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

Chapter · August 2019

DOI: 10.1007/978-3-030-29238-6_8

6 authors, including:

Iago Sestrem Ochôa
Universidade do Vale do Itajaí (Univali)
11 PUBLICATIONS **123** CITATIONS
SEE PROFILE

Luis Augusto Silva
Universidad de Salamanca
52 PUBLICATIONS **378** CITATIONS
SEE PROFILE

Abel JP Gomes
Universidade da Beira Interior
121 PUBLICATIONS **849** CITATIONS
SEE PROFILE

Anita Maria Rocha Fernandes
Universidade do Vale do Itajaí (Univali)
82 PUBLICATIONS **187** CITATIONS
SEE PROFILE

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

Iago Sestrem Ochoa[1(✉)], Gabriel de Mello[1], Luis A. Silva[1], Abel J. P. Gomes[2,3], Anita M. R. Fernandes[1], and Valderi Reis Quietinho Leithardt[1,2]

[1] University of Vale do Itajai, Itajai, SC 88302-901, Brazil
{iago.ochoa,gabrieldemello,luis.silva}@edu.univali.br, anita.fernandes@univali.br
[2] Universidade da Beira Interior, 6200-001 Covilhã, Portugal
valderi.leithardt@ubi.pt
[3] Instituto de Telecomunicações, Covilhã, Portugal
agomes@di.ubi.pt

Abstract. The electoral period has great importance in any democracy, but nowadays, different groups try to get an advantage in the democratic process by posting fake news on social media networks. The use of data mining technique to identify fake news is on development stage, and there is no holistic solution to this problem yet. In our work, we proposed an architecture that uses a centralized blockchain on fake news detection process. The primary characteristic of our architecture is the use of data mining as a consensus algorithm to authenticate the information published on social networks. Using our architecture is possible to identify fake news, alert readers, punish who dissolves this type of information and reward who publish true information on the network.

Keywords: Blockchain · Data mining · Fake news

1 Introduction

The Brazilian 2018 presidential election was one of the most important in the Brazilian history. The political polarization has generated two extremes in the dispute for power. According to the New York Times [13], 44% of the Brazilian population uses WhatsApp as a source of political information. On the eve of the election, the application was used to disseminate an alarming quantity of fake news, in favor of both candidates.

Fake news is an information type that does not represent real facts, and this information is published most of the time on social networks. The purpose of fake news is to generate controversy around a person, aiming to denigrate or benefit his/her image. According to [3], on the 2016 presidential elections of the United States, 8.7 million fake news was shared on Facebook. The negative impact of fake news can be seen from the economic, social, and political point of view.

M. Piattini et al. (Eds.): QUATIC 2019, CCIS 1010, pp. 105–118, 2019.
https://doi.org/10.1007/978-3-030-29238-6_8

With increasing technology evolution, the use of fake news detection techniques becomes necessary to protect users of social networks from being influenced by this kind of news.

In [10] is presented an in-depth study about the definition of fake news and different ways to identify them. Among the techniques presented, the truth-detection method is more consistent with the current scenario, where the main objective is to discover the reliability of the news source and the veracity of the news at the same time. A problem that can restrict the use of this technique is the need for a database to store what sources publish about determined news. For this, it is necessary to use a technique that allows to store the data and keep them continually updated.

In 2008, Nakamoto developed blockchain technology and showed it to the world through bitcoin, a cryptocurrency without a centralizing bank unit [6]. This technology proved to be revolutionary because it ensures users privacy and authenticity in the transactions performed on the platform. Over the years, various applications focused on different scenarios have been developed using this technology.

Considering the scenario of fake news detection, blockchain technology has attracted the attention of researchers because it guarantees the integrity and reliability of the information stored in its block structure. The works presented in [9,11], and [2] show three blockchain architectures focused on the scenario of fake news detection on social networks. However, the solutions presented only address the issue of detecting fake news in social media, dismissing the issue that refers to the reliability of the sources that publish them.

In this way, we intend to use the blockchain technology to detect fake news on social networks and update the reliability level of each source, as shown in [7]. The differential of our architecture is on the consensus algorithm. We used the truth detection technique to guarantee the authenticity of the information published on social networks.

The remainder of this paper is structured as follows. In Sect. 2 is presented the background with the fundamental concepts to understand the proposed architecture. in Sect. 3 is shown the proposed architecture for fake news detection on social networks. Section 4 presents a proof of concept of the proposed architecture and the results obtained through the tests performed. In Sect. 5 is made a comparison between the related works and our architecture, showing the positive and negative features of each work. Finally, Sect. 6 presents the conclusions obtained with this work and the suggestions for future work.

