontuação 0 se achar que a notícia é falsa ou pontuação 1 se achar que não é. Após a pontuação de cada usuário, o PSC resume as pontuações do usuário e calcula a pontuação final dos usuários para esta notícia, que são as crenças das pessoas, e atualiza o crédito do repórter e dos analistas. A Figura 6 ilustra esse processo de avaliação.

No **SANUB**, uma média de pontuações de usuários em notícias mostra a crença das pessoas nessas notícias e análises que as suportam. A quantidade de usuários que participam da validação de notícias mostra a importância dessa notícia.

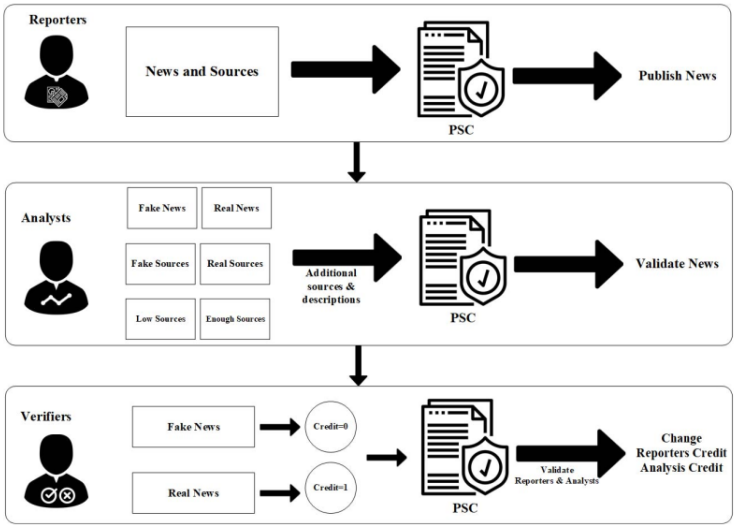
4.1.6 Determinar Validade de notícias e créditos

A determinação da validade das notícias deve ser feita de forma que as pessoas possam estimar o crédito dessas notícias o mais rápido possível. O crédito dos repórteres desempenha um papel importante na validade de suas notícias.

Se um repórter confiável compartilha notícias, a validade dessas notícias é alta no início, e outro fator importante para determinar a validade das notícias é o crédito dos analistas que as verificaram ou negaram. As notícias que são confirmadas por um grande número de analistas confiáveis são confiáveis.

No **SANUB**, uma média de pontuações de usuários em notícias mostra a crença das

Figura 6 – Processo de avaliação do SANUB.



Fonte: Adaptado de Balouchestani *et al.* (2019).

pessoas nessas notícias e análises que as suportam. A quantidade de usuários que participam da validação de notícias mostra a importância dessa notícia e quanto mais participantes avaliam as notícias, mais importante elas são. O crédito de analistas é baseado na crença das pessoas nas notícias que analisaram. Quanto mais as pessoas acreditam nas notícias que um analista confirma, mais confiável é o analista.

O crédito dos repórteres é calculado em relação ao crédito dos analistas que confirmaram suas notícias, bem como a importância das notícias que publicaram. O impacto de notícias falsas importantes em uma comunidade pode ser muito mais do que um grande número de notícias corretas, mas sem valor. Por esse motivo, o **SANUB** determina o crédito do repórter de forma que a punição por compartilhar notícias falsas seja muito maior do que a recompensa por compartilhar as corretas, e notícias importantes mudam o crédito de um repórter mais do que notícias inúteis.

4.1.7 Análise de segurança

Analistas podem conspirar com usuários para aumentar a opinião pública sobre as notícias que analisaram. Mas, como o número de usuários do verificador é muito alto e suas identidades são desconhecidas para os analistas, o analisador não pode conspirar com todos eles. Com isso, o número de pessoas honestas no sistema é maior do que os colaboradores e, no final das contas, a avaliação será feita de maneira correta.

Os repórteres podem conspirar com analistas para apoiar suas notícias, mas se a crença do público for baixa, o crédito dos analistas que a apoiam é reduzido. Como resultado, os

analistas não apoiam notícias falsas para evitar a perda de crédito.

A importância das notícias é diretamente proporcional ao crédito dos repórteres, dessa forma, o repórter não pode aumentar seu crédito com a publicação de notícias verdadeiras, mas sem valor. Além disso, repórteres podem criar várias identidades para confirmar suas notícias como analista. Entretanto, devido à baixa credibilidade das novas identidades, seu suporte não terá muito impacto nos cálculos. Além disso, se as análises fornecidas por eles não convencem os usuários, isso pode ter um efeito negativo sobre as crenças públicas.

4.1.8 Conclusão

Como o *Blockchain* forneceu uma estrutura para aplicativos descentralizados e confiáveis, ele pode ser usado para transmitir notícias anonimamente. Porém, nesta rede cada pessoa poderá veicular as notícias, possibilitando assim a geração de notícias falsas.

Este trabalho propôs um ambiente descentralizado para as pessoas compartilharem suas notícias e avaliarem outras notícias com base no *Blockchain* com a ajuda do contrato inteligente e DAPP.

A existência de terceiros no processo de publicação de notícias pode levar a problemas como a eliminação de algumas notícias ou a criação de notícias falsas. Por isso, se a notícia for publicada sem a presença de terceiros, as pessoas confiarão na notícia.

Deixando o problema de rastreio ainda em aberto. Por mais que exista uma classificação de notícias para ajudar no reconhecimento de FN. Este trabalho não verifica a possibilidade de um rastreio para ajudar a resolver o problema da identificação de uma fonte inicial.

4.2 FakeChain: *A Blockchain Architecture to Ensure Trust in Social Media Networks*

4.2.1 Motivação

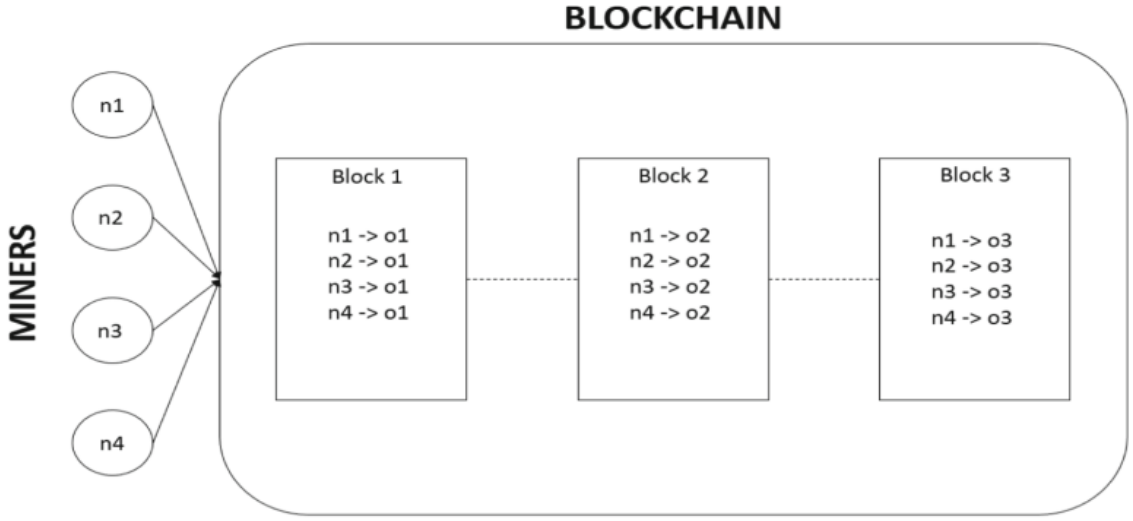
O período eleitoral tem grande importância em qualquer democracia, mas hoje em dia, diferentes grupos tentam tirar vantagem no processo democrático postando FN nas redes sociais. O uso da técnica de mineração de dados para identificar notícias falsas está em estágio de desenvolvimento e ainda não há uma solução holística para esse problema.

No trabalho de Ochoa *et al.* (2019), foi apresentado uma arquitetura de *Blockchain* centralizado com foco na detecção de FN. A principal característica da estrutura é o uso da mineração de dados como um algoritmo de consenso para autenticar as informações publicadas

nas redes sociais, onde é possível identificar FN, alertar leitores, punir quem dissolve esse tipo de informação e premiar quem publica informações verdadeiras na rede.

Na estrutura foi definido que cada fonte de notícias é considerada um nó da rede no *Blockchain*. Diante disso, todas as fontes de notícias também são mineradoras. O objetivo de utilizar este tipo de estrutura é garantir o nível de confiabilidade de cada fonte de rede, já que qualquer fonte que publica notícias pode ser avaliada por quem publica. A Figura 7 mostra a estrutura do **FakeChain**.

Figura 7 – Desenho da estrutura *FakeChain*



Fonte: Adaptado de Ochoa *et al.* (2019).

