

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DO RIO GRANDE DO SUL
CAMPUS RESTINGA
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

**SISTEMA DE REPUTAÇÃO BASEADO EM BLOCKCHAIN PARA
DETECÇÃO DE FAKE NEWS**

BRUNO FONTENELE SCHELTZKE

PORTO ALEGRE

2018

BRUNO FONTENELE SCHELTZKE

**SISTEMA DE REPUTAÇÃO BASEADO EM BLOCKCHAIN PARA DETECÇÃO DE
FAKE NEWS**

Trabalho de Conclusão de Curso apresentada como requisito parcial para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas da Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - IFRS, Campus Restinga.

Orientador: Mestre Régio Antônio Michelin

Co-orientador: Mestre Roben Castagna Lunardi

Porto Alegre

2018

BRUNO FONTENELE SCHELTZKE

**SISTEMA DE REPUTAÇÃO BASEADO EM BLOCKCHAIN PARA DETECÇÃO DE
FAKE NEWS**

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - IFRS, Campus Restinga.

Data de Aprovação: 14/12/2018

Banca Examinadora

Mestre Régio Antônio Michelin - IFRS - Campus Restinga
Orientador

Mestre Roben Castagna Lunardi - IFRS - Campus Restinga
Co-Orientador

Doutor Rafael Pereira Esteves- IFRS- Campus Restinga
Membro da Banca

Doutor Avelino Francisco Zorzo- PUCRS-
Membro da Banca

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL

Reitor: Júlio Xandro Heck

Pró-Reitora de Ensino: Lucas Coradini

Diretor do Campus Restinga: Gleison Samuel do Nascimento

Coordenador do Curso de Ciência da Computação: Régio Antônio Michelin

Bibliotecária-Chefe do Campus Restinga: Paula Porto Pedone

Dedico todo meu esforço à meus pais.

RESUMO

Atualmente, notícias falsas se tornaram um grande desafio para a sociedade por normalmente conter conteúdos polêmicos e apelativos que atraem facilmente a atenção da população. Portanto, diferentes organizações buscam por soluções para reduzir o impacto das fake news. Dessa forma, este trabalho avança sobre este problema, propondo um sistema que registra e computa votos de usuários em determinadas notícias, com a finalidade de indicar a possibilidade de uma notícia ser falsa. A solução proposta consiste do uso de blockchain em conjunto com um aplicativo para dispositivos móveis, através dos quais o usuário executa as ações, e um sistema que calcula as reputações desses usuários.

Palavras-chave: Análise e Desenvolvimento de Sistemas. FakeNews. Blockchain. Política.

ABSTRACT

Currently, fake news have become a big challenge for the society due to their controversial and appealing content which easily attract the attention of the population. Consequently, different organizations are searching for solutions to reduce the impact of fake news. Therefore, this paper advances the solution for this problem proposing a system which registers opinions of users on certain news, with the purpose of indicating the possibility of a news being fake. The proposed solution consists of the use of blockchain in conjunction with a mobile application, through which the user performs the actions, and a system that calculates the reputations of those users.

Keywords: FakeNews. System Analysis. Blockchain. Politics.

LISTA DE FIGURAS

Figura 1 – Disposição de informações na <i>Blockchain</i>	16
Figura 2 – Disposição de informações na <i>Speedychain</i>	17
Figura 3 – Checagem de fatos por leitores	19
Figura 4 – Arquitetura do Sistema.	24
Figura 5 – Demonstração da arquitetura da <i>SpeedyChain</i>	29
Figura 6 – Demonstração da criação de um usuário	29
Figura 7 – Demonstração a tela inicial do aplicativo	31
Figura 8 – Demonstração de notícias com os possíveis índices de confiabilidade	32
Figura 9 – Demonstração a pesquisa inválida e válida por uma notícia	33
Figura 10 – Demonstração de voto em uma notícia	34
Figura 11 – Demonstração do processo de criptografia de um voto	34
Figura 12 – Desmonstração do uso de <i>tags</i> com o voto do usuário	38
Figura 13 – Demonstração a descrição de uma notícia	39
Figura 14 – Demonstração da tela de notícias votadas	40
Figura 15 – Demonstração de um <i>card</i> de uma notícia.	40

LISTA DE TABELAS

Tabela 1 – Comparação de soluções existentes com este sistema	22
Tabela 2 – Valores relacionados a reputação dos usuários	25
Tabela 3 – Valores relacionados a índices de confiabilidade por votos maliciosos	26
Tabela 4 – Valores relacionados a índices de confiabilidade por votos positivos	27

LISTA DE ABREVIATURAS E SIGLAS

TCC	Trabalho de Conclusão do Curso
STF	Supremo Tribunal Federal

SUMÁRIO

1	INTRODUÇÃO	14
2	FUNDAMENTAÇÃO TEÓRICA	16
2.1	BLOCKCHAIN	16
2.2	IDENTIFICAÇÃO DE <i>FAKE NEWS</i>	17
2.3	USUÁRIOS DE REDES SOCIAIS E <i>FAKE NEWS</i>	18
3	TRABALHOS RELACIONADOS	21
3.1	COMPARAÇÃO COM TRABALHOS RELACIONADOS	21
4	SOLUÇÃO CONCEITUAL	23
4.1	REPUTAÇÃO DOS USUÁRIOS	24
4.2	ÍNDICE DE CONFIABILIDADE DE NOTÍCIAS	26
5	IMPLEMENTAÇÃO	28
5.1	SPEEDYCHAIN	28
5.2	CADASTRO DE USUÁRIO	29
5.3	PESQUISA POR NOTÍCIAS	30
5.4	VOTOS E INSERÇÕES DE NOTÍCIAS	33
5.5	SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA DO VOTO	34
5.6	ATRIBUTOS DE CONFIABILIDADE DE NOTÍCIAS	35
6	MELHORIAS DE USABILIDADE	37
7	CONCLUSÃO	41
7.1	TRABALHOS FUTUROS	41
	REFERÊNCIAS	43

1 INTRODUÇÃO

O termo *fake news*, ou, notícia falsa em português, trata de uma notícia que passa uma informação não verídica intencionalmente com o objetivo de criar uma polêmica e/ou denegrir pessoas ou organizações (SHU et al., 2018). *Fake news* tornou-se um assunto recorrente na mídia, dado que, com o avanço da tecnologia da informação qualquer pessoa com acesso a Internet pode disseminar informações falsas e maliciosas. Sendo assim, nenhuma notícia de fonte conhecida pode ser considerada verdadeira até que seja confirmada sua veracidade (SHU et al., 2018). Uma notícia falsa possui vários indicadores de sua falsidade, tais como: ausência de fonte, sensacionalismo, erros de formatação ou ortografia. Contudo, usualmente, o trabalho de busca de veracidade é realizado por pessoas especializadas, demandando tempo considerável para ser finalizado (KRISHNAN; CHEN, 2018).

Por ter um potencial de atingir milhões de usuários em pouco tempo, *fake news* tornou-se uma das principais armas políticas, através de manchetes falsas e tendenciosas. Por exemplo, essas notícias podem influenciar diretamente no resultado de uma eleição. (HYMAN, 2017). Desta forma, *fake news* tornou-se uma ferramenta de difamação que possui potencial para influenciar usuários online.

Um exemplo de aplicação das *fake news* aconteceu durante as eleições americanas de 2016. Houveram vários estudos a respeito das eleições americanas e da atividade das *fake news* a favor de candidatos. Esses estudos mostram como as notícias falsas impactaram nas decisões tomadas pelos eleitores americanos.

Através de um estudo realizado na universidade Dartmouth, nos Estados Unidos da América (GUESS et al., 2018) pesquisadores concluíram que cerca de 27 por cento dos americanos elegíveis a voto tiveram acesso a pelo menos uma notícia falsa antes de realizar o seu voto. Essa proporção representa cerca de 65 milhões de eleitores no país. A pesquisa também alegou que a maioria das notícias falsas que os eleitores tiveram acesso, eram favoráveis ao candidato, então eleito, Donald Trump, e que muitas pessoas das quais acessaram o conteúdo acreditaram na notícia.

As redes sociais forneceram um grande poder para que notícias falsas se dispersassem com facilidade. Outro estudo realizado na universidade de Stanford (ALLCOTT; GENTZKOW, 2017) apresentou que 115 notícias falsas que favoreciam o candidato Donald Trump, ou denegriam seus oponentes, foram compartilhadas cerca de 30 milhões de vezes no Facebook.

O tema tem ganhado tamanha relevância que o tema vem sendo tratado como assunto de

segurança nacional em alguns países da Europa (CASADO, 2017) . No Brasil, o ministro do STF, Luiz Fux, se organizou para discutir a proliferação de *fake news* no país com o objetivo de implantar medidas que diminuam a sua influência nas eleições brasileiras do ano de 2018. Essa movimentação é produto de passados eventos influenciados por *fake news* como as eleições americanas e argentinas.

Outro ponto a se levar em consideração, é o fato da população brasileira ser uma das que mais utiliza as redes sociais no mundo de acordo conforme (HOOTSUITE, 2018) . Através dos resultados alcançados nesta pesquisa, se consta que no ano de 2017 o brasileiro passou em média 3 horas e 40 minutos do seu dia acessando redes sociais. A partir de um uso contínuo das redes sociais, seus usuários se tornaram o principal alvo das *fake news*.

Sendo assim, o sistema proposto neste trabalho consiste em um sistema que coleta opiniões públicas sobre uma determinada notícia a fim de determinar sua veracidade e, assim, levantar suspeita sobre *fake news*. Nessa proposta, o meio utilizado para determinar a autenticidade de uma notícia é a opinião dos usuários que votaram na notícia em questão e a reputação destes usuários.

2 FUNDAMENTAÇÃO TEÓRICA

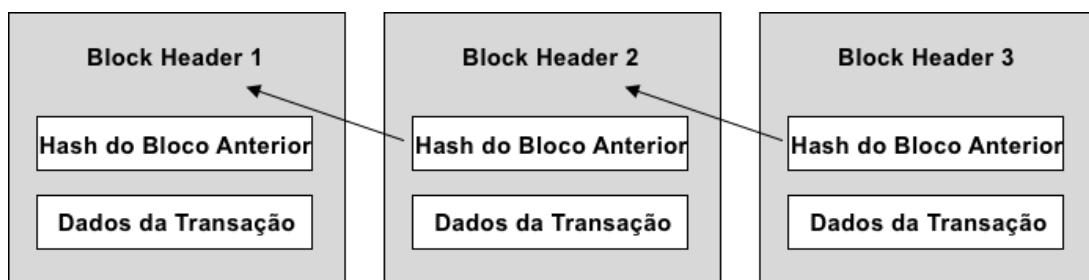
Este trabalho consiste em um sistema que coleta opiniões públicas sobre uma determinada notícia a fim de determinar sua veracidade e, assim, indicar *fake news*. Cada voto fornecido por um usuário é armazenado em uma *blockchain* que garante a segurança e auditabilidade da informação. Para determinar a autenticidade de uma notícia o sistema analisa as opiniões dos usuários que votaram na notícia em questão e a reputação dos mesmos.

2.1 BLOCKCHAIN

Blockchain surgiu em conjunto com *Bitcoins* em 2008 com o artigo Bitcoin: A Peer-to-Peer Electronic Cash System, de Satoshi Nakamoto (NAKAMOTO, 2008). Tinha como principal objetivo transferir Bitcoins de forma segura sem depender de uma organização mediadora como bancos ou o estado.

Blockchains armazenam a informação em blocos ligados de forma encadeada utilizando o *hash* do bloco anterior conforme a Figura 1. Cada hash é um valor único utilizado para identificar um dado. Essa valor é calculado a partir de um outro dado inicial. Dessa forma, o hash garante a unicidade e é significamente menor do que o valor originário, o que auxilia os dados à serem acessados com mais eficiência. (TECHTERMS, 2018)

Figura 1 – Disposição de informações na *Blockchain*



Este conjunto de blocos encadeados é distribuído e validado pelos demais nodos. Desta forma, alterações na *blockchain* são dificultadas devido à necessidade desta validação (TSCHORSCH; SCHEUERMANN, 2016). Sendo assim, caso um destes nodos tente inserir uma informação que não condiz com um certo conjunto de regras predefinidas ou tente alterar um dado que foi armazenado, os valores *hash* armazenados em cada bloco não serão satisfeitos, e o bloco não será aceito (ORMAN, 2018).

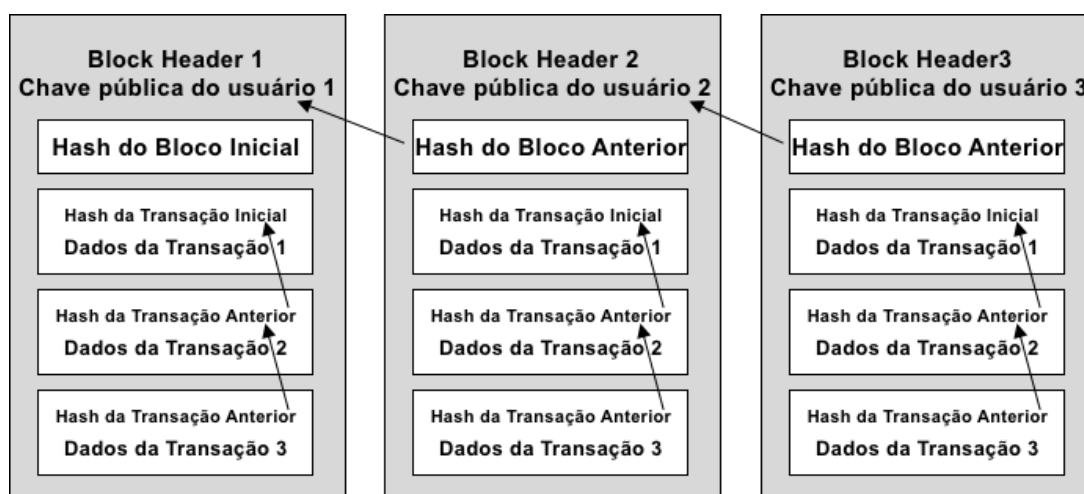
Após o surgimento do Bitcoin, diversas propostas de *blockchain* surgiram para garantir a integridade, autenticidade e disponibilidade da informação em diferentes contextos. Devido ao

fato de esta tecnologia operar distribuindo sua informação armazenada de uma forma descentralizada, a *blockchain* fornece segurança para transferência de dados. Desse modo, muitas indústrias que operam na base de troca de valores podem se beneficiar dessa tecnologia (LONG, 2018).