2 Background

Blockchain is a data structure where the blocks are linked together, forming a chain. Inside each block is stored information, this information may vary for each kind of blockchain (i.e., Ethereum and Bitcoin). A cryptographic hash function connects the blocks of the structure, where the hash of the n block is linked with the hash of $n + 1$ block. Some of the characteristics of a blockchain can be defined as type, access, and consensus.

The blockchain type refers to its distribution. Centralized blockchains are stored on a single server, where users have restricted permissions that are set by the network host. In decentralized blockchains, any user can perform operations of writing and reading data. Usually, this type of blockchain is public, allowing access to anyone [5].

The access to a blockchain is characterized by full nodes clients, where the clients who store the blockchain in their device and perform the mining process without relying on other parts. Light clients do not store the blockchain itself and do not participate in the mining process. However, they can access the information contained in the blockchain through the connection with third parties [8].

The consensus is how the blockchain validates the information. The PoW (Proof-of-Work) algorithm ensures consensus in the network by solving a cryptographic problem. The Proof-of-Stake (PoS) algorithm selects the miners of the blocks based on the amount of cryptocurrency the user has, users with higher amount of cryptocurrency has more chances for being chosen to validate the block. The algorithms mentioned above are the most popular ones nowadays, but with the evolution of blockchain technology, new consensus algorithms have been developed to optimize the network and solve existing problems [1].

The truth-discovery algorithm is used to solve conflicts of information that come from different noise sources. This algorithm defines degrees of reliability for a given set of sources, based on the information provided by this sources [4].

Figure 1 illustrates the operation of the truth-discovery algorithm. For an object of interest called *object*, diverse sources s provide an information o in relation to the object. The truth-discovery algorithm processes this information by considering the reliability index of each w source, to get at a conclusion from which sources comes the true information t.

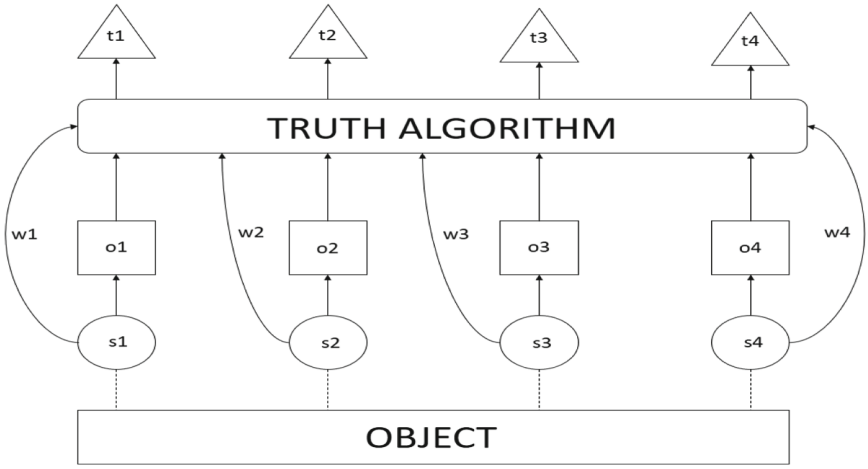

Fig. 1. Truth-discovery algorithm fluxogram.

3 Proposed Architecture

In our architecture, we defined that each news source is considered a network node in the blockchain. Considering that, all sources of news are also miners. The purpose of using this type of architecture is to guarantee the reliability level of each network source since any source that publishes news can be evaluated by what it published.

As the primary goal of our architecture is to prevent fake news spam on social networks, we chose to use a centralized blockchain. News sources are considered full nodes, they are responsible for doing reading and writing operations in the blockchain, in addition to participating in the mining process. The light clients can access the information stored in the blockchain, but they are not able to publish news on it.

As a consensus algorithm, we choose to use the truth-discovery algorithm. When one of the mining nodes defines the veracity of the recorded news of each source, this node earns an increase in its degree of reliability. The nodes that disseminated fake news get their reliability degree decreased as punishment. To be fair to the nodes which have also published real news, even if they can not mine the block, they will also receive a small increase in their reliability degree. In order to not monopolize the network with computational power, our algorithm will use the PoS algorithm concept, where nodes with higher degrees of reliability have more chances to mine new blocks.