Com o objetivo de evitar o *spam* de FN nas redes sociais, foi usado um *Blockchain* centralizado. As fontes de notícias são consideradas nós completos, onde elas são responsáveis por fazer operações de leitura e escrita no *Blockchain*, além de participar do processo de mineração. Os clientes podem acessar as informações armazenadas no *Blockchain*, mas não podem publicar notícias.

4.2.2 Algoritmo de consenso

Como o algoritmo de consenso, foi considerado o *Truth Algorithm* quando um dos nós de mineração define a veracidade das notícias registradas de cada "fonte", esse nó ganha um aumento em seu grau de confiabilidade. Os nós que disseminam FN têm seu grau de confiabilidade diminuído como punição. Para ser justo com os nós que também publicaram notícias reais, mesmo que não possam minerar o bloco, eles também receberão um pequeno aumento em seu grau de confiabilidade para não monopolizar a rede com poder computacional.

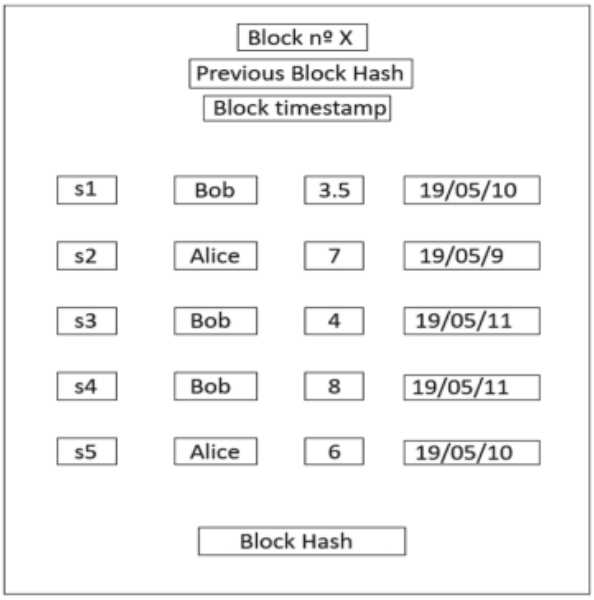
O algoritmo *Proof of Stake* (PoS) foi usado, onde nós com maior grau de confiabilidade têm mais chances de minerar novos blocos.

4.2.3 Estrutura do Blockchain

Dentro de cada bloco é armazenado o que cada "fonte" que publicou sobre um determinado objeto. Foi considerado que todo bloco é um objeto, portanto, toda notícia gerada é considerada um bloco para gerar transparência aos usuários devido à arquitetura de *Blockchain* centralizada, garantindo que o provedor de serviço que armazena o *Blockchain* não faça alterações sem o consentimento dos mineradores.

A Figura 8 mostra um exemplo de informação armazenada na estrutura interna de um bloco na arquitetura.

Figura 8 – Dados armazenados na *Blockchain* da estrutura *Fakechain*.



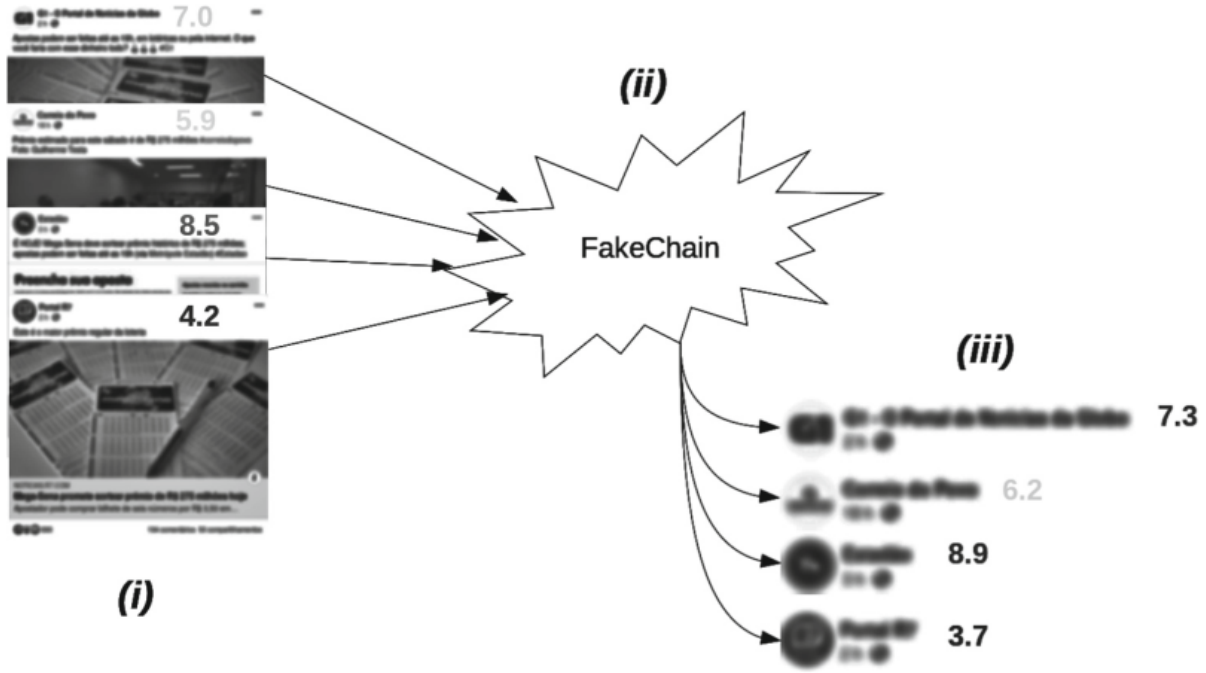
Fonte: Adaptado de Ochoa *et al.* (2019).

Armazenar dados em um *Blockchain* é uma operação cara, desta forma, as informações armazenadas foram metadados abstraídos das notícias publicadas. Onde cada bloco armazena a fonte, metadados da notícia publicada e o índice de confiabilidade da fonte após a publicação da notícia e a data de publicação da notícia. Utilizando este tipo de estrutura de blocos, tende a reduzir o custo de armazenamento das informações.

4.2.4 Avaliação de notícias

Foi usado o cenário do *Facebook* como exemplo na Figura 9.

Figura 9 – Arquitetura *Fakechain*.



Fonte: Adaptado de Ochoa *et al.* (2019).

Em **i)**: A notícia é veiculada na rede social por meio de uma fonte de notícias.

Em **ii)**: O *Blockchain* cria um bloco e adiciona o que outras fontes publicaram no mesmo objeto.

Em **iii)**: O bloco é extraído e os níveis de confiabilidade de cada fonte são atualizados conforme calculado pelo algoritmo de descoberta da verdade.

No trabalho, foi usado *Blockchain* como a fonte de processamento para o *Truth Algorithm*, reduzindo o custo de armazenamento de dados para garantir a autenticidade das informações, e a legibilidade das informações publicadas. O *Truth Algorithm* permite descobrir a veracidade de um fato (autenticidade) e atualizar o nível de confiabilidade de uma fonte com base nas notícias por ela publicadas.

A principal desvantagem observada foi o número de fontes de notícias para determinar a veracidade de um fato. Se houver um pequeno número de fontes de notícias, o valor do cálculo da veracidade da informação pode ser falso-negativo.

4.2.5 Conclusão

Neste artigo, foi apresentado uma arquitetura de *Blockchain* com foco na detecção de notícias falsas. Além disso foi necessário o estudo de técnicas de mineração de dados e *Blockchain*. E com a prova de conceito desenvolvido, foi comprovada a viabilidade de implementação da arquitetura referida. O contrato inteligente desenvolvido provou ser eficiente em termos de detecção de FN.

A simulação de uma situação real mostrou a eficácia da arquitetura proposta para identificação de FN, mais ainda existe o problema de rastreio em si de cada notícia considerada falsa. Deste modo é citado mais uma vez a carência de um armazenamento destinado a obter os metadados de cada artigo notícias.

4.3 *Fake News Detection in Social Media using Blockchain*

4.3.1 Motivação

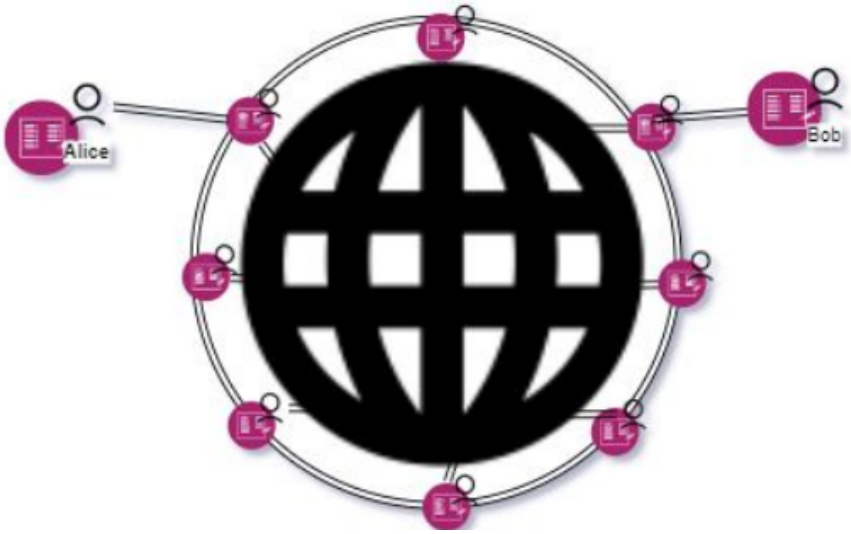
Ao longo dos anos, algumas fontes publicam FN atraentes devido à falta de qualquer sistema regulatório, essas notícias não podem ser verificadas. Portanto, essas fontes não confiáveis podem publicar o que quiserem e, mesmo em alguns casos, causam caos na sociedade. Nos últimos tempos, devido à facilidade na disponibilidade da Internet e nas mídias sociais, notícias inadequadas podem se espalhar mais rapidamente do que nunca.