Photochain é uma plataforma de fotografia construída baseada na tecnologia *blockchain*. Ela utiliza dessa tecnologia para, de forma segura, manter a ligação entre um trabalho digital e um artista. Dessa forma, esta plataforma busca eliminar a maioria das taxas e problemas relacionados a direitos autorais encontrados no atual mercado de ações fotográficas. Dessa forma, fotógrafos retêm até 95% dos seus potenciais ganhos, mantendo a certeza de que os direitos autorais de suas produções serão garantidos (PHOTOCHAIN, 2018).

Este trabalho utiliza uma variação da *blockchain* chamada Speedychain (Michelin et al., 2018) (LUNARDI et al., 2018). Nessa implementação, cada bloco é relacionado à um único usuário. Assim, cada bloco contém uma série de transações feitas por esse usuário em questão, conforme a Figura 2

Figura 2 – Disposição de informações na Speedychain



Estes atributos e seus benefícios para com este sistema são melhor explicados no Capítulo 4 e Seção 5.1.

2.2 IDENTIFICAÇÃO DE *FAKE NEWS*

Empresas de checagem de fatos (*fact checking*), tem o intuito de combater as *fake news* diretamente verificando a veracidade da informação disseminada. Estas empresas determinam a veracidade de notícias baseado em informações relacionadas a matéria em questão, especialistas da área, pessoas pronunciadas na notícia, consulta de dados oficiais, entre outros (MERELES, 2017).

Dentre as empresas, cabe ressaltar iniciativas como a do Google, que criou uma ferramenta que utiliza de serviços especializados de checagem de fatos como o PolitiFact e o Snopes para determinar a autenticidade de informações. A partir disso, a plataforma pode informar seus usuários da veracidade de notícias resultantes de suas buscas (TECH, 2017).

Além de combater as *fake news* diretamente, outra abordagem é de se combater o agente manipulador, ou seja, quem dissemina a notícia.

O Facebook criou um sistema em que usuários podem reportar uma notícia, que circula na sua plataforma, alegando ser falsa (FACEBOOK, 2018). A partir desses relatos de seus usuários, o sistema utiliza de agências de *fact checking* após desconfiar da veracidade de notícias reportadas. Ao passo que o Facebook determina que uma notícia tem sua autenticidade comprometida, a plataforma passa a diminuir o acesso de usuários à esses conteúdos que foram determinados falsos ou distorcidos. Além disso, caso haja uma recorrência de notícias falsas de uma mesma origem, o Facebook toma medidas mais severas contra essa fonte para que seu conteúdo tenha um menor alcance dentro de sua plataforma e assim impactando menos pessoas. Em 2018, a rede social desativou 196 páginas e 96 contas por atividades relacionadas a *fake news* (G1, 2018).

O WhatsApp, plataforma de troca de mensagens instantâneas, banuiu centenas de milhares de contas no período eleitoral brasileiro de 2018 por disseminar notícias falsas em massa (SENRA, 2018). A plataforma elaborou algoritmos que identificam padrões irregulares de disseminação de mensagens e repetição de conteúdos. A partir disso, ela pôde remover contas suspeitas de atividades relacionadas à *fake news*.

Outra forma de se combater *fake news*, é através da conscientização da população. Medidas como observar a URL de uma notícia, checar a fonte, não confiar na manchete de uma notícia, podem levar pessoas a duvidar das notícias, o que pode fazer com que elas não as compartilhem, diminuindo assim a dissipação dessas notícias (GLOBO, 2018).

2.3 USUÁRIOS DE REDES SOCIAIS E *FAKE NEWS*

De modo a identificar o conhecimento das pessoas sobre o assunto de *fake news*, fora conduzido uma pesquisa qualitativa e quantitativa com 201 pessoas. O objetivo da pesquisa é descobrir o real interesse sobre o assunto *fake news* de pessoas que utilizam redes sociais com frequência. Outro objetivo da pesquisa era descobrir o nível de engajamento das pessoas em descobrir a veracidade de uma notícia a partir de atividades simples como pesquisas em outros sites, verificação de fonte e autor.

A pesquisa foi realizada com 201 pessoas, sendo que 64,4% dos 156 pesquisados que

quiseram responderam sua idade informaram que possuem entre 15 e 27 anos, enquanto que 35,6% tem 28 e 52 anos de idade.

Quanto ao gênero, dentre 159 participantes que optaram por responder, 52,2% informaram que são do gênero masculino, enquanto que 45,3% informaram que são do gênero feminino. 1,5% preferiu omitir seu gênero.

A pesquisa trouxe como resultado que 89,1% dos pesquisados considera *fake news* um problema relevante.

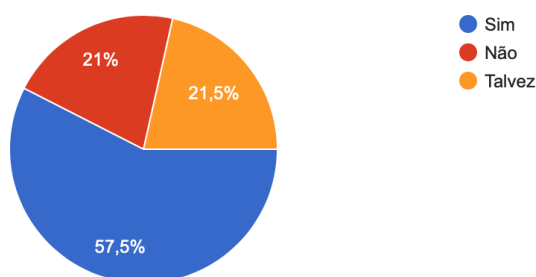
Dentre os pesquisados, 92,5% afirma que previamente recebeu alguma notícia falsa e que descobriu a sua veracidade através de pesquisas e conhecimentos prévios.

A pesquisa informa que a maioria dos pesquisados utiliza redes sociais e 66% deles tendem a compartilhar conteúdo nas plataformas, apesar de que apenas 57,5% dos pesquisados tem certeza que checaram as últimas três informações compartilhadas nas redes sociais conforme a Figura 3.

Figura 3 – Checagem de fatos por leitores

Das últimas três coisas que compartilhou nas redes, você checkou a veracidade do conteúdo?

200 respostas



Como conclusão, a pesquisa informa que o usuário jovem que utiliza redes sociais reconhece o problema das *fake news*, mas nem sempre se engaja o suficiente para combatê-las. Além de nem sempre saber identificar a veracidade de uma notícia, os usuários das redes sociais não se preocupam em checar a veracidade de notícias antes de compartilhá-las. O questionário aplicado, bem como a íntegra das respostas, pode ser visto no Apêndice B.

Tendo em vista os problemas gerados por informações falsas e a proposta que a tecnologia *blockchain* oferece, este trabalho propõe uma solução para indicar a veracidade de notícias a partir

de avaliações de usuários cadastrados. Com o objetivo de fornecer integridade e auditabilidade das informações, o sistema desenvolvido armazena opiniões sobre notícias utilizando a plataforma SpeedyChain (LUNARDI et al., 2018) (Michelin et al., 2018). A veracidade de uma notícia é dada a partir do momento em que uma notícia é visualizada. Para seu cálculo, o sistema calcula a reputação dos usuários que votaram na notícia em questão, para assim sugerir sua veracidade. Conseqüentemente, o sistema se propõe a alertar usuários de portais de notícia sobre a veracidade da informação. Portanto, diminuindo consideravelmente o impacto que *fake news* têm sobre o cotidiano das pessoas.

O detalhamento do sistema de reputação e do funcionamento dos algoritmos será dado nas seções 4.1, 4.2 e 5.6.

3 TRABALHOS RELACIONADOS

A área de verificação de notícias tem recebido atenção da comunidade científica nos últimos anos, desta forma, sistemas para identificação de informações falsas foram propostos.

Bountain e Golbeck (BUNTAIN; GOLBECK, 2017) desenvolveram um método para identificar notícias falsas na rede social Twitter. Os autores propõem um algoritmo que pesquisa, em dois bancos de dados, assuntos que potencialmente podem ser usados para criar uma *fake news*. A partir disto, o algoritmo analisa a estrutura das informações inseridas na rede social e utiliza *machine learning* para concluir se a informação é verdadeira ou não. Este mecanismo tem uma taxa de sucesso na identificação de *fake news* de aproximadamente 69%. Apesar de um índice elevado para a identificação automatizada de *fake news*, a solução proposta está limitado a plataforma Twitter.

Eleição Sem Fake (BENEVENUTO, 2018) é um projeto capaz de monitorar notícias no Facebook e identificar *bots* nas redes sociais. Apesar de ser uma ferramenta para auditar dados, ela não permite que o usuário decida quais notícias pretende analisar e não permite a análise de notícias de temas variados. Como a ferramenta possui um enfoque no cenário político, o sistema se limita a dados demográficos referentes a distribuição do público que os portais de notícias possuem, assim como páginas de Facebook.

O Detector de *fake news* (CHAVES, 2018) é um software onde os usuários podem informar se determinada notícia é uma *fake news* ou *click bait* (notícia com título tendencioso para que o usuário clique no *link* da notícia). Apesar de ser uma proposta promissora, analisa apenas notícias do Twitter e Facebook, além de não permitir que o usuário realize buscas por notícias específicas na base de dados.

3.1 COMPARAÇÃO COM TRABALHOS RELACIONADOS

A Tabela 1 apresenta uma comparação do sistema proposto com outros sistemas disponíveis. Nesta tabela foram elencados os atributos: público alvo; origem da notícia; método de validação de notícias; pesquisa por uma notícia; para comparação dos diferentes sistemas.

Tabela 1 – Comparação de soluções existentes com este sistema

Sistema	Público alvo	Origem da notícia	Método de validação de notícias	Pesquisa por uma notícia
Este TCC	Qualquer usuário	Qualquer website	Reputação dos usuários que opinaram	Disponível a qualquer pessoa
Eleição Sem Fake	Facebook	Facebook	Monitoramento de notícias anunciadas	Notícias políticas da região do usuário
Detector de fake news	Facebook ou Twitter	Facebook ou Twitter	Índices de veracidade baseado em reputação	Não disponível

Na Tabela 1 pode-se observar que o algoritmo de validação das notícias do sistema proposto, gerará resultados automatizados (atualmente gera apenas índices) sobre a veracidade de uma notícia pois independe de interações humanas. O sistema proposto é baseado na reputação dos votantes, diminuindo assim custo e tempo com a utilização de agências de checagem de fatos.

O sistema proposto apresenta transparência, descentralização e integridade das informações. Os índices sobre veracidade das notícias podem ser acessados por qualquer pessoa ou sistema, sem requerer cadastro, diferente das outras soluções (Tabela 1).

4 SOLUÇÃO CONCEITUAL

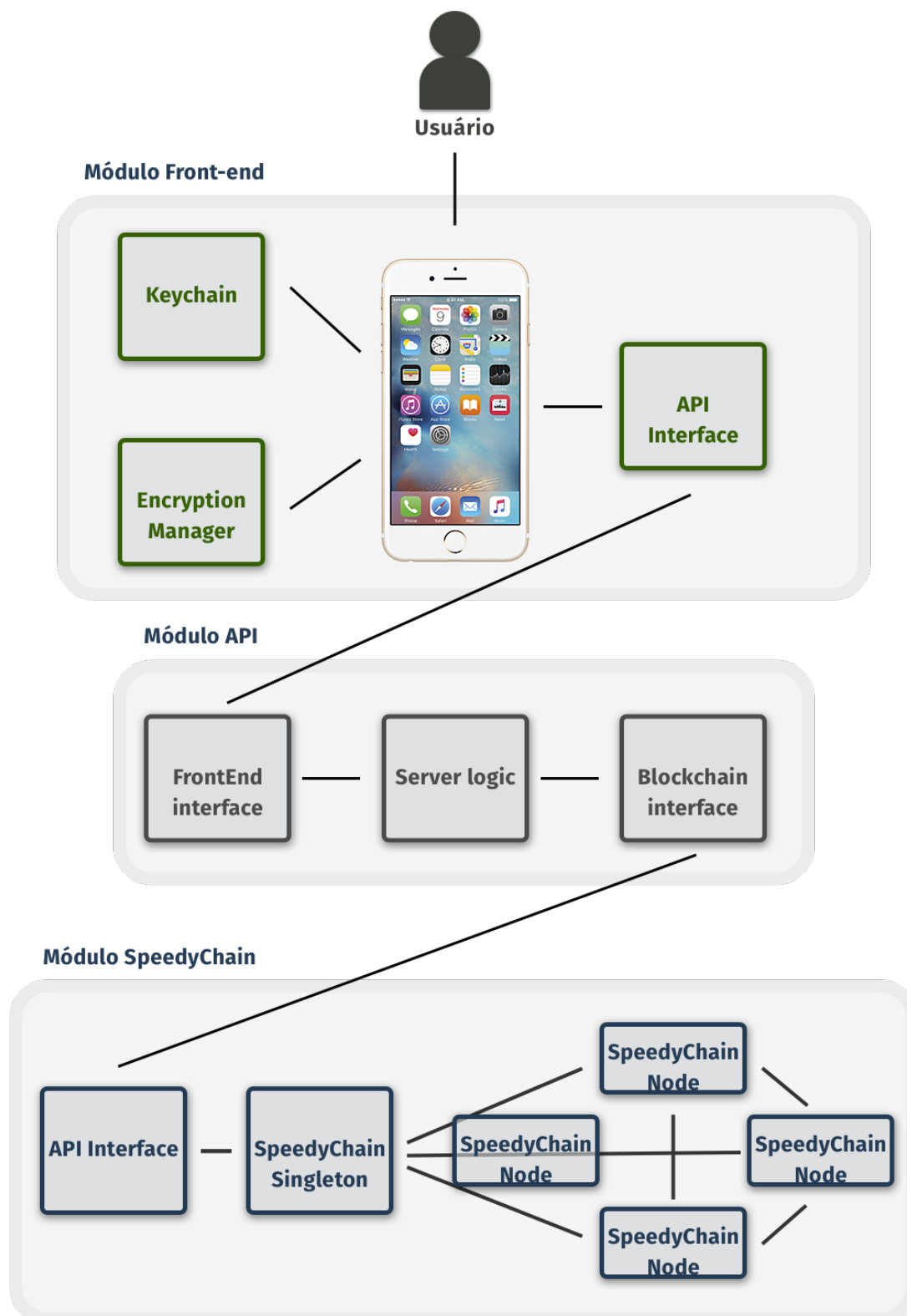
Buscando a garantia de resiliência, disponibilidade, não repúdio e integridade dos dados a proposta do sistema aqui proposto utiliza a tecnologia *blockchain*, dado que esta garante as propriedades necessárias ao sistema. Além destas propriedades, é possível que qualquer usuário audite os dados disponíveis. Esta proposta, além de possibilitar o envio de notícias para avaliação, permite que o usuário busque - nos dados armazenados na *blockchain* - notícias específicas. Desta forma, calcula-se a reputação dos usuários que interagem com o sistema e os atributos que possibilitam definir um índice de confiabilidade de uma notícia (ver Seção 4.2). Portanto, esta proposta torna-se, também, uma base de dados distribuída para pesquisa de *fake news* com garantia de integridade dos votos.