Unlike conventional blockchains, we consider in our architecture that every block is an object, so every generated news is considered a blockchain block. Inside each block is stored what each node (source) published about a given object. We choose to define each news as a block to generate transparency to users due to the centralized blockchain architecture, ensuring that the service provider that stores the blockchain does not make changes to it without the consent of the miners. Figure 2 shows the structure described.

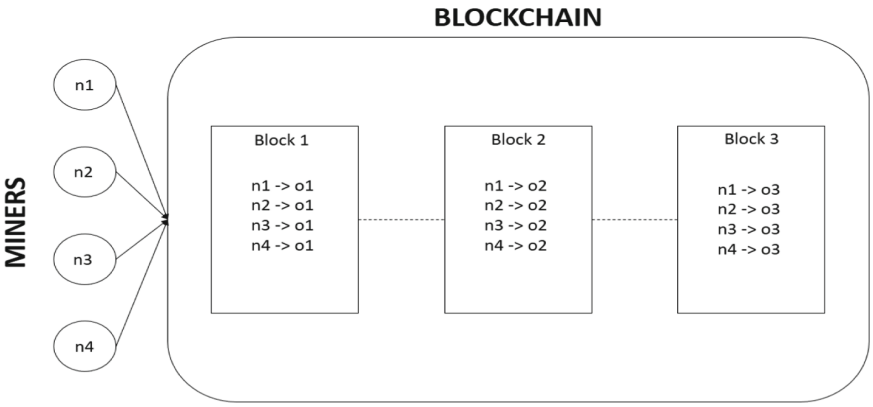

Fig. 2. Blockchain structure.

Storing data in a blockchain is an expensive operation. In this way, the information stored in our blockchain will be metadata abstracted from the published news. Figure 3 shows an example of information stored in the internal structure of a block in our architecture. As can be seen, each block has stored the source, the metadata of the published news, the reliability index of the source after the publication of the news, and the date of publication of the news. Using this type of block structure, we can reduce the storage cost regarding the information.

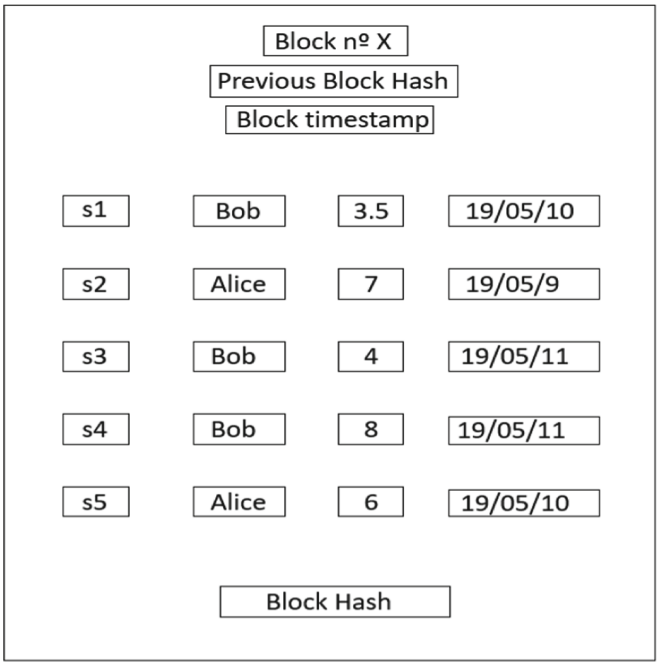

Fig. 3. Blockchain structure.

As can be seen in Fig. 4, our architecture ensures reliability through a degree level given to each source. Even if only one source (node) mines the block the others will gain an increase or decrease in their grade based on what was published, thus guaranteeing democratization in the mining process since the PoS algorithm was chosen to ensure that. We used the Facebook scenario as an example. In (i), the news is published on the social network through a news source. In (ii), the blockchain creates a block and adds what other sources have published on the same object. In (iii), the block is mined, and the reliability levels of each source are updated as calculated by the truth-discovery algorithm.