Em alguns casos, as FN são mais atraentes que as reais. Assim, as pessoas ficam desorientadas. Usando as vantagens dos conceitos de rede ponto a ponto do *Blockchain*, discutiremos uma maneira de detectar FN nas mídias sociais.

(PAUL *et al.*, 2019) propõem um modelo para detectar FN onde foi usado o conceito de descentralização, contratos inteligentes do *Ethereum* e o algoritmo *Breadth First Search* (BFS) para calcular a proximidade de um usuário.

Neste modelo sempre que as notícias começam a ser criadas, elas serão transmitidas para uma *Blockchain*. Onde apenas as notícias que ultrapassarem um certo limite de viralidade, por exemplo, mais de 5.000 ações serão revisadas por usuários com pesos diferentes. A Figura 10 ilustra a visão do *Blockchain* nas mídias sociais.

Figura 10 – Compartilhamento de notícias no *Blockchain*



Fonte: Adaptado de Paul *et al.* (2019).

4.3.2 Estrutura do modelo proposto

Cada usuário pode revisar uma notícia de acordo com seu peso, onde será feito uma BFS nos usuários de acordo com a localidade da notícia. Uma classificação final foi gerada a partir de alguns cálculos simples e usando conceitos de BFS, *Blockchain* e contratos inteligentes.

A ideia proposta do modelo, foi integrar mídias sociais em um *Blockchain* de forma que usuários aleatórios (incluindo jornalistas) atuem como validadores de notícias. Por conta do anonimato, eles podem validar notícias sem nenhuma pressão externa. Portanto, eles não podem ser tendenciosos nem pressurizados por qualquer outra pessoa ou organização. Após a publicação das notícias, elas serão implantadas como uma transação em uma cadeia.

Após um certo nível de viralidade, os usuários como validador receberão uma solicitação para verificar essas notícias. Como validador, eles atribuirão um valor de correção para as notícias. A média desses valores será a autenticidade dessas notícias.

Depois da verificação, as notícias terão uma classificação de autenticidade de forma a mostrar ao usuário o nível de confiabilidade de cada notícia. Essa classificação será adicionada sempre que as notícias forem compartilhadas. As notícias terão uma classificação de autenticidade no topo e essa classificação será adicionada sempre que as notícias forem compartilhadas.

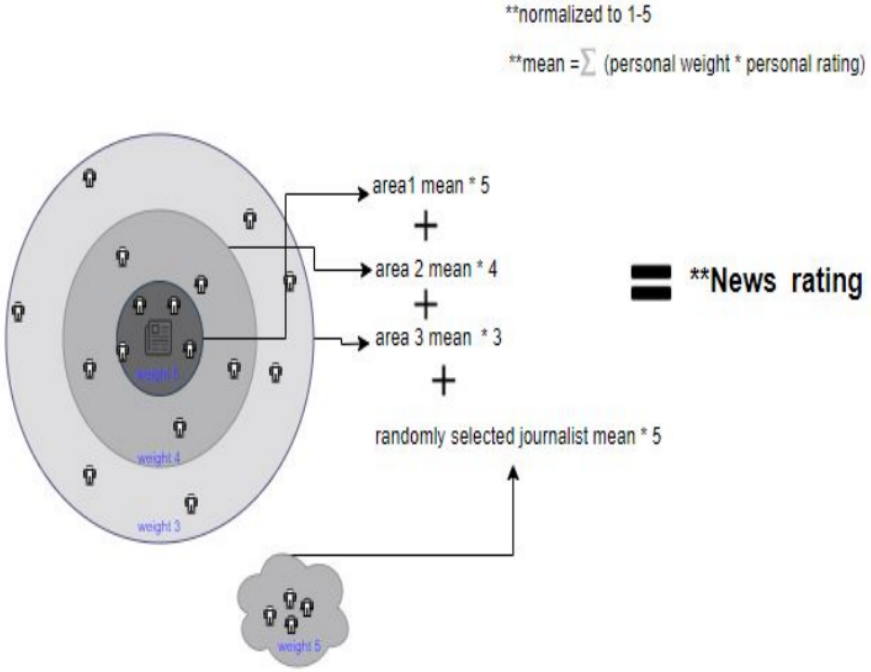
4.3.3 Implementação do modelo

As mídias sociais serão integradas ao *Blockchain*, onde podemos obter o ID do usuário. Sempre que as notícias forem criadas, elas serão transmitidas pela cadeia pela transação. Onde será revisada apenas as notícias em particular que ultrapassaram um certo limite de viralidade, por exemplo, mais de 5.000 ações. As notícias se espalharão pela cadeia.

Usuários gerais também podem receber as notícias, mas, inicialmente, essas notícias não possuem avaliações. Com o passar do tempo, os validadores fornecerão suas análises e as notícias aparecerão com uma classificação para os usuários. Essa classificação representa a correção/autenticidade de notícias específicas.

Existem dois tipos de pesos que desempenham um papel fundamental na determinação da probabilidade de um usuário ser selecionado como validador. Um peso está associado a cada usuário individual, e o outro peso está associado às fases de validação. A classificação mais alta do usuário também contribuirá mais do que a pessoa mais baixa na pontuação total onde é um processo de duas fases. A primeira fase tem um único peso associado, enquanto na segunda fase vários pesos estão associados ao seu nível correspondente. A Figura 11 ilustra o processo de classificação de notícias.

Figura 11 – Processo de geração de classificação de notícias



Fonte: Adaptado de Paul *et al.* (2019).

4.3.4 Fases do modelo

Na primeira fase os validadores são os usuários selecionados que trabalham em periódicos e jornais de um país específico, enquanto na segunda fase, os validadores serão selecionados com base na proximidade, ou seja, na área do incidente em que as notícias foram feitas.

Os validadores que são exatamente da mesma área têm o pico de peso para o cálculo da classificação em uma escala de 1 a 5. Os validadores podem ser indivíduos ou uma equipe de um portal de notícias. No sentido de inicializar o peso, a próxima prioridade será os validadores que são o vizinho mais próximo dessa área específica e os renomados portais de notícias.

No final de todo o processo de validação e verificação, as notícias possuirão um escala de 1 a 5, onde notícias que obtiverem 1, na escala de classificação de 1 a 5, não serão confiáveis e se alguma notícia obtiver 5, é altamente confiável. Essa classificação será exposta no topo de cada notícia, sempre que for transmitida.

Os validadores na *Blockchain* que estão validando as notícias para avaliações são conhecidos como menores. Os menores que são profissionais (por exemplo, portais de notícias, jornalistas etc.) são recompensados pela revisão válida das notícias da rede *Ethereum*.

4.3.5 Conclusão

Existem alguns desafios significativos para a adoção do *Blockchain*. Às vezes, se os menores estão sob influência política, podem observar que as notícias falsas são válidas, publicadas no apoio de seus partidos políticos. Portanto, usando a *Blockchain Ethereum*, é difícil detectar as notícias com base na política e na religião. Por seu sistema de verificação verídica, os periódicos e portais de notícias precisam enfrentar riscos de emprego, pois os levam a uma competição de obtenção de classificações.

Embora o *Blockchain* e a cadeia *Ethereum* possam evitar que os usuários sejam enganados ao ler notícias falsas nas mídias sociais, o consumo de poder computacional também não pode ser negligenciado. Apesar de ter algumas limitações, o método proposto poderá ser útil para detectar notícias falsas nas mídias sociais, pois espalhar notícias falsas pelas mídias sociais, o que é um grande problema.

4.4 ProBlock: *A novel approach for fake news detection*

4.4.1 Motivação

O mundo está mergulhando cada vez mais na era digital, e as fontes de primeira informação estão se movendo para as mídias sociais e portais de notícias online. As chances de ser mal informado aumentam à medida que nossa confiança em fontes de informação está ficando ambígua. A ausência de quaisquer determinantes da veracidade de tais notícias na Internet exige uma nova abordagem para determinar o quociente de veracidade de notícias não verificadas, aproveitando a tecnologia.