De forma a prover os atributos necessários ao sistema NoFakeNews, adotou-se uma arquitetura modular baseado no modelo REST para realizar a comunicação entre os 3 módulos do sistema: SpeedyChain (*blockchain*); API; e Front-End; para interação com usuário. Os atributos relacionados a veracidade de uma notícia são calculados em tempo real a cada interação do usuário. A Figura 4 apresenta uma definição estrutural da proposta, bem como os principais módulos desenvolvidos para o projeto.

No sistema proposto, o usuário pode realizar operações de voto em uma notícia específica, e verificar o indicativo de confiabilidade de notícias através do módulo Front-End. Através dos votos de usuários, o módulo API pode calcular a veracidade das notícias (ver Seção 4.2).

O módulo API, na camada Front-End interface, é responsável por expor métodos que fornecem as funcionalidades para o módulo Front-End, que se comunica através da camada API interface. Este módulo do sistema provê a possibilidade de registrar a opinião sobre uma notícia, e encaminhar para inserção na *blockchain* através da camada Blockchain interface. Além disso, a API tem função de receber o pedido e conferir a veracidade de uma determinada notícia. Desse modo, cabe a esse módulo coletar as informações necessárias diretamente da SpeedyChain que utiliza da camada API interface para receber essas requisições. A veracidade de uma notícia é definida pela reputação dos usuários que opinaram sobre ela e calculada na camada Server logic. A API solicita informações desses usuários para a SpeedyChain, que entrega todas as chaves públicas de identificação desses usuários.

Figura 4 – Arquitetura do Sistema.



4.1 REPUTAÇÃO DOS USUÁRIOS

A reputação de um usuário é definida pelas suas opiniões em notícias. Ao passo que um usuário requiere o índice de confiabilidade de uma notícia, a API coleta da SpeedyChain os

usuários que votaram nessa notícia. Após isso, o módulo API coleta as notícias que cada usuário votou, e, caso existam votos suficientes para determinar a veracidade dessas notícias, conforme a Seção 4.2, o sistema pode comparar esses resultados com as opiniões dos usuários e assim determinar suas reputações.

Um usuário inicia sua atividade no sistema com uma reputação inicial (*Initial* conforme a Tabela 2) e pode variar a mesma de acordo com sua atividade no sistema. A reputação de um usuário é calculada a partir da comparação de seus votos em notícias com os índices de confiabilidade das mesmas Seção 4.2. A reputação de um usuário será modificada no momento em que o usuário em questão atingir um número mínimo de votos em notícias. Após isso, é comparado o percentual de erros de seus votos com os índices de confiabilidades das notícias. A reputação de um usuário é atribuída conforme a Tabela 2.

Tabela 2 – Valores relacionados a reputação dos usuários

Reputação	Número de votos mínimos	Porcentagem de erro	Peso
Initial	0	0	1
Low	50	>20	35
Spam	100	>90	20
High	50	<= 20	250
Specialist	200	<= 10	500

Características preventivas à interferências maliciosas ao sistema foram implementadas de acordo com pesquisas no campo de sistemas de reputações. Por exemplo, um usuário nunca terá uma reputação mais baixa do que a inicial recebida no ingresso do sistema. O contrário pode acarretar em usuários maliciosos com baixa reputação trocando identidades para ter mais relevância no sistema, conforme (ZACHARIA et al., 2000). Desse modo, um usuário que recebe uma reputação baixa (*Low*, *Spam*) terá uma baixa relevância no sistema, mas nunca terá um peso mais baixo do que a reputação inicial (*Initial*).

No sistema implementado, um usuário com reputação *Low* tem uma relevância 35 vezes maior do que um usuário com reputação *Initial* conforme a Tabela 2.

A estrutura do sistema de reputação e os diferentes atributos calculados para a veracidade de uma notícia trazem algumas precauções contra possíveis usuários maliciosos que possam votar em uma certa opinião em massa (ZACHARIA et al., 2000). Entretanto, os valores relacionados às demais reputações possuem limitações quanto à sua funcionalidade e podem ser refinados a partir de outras pesquisas mais profundas em sistemas de reputações existentes. Artigos como Taxonomy of trust: Categorizing P2P reputation systems (MARTI; GARCIA-MOLINA, 2006) e The Beta Reputation System (COMMERCE et al., 2002) foram utilizados como base para este

trabalho.

Além disso, possíveis inserções manuais de veracidade ou falsidade de notícias por órgãos confiáveis pode ser implementados para facilitar a elaboração de reputações de usuários iniciais. Outra opção, seria uma parceria com esses mesmos órgãos confiáveis para inserí-los no sistema como usuários de reputações fortes (*Specialist*) para que votem em notícias e os próximos usuários tenham uma base inicial.

4.2 ÍNDICE DE CONFIABILIDADE DE NOTÍCIAS

Ao passo que um usuário requiere a veracidade de uma notícia, o sistema calcula as reputações de todos os votantes e utiliza desses valores para determinar um índice de confiabilidade para a notícia.

Para se alcançar o índice de veracidade de uma notícia, o módulo de API, mais precisamente na camada Server Logic, calcula três atributos relacionados aos votantes da notícia: Maioria qualificada (resulta em Fake ou Fato); Nível de certeza (resulta num valor entre 0 e 100); Média de reputação (resulta na média de reputação dos votantes baseado no valor do primeiro atributo); conforme a Seção 5.6.

Após ter estes atributos calculados, a camada Server Logic do módulo API pode compará-los e atribuir um índice de confiabilidade. É necessária a constante preocupação com usuários maliciosos (ZACHARIA et al., 2000), logo, o sistema primeiramente valida essa possibilidade conforme a Tabela 3.

Tabela 3 – Valores relacionados a índices de confiabilidade por votos maliciosos

Índice	Número mínimo de votos	Maioria qualificada	Nível de certeza	Média de reputação
Tendência a Fake	50	Fato	>=40	<Low
Tendência a Fato	50	Fake	>=40	<Low

Caso não haja relacionamento entre os atributos calculados e os valores para caracterizar votos maliciosos, o sistema compara os valores para relacionar a notícia com um índice de confiabilidade adequado de acordo com a Tabela 4.

Tabela 4 – Valores relacionados a índices de confiabilidade por votos positivos

Índice	Número mínimo de votos	Maioria qualificada	Nível de certeza	Média de reputação
Neutra	0	Não aplicável	Não aplicável	Não aplicável
Tendência a Fake	50	Fake	≤ 20	\geq Low
Fake	80	Fake	> 20	\geq High
Tendência a Fato	50	Fato	≤ 20	\geq Low
Fato	80	Fato	> 20	\geq High

Assim como os valores relacionados a reputação do usuário, os valores relacionados aos índices de confiabilidade não apresentam sua máxima eficácia e necessitam de um estudo maior de análise de reputação dos usuários para alcançar um maior nível de confiabilidade. Isso pode ser alcançado a partir de um desenvolvimento evoluído do atual sistema de reputações já mencionado na Seção 4.1.

5 IMPLEMENTAÇÃO

Tendo como base a definição conceitual do sistema apresentada no Capítulo 4, a sua implementação foi feita utilizando tecnologias apropriadas para cada módulo. O módulo front-end foi implementado como um aplicativo para iPhone utilizando a linguagem Swift 4.2. O módulo API utilizou Node.js para sua implementação enquanto que o módulo blockchain recebeu mudanças adicionais da já implementada SpeedyChain.

5.1 SPEEDYCHAIN

Dentre as tecnologias atuais buscou-se uma opção de implementação de *blockchain* que fosse capaz de atender as necessidades do sistema, e dadas as opções disponíveis, SpeedyChain mostrou-se uma escolha adequada, visto que a mesma consiste de uma *blockchain* composta de blocos que podem continuar recebendo transações após serem inseridos na *blockchain* (LUNARDI et al., 2018; Michelin et al., 2018). Desta forma, todos o votos passados e os futuros votos de um usuários são armazenados em um mesmo bloco. Cada novo voto (transação) é inserido mantendo um *link* com os demais através de função *hash* (Michelin et al., 2018) de acordo com a Figura 2.

A partir da estrutura da SpeedyChain, um usuário pode inserir mais de um voto em uma mesma notícia, em um cenário em que ele(a) mudasse de opinião sobre a mesma. Dessa forma, o voto posterior realizado é gravado na *blockchain* como uma transação adicional no bloco do usuário em questão. Em relação aos cálculos de reputação e de veracidade de notícia, apenas o último voto do usuário é levado em conta.

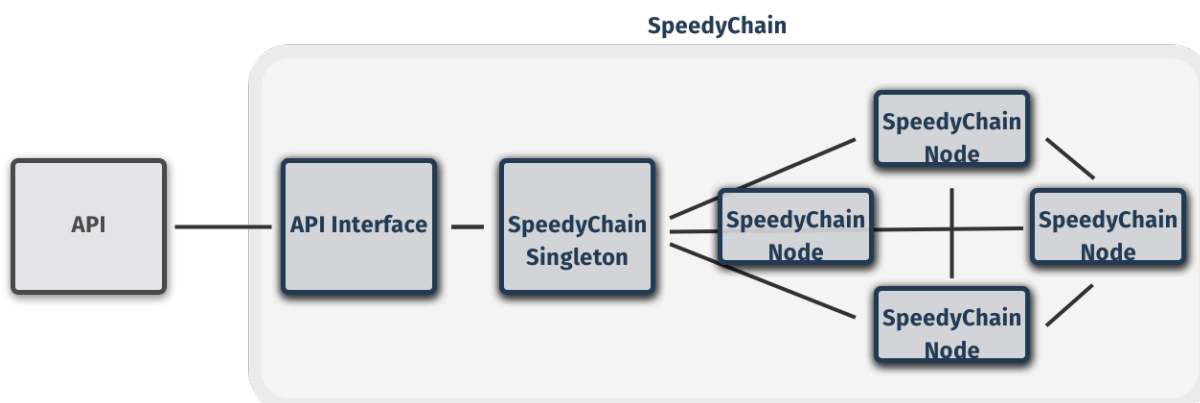
Para satisfazer aos requisitos do sistema em geral, foi necessário adicionar algumas modificações na implementação da SpeedyChain conforme demonstra a Figura 5.

A SpeedyChain, que já possuía previamente os nodos estabelecidos com a posse das informações (que garante a descentralização dos dados), bem como a instância compartilhada de sua classe (a partir do modelo *Singleton*), recebeu a incrementação de uma interface de comunicação, seguindo os padrões *REST*, utilizando o framework em Python *Flask*.

A partir desta camada de comunicação, a Speedychain é capaz de expor funções que permitem a API requisitar informações pertinentes aos usuários e as notícias. Essa interface permite também que ao módulo API faça requisições para inserção de votos e de criação de usuários.

Além da inserção desta camada, foi necessário modificar a instância compartilhada da

Figura 5 – Demonstração da arquitetura da SpeedyChain

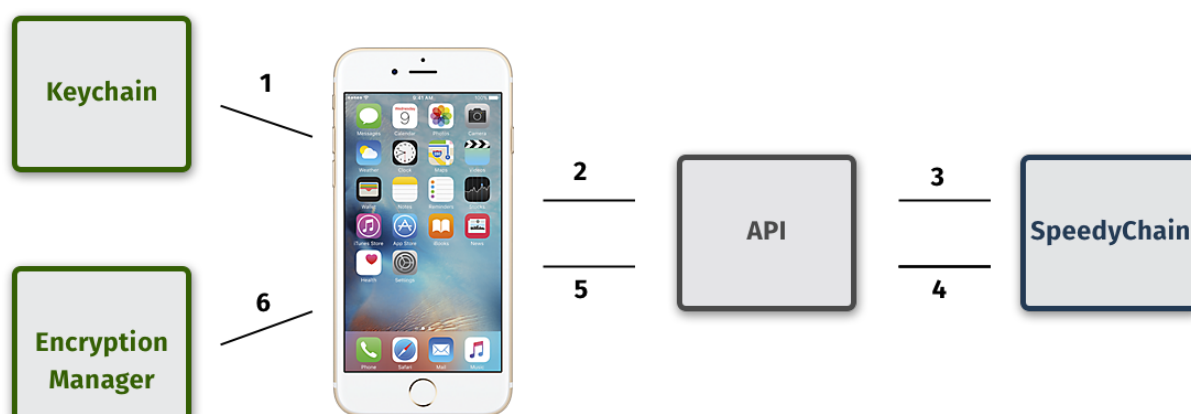


Speedychain para que fosse compatível com a inserção de dados relevantes ao projeto, como votos em notícias.

5.2 CADASTRO DE USUÁRIO

Para um usuário autenticar no sistema, primeiro este deve acessar o módulo de Front-End (conforme Figura 4). No sistema proposto, foi desenvolvido um aplicativo no sistema operacional iOS para iPhone utilizando a linguagem Swift 4.2. Para um usuário ser capaz de votar em notícias, ele(a) deve estabelecer uma comunicação inicial com o back-end do sistema para que tenha-se conhecimento do novo usuário em questão conforme a Figura 6.

Figura 6 – Demonstração da criação de um usuário



O sistema atual não requer informações pessoais do usuário, desse modo, não foi implementada nenhuma tela de login ou cadastro para o usuário. A partir desta medida, o usuário

não precisa passar tempo com atividades desnecessárias, melhorando assim sua experiência com o sistema (GOOGLE, 2015).

Entretanto, é requerido do aplicativo a criação e a manutenção do usuário de acordo com os requisitos do sistema. Este projeto utiliza um mecanismo de criptografia assimétrica onde cada usuário é identificado por sua chave pública. A *blockchain* requer esta chave no padrão *RSA 1024 bytes* que deve ser gerada e controlada pelo front-end. No sistema desenvolvido, o aplicativo verifica a existência dessa chave internamente a cada vez que o aplicativo é aberto pelo usuário. Caso essa chave não exista, o aplicativo gera uma chave privada e a salva localmente na *Keychain*, sistema interno do iOS para controle de chaves e senhas: Figura 6.1. Após gerar a chave privada, o front-end exporta uma chave pública e envia para o módulo de *API* a partir de uma requisição *REST* para criação de usuário: Figura 6.2.

O módulo *API* não tem função relacionada a criação de usuários, visto que a criação de um usuário consiste da geração de um par de chaves no cliente, e posteriormente a inserção do mesmo na *blockchain*. Logo, cada requisição deste tipo é automaticamente redirecionada para o módulo de *blockchain*: Figura 6.3. A *SpeedyChain*, ao receber essa requisição, verifica se a chave está no padrão esperado, e cria um bloco novo na *blockchain* para representar este novo usuário. Após isso, a *blockchain* cria uma chave de comunicação para com este usuário, que deve ser utilizada para qualquer futura comunicação entre as partes. Essa chave é encriptada com a chave pública enviada pelo usuário, utilizando *RSA* básico, e então redirecionada para o front-end: Figura 6.4 e Figura 6.5.

O aplicativo, ao receber essa resposta positiva da requisição de criação de usuário, utiliza de sua chave privada para decriptar a chave de comunicação e salvá-la para comunicações futuras com o sistema: Figura 6.6.

Todos esses passos são executados transparentemente sem necessitar de interação por parte do usuário. Nas próximas vezes que o usuário abrir o aplicativo, o sistema verifica a existência de sua chave privada na *Keychain* e já considera o usuário autenticado.

5.3 PESQUISA POR NOTÍCIAS

Um dos benefícios proporcionados pelo sistema proposto é que qualquer indivíduo ou sistema pode verificar o índice de confiabilidade de notícias gerados por este projeto. O módulo de *API* é reponsável por este cálculo e expõe um método *HTTP* que solicita apenas a URL de uma notícia como parâmetro. Desse modo, o modelo proposto pode ser utilizado por diferentes sistemas, desde que utilizem o protocolo definido.

Na implementação de front-end desta proposta, o aplicativo de iPhone apresenta, como tela inicial, uma lista das 10 notícias atualmente mais votadas no sistema conforme a Figura 7.

Figura 7 – Demonstração a tela inicial do aplicativo



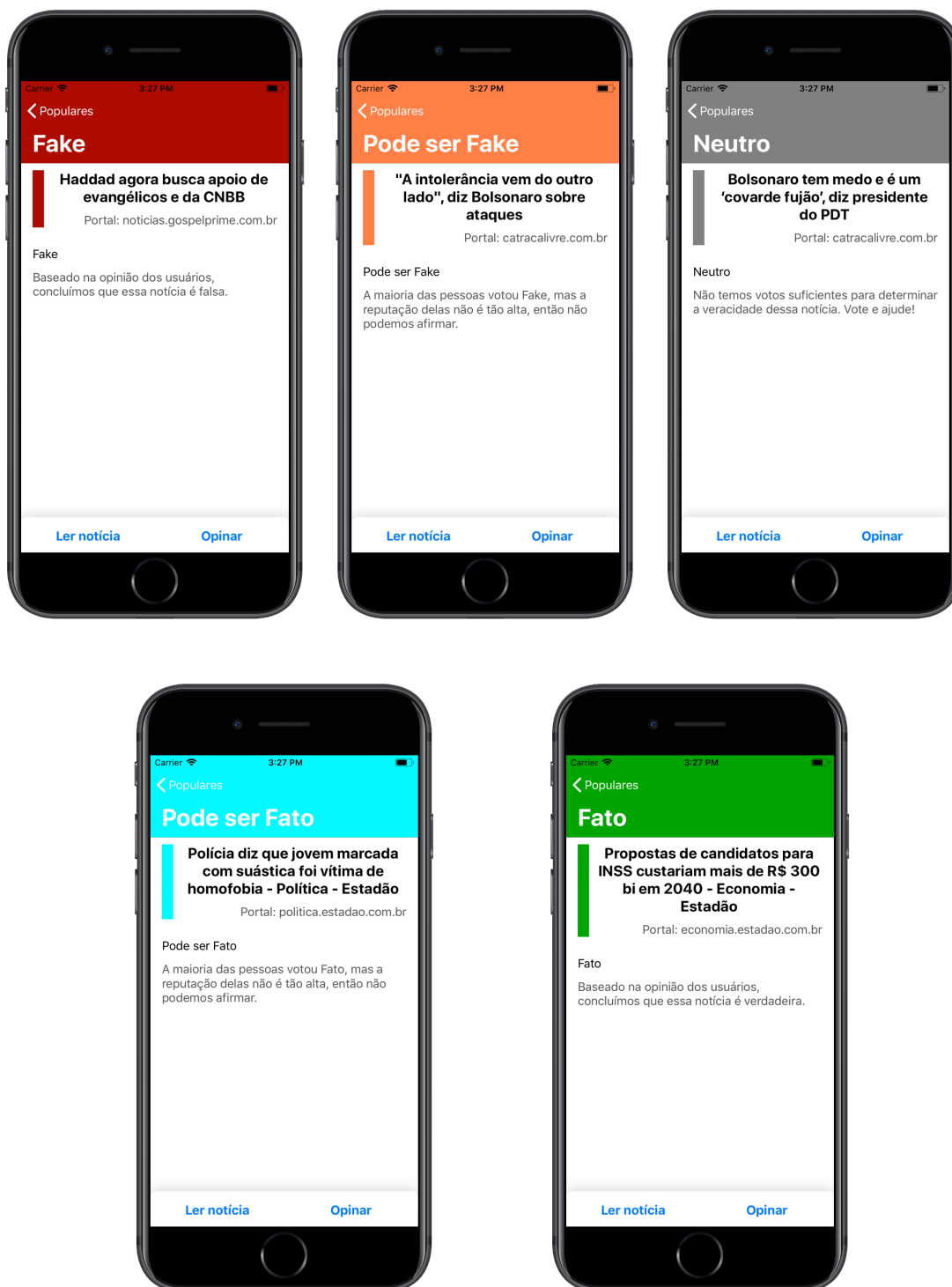
A partir desta lista, o usuário pode conferir o atual índice de confiabilidade atribuído para cada notícia e uma mensagem indicando o significado deste índice conforme a Figura 8.

Além disso, o usuário pode usar a barra de pesquisa para pesquisar por notícias inserindo a URL das mesmas conforme a Figura 9. Para realizar essa pesquisa, o sistema front-end é responsável por verificar a validade da URL e informar o usuário caso a URL seja inválida. A linguagem Swift possui um framework nativo (NSURL) que possibilita a verificação de uma URL. Caso a URL seja válida, o aplicativo solicita o índice de confiabilidade da notícia correspondente para o módulo da API. Com a resposta, o aplicativo apresenta uma prévia do que a notícia se trata, que inclui o título da notícia e o portal conforme a Figura 9.

Essa funcionalidade é necessária para melhor a experiência do usuário com o sistema pois proporciona a certeza para o usuário de que ele(a) está tratando da notícia correta.

Para atingir essa funcionalidade, o sistema desenvolvido utilizou de uma biblioteca

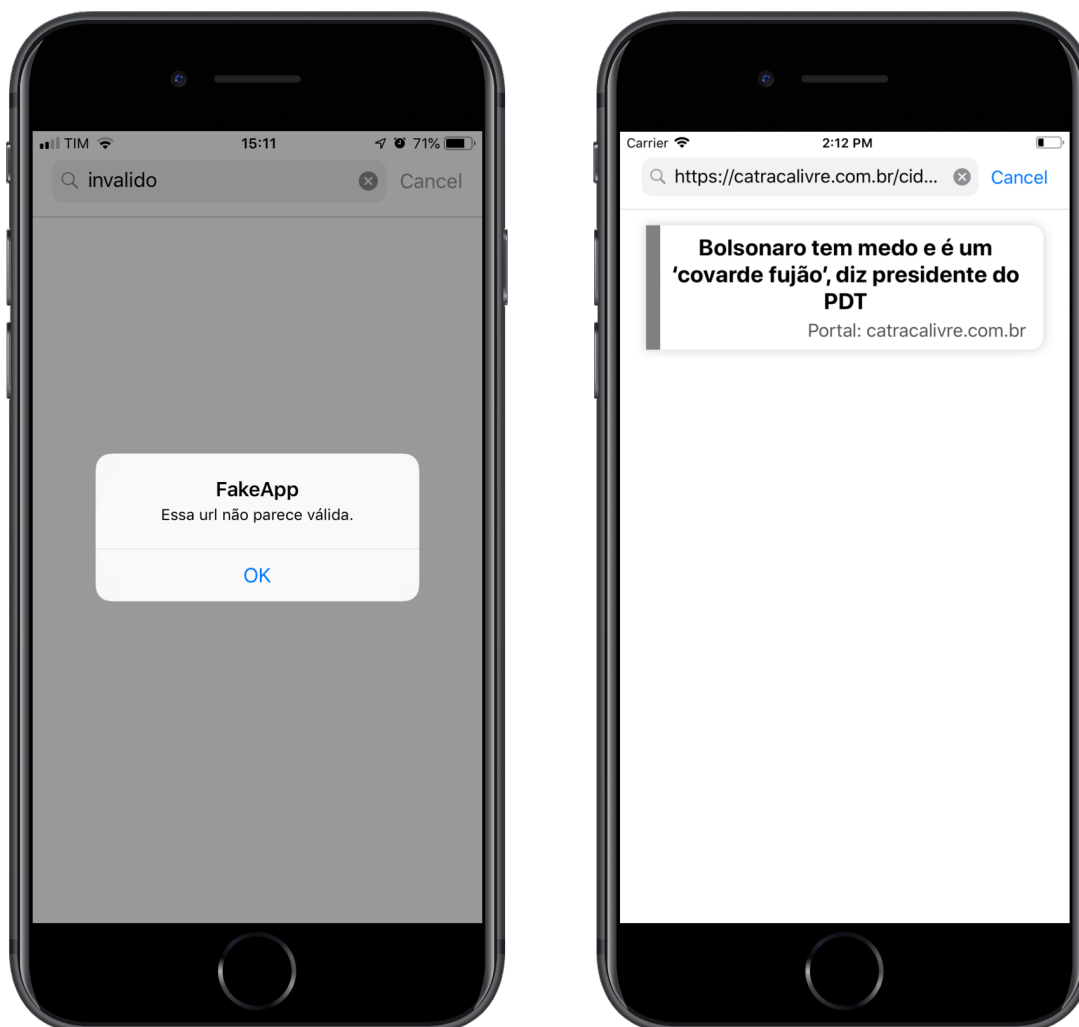
Figura 8 – Demonstração de notícias com os possíveis índices de confiabilidade



chamada *SwiftLinkPreview*, que realiza uma chamada *HTTP* para a URL da notícia e busca informações prévias da notícia no corpo da resposta da requisição.

Caso o usuário queira saber mais sobre a notícia, ele(a) pode clicar no botão "Ler notícia", no canto inferior da tela conforme a Figura 8, que o/a redirecionará para o navegador padrão do seu smartphone com o link da notícia, onde poderá ler a obra completa.

Figura 9 – Demonstração a pesquisa inválida e válida por uma notícia

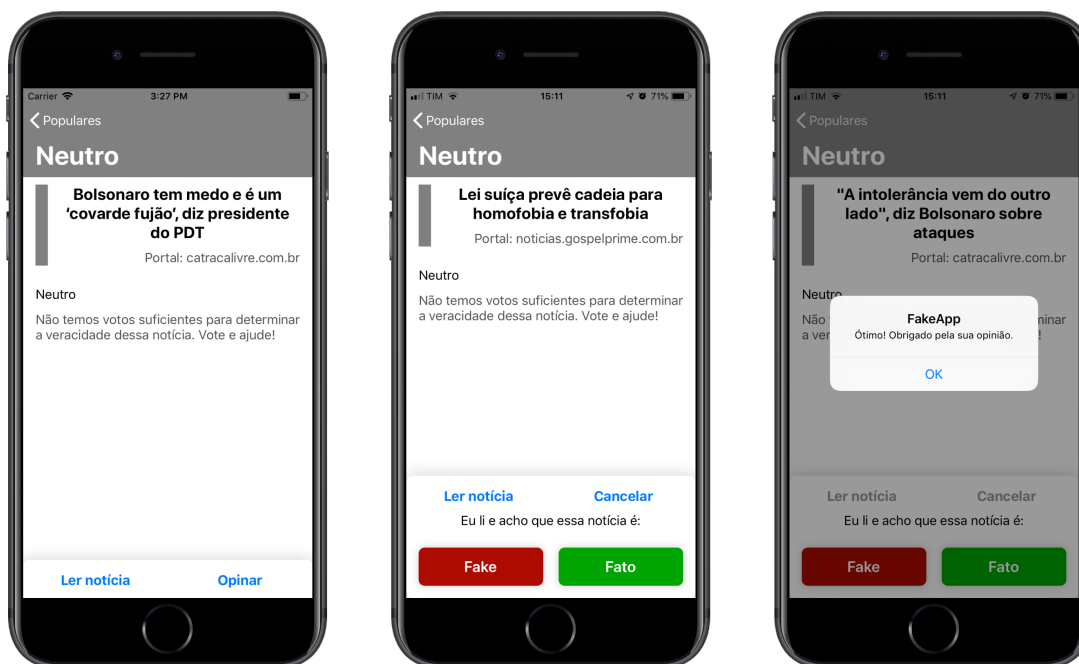


5.4 VOTOS E INSERÇÕES DE NOTÍCIAS

Para votar em uma notícia, o usuário tem a opção de votar nas notícias listadas na tela inicial conforme a Figura 7, ou pesquisar por uma notícia diferente inserindo sua URL no campo de pesquisa conforme a Figura 9. Caso não exista nenhum voto nessa notícia, o aplicativo apresenta esta notícia para o usuário com o índice *Neutro* e, caso o usuário venha a votar nessa notícia, a notícia é inserida na *blockchain* para futuras consultas.

Para realizar a operação de voto, o usuário acessa uma notícia, clica no botão inferior "Opinar", e seleciona entre as duas opções de voto disponíveis: *Fake* ou *Fato* conforme a Figura 10.