Com esse cenário (SENGUPTA *et al.*, 2021) apresenta um modelo dinâmico com um sistema de votação seguro, onde os revisores de notícias podem fornecer *feedback* sobre as notícias, e um modelo matemático probabilístico é usado para prever a veracidade da notícia com base no *feedback* recebido. Um modelo baseado em *Blockchain*, ***ProBlock*** é um *framework* proposto para que seja assegurada a veracidade das informações propagadas.

O ***ProBlock*** visa implementar um ambiente seguro de votação e armazenamento de notícias para detectar FN por meio de votação por maioria ponderada. Um modelo de votação por maioria pura é uma decisão que seleciona alternativas que possuem maioria, ou seja, mais da metade dos votos.

4.4.2 Estrutura do modelo proposto

O modelo de votação por maioria ponderada calcula uma pontuação com base na interpretação dos especialistas. O peso dos votos dos especialistas é avaliado usando uma abordagem de pontuação dinâmica, onde são consideradas as estatísticas de carreira dos especialistas e sua confiança em seu voto para o *news-Piece*. Um *exp-Score* é calculado para cada ciclo de revisão consistindo de entradas estáticas e dinâmicas para cada especialista.

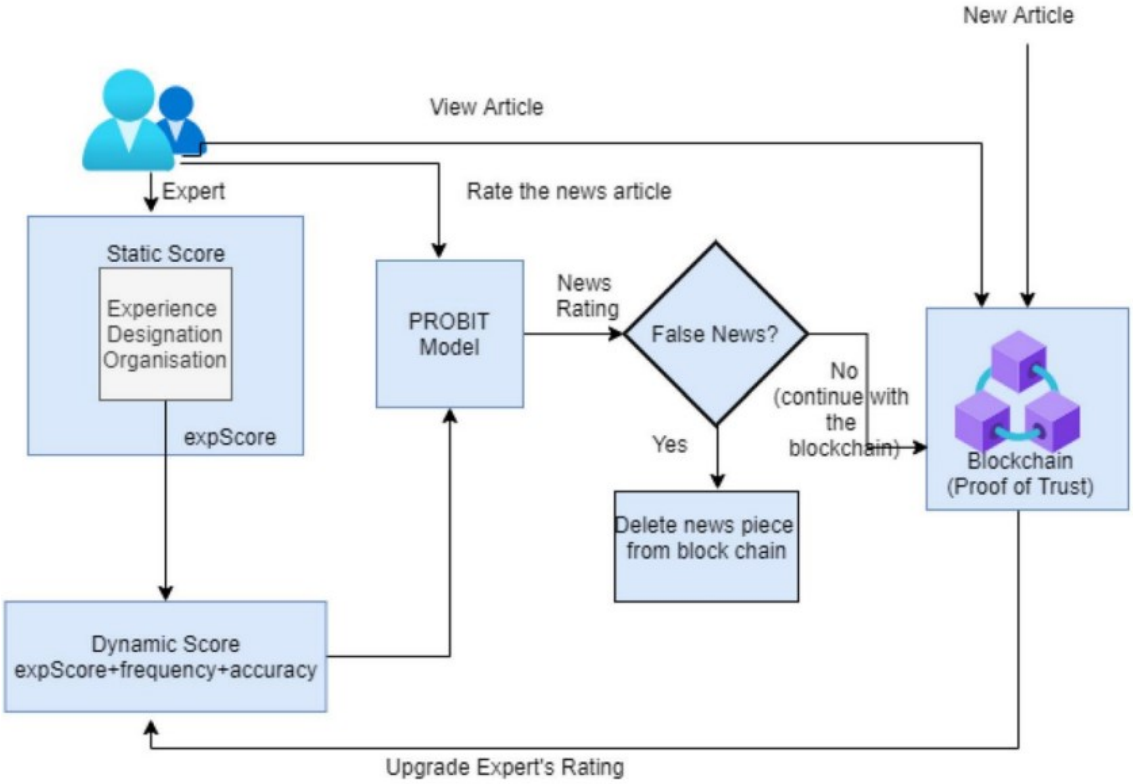
O *exp-Score* consiste em uma pontuação baseada na análise da experiência dos revisores, organização de afiliação e designação. A pontuação dinâmica é calculada com base na frequência do revisor e na precisão de cada revisão.

A probabilidade de o *news-Piece* ser genuíno é calculada usando o modelo *Pro-Bit*, onde as classificações de diferentes especialistas e seu *news-Piece* são considerados como entrada. Com base na classificação de notícias, onde as FN são excluídas da cadeia de blocos. O algoritmo de consenso *Proof of Trust* (PoT) é usado para a implementação do modelo.

Um *Blockchain* privado é usado para garantir a privacidade dos votos dos revisores em todos os momentos. O ***ProBlock*** envolve processos simplificados de manipulação de dados que não são acessíveis a todos os blocos. Os registros distribuídos criados por cada voto do revisor são transparentes e imutáveis.

No entanto, o modelo de votação por maioria pura é precário. O fator que torna esse modelo de votação por maioria pura bem-sucedido para detectar FN é que os votos de todos os revisores ou especialistas podem não estar no mesmo nível. Em termos de confiabilidade e experiência, alguns especialistas superam outros. A Figura 12 mostra a estrutura do **Problock**.

Figura 12 – Estrutura do *ProBlock*



Fonte: Adaptado de Sengupta *et al.* (2021).

4.4.3 Votação por maioria

Um modelo de votação por maioria pura é uma decisão que seleciona alternativas que possuem mais que metade dos votos. Cada voto é igual e tem o mesmo valor. Um modelo de votação majoritária pode ser incorporado para a detecção de FN e incluiria um painel de jornalistas, especialistas e revisores que estudariam e analisariam as notícias antes de serem carregadas no portal e tomariam decisões booleanas sobre sua veracidade.

Cada revisor ou especialista pode votar sobre a veracidade da notícia após uma verificação completa da notícia. Um modelo de votação por maioria pura idealmente teria apenas dois votos, reais ou falsos, e, portanto, o resultado do processo de votação seria determinístico, excluindo o caso de empate.

O modelo de votação por maioria ponderada é incorporado ao *Blockchain* por meio do protocolo de consenso PoT. No PoT, um *token* digital é enviado para os usuários da rede, e uma classe especial de usuários (especialistas neste caso) recebe um "quebra-cabeça" que deve ser resolvido, e suas soluções são comparadas. A solução que obtiver o maior número de respostas é considerada correta e o bloco é colocado na cadeia.

No cenário dado, o "quebra-cabeça" é o sistema de votação onde os especialistas dão votos (que são ponderados de acordo com os cálculos) e são comparados para encontrar a solução ou gama de soluções mais comum. Se para um determinado bloco, a solução está nas peças até a faixa totalmente confiável, o bloco é incorporado à cadeia

4.4.4 Sistema de votação

Para o ***ProBlock***, um sistema de votação é implementado criando uma classe de usuários composta por revisores, especialistas no assunto e jornalistas que são os eleitores do sistema de votação majoritária. Cada *news-Piece* é revisto e analisado por essa classe de usuários, e cada especialista passa por um voto semi-determinístico como um julgamento sobre a veracidade do *news-Piece*.

A pontuação relativa é atribuída a cada critério e ajuda a criar o perfil do especialista, o que ajuda a adicionar maior responsabilidade e confiança com o voto. O perfil do especialista ajuda a atribuir maior responsabilidade e confiança ao voto.

O componente dinâmico do *exp-Score* é calculado novamente após cada revisão. Baseia-se na frequência do revisor e na precisão de cada revisão. Com base no número de previsões corretas de avaliações para o número total de avaliações, o revisor recebe uma pontuação de precisão *acc-Score* que determina a taxa de sucesso do revisor. Ele atua como uma medida de confiabilidade para o sistema.

O algoritmo de consenso que está sendo usado é uma versão modificada do protocolo de consenso PoT padrão. A votação ponderada e o componente dinâmico adicionam ainda mais camadas de confiança em relação ao sistema, determinando a credibilidade do eleitor e seus votos correspondentes.

4.4.5 Conclusão

O modelo proposto por Sengupta *et al.* (2021) é de maneira geral abrangente para detecção de FN e vantajoso sobre as abordagens existentes em muitas dimensões. Onde ele pode lidar com qualquer tipo de notícia, seja texto, imagem, vídeo ou formato de áudio. A autenticidade do modelo é alta, pois considera o conhecimento especializado para testar as notícias, e é utilizada uma abordagem dinâmica de votação por peso que considera a credibilidade dos revisores.

As notícias são classificadas como falsas ou genuínas usando o modelo *Pro-Bit*. Todo o modelo é implementado usando a tecnologia *blockchain* que permite votação simultânea e *feedback* imediato para reduzir problemas de escalabilidade.

O modelo dado de detecção de notícias falsas por meio de uma análise probabilística em uma *Blockchain* pode se tornar mais eficiente com a implantação de um número maior de servidores na rede. O modelo pode ser implementado no *back-end* de uma aplicação web *front-end* para ser usado mais amplamente por um número maior de pessoas.