Figura 10 – Demonstração de voto em uma notícia



5.5 SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA DO VOTO

A cada interação de inserção do usuário, o módulo blockchain requer que o front-end seja capaz de encriptar a informação referente ao voto do usuário conforme a Figura 11 para que haja segurança das informações de voto dos usuários.

Figura 11 – Demonstração do processo de criptografia de um voto



Para isso, o aplicativo cria um dicionário contendo o voto do usuário e a URL da notícia, assina a informação com sua chave privada e a cifra (AES CBC Padding PKCS7) com a chave de comunicação estabelecida com a SpeedyChain. Após isso, o front-end cria um segundo dicionário contendo o dado encriptado e a chave pública do usuário e a envia para o módulo de API que redireciona automaticamente para o módulo de blockchain. Ao passo que a SpeedyChain recebe essa requisição, esse módulo faz o processo inverso utilizando a chave pública e chave de comunicação já conhecidas pelo sistema e insere o dado de voto no bloco do usuário como uma nova transação.

Caso um usuário tente inserir algum voto e sua comunicação não foi estabelecida, ou há erros na criptografia ou assinatura dos dados, nenhum dado é enviado para outros nodos da *blockchain* para sua inserção e uma mensagem de erro é retornada para o Front-End.

5.6 ATRIBUTOS DE CONFIABILIDADE DE NOTÍCIAS

Para calcular o índice de confiabilidade de notícias, o sistema proposto (no módulo API da Figura 4) calcula um conjunto de atributos: voto de um usuário para a notícia sendo verdadeira (VT); voto de um usuário para a notícia sendo falsa (VF); a reputação do usuário votante na notícia (R); índice de veracidade da notícia (T); índice de falsidade da notícia (F); diferença de índice de veracidade e falsidade (Df); média da reputação dos votantes como verdadeiro (MT); média da reputação dos votantes como falso (MF).

O usuário pode incrementar a reputação (R) inicial no sistema de acordo com sua atividade no sistema. Um usuário nunca terá uma reputação mais baixa do que a inicial. O contrário pode acarretar em usuários maliciosos com baixa reputação trocando identidades, conforme (ZACHARIA et al., 2000).

Para cálculo dos atributos T e F , que determinam a maioria qualificada, o sistema proposto separa os usuários que interagiram com a notícia pelas suas opiniões (verdadeiro/falso), e agrega o valor do peso de suas reputações conforme a Equação 1:

$$\begin{aligned} T &= \sum_{i=1}^n (VT_i * RT_i) \\ F &= \sum_{j=1}^m (VF_j * RF_j) \end{aligned} \quad (1)$$

Conforme apresentado nas fórmulas para T e F , o usuário pode verificar os parâmetros de veracidade e falsidade alcançados pela notícia. Quanto maior o índice, maior o peso para ser considerado.

O índice Df é o índice de confiança no resultado com maior peso (entre T e F), conforme a Equação 2:

$$Df = \left| \frac{(T - F)}{(T + F)} \right| \quad (2)$$

Desta forma, considera-se o percentual do peso de veracidade ou falsidade (o que for maior) da diferença de pesos em relação ao total opinado. A partir dessa medida, o sistema determina o nível de certeza da decisão tomada.

Finalmente, o sistema determina a qualidade da análise. Para isto o sistema calcula a média das reputações dos usuários que opinaram de acordo com a Equação 3:

$$\begin{aligned} MT &= \frac{\sum_{i=1}^n RT_i}{n} \\ MF &= \frac{\sum_{j=1}^m RF_j}{m} \end{aligned} \quad (3)$$

Portanto, uma notícia com muitos votos de baixa reputação tem um peso menor na análise, mesmo que tenha um número significativo de votos.

6 MELHORIAS DE USABILIDADE

Com o objetivo de avaliar a usabilidade do aplicativo front-end e da funcionalidade do back-end, o sistema foi submetido a testes com usuários em situações reais. Para que os usuários pudessem utilizar o aplicativo, o mesmo foi lançado através da plataforma *TestFlight*. Desse modo, apenas uma parcela de usuários controlados teriam acesso ao aplicativo.

Para funcionamento em conjunto com o aplicativo, o módulo API em conjunto com a *blockchain* foram instalados em um computador com acesso externo para fornecer disponibilidade e suporte às requisições realizadas pelos usuários.

Em um primeiro momento, o aplicativo recebeu um número de 14 downloads e 156 sessões (cada sessão é caracterizada por vezes em que um usuário abriu e interagiu com o aplicativo).

A partir destas interações, os usuários do aplicativo sugeriram melhorias relacionadas à funcionalidades e características da interface que melhorariam sua experiência para com o aplicativo.

Anteriormente, os usuários não tinham acesso às notícias que eles tinham opinado, e isso os deixavam em dúvida se teriam que votar novamente nas mesmas, ou não se lembravam se haviam votado. A partir disso, foi sugerido algum meio de informar os usuário sobre seus votos passados em notícias. Em uma segunda versão, foi implementado características visuais de uma notícia que informassem ao usuário de seu voto na mesma. Essas características foram alcançados a partir da inclusão de *tags* nos *cards* de uma notícia Figura 12. Além disso, foi incluído o voto do usuário na descrição da notícia conforme a Figura 13.

A partir do uso constante do aplicativo e da inserção de mais notícias, a tela principal do front-end, que consiste no *feed* com as 10 notícias mais votadas, não apresentava mais as notícias que um usuário tinha votado, ao passo que novas notícias eram inseridas. Para os usuário que testaram o aplicativo, era necessário o conhecimento das notícias que foram votadas e, assim, foi inserido uma nova tela com um histórico de todas notícias votadas pelo usuário e seus índices de veracidades atuais Figura 14.

Os usuários do sistema também sentiram a necessidade de saber o progresso de votos em uma notícia para que ela mudasse do índice neutro, o status inicial de uma notícia. Para isso, foram inseridos dois novos indicadores na tela de descrição de notícia, Figura 13, para demonstrar a atual quantidade de votos *Fake* e *Fato* em uma notícia, e a quantidade de votos necessários para a notícia alcançar um novo índice.

Figura 12 – Desmonstração do uso de *tags* com o voto do usuário

Esses indicadores foram também aplicados de forma visual nos *cards* das notícias com índice Neutro, onde eles apresentam um gráfico na sua barra lateral esquerda com as cores verde (para votos Fato) e vermelha (para votos Fake) representando os votos realizados na notícia até o momento Figura 15.

Além da submissão do aplicativo móvel para o TestFlight, os outros módulos do sistema foram disponibilizados através de um servidor externo. A partir deste, o aplicativo móvel pôde fazer as requisições necessárias para seu funcionamento. Devido à ocasionais instabilidades que o servidor teve, as informações de votos dos usuários foram perdidas o que, somadas ao curto prazo, impossibilitaram uma maior coleta de dados e análise dos mesmos para avaliar o sistema de reputação.

Figura 13 – Demonstração a descrição de uma notícia

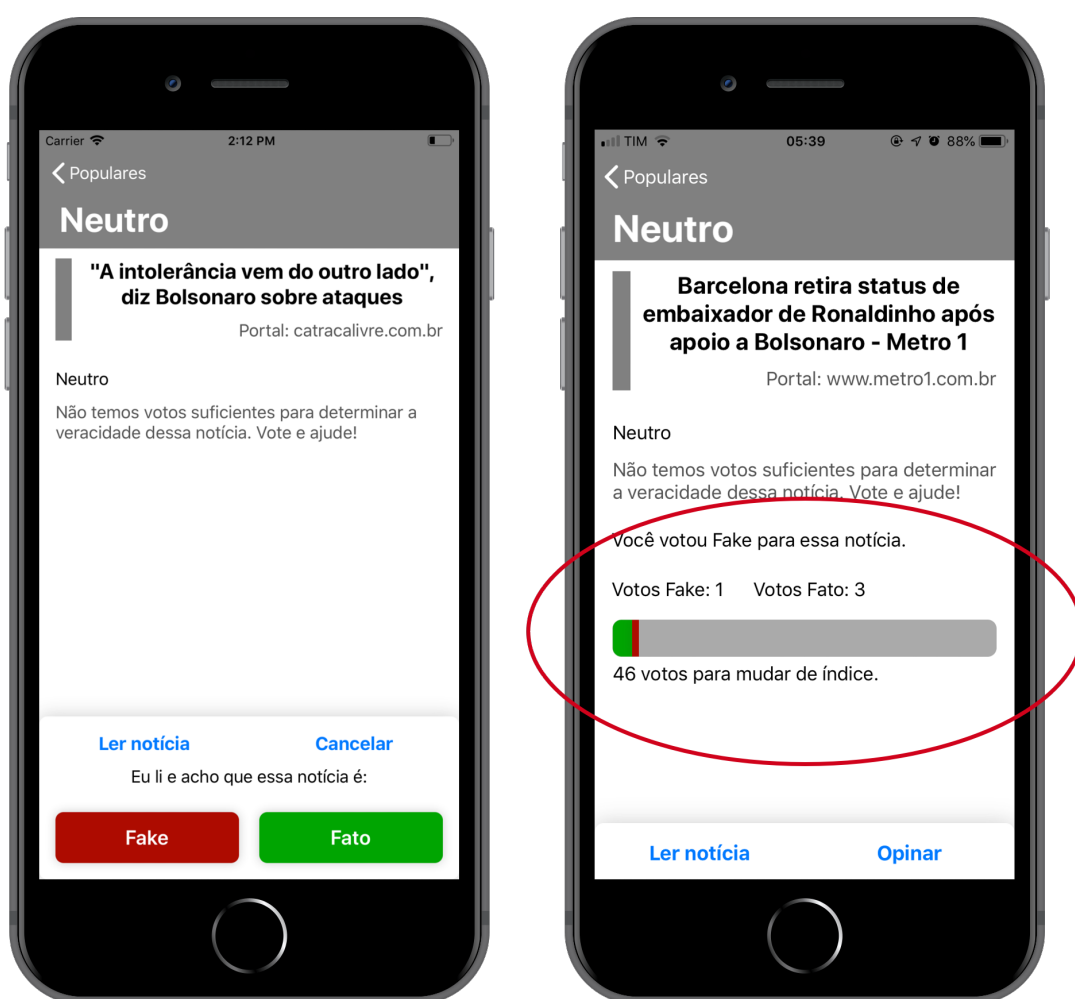
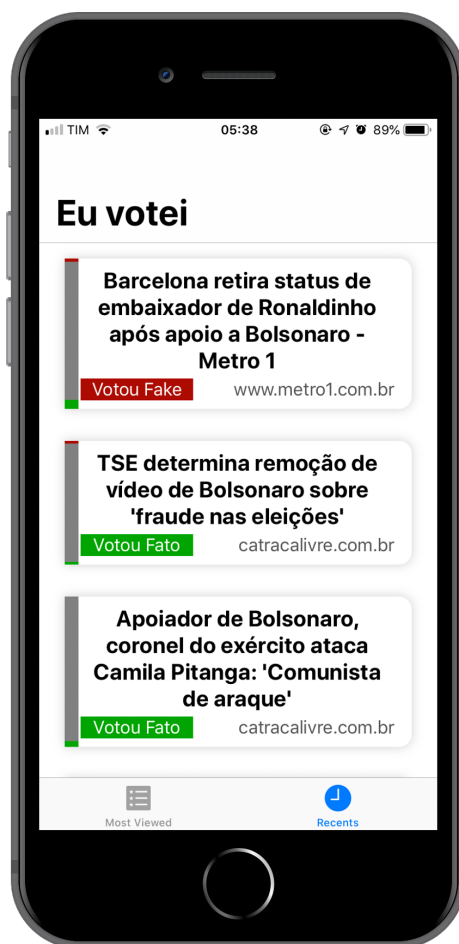
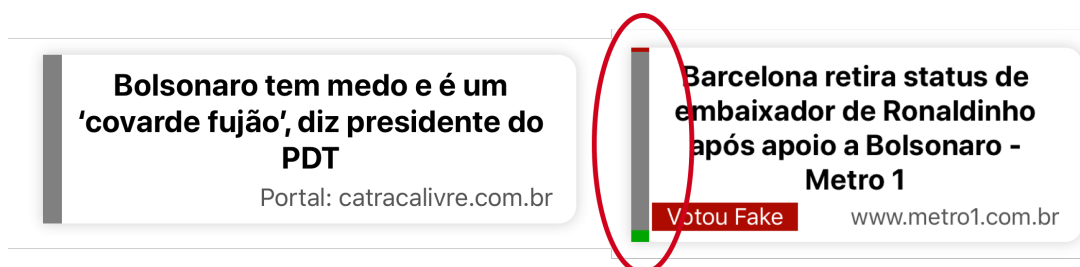


Figura 14 – Demonstração da tela de notícias votadas

Figura 15 – Demonstração de um *card* de uma notícia.

7 CONCLUSÃO

Na solução proposta, a veracidade de uma notícia é dependente da reputação dos usuários que votaram, e suas reputações são da mesma forma dependentes do resultado das notícias que votaram. Devido ao fato de que a reputação de um usuário pode variar, o índice de confiabilidade calculado pelo sistema não é um valor final. Logo, um benefício do sistema proposto é trazer suas definições de veracidades de notícias de maneira atual de acordo com o estado do sistema e reputações de seus usuários. Para isso, adotou-se uma abordagem de cálculo de reputação e veracidade em tempo real mesmo com o possível detrimento de desempenho do sistema. Sobrecarga de requisições e um aumento do tempo de espera podem ocorrer dependendo da quantidade de notícias e usuários utilizando o sistema.

A estrutura do sistema de reputação e os diferentes atributos calculados para a definir a veracidade de uma notícia trazem algumas precauções contra possíveis usuários maliciosos que possam votar em massa em uma certa notícia com uma opinião que os favoreça (ZACHARIA et al., 2000).

A interface do aplicativo desenvolvido para o usuário se mostrou satisfatório com informações suficientes para satisfazer os usuários. A partir da tela principal, o usuário pode acessar notícias populares e verificar o atual índice de confiabilidade atribuído à elas. Um usuário pode, também através dessa tela, verificar se realizou votos nessas notícias através do uso de *tags*. Em uma segunda tela, é possível encontrar uma lista de todas as notícias que o usuário votou e seu atual índice de confiabilidade.

Na tela de detalhes de uma notícia, o usuário pode verificar o atual índice de confiabilidade sugerido pelo sistema, a quantidade de votos necessários para se alterar este índice e a sua opinião para com esta notícia caso a tenha provido.

A utilização de *blockchain* traz um maior nível de segurança devido à descentralização da informação e à comunicação de dados baseado em comunicação assimétrica. A Speedychain facilitou a organização das informações devido ao fato de proporcionar o anexo de múltiplas transações em um mesmo bloco. Dessa forma, cada bloco na *blockchain* é representado por um usuário e, ao passo que ele/a adiciona votos no sistema, transações são adicionadas ao seu bloco.

7.1 TRABALHOS FUTUROS

Devido ao fato do sistema calcular as reputações dos usuários e dos índices de confiabilidades das notícias em tempo real, problemas de desempenho podem ocorrer. Portanto, questões

de escalabilidade devem ser discutidas em trabalhos futuros para evitar este problema. Uma possível solução seria o desenvolvimento de um modelo de cache temporário de reputação dos usuários. O mesmo modelo pode ser aplicado para o cálculo do índice de confiabilidade de notícias.

Em relação ao sistema de reputação, é necessário um trabalho e estudo mais aprofundado para determinar valores mais precisos. O mesmo é necessário para os valores de base para os cálculos dos índices de confiabilidade das notícias. Em trabalhos futuros pode-se adaptar o uso de parcerias com agências de checagem de fatos para possíveis inserções manuais de veracidade de notícias. Dessa forma futuras reputações podem se basear nessas notícias iniciais o que facilitaria a escalabilidade do sistema.

Devido à estrutura da Speedychain, que permite a inserção contínua de transações em um bloco, e a possibilidade de um usuário poder modificar seu voto em uma notícia, o sistema atual permite uma análise maior do comportamento de um usuário perante sua mudança de opinião em uma notícia. A partir desta análise, um trabalho futuro pode utilizar destes dados para influenciar o atual sistema de reputação de usuários e trazer melhorias mais precisas ao mesmo.

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.
- BENEVENUTO, F. **Eleições Sem Fake**. 2018. <<http://www.eleicoes-sem-fake.dcc.ufmg.br/>>. Acesso em: 25 set. 2018.
- BUNTAIN, C.; GOLBECK, J. Automatically identifying fake news in popular twitter threads. In: **2017 IEEE International Conference on Smart Cloud (SmartCloud)**. [S.l.: s.n.], 2017. p. 208–215.
- CASADO, L. **Luiz Fux pretende 'imprimir marca' no combate a 'fake news'**. 2017. <<https://www1.folha.uol.com.br/poder/2017/12/1941395-luiz-fux-pretende-imprimir-marca-no-combate-a-fake-news.shtml>>. Acesso em: 02 out. 2018.
- CHAVES, R. **Detector de Fake News**. 2018. <<https://fakenewsdetector.org/pt>>. Acesso em: 25 set. 2018.
- COMMERCE, B. E.; JØSANG, A.; ISMAIL, R. The beta reputation system. In: **In Proceedings of the 15th Bled Electronic Commerce Conference**. [S.l.: s.n.], 2002.
- FACEBOOK, N. **Facebook lança produto de verificação de notícias no Brasil em parceria com Aos Fatos e Agência Lupa**. 2018. <<https://br.newsroom.fb.com/news/2018/05/facebook-lanca-produto-de-verificacao-de-noticias-no-brasil/penalty-@M-em-parceria-com-aos-fatos-e-agencia-lupa/>>. Acesso em: 20 out. 2018.
- G1. **Facebook exclui páginas de 'rede de desinformação'; MBL fala em 'censura'**. 2018. <<https://g1.globo.com/economia/tecnologia/noticia/2018/07/25/facebook-retira-do-ar-rede-de-fake-news-ligada-ao-mbl-antes-das-eleicoes-dizem-fontes.ghml>>. Acesso em: 27 dez. 2018.
- GLOBO, O. G. C. A. I. **Após escândalo, Facebook dá dicas para evitar fake news no México**. 2018. <<https://oglobo.globo.com/mundo/apos-escandalo-facebook-da-dicas-para-evitar-fake-news-no-mexico-22511786>>. Acesso em: 20 out. 2018.
- GOOGLE. **UX - A experiência do usuário**. 2015. <<https://www.thinkwithgoogle.com/intl/pt-br/marketing-resources/ux-e-design/ux-user-experience/>>. Acesso em: 20 out. 2018.
- GUESS, A.; NYHAN, B.; REIFLER, J. Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 us presidential campaign. **European Research Council**, 2018.
- HOOTSUITE. **Essential insights into internet, social media, mobile, and e-commerce use around the world**. 2018. <<https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338>>. Acesso em: 03 out. 2018.
- HYMAN, J. Addressing fake news: Open standards easy identification. In: **2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)**. [S.l.: s.n.], 2017. p. 63–69.

KRISHNAN, S.; CHEN, M. Identifying tweets with fake news. In: **2018 IEEE International Conference on Information Reuse and Integration (IRI)**. [S.l.: s.n.], 2018. p. 460–464.

LONG, J. **12 Startups Utilizing Blockchain Technology in New Ways**. 2018. <<https://www.entrepreneur.com/article/310373>>. Acesso em: 01 out. 2018.

LUNARDI, R. C.; MICHELIN, R. A.; NEU, C. V.; ZORZO, A. F. Distributed access control on iot ledger-based architecture. In: **16th IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)**. Taipei, Taiwan: [s.n.], 2018. p. 1–8.

MARTI, S.; GARCIA-MOLINA, H. Taxonomy of trust: Categorizing p2p reputation systems. **Computer Networks**, v. 50, n. 4, p. 472 – 484, 2006. ISSN 1389-1286. Management in Peer-to-Peer Systems. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S138912860500215X>>.

MERELES, C. **Checagem de fatos: Um novo nicho no jornalismo**. 2017. <<https://www.politize.com.br/checagem-de-fatos/>>. Acesso em: 03 out. 2018.

Michelin, R. A.; Dorri, A.; Lunardi, R. C.; Steger, M.; Kanhere, S. S.; Jurdak, R.; Zorzo, A. F. SpeedyChain: A framework for decoupling data from blockchain for smart cities. **ArXiv e-prints**, jul. 2018.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008.

ORMAN, H. Blockchain: the emperors new pki? **IEEE Internet Computing**, v. 22, n. 2, p. 23–28, Mar 2018. ISSN 1089-7801.

PHOTOCHAIN. **Rewriting the rules for monetizing your images**. 2018. <<https://photochain.io>>. Acesso em: 01 out. 2018.

SENRA, R. **Eleições 2018: novas ferramentas contra fake news são impossíveis a uma semana da votação, diz WhatsApp**. 2018. <<https://www.bbc.com/portuguese/brasil-45897170>>. Acesso em: 20 out. 2018.

SHU, K.; WANG, S.; LIU, H. Understanding user profiles on social media for fake news detection. In: **2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)**. [S.l.: s.n.], 2018. p. 430–435.

TECH, C. **Contra fake news, Google traz nova ferramenta de checagem de fatos**. 2017. <<https://canaltech.com.br/mercado/contrafake-news-google-traz-nova-ferramenta-de-checagem-de-fatos-91894/>>. Acesso em: 20 out. 2018.

TECHTERMS. **Hash Definition**. 2018. <<https://techterms.com/definition/hash>>. Acesso em: 26 dez. 2018.

TSCHORSCH, F.; SCHEUERMANN, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. **IEEE Communications Surveys Tutorials**, v. 18, n. 3, p. 2084–2123, 2016. ISSN 1553-877X.

ZACHARIA, G.; MOUKAS, A.; MAES, P. Collaborative reputation mechanisms for electronic marketplaces. **Decision Support Systems**, v. 29, n. 4, p. 371 – 388, 2000. ISSN 0167-9236. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0167923600000841>>.

APÊNDICE A – Artigo aceito na WRSEG2018

Sistema de Reputação Baseado em Blockchain para Detecção de *Fake News**

Bruno H. Lippert¹, Bruno F. Scheltzke², Roben C. Lunardi^{1,2}, Regio A. Michelin^{1,2},
Avelino F. Zorzo¹

¹Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre, Brasil

²Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)
Porto Alegre, Brasil.

Abstract. *Currently, fake news have become a big challenge for the society. Consequently, different organizations are searching for solutions to reduce the impact of fake news. Therefore, this paper advances the solution for this problem proposing a system, based on blockchain and user reputation, that registers fake news in a distributed ledger. The architecture and implementation of the system, called “No Fake News”, is still under development. This paper presents the proposed solution and a discussion about its adoption.*

Resumo. *Atualmente, a identificação de notícias falsas se tornou um grande desafio para a sociedade. Desta forma, diferentes organizações buscam por soluções para reduzir o impacto das ditas fake news. Portanto, este trabalho avança sobre este problema, propondo um sistema, baseado em blockchain e reputação do usuário, que registra notícias falsas em uma blockchain. A arquitetura e implementação do sistema, chamado “No Fake News”, ainda está em desenvolvimento. Este artigo apresenta a solução proposta e discussões sobre sua adoção.*

1. Introdução

O termo *fake news*, ou, “notícia falsa” em português, trata de uma notícia que passa uma informação não verídica intencionalmente com o objetivo de criar uma polêmica e/ou denegrir pessoas ou organizações [Shu et al. 2018]. *Fake news* tornou-se um assunto recorrente na mídia, dado que, com o avanço da tecnologia da informação qualquer pessoa com acesso a Internet pode disseminar informações falsas e maliciosas. Sendo assim, nenhuma notícia de fonte pouco conhecida pode ser considerada verdadeira até que seja confirmada sua veracidade [Shu et al. 2018]. Uma notícia falsa possui vários indicadores de sua falsidade, tais como: ausência de fonte, sensacionalismo, erros de formatação ou ortografia. Contudo, usualmente, o trabalho de busca de veracidade é realizado por pessoas especializadas, demandando tempo considerável para ser finalizado [Krishnan and Chen 2018].

Por ter um potencial de atingir milhões de usuários em pouco tempo, *fake news* tornou-se uma das principais armas políticas, através de manchetes falsas e tendenciosas. Por exemplo, essas notícias podem influenciar diretamente no resultado de uma eleição

*O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal Nível Superior – Brasil (CAPES) – Código de Financiamento 001, pelo INCT em Ciências Forenses financiado pelo CNPq, pela HP Brasil usando incentivos da Lei de Informática, e também da Totvs S/A.

[Hyman 2017]. Desta forma, *fake news* tornou-se uma ferramenta de difamação que possui potencial para influenciar usuários *online*.

Após o surgimento do Bitcoin, diversas propostas de *blockchain* surgiram para garantir a integridade, autenticidade e disponibilidade da informação em diferentes contextos. *Blockchains* armazenam a informação em blocos ligados de forma encadeada utilizando o *hash* do bloco anterior. Este conjunto de blocos encadeados é distribuído e validado pelos demais nodos. Desta forma, alterações na *blockchain* são dificultadas devido às características da mesma [Tschorsch and Scheuermann 2016]. Sendo assim, caso um destes nodos tente inserir uma informação que não condiz com um certo conjunto de regras predefinidas ou tente alterar um dado que foi armazenado, os valores *hash* armazenados em cada bloco não serão satisfeitos, e o bloco não será aceito [Orman 2018].

Tendo em vista os problemas gerados por informações falsas e a proposta que a tecnologia *blockchain* oferece, este artigo propõe uma solução para determinar a veracidade de notícias a partir de avaliações de usuários cadastrados. Com o objetivo de fornecer integridade e auditabilidade das informações, o sistema desenvolvido armazena opiniões sobre notícias utilizando a plataforma Speedy-Chain [Lunardi et al. 2018] [Michelin et al. 2018]. Quando a veracidade de uma notícia é requisitada, o sistema calcula a reputação dos usuários que votaram na notícia em questão, para assim determinar sua veracidade. Consequentemente, o sistema se propõe a alertar usuários de portais de notícia sobre a veracidade da informação. Portanto, diminuindo consideravelmente o impacto que *fake news* têm sobre o cotidiano das pessoas.

2. Trabalhos Relacionados

A área de verificação de notícias tem recebido atenção da comunidade científica nos últimos anos [Hyman 2017] [Buntain and Golbeck 2017] [Krishnan and Chen 2018] [Shu et al. 2018]. Desta forma, sistemas para identificação de informações falsas foram propostos [Benevenuto 2018] [Chaves 2018].

Buntain e Golbeck [Buntain and Golbeck 2017] desenvolveram um método para identificar notícias falsas na rede social Twitter. Os autores propõem um algoritmo que pesquisa, em dois bancos de dados, assuntos que potencialmente podem ser usados para criar uma *fake news*. A partir disto, o algoritmo analisa a estrutura das informações inseridas na rede social, com base em diversos critérios pré-definidos, para concluir se a informação é verdadeira ou não. Este mecanismo tem uma taxa de sucesso na identificação de *fake news* de aproximadamente 69%. Apesar de um índice elevado para a identificação automatizada de *fake news*, a solução proposta está limitada a plataforma Twitter.

Eleição Sem Fake [Benevenuto 2018] é um projeto capaz de monitorar notícias no Facebook e identificar “bots” nas redes sociais. Apesar de ser uma ferramenta para auditar dados, ela não permite que o usuário decida quais notícias pretende analisar e não permite a análise de notícias de temas variados. Como a ferramenta possui um enfoque no cenário político, o sistema se limita a dados demográficos referentes a distribuição do público que os portais de notícias possuem, assim como páginas de Facebook.

O Detector de Fake News [Chaves 2018] é um software onde os usuários podem informar se determinada notícia é uma *fake news* ou “click bait” (notícia com título

tendencioso para que o usuário clique no *link* da notícia). Apesar de ser uma proposta promissora, analisa apenas notícias do Twitter e Facebook, além de não permitir que o usuário realize buscas por notícias específicas na base de dados.

3. Solução Conceitual

Buscando a garantia de resiliência, disponibilidade, não repúdio e integridade dos dados a proposta do sistema No Fake News utiliza a tecnologia *blockchain*, dado que esta garante as propriedades necessárias ao sistema. Além destas propriedades, é possível que qualquer usuário audite os dados disponíveis. Esta proposta, além de possibilitar o envio de notícias para avaliação, permite que o usuário busque - nos dados armazenados na *blockchain* - notícias específicas. Desta forma, calcula-se a reputação dos usuários que interagem com o sistema e os atributos que possibilitam definir um índice de confiabilidade de uma notícia (ver Seção 4). Portanto, esta proposta torna-se, também, uma base de dados distribuída para pesquisa de *fake news* com garantia de integridade dos votos.