4.5 Ushare: *User controlled social media based on blockchain*

4.5.1 Motivação

O mundo moderno está se tornando cada vez mais movido por dados. Isso não se limita apenas à *Internet of Things* (IoT), computação móvel, redes de energia inteligentes e cidades, mas mais ainda nas redes sociais. Usuários e corporações agora estão conectados, interagindo e compartilhando dados entre si em um ritmo cada vez maior. A infraestrutura de tais serviços tem sido tradicionalmente suportada por redes centralizadas. No entanto, a falta de confiança, transparência e controle sobre as organizações.

Chakravorty e Rong (2017) apresentam o **Ushare**, uma rede social suportada por *Blockchain* centrada no usuário que permite a eles controlar, rastrear e reivindicar a propriedade de cada parte do conteúdo que compartilham. Onde Aproveitam os recursos *peer-to-peer* da tecnologia *Blockchain* que permite uma rede de distribuição de conteúdo verdadeiramente descentralizada, segura, anônima e rastreável.

O **Ushare** consiste em quatro componentes principais: o *Blockchain*, uma tabela de *hash* com conteúdo criptografado compartilhado por um usuário, um sistema de relaciona-

mento *turing* completo para controlar o número máximo de compartilhamentos realizados pelos membros do círculo do usuário e uma autoridade de certificação pessoal local que gerencia os círculos do usuário e criptografa os dados a serem compartilhados antes de serem transmitidos para a rede.

4.5.2 Modelo proposto

O **Ushare** permite que os usuários tenham controle sobre suas interações sociais. Ele apresenta um *Blockchain* exclusivo que descreve ativos como dados compartilhados ou transmitidos para a rede. Ao contrário dos sistemas de transição de estado regular que descrevem o status de propriedade dos ativos, ele descreverá um estado como um esgotamento de um valor de *token* que determina o número de transações ou compartilhamentos que podem ser executados com esse ativo.

Um sistema de relacionamento *Turing* Completo lidaria com a transição dos estados por meio da validação dos *tokens* até que eles se esgotassem completamente. Por fim, uma Autoridade de Certificação Pessoal (PCA) baseada no cliente manteria os relacionamentos de um usuário e garantiria que os ativos criptografados que foram compartilhados fossem visíveis apenas pelo círculo pretendido de membros.

O **Ushare** pode ser classificado como um *Blockchain* autorizado, pois os atores da rede precisam ser nomeados para desenvolver consistência, responsabilidade e rastreabilidade dos dados compartilhados. E pode contar com um conjunto de terceiros para realizar a verificação de cada novo usuário que ingressa na rede, assumindo a eles uma identidade única. Uma transação no **Ushare** é feita entre um usuário e os membros pertencentes ao círculo do usuário. O PCA cria uma versão criptografada dos dados com a chave pública do círculo e os armazena em uma tabela de *hash* distribuída.

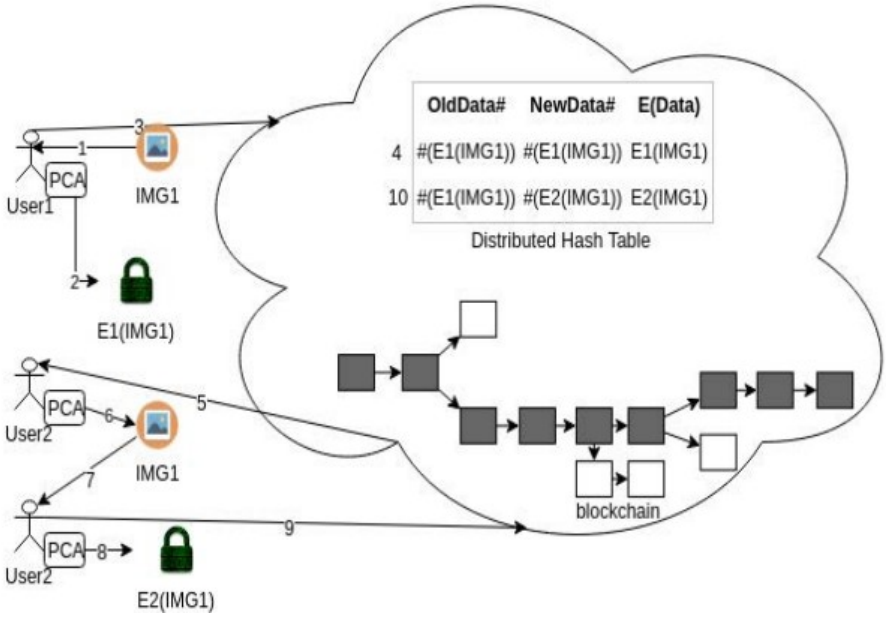
Como vários usuários podem criptografar os dados para compartilhar entre seus próprios círculos, a tabela de *hash* contém três colunas. O primeiro é o *hash* do item de dados criptografado compartilhado com eles, o segundo é o *hash* do item de dados descriptografado e criptografado novamente usando a chave pública de seu círculo para outros compartilhamentos e a terceira coluna armazena esse item de dados que eles criptografaram.

O usuário compartilha o *hash* id dos dados criptografados com cada membro de seu círculo. Isso permite a manutenção da rastreabilidade precisa e o controle sobre a capacidade de compartilhamento. As transações são transmitidas para o *Blockchain* com a identidade do

usuário e o *hash* id de dados para registrar as trilhas. Ele também contém um valor de *token*, definido pelo proprietário dos dados, que especifica o número permitido de compartilhamentos adicionais. Sempre que uma transação é transmitida, o Sistema de Relacionamento é acionado e verifica se o compartilhamento é permitido verificando o valor do *token*.

Os compartilhamentos de um usuário podem ser do tipo imagem ou vídeo. Esses são arquivos de tamanhos grandes e precisam ser armazenados de maneira distribuída para armazenamento. O próprio *Blockchain* conteria as transações em termos de compartilhamentos de usuários, referindo-se ao *hash* um id compartilhado de um arquivo. A Figura 13 mostra o fluxo de trabalho para criar a tabela de *hash*.

Figura 13 – Fluxo de trabalho da tabela *hash*



Fonte: Adaptado de Chakravorty e Rong (2017).

Um usuário, **User1**, obtém uma imagem **IMG1(1)** e a criptografa com a chave pública do círculo com quem será compartilhada usando o **PCA(2)**. O usuário então armazena a imagem criptografada em **Ushare *hash* table(3)** com o *hash* de sua imagem criptografada como ***OldData*** e ***NewData*****(4)**.

Como o usuário é o proprietário da imagem, as chaves *hash* antigas e novas são as mesmas. Outro usuário, **User2**, é um membro do círculo que tem acesso à imagem compartilhada. Depois de percorrer o *Blockchain*, o usuário pode acessar a imagem da **tabela *hash*(3)** e **descriptografá-la(6)**. Este usuário agora compartilha novamente esta **imagem (7)** com seu círculo, criptografando-a com a **chave pública do círculo (8)**. Essa imagem criptografada é armazenada na **tabela *hash* (10)** com a chave *hash* da criptografia anterior como ***oldData*** e seu

novo *hash* como ***NewData***.

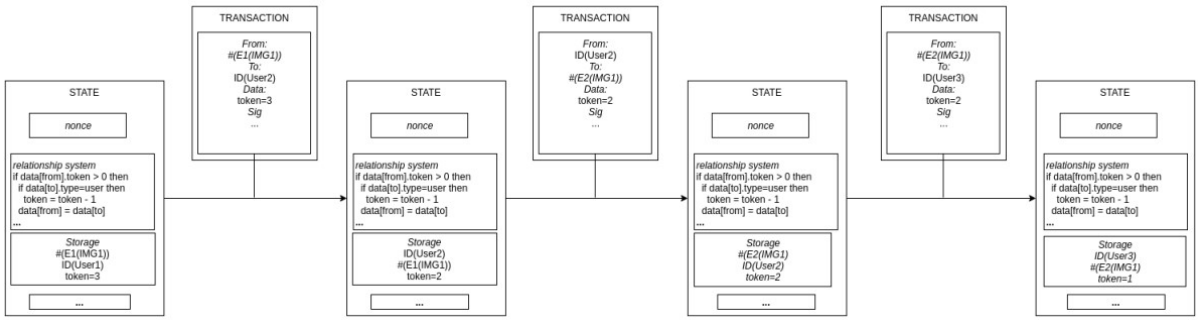
4.5.3 Blockchain Ushare

Um usuário que deseja compartilhar um item de dados com seu círculo, cria a primeira transmissão como uma transação com sua identidade como “de” e a chave *hash* do item de dados criptografado como endereço “para”. A transação também contém um “valor de *token*” que especifica o número de compartilhamentos permitidos com aquele item de dados.