De forma a prover os atributos necessários ao sistema No Fake News, adotou-se uma arquitetura modular baseado no modelo REST para realizar a comunicação entre o módulo da SpeedyChain (*blockchain*), módulo para representação da API, e Front-End para interação com usuário. Os atributos relacionados a veracidade de uma notícia são calculados em tempo real a cada interação do usuário. A Figura 1 apresenta uma definição estrutural da proposta, bem como os principais módulos desenvolvidos para o projeto.

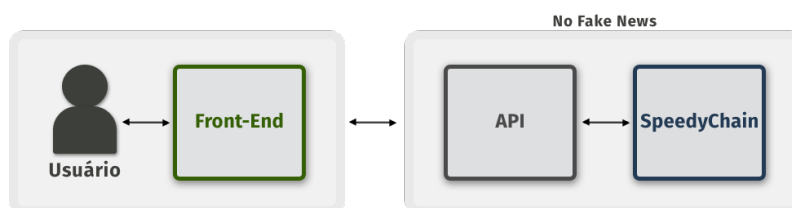


Figura 1. Arquitetura do No Fake News.

No sistema proposto, o usuário pode realizar operações de voto em uma notícia específica, e verificar atributos de confiabilidade de notícias através do componente de Front-End. Através dos votos de usuários, a API pode, enfim, calcular a veracidade das notícias (ver Seção 4). Além disso, o módulo de Front-End pode futuramente ser responsável por recolher o cadastro de notícias por parte da mídia e apresentar a reputação dos usuários, portais e autores.

A API é responsável por expor métodos que fornecem as funcionalidades para o Front-End. Este módulo do sistema provê a possibilidade de registrar a opinião sobre uma notícia, e encaminhar para inserção na *blockchain*. Além disso, a API tem função de receber o pedido e conferir a veracidade de uma determinada notícia. Desse modo, cabe a esse módulo coletar as informações necessárias diretamente da SpeedyChain. A veracidade de uma notícia é definida pela reputação dos usuários que opinaram sobre ela. A API solicita informações desses usuários para a SpeedyChain, que entrega todas as chaves públicas de identificação desses usuários.

A reputação de um usuário é definida pelas suas opiniões em notícias. A API coleta da SpeedyChain as notícias que o usuário votou, e, ao passo que existam votos su-

ficientes para determinar atributos de veracidade dessas notícias, o sistema pode comparar esses resultados com a opinião do usuário e assim determinar sua reputação.

Após ter todas as informações necessárias, a API é capaz de calcular as reputações dos usuários que opinaram na notícia requerida, e assim determinar sua veracidade para o usuário que originou a solicitação.

4. Implementação

Tendo como base a definição conceitual do sistema apresentada na Seção 3, a sua implementação foi feita utilizando tecnologias atuais. Dentre estas tecnologias buscou-se uma opção de implementação de blockchain que fosse capaz de atender as necessidades do sistema, e dadas as opções disponíveis SpeedyChain mostrou-se uma escolha adequada, visto que a mesma consiste de uma *blockchain* composta de blocos que podem continuar recebendo transações após serem inseridos na *blockchain* [Lunardi et al. 2018, Michelin et al. 2018]. Desta forma, todos os votos passados e os futuros votos de um usuário são armazenados em um mesmo bloco. Cada novo voto (transação) é inserido mantendo um *link* com os demais através da função *hash* [Michelin et al. 2018].

Para um usuário autenticar no sistema, primeiro este deve acessar o módulo de Front-End (conforme Figura 1). Após a confirmação de que a chave pública está registrada na SpeedyChain (caso não esteja, é preciso criar um novo usuário), trocam-se as chaves entre o sistema e o usuário para realizar a criptografia dos dados comunicados. Desta forma, estabelece-se a comunicação inicial com o sistema. A cada interação de inserção do usuário, a SpeedyChain requer que o Front-End seja capaz de assinar a informação com sua chave privada e cifra-la com sua chave de comunicação para que haja um maior nível de confiabilidade no sistema. Caso um usuário tente inserir algum voto e sua comunicação não foi estabelecida, ou há erro na criptografia ou na assinatura dos dados, nenhum dado é enviado para outros nodos da *blockchain* para sua inserção e uma mensagem de erro é retornada para o Front-End.

Para dar suporte para o usuário determinar se a notícia é ou não verdadeira, o sistema No Fake News (no módulo API da Figura 1) possui um conjunto de indicadores: voto de um usuário para a notícia sendo verdadeira (*VT*); voto de um usuário para a notícia sendo falsa (*VF*); a reputação do usuário votante na notícia (*R*); índice de veracidade da notícia (*T*); índice de falsidade da notícia (*F*); diferença de índice de veracidade e falsidade (*Df*); média da reputação dos votantes como verdadeiro (*MT*); média da reputação dos votantes como falso (*MF*).

O usuário pode incrementar a reputação (*R*) inicial no sistema de acordo com sua atividade no sistema. Um usuário nunca terá uma reputação mais baixa do que a inicial. O contrário pode acarretar em usuários maliciosos com baixa reputação criando novas contas no sistema, conforme [Zacharia et al. 2000].

Para cálculo dos índices *T* e *F*, o No Fake News separa os usuários que interagiram com a notícia pelas suas opiniões (verdadeiro/falso), e agrega o valor do peso de suas reputações: $T = \sum_{i=1}^n (VT_i * RT_i)$ e $F = \sum_{j=1}^m (VF_j * RF_j)$. Conforme apresentado nas fórmulas para *T* e *F*, o usuário pode verificar os parâmetros de veracidade e falsidade alcançados pela notícia. Quanto maior o índice, maior o peso para ser considerado.

O índice Df é o índice de confiança no resultado com maior peso (entre T e F), onde: $Df = \left| \frac{(T - F)}{(T + F)} \right|$. Desta forma, considera-se o percentual do peso de veracidade ou falsidade (o que for maior) da diferença de pesos em relação ao total opinado.

Finalmente, o sistema determina a qualidade da análise. Para isto o sistema calcula a média das reputações dos usuários que opinaram: $MT = \frac{\sum_{i=1}^n RT_i}{n}$ e $MF = \frac{\sum_{j=1}^m RF_j}{m}$. Portanto, uma notícia com muitos votos de baixa reputação tem um peso menor na análise, mesmo que tenha um número significativo de votos.

Atualmente foram implementadas duas versões do *Front-End*: uma versão como um *plugin* para o Google Chrome; e uma versão como aplicativo para iPhone. Ambas realizam a interação do usuário com o sistema. O sistema atual fornece parâmetros para facilitar a decisão por um usuário, consultando uma base resiliente e confiável. Todavia, a indicação automatizada se uma notícia é falsa (ou não) ainda está em desenvolvimento.

5. Comparação com soluções existentes

O No Fake News possibilita a validação de qualquer notícia disponível na Internet, independente da plataforma publicada. O que difere dos sistemas comparados, que utilizam informações do Facebook ou Twitter conforme apresentado na Tabela 1.

Sistema	Público alvo	Origem da notícia	Método de validação de notícias	Pesquisa por uma notícia
No Fake News	Qualquer usuário	Qualquer website	Reputação dos usuários que opinaram	Disponível a qualquer pessoa
Eleição Sem Fake	Facebook	Facebook	Monitoramento de notícias anunciadas	Notícias políticas da região do usuário
Detector de Fake News	Facebook ou Twitter	Facebook ou Twitter	Índices de veracidade baseado em reputação	Não disponível

Tabela 1. Comparação de soluções existentes com o No Fake News

Na Tabela 1 pode-se observar que o algoritmo de validação das notícias do sistema proposto, gerará resultados automatizados (atualmente gera apenas índices) sobre a veracidade de uma notícia. O No Fake News é baseado na reputação dos votantes, diminuindo assim custo e tempo com a utilização de agências de checagem de fatos.

O sistema proposto apresenta transparência, descentralização e integridade das informações. Os índices sobre veracidade das notícias podem ser acessados por qualquer pessoa ou sistema, sem requerer cadastro, diferente das outras soluções (Tabela 1).

6. Conclusões e Trabalhos Futuros

Na solução proposta, a veracidade de uma notícia é dependente da reputação dos usuários que votaram, e suas reputações são da mesma forma dependentes do resultado das notícias que votaram. Devido ao fato de que a reputação de um usuário pode variar, o sistema não pode dar um veredito final sobre uma notícia. Desse modo, adotou-se uma abordagem de cálculo de reputação e veracidade em tempo real mesmo com o eminente detrimento

da performance do sistema. Sobrecarga de requisições e tempo de espera podem ocorrer dependendo do tamanho do número de notícias e usuários do sistema. Portanto, questões de escalabilidade devem ser discutidas em trabalhos futuros.

A estrutura do sistema de reputação e os diferentes atributos calculados para a veracidade de uma notícia trazem algumas precauções contra possíveis usuários maliciosos que possam votar em uma certa opinião em massa [Zacharia et al. 2000]. Entretanto, está em análise inserções manuais de veracidade ou falsidade de notícias por órgãos confiáveis. Ainda pretende-se desenvolver um modelo de cache temporário de reputação no usuário. Dessa forma, o tempo de resposta do sistema pode ter melhor desempenho. No sistema proposto neste artigo, o módulo da API calcula atributos de uma notícia e encaminha aos usuários que podem tomar uma decisão sobre a veracidade da notícia. Pretende-se, como trabalho futuro, desenvolver uma solução automatizada para calcular o índice de confiabilidade, baseado nos índices apresentados na Seção 4.

Referências

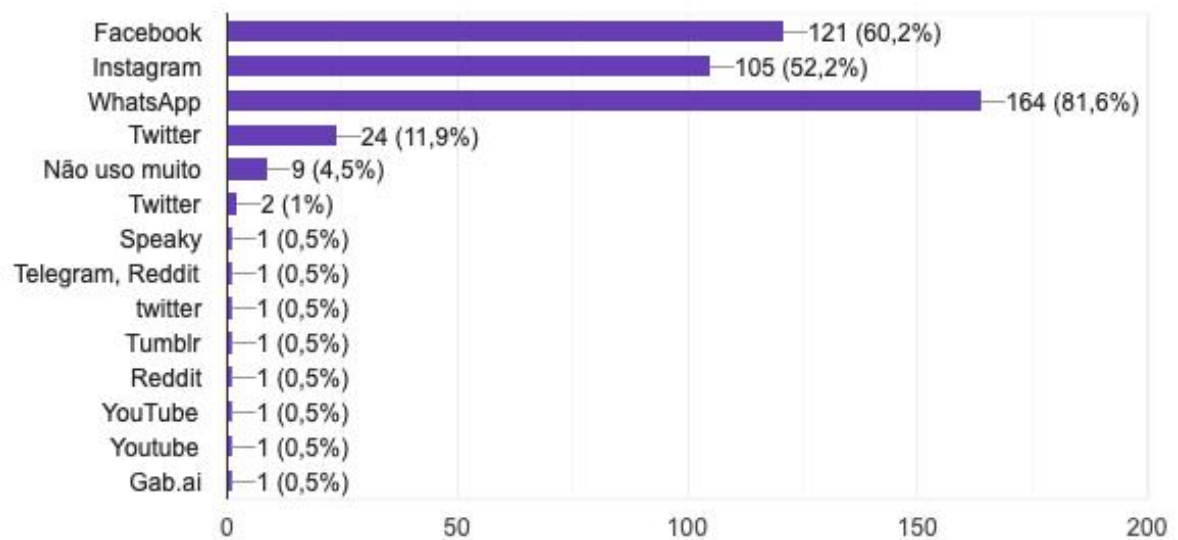
- Benevenuto, F. (2018). Eleições sem fake. <http://www.eleicoes-sem-fake.dcc.ufmg.br/>. Acesso em: 25 set. 2018.
- Buntain, C. and Golbeck, J. (2017). Automatically identifying fake news in popular twitter threads. In *2017 IEEE International Conference on Smart Cloud (SmartCloud)*, pages 208–215.
- Chaves, R. (2018). Detector de fake news. <https://fakenewsdetector.org/pt>. Acesso em: 25 set. 2018.
- Hyman, J. (2017). Addressing fake news: Open standards amp; easy identification. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pages 63–69.
- Krishnan, S. and Chen, M. (2018). Identifying tweets with fake news. In *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 460–464.
- Lunardi, R. C., Michelin, R. A., Neu, C. V., and Zorzo, A. F. (2018). Distributed access control on iot ledger-based architecture. In *16th IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*, pages 1–8, Taipei, Taiwan.
- Michelin, R. A., Dorri, A., Lunardi, R. C., Steger, M., Kanhere, S. S., Jurdak, R., and Zorzo, A. F. (2018). SpeedyChain: A framework for decoupling data from blockchain for smart cities. *ArXiv e-prints*.
- Orman, H. (2018). Blockchain: the emperors new pki? *IEEE Internet Computing*, 22(2):23–28.
- Shu, K., Wang, S., and Liu, H. (2018). Understanding user profiles on social media for fake news detection. In *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, pages 430–435.
- Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123.
- Zacharia, G., Moukas, A., and Maes, P. (2000). Collaborative reputation mechanisms for electronic marketplaces. *Decision Support Systems*, 29(4):371 – 388.

APÊNDICE B – Pesquisa sobre Fake News e Redes Sociais

Quais redes sociais voce usa mais?