Em seguida, o usuário transmite várias transações, cada uma contendo a chave de *hash* de dados criptografados como endereço e identidade dos membros do círculo como endereço. O valor do *token* também está presente na transação. Quaisquer compartilhamentos feitos com este item de dados fazem outra transação com a identidade do novo usuário a partir do endereço e do *hash* dos dados criptografados com a chave de círculo deste novo usuário como endereço.

Em seguida, várias transações são novamente feitas para os membros do círculo desse usuário com a nova chave *hash* de e a identidade dos membros do círculo do usuário como endereço. Uma transação contém um endereço de origem, um endereço de destino, o valor dos dados e uma assinatura digital. A Figura 14 mostra as transições de estado.

Figura 14 – Transições de estado do *Ushare*



Fonte: Adaptado de Chakravorty e Rong (2017).

4.5.4 Sistema de Relacionamento

O sistema de relacionamento seria uma unidade programável Turing completa que permanece como parte do *Blockchain*. Ele pode apresentar *loops*, estados internos e até fazer transações com outros atores. O principal objetivo deste sistema é verificar se as transações compartilhadas são válidas. Antes de criar um estado, ele verifica o valor do *token* e o decrementa.

Sempre que um valor de *token* chega a zero, ele reverte para o estado anterior e não permite nenhum compartilhamento futuro desse item de dados.

4.5.5 Autoridade de Certificação Pessoal (PCA)

O PCA é um software cliente que gerencia os círculos de um usuário, compartilha com segurança as chaves privadas dos círculos com seus membros, mantém registros das chaves compartilhadas com ele e criptografa todos os dados compartilhados com um círculo com sua chave pública. O gerenciamento de chaves para PCA pode ser construído sobre a solução *Bitcoin Wallet* existente. No entanto, com o crescimento do *Blockchains* com vários círculos e membros, os principais problemas de gerenciamento podem ter um grande impacto na segurança e no desempenho.

4.5.6 Conclusão

A descentralização, o anonimato, a rastreabilidade e a resistência à censura das *Blockchains* poderiam suportar o **Ushare**.

As funcionalidades seriam entregues por meio de quatro componentes principais: o *Blockchain* que manteria o registro da propriedade dos itens de dados e o número de compartilhamentos feitos, um sistema de relacionamento que permitiria que o código programável fosse executado no *Blockchain* e controlasse o número de compartilhamentos permitidos para um item de dados, uma tabela de *hash* que armazena dados criptografados que o usuário compartilha e, finalmente, uma autoridade de certificação pessoal local que gerencia os círculos de um usuário, chaves de criptografia e controla o acesso ao conteúdo.

5 SÍNTESE DOS RESULTADOS

Nesta seção, apresentaremos os principais resultados obtidos a partir da análise dos cinco artigos relacionados ao uso do *blockchain* no combate às FN. Os resultados estão organizados de acordo com os temas identificados nos estudos revisados. Com base na análise dos artigos selecionados, é possível identificar os pontos fortes e fracos de cada um.

5.1 Análise dos artigos selecionados

O Quadro 2 apresenta uma comparação dos principais aspectos abordados nos artigos do trabalho. Essa análise comparativa oferece uma visão geral das metodologias, objetivos, contribuições e resultados obtidos em cada estudo, onde permite uma fácil visualização das diferenças e semelhanças entre os artigos, fornecendo percepções importantes sobre as abordagens utilizadas no trabalho proposto.

Quadro 2 – Quadro Comparativo dos Artigos

Artigo	**Metodologia**	**Objetivo**	**Contribuições**	**Resultados Obtidos**
SANUB	Métodos estatísticos	Detecção de FN	Método baseado em análise de padrões linguísticos para identificar notícias falsas	Alcançou uma taxa de acurácia de 90% na detecção de FN
FakeChain	Blockchain	Confiança em redes sociais	Arquitetura baseada em *blockchain* para garantir a confiabilidade das informações em redes sociais	Demonstra que a arquitetura proposta melhora a confiança dos usuários em relação às informações compartilhadas
ProBlock	Aprendizado de Máquina	Detecção de FN	Método de detecção de FN baseado em algoritmos de aprendizado de máquina	Alcançou uma taxa de detecção de 85% na identificação de notícias falsas
Ushare	Blockchain	Controle do usuário em redes sociais	Uma plataforma baseada em *blockchain* que permite aos usuários ter controle sobre o conteúdo compartilhado em redes sociais	Mostra que os usuários têm maior confiança e controle sobre as informações compartilhadas
FNDSM	Blockchain	Detecção de FN em redes sociais	Método baseado em *blockchain* para detectar e combater FN em redes sociais	Alcançou uma precisão de 92% na detecção de FN em uma rede social simulada

Fonte: elaborado pelo autor.

Podemos observar que diferentes metodologias foram utilizadas, incluindo métodos estatísticos, uso de *blockchain* e algoritmos de aprendizado de máquina. Cada artigo teve como

objetivo principal, combater a disseminação de FN, buscando aumentar a confiança dos usuários e garantir a integridade das informações compartilhadas.

5.2 SANUB: A new method for Sharing and Analyzing News Using Blockchain

Os autores propõem um novo método para compartilhar e analisar notícias utilizando a tecnologia *blockchain*. Os autores apresentam uma arquitetura que permite a verificação da autenticidade e integridade das notícias, bem como a rastreabilidade de sua origem. A utilização do *blockchain* proporciona maior transparência e confiabilidade na disseminação de informações, contribuindo para combater as FN.

- **Pontos Fortes:** Propõe um método inovador para compartilhamento e análise de notícias usando *blockchain*. Aumenta a confiabilidade na verificação de notícias.
- **Pontos Fracos:** A metodologia utilizada foi baseada principalmente em estudos de caso e experimentação, o que pode limitar a generalização dos resultados. Pode exigir uma infraestrutura complexa para implementação em larga escala.

5.3 FakeChain: *A Blockchain Architecture to Ensure Trust in Social Media Networks*

Os autores propõem uma arquitetura baseada em *blockchain* para garantir a confiança em redes sociais. Através do uso de contratos inteligentes e registros imutáveis, a plataforma FakeChain busca detectar e prevenir a disseminação de notícias falsas. A utilização do *blockchain* permite a criação de um ambiente seguro e confiável para compartilhamento de informações.

- **Pontos Fortes:** Apresenta uma arquitetura de *blockchain* que visa garantir confiança em redes sociais. Realiza simulações e implementação para validar a eficácia da abordagem.
- **Pontos Fracos:** Ainda está em fase de desenvolvimento e pode exigir mais estudos e testes para avaliar sua viabilidade em diferentes cenários. Pode enfrentar desafios de escalabilidade ao lidar com grandes volumes de dados em redes sociais.

5.4 *Fake News Detection in Social Media using Blockchain* (FNDSM)

Os resultados obtidos nesse estudo demonstraram que a abordagem utilizando *blockchain* para a detecção de FN em redes sociais apresentou altas taxas de detecção de notícias

falsas, ao mesmo tempo em que minimizou os falsos positivos. Isso indica que a utilização da tecnologia *blockchain* pode ser uma solução promissora para combater a disseminação de FN, oferecendo maior confiabilidade e transparência na detecção e verificação de informações.

- **Pontos Fortes:** O artigo aborda a detecção de FN em redes sociais usando a tecnologia *blockchain*. Ele apresenta uma metodologia que combina técnicas de aprendizado de máquina e a imutabilidade da *blockchain* para identificar e filtrar notícias falsas. Também fornece uma análise empírica dos resultados, demonstrando a eficácia da abordagem proposta.
- **Pontos Fracos:** O artigo pode não abordar detalhadamente os desafios de implementação da solução proposta em larga escala. Além disso, pode faltar uma discussão aprofundada sobre os possíveis impactos e limitações da utilização da *blockchain* na detecção de FN. E por último, é necessário levar em conta a escalabilidade e os custos associados ao uso da tecnologia *blockchain* em sistemas de detecção de FN em redes sociais.

5.5 ProBlock: *a novel approach for fake news detection*

O estudo apresenta uma abordagem inovadora para detecção de notícias falsas. Os pesquisadores utilizam técnicas de NLP e análise de sentimento em conjunto com a tecnologia *blockchain* para identificar e verificar a veracidade das notícias. A integração do *blockchain* proporciona maior confiabilidade e imutabilidade aos resultados obtidos.

- **Pontos Fortes:** Propõe uma abordagem inovadora para detecção de notícias falsas. Utiliza experimentação e análise estatística para validar a eficácia da abordagem.
- **Pontos Fracos:** Pode enfrentar desafios na detecção de notícias falsas sofisticadas que se adaptam às técnicas de detecção. A precisão da detecção pode depender da disponibilidade e qualidade dos conjuntos de dados utilizados.

5.6 Ushare: user controlled social media based on blockchain

O artigo propõe uma plataforma de mídia social baseada em *blockchain*, chamada **Ushare**, que coloca o controle das informações nas mãos dos usuários. Através do uso do *blockchain*, os usuários têm maior autonomia sobre o compartilhamento de conteúdo e podem verificar

a autenticidade das informações compartilhadas. Essa abordagem contribui para combater a propagação de FN em redes sociais.

- **Pontos Fortes:** Propõe uma plataforma de mídia social baseada em *blockchain* controlada pelos usuários. Enfatiza o controle e a transparência do usuário sobre o compartilhamento de informações.
- **Pontos Fracos:** Ainda está em fase de desenvolvimento e pode enfrentar desafios de adoção em massa pelos usuários. Requer uma infraestrutura robusta e uma comunidade ativa de usuários para funcionar de forma eficaz.

5.7 Considerações

A comparação entre os trabalhos selecionados revela que cada um deles oferece contribuições significativas para a detecção e combate às FN, bem como para o fortalecimento da confiança nas informações compartilhadas. Embora os métodos e abordagens possam variar, todos os artigos buscam soluções inovadoras para lidar com o problema das FN, utilizando tecnologias como *blockchain*, NLP e aprendizado de máquina. Essas pesquisas fornecem *insights* valiosos para a compreensão do tema e indicam possíveis direções futuras para o avanço nessa área.

6 LIMITAÇÕES

A presente pesquisa possui algumas limitações que devem ser consideradas ao interpretar os resultados:

- **Limitações de amostra:** Alguns estudos tiveram uma amostra pequena, o que pode limitar a generalização dos resultados para uma população maior. Amostras maiores podem ser necessárias para obter conclusões mais robustas.
- **Limitações de metodologia:** Alguns estudos utilizaram metodologias específicas que podem ter suas próprias limitações. Por exemplo, algumas abordagens de detecção de FN podem não ser totalmente precisas ou eficientes em identificar todas as informações falsas.
- **Limitações de aplicabilidade:** Alguns estudos podem ter focado em contextos ou plataformas específicas, o que pode restringir a aplicabilidade dos resultados a outros cenários. É importante considerar a adaptabilidade das abordagens propostas em diferentes contextos.
- **Limitações de dados:** Alguns estudos podem ter enfrentado desafios na obtenção de conjuntos de dados representativos ou de alta qualidade. A disponibilidade limitada de dados confiáveis e rotulados de FN pode afetar a precisão e eficácia dos modelos e algoritmos utilizados.
- **Limitações de validação:** Alguns estudos podem ter enfrentado dificuldades na validação e avaliação dos resultados. A falta de métricas padronizadas para avaliar a detecção de FN pode dificultar a comparação entre diferentes abordagens.

É importante considerar essas limitações ao interpretar os resultados dos estudos e ao aplicar suas conclusões em outros contextos. Futuras pesquisas podem abordar essas limitações para aprimorar a compreensão e eficácia das abordagens de detecção e combate às FN.

7 CONCLUSÕES E TRABALHOS FUTUROS

A partir da análise dos artigos relacionados ao uso do *blockchain* no combate às FN, foi possível observar que essa tecnologia tem sido amplamente explorada como uma solução promissora para lidar com esse desafio crescente na sociedade atual. Os estudos revisados demonstraram diferentes abordagens e perspectivas em relação ao papel do *blockchain* na verificação da autenticidade, integridade e confiabilidade das informações compartilhadas.

Uma das principais vantagens identificadas no uso do *blockchain* é a sua capacidade de criar registros imutáveis e transparentes, o que contribui para aumentar a confiança nas informações disseminadas. Através do uso de contratos inteligentes, é possível estabelecer regras e mecanismos de verificação que dificultam a propagação de FN.

Além disso, algumas propostas apresentaram a importância do controle do usuário sobre as informações compartilhadas. A capacidade de rastrear a origem das notícias e permitir que os usuários tenham autonomia para verificar a veracidade dos conteúdos contribui para a construção de um ambiente mais seguro e confiável.

Apesar das abordagens promissoras apresentadas, é importante ressaltar que a aplicação prática do *blockchain* no combate às FN ainda enfrenta desafios significativos. A escalabilidade, a privacidade dos dados e a adoção em larga escala são algumas das questões que precisam ser consideradas e abordadas para que o potencial do *blockchain* seja plenamente explorado nesse contexto.

Aperfeiçoamento de algoritmos de detecção: Os estudos revisados propuseram diferentes abordagens para a detecção de FN, incluindo o uso de técnicas de processamento de linguagem natural e aprendizado de máquina. No entanto, existem oportunidades para aprimorar e desenvolver novos algoritmos mais eficazes, capazes de lidar com o constante surgimento de técnicas sofisticadas de criação de FN.

Melhoria da escalabilidade e eficiência do *blockchain*: Um desafio significativo no uso do *blockchain* é a sua limitação em termos de escalabilidade e capacidade de processamento. Trabalhos futuros podem explorar soluções para melhorar a capacidade de processamento das redes *blockchain*, tornando-as mais eficientes e capazes de lidar com um grande volume de transações.

Exploração de técnicas de consenso alternativas: Os estudos revisados propuseram diferentes mecanismos de consenso para validar as informações no contexto do *blockchain*. Futuras pesquisas podem investigar técnicas de consenso alternativas, buscando uma combinação

ideal de escalabilidade, segurança e eficiência para o contexto específico da detecção de FN.

Avaliação de aspectos legais e éticos: O uso do *blockchain* para combater as FN levanta questões legais e éticas, como a privacidade dos usuários e a responsabilidade pelos conteúdos compartilhados. Trabalhos futuros podem investigar a melhor forma de lidar com essas questões, buscando um equilíbrio entre a segurança e a privacidade dos usuários.

Implementação de sistemas práticos: Embora os estudos revisados tenham proposto abordagens teóricas e arquiteturas conceituais, é necessário realizar implementações práticas desses sistemas. Trabalhos futuros podem se concentrar na construção de plataformas reais baseadas em *blockchain* para a detecção e combate às FN, a fim de avaliar a viabilidade e a eficácia dessas soluções em um ambiente de produção.

Colaboração e padronização: O combate às FN é um desafio global que requer esforços colaborativos entre pesquisadores, profissionais da área, legisladores e plataformas de mídia social. Trabalhos futuros podem explorar a colaboração entre diferentes partes interessadas e a criação de padrões e diretrizes para o uso do *blockchain* no combate às FN, a fim de promover uma abordagem mais unificada e eficaz.

Dessa forma, concluímos que o *blockchain* possui um papel relevante na mitigação das FN, fornecendo maior confiabilidade, transparência e controle aos usuários. A interdisciplinaridade entre as áreas de *blockchain*, ciência da computação e comunicação é fundamental para avançar nesse campo de pesquisa e desenvolver soluções efetivas que enfrentem o desafio das FN.

É importante ressaltar que a presente pesquisa bibliográfica e comparativa proporcionou uma visão ampla e atualizada sobre o estado da arte do uso do *blockchain* no contexto das FN. Contudo, novas pesquisas e investigações são necessárias para aprofundar o conhecimento e explorar ainda mais as potencialidades dessa tecnologia.

Em resumo, o uso do *blockchain* no combate às FN é um campo promissor que requer pesquisas e desenvolvimentos contínuos. Trabalhos futuros podem se concentrar em aprimorar algoritmos de detecção, melhorar a escalabilidade do *blockchain*, explorar técnicas de consenso alternativas, abordar questões legais e éticas, implementar sistemas práticos e promover colaboração e padronização. Esses esforços podem contribuir para o desenvolvimento de soluções mais robustas e eficazes para lidar com o problema das FN na era da informação digital.

REFERÊNCIAS

ALLCOTT, H.; GENTZKOW, M. Social media and fake news in the 2016 election. **Journal of economic perspectives**, v. 31, n. 2, p. 211–36, 2017. Acesso em: 10 jul. 2023.

ANGELIS, S. D. Assessing security and performances of consensus algorithms for permissioned blockchains. **arXiv preprint arXiv:1805.03490**, 2018. Acesso em: 10 jul. 2023.

APRÁ, A. Estudo da usp embasa lista dos 10 maiores sites de "falsas notícias" no brasil. **Isso é notícia**, 2017. Disponivel em: https://bemblogado.com.br/site/estudo-da-usp-embasa-lista-dos-10-maiores-sites-de-falsas-noticias-no-brasil. Acesso em: 10 jul. 2023.

BALLOUSSIER, A. V. Movido por notícia falsa, homem atira dentro de pizzaria nos eua. **Folha de São Paulo**, 2016. Disponível em: https://www1.folha.uol.com.br/mundo/2016/12/1838481-movido-por-noticia-falsa-homem-atira-dentro-de-pizzaria-nos-eua.shtml. Acesso em: 10 jul. 2023.

BALOUCHESTANI, A.; MAHDAVI, M.; HALLAJ, Y.; JAVDANI, D. Sanub: A new method for sharing and analyzing news using blockchain. In: IEEE. **2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)**. [*S. l.*], 2019. p. 139–143. Acesso em: 10 jul. 2023.

CARNEIRO, F. L. **Fake news propagadas por meio digital no Brasil**: desafios para a governança e a gestão pública contemporânea. [*S. l.*], 2018. Acesso em: 10 jul. 2023.