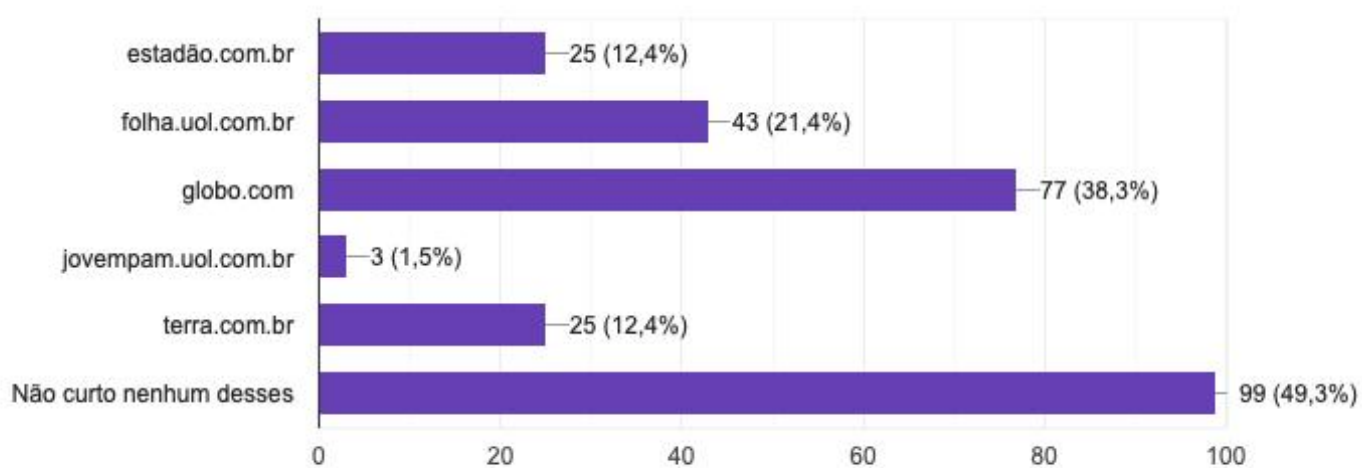
201 respostas



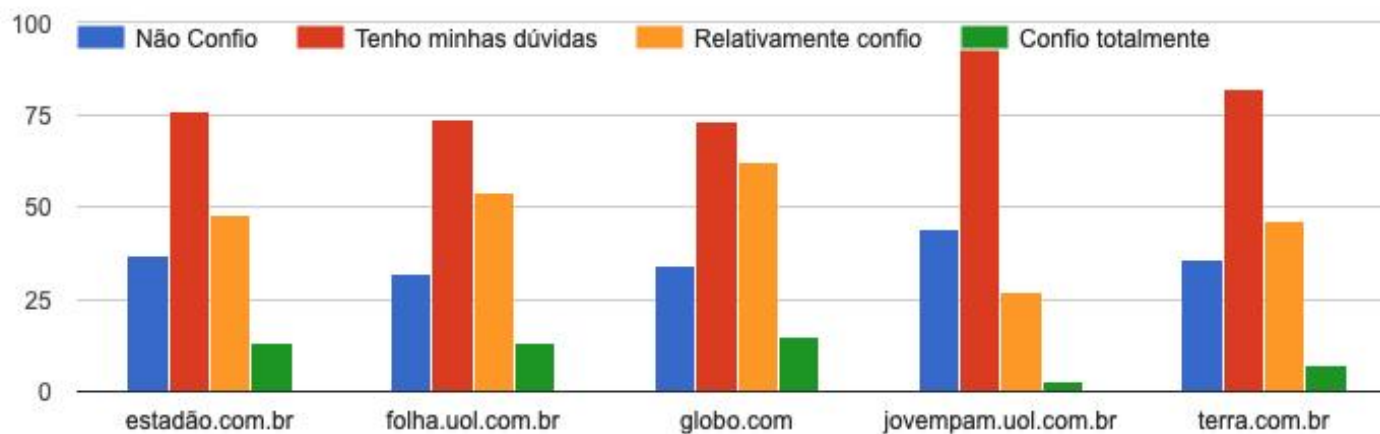
Quais desses portais de notícia você usa pra se manter atualizado?



201 respostas

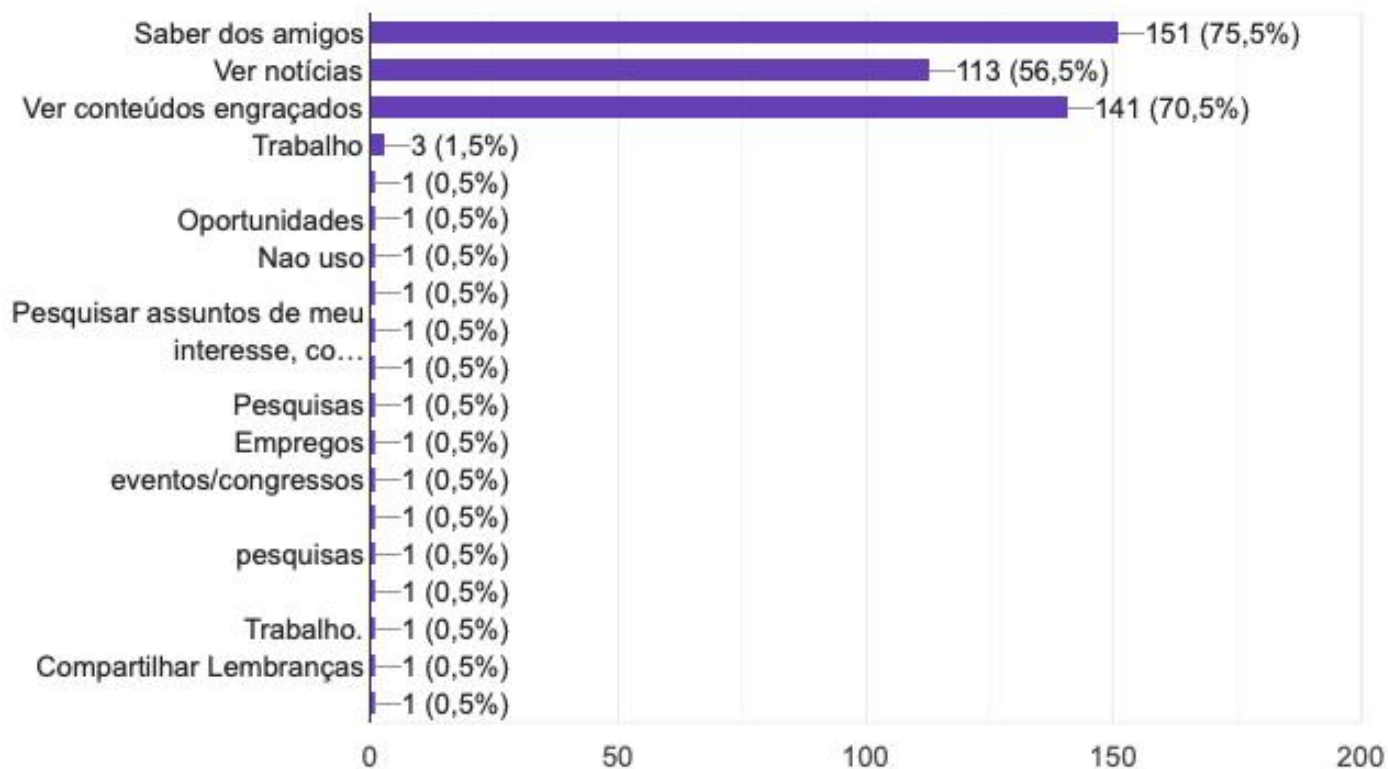


Quão confiável você acha que esses portais são?



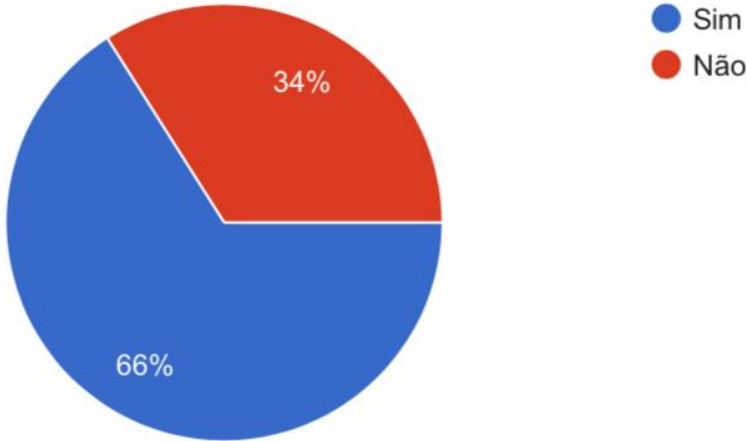
Para que você usa as redes sociais?

200 respostas



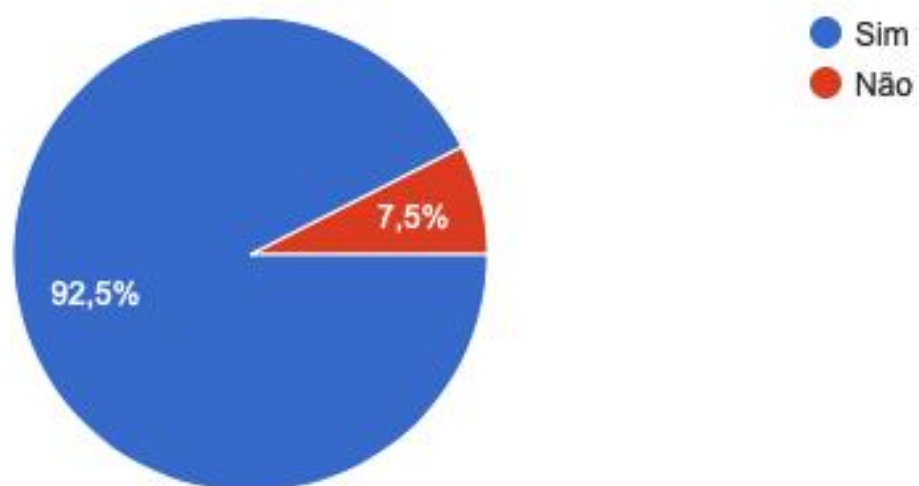
Você tende a compartilhar coisas com seus amigos, família nas redes?

200 respostas



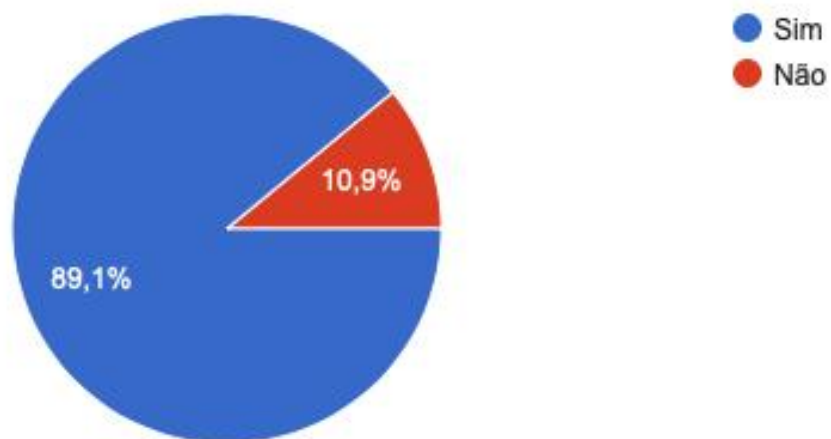
Você já recebeu alguma notícia falsa na internet?

200 respostas



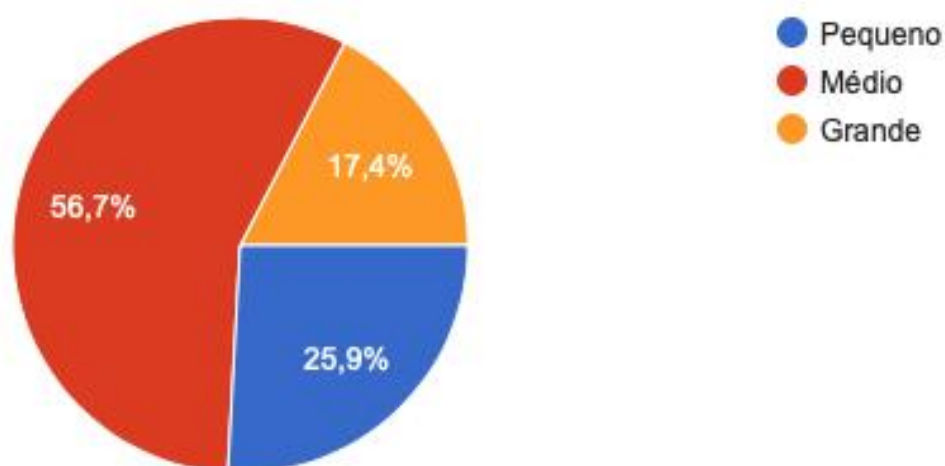
Você acha que Fake News é um problema relevante?

201 respostas



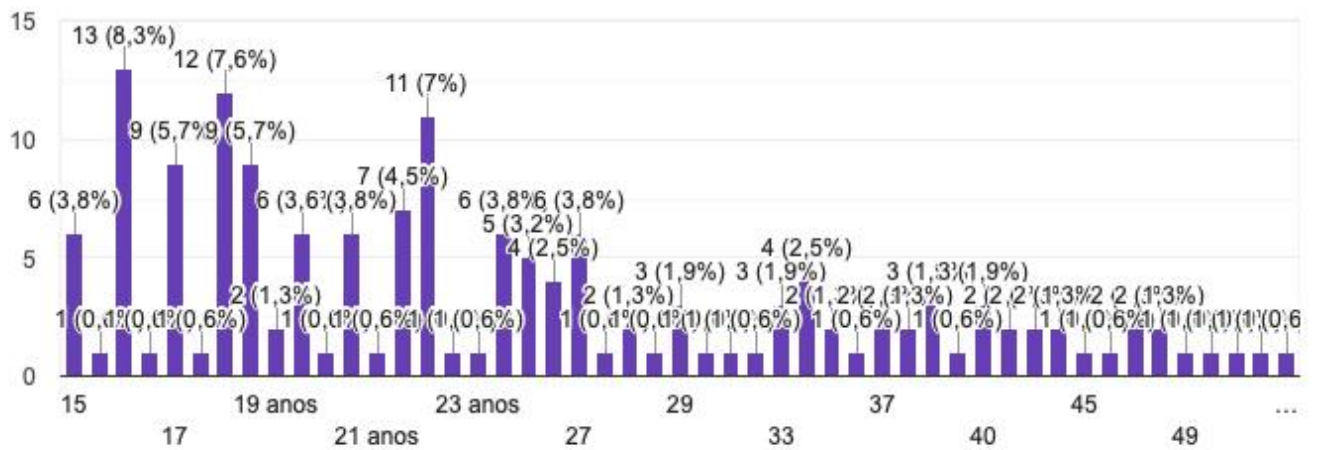
Qual seu nível de interesse pelo tema Fake News?

201 respostas



Poderia nos informar a sua idade?

157 respostas



E gênero?

159 respostas