CHAKRAVORTY, A.; RONG, C. Ushare: user controlled social media based on blockchain. In: **Proceedings of the 11th international conference on ubiquitous information management and communication**. [*S. l.*: *s. n.*], 2017. p. 1–6. Acesso em: 10 jul. 2023.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **Ieee Access**, Ieee, v. 4, p. 2292–2303, 2016. Acesso em: 10 jul. 2023.

GOMES, N. L. C. **Uma análise acerca do fenômeno das fake news no processo eleitoral e suas interfaces com o direito fundamental à liberdade de expressão**. [*S. l.*], 2018. Acesso em: 10 jul. 2023.

GREVE, F. G.; SAMPAIO, L. S.; ABIJAUDE, J. A.; COUTINHO, A. C.; VALCY, Í. V.; QUEIROZ, S. Q. Blockchain e a revolução do consenso sob demanda. **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos**, 2018. Acesso em: 10 jul. 2023.

ISLAM, A.; KADER, M. F.; ISLAM, M. M.; SHIN, S. Y. Newstradcoin: A blockchain based privacy preserving secure news trading network. In: **IC-BCT 2019**. [*S. l.*]: Springer, 2020. p. 21–32. Acesso em: 10 jul. 2023.

JOHNSTON, M. Privacy implications of blockchain. In: SPRINGER. **International Conference on Cybersecurity**. [*S. l.*], 2018. p. 164–176. Acesso em: 10 jul. 2023.

LEE, D. M. S.; LEE, D.; KIM, H.; LEE, H. Blockchain as an enabler for media trust: Insights from multiple stakeholders. In: **Proceedings of the 52nd Hawaii International Conference on System Sciences**. [*S. l.*: *s. n.*], 2019. Acesso em: 10 jul. 2023.

LI, X.; JIANG, P.; CHEN, T.; LUO, X.; WEN, Q. A survey on the security of blockchain systems. **Future Generation Computer Systems**, Elsevier, v. 107, p. 841–853, 2020. Acesso em: 10 jul. 2023.

MARCHI, R. With facebook, blogs, and fake news, teens reject journalistic "objectivity". **Journal of communication inquiry**, SAGE Publications Sage CA: Los Angeles, CA, v. 36, n. 3, p. 246–262, 2012. Acesso em: 10 jul. 2023.

MARUMO, F. S. **Deep Learning para classificação de Fake News por sumarização de texto**. [*S. l.*]: Londrina, 2018. Acesso em: 10 jul. 2023.

MASSESSI, D. Public vs private blockchain in a nutshell. **Hentet**, v. 17, n. 2019, 2018. Acesso em: 10 jul. 2023.

NAKAMOTO, S. *et al.* **Bitcoin**: A peer-to-peer electronic cash system. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 jul. 2023.

NETO, M. M.; COUTINHO, E. F.; MOREIRA, L. O. Reflexoes sobre os aspectos sociais da tecnologia blockchain na pandemia do sars-cov2. **Revista Sistemas e Mídias Digitais**, v. 5, p. 20–34. Acesso em: 10 jul. 2023.

NEVES, B. C.; BORGES, J. Por que as fake news têm espaço nas mídias sociais? : uma discussão a luz do comportamento infocomunicacional. **Informação amp;amp; Sociedade: Estudos**, v. 30, n. 2, abr. 2020. Acesso em: 10 jul. 2023.

NEWMAN, N.; FLETCHER, R.; KALOGEROPOULOS, A.; LEVY, D.; NIELSEN, R. K. Reuters institute digital news report. **Reuters Institute**, 2017. Acesso em: 10 jul. 2023.

NIKITIN, V.; PETROV, I.; IVANOV, I. Formal verification of smart contracts for combating fake news. **Journal of Blockchain Research**, 2021. Acesso em: 10 jul. 2023.

OCHOA, I. S.; MELLO, G. de; SILVA, L. A.; GOMES, A. J.; FERNANDES, A. M.; LEITHARDT, V. R. Q. Fakechain: A blockchain architecture to ensure trust in social media networks. In: SPRINGER. **International Conference on the Quality of Information and Communications Technology**. [*S. l.*], 2019. p. 105–118. Acesso em: 10 jul. 2023.

OUYANG, L.; LI, L.; XIE, Y.; WANG, Q. Blocknews: A blockchain-based framework for trustworthy news sharing. **Journal of Information Security and Applications**, Elsevier, v. 51, p. 102430, 2020. Acesso em: 10 jul. 2023.

PAUL, S.; JOY, J. I.; SARKER, S.; AHMED, S.; DAS, A. K. *et al.* Fake news detection in social media using blockchain. In: IEEE. **2019 7th international conference on smart computing & communications (ICSCC)**. [*S. l.*], 2019. p. 1–5. Acesso em: 10 jul. 2023.

PÉREZ-SOLÀ, C.; BREGOLI, L.; VATTANI, A. Trustworthy digital journalism based on blockchain. **Electronics**, Multidisciplinary Digital Publishing Institute, v. 9, n. 11, p. 1941, 2020. Acesso em: 10 jul. 2023.

RAMÍREZ, J. P. V. Contratos inteligentes. **Revista de Investigación en Tecnologías de la Información**, v. 7, n. 14, p. 1–10, 2019. Acesso em: 10 jul. 2023.

SENGUPTA, E.; NAGPAL, R.; MEHROTRA, D.; SRIVASTAVA, G. Problock: a novel approach for fake news detection. **Cluster Computing**, Springer, v. 24, n. 4, p. 3779–3795, 2021. Acesso em: 10 jul. 2023.

SENRA, R. Na semana do impeachment, 3 das 5 notícias mais compartilhadas no facebook são falsas. **BBC. Brasília**, v. 17, 2017. Disponível em: https://www.bbc.com/portuguese/noticias/2016/04/160417_noticias_falsas_redes_brasil_fd. Acesso em: 10 jul. 2023.

SHU, K.; SLIVA, A.; WANG, S.; TANG, J.; LIU, H. Fake news detection on social media: A data mining perspective. **ACM SIGKDD Explorations Newsletter**, v. 19, 08 2017. Acesso em: 10 jul. 2023.

SMITH, J.; GARCIA, M. Tracking fake news: An exploratory study of online fact-checking tools. **Journal of Media Studies**, Mary Ann Liebert, Inc., publishers 140 Huguenot Street, 3rd Floor New, v. 15, n. 2, p. 45–62, 2020. Acesso em: 10 jul. 2023.

SMITH, J.; JOHNSON, M. Blockchain-based news verification system using smart contracts. In: **IEEE International Conference on Blockchain and Cryptocurrency**. [*S. l.*: *s. n.*], 2022. Acesso em: 10 jul. 2023.

SOARES, I.; DAVEY-ATTLEE, F. **The fake news machine**: Inside a town gearing up for 2020. [*S. l.*], 2017. Disponível em: https://money.cnn.com/interactive/media/the-macedonia-story/. Acesso em: 10 jul. 2023.

SWAN, M. **Blockchain**: Blueprint for a new economy. [*S. l.*]: O'Reilly Media, 2015. Acesso em: 10 jul. 2023.

TSCHORSCH, F.; SCHEUERMANN, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. **IEEE Communications Surveys & Tutorials**, IEEE, v. 18, n. 3, p. 2084–2123, 2016. Acesso em: 10 jul. 2023.

UNDERWOOD, S. **Blockchain beyond bitcoin**. [*S. l.*]: ACM New York, NY, USA, 2016. Acesso em: 10 jul. 2023.

VANCE, T. R.; VANCE, A. Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology. In: IEEE. **2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)**. [*S. l.*], 2019. p. 107–112. Acesso em: 10 jul. 2023.

VICTOR, F. Noticias falsas existem desde o século 6, afirma historiador robert darnton. **Folha de São Paulo**, 2017. Disponível em: http://www1.folha.uol.com.br/ilustrissima/2017/02/1859726-noticias-falsas-existem-desde-o-seculo-6-afirma-historiador-robert-darnton.shtml. Acesso em: 10 jul. 2023.

WANG, Q.; LI, Z.; ZHANG, W. A blockchain-based news tracking system for combating fake news. **International Journal of Distributed Sensor Networks**, 2021. Acesso em: 10 jul. 2023.

YAGA, D.; MELL, P.; ROBY, N.; SCARFONE, K. Blockchain technology overview. **arXiv preprint arXiv:1906.11078**, 2019. Acesso em: 10 jul. 2023.

YANO, I.; SANTOS, E.; CASTRO, A.; BERGIER, I.; SANTOS, P.; OLIVEIRA, S.; ABREU, U. **Bovine livestock tracking through Smart Contracts with Blockchain technology**. 2018. Acesso em: 10 jul. 2023.

ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: A survey. **International Journal of Web and Grid Services**, Inderscience Publishers (IEL), v. 14, n. 4, p. 352–375, 2018. Acesso em: 10 jul. 2023.