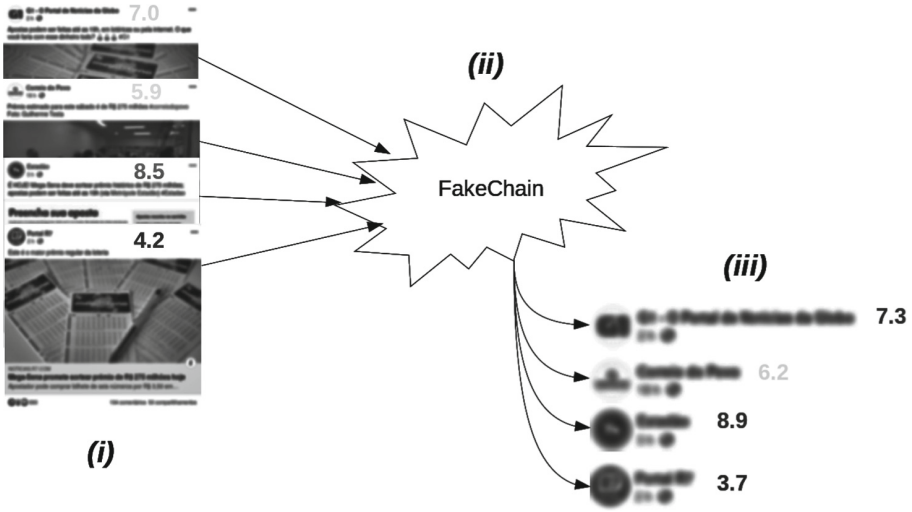

Fig. 4. FakeChain architecture.

4 Proof of Concept and Results

In order to verify the feasibility of using the proposed architecture in a real scenario, we implemented a proof of concept in the Ethereum platform. We used the truffle suite integrated with ganache-cli to create a private network and develop the tests.

We used the smart contracts available in the Ethereum platform to implement the truth finder algorithm. The smart contract developed allowed us to verify and update the reliability levels of each news source. As ganache generates a block for each contract mined, our architecture fit the test environment used.

The tests developed attempted to verify the operation of the contract developed in the Solidity language. We also evaluated the association between the contracts in order to automate the system through the blockchain. Finally, we look at the cost of the contract by varying the number of news publishing sources and checking the overall system operation. We used a desktop computer with Windows 7 OS with 8 GB RAM and AMD FX 6300 3.5 GHz processor. The private network used in the tests had one processing node, with a block size of 12,176,426 gas and 2 Wei gas price.

4.1 Contract Operation

The first test developed corresponds to the operation of the algorithm adapted from Python to the smart contract through solidity programming language. In this test, we attempted to verify the reliability level of the algorithm through the final result of veracity given for each published object. Table 1 shows the results obtained from both algorithms.

Table 1. Precision variation.

Source	Fact	Object	Python algorithm result	Smart contract result
A	Einstein	Special Relativity	True	True
A	Newton	Univ. Gravitation	True	True
B	Einstein	Special Relativity	True	True
B	Galilei	Heliocentrism	True	True
C	Newton	Special Relativity	False	False
C	Galilei	Univ. Gravitation	False	False
C	Einstein	Heliocentrism	False	False

As can be seen in Table 1, the implementation of our algorithm on a smart contract obtained 100 % accuracy result to determine if the presented facts are real or not. We have developed the same test by varying the number of times the contract is executed to verify the accuracy of the results obtained. Figure 5 illustrates the average precision of hits by varying the number of times the contract is executed.

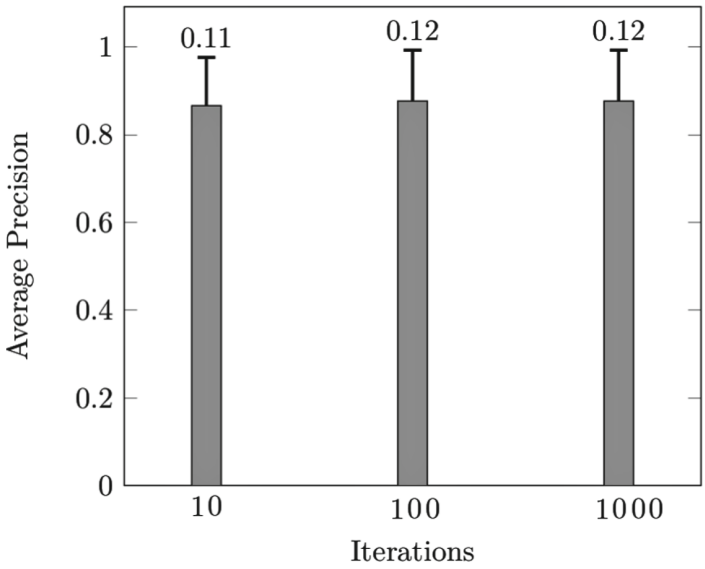

Fig. 5. Average precision and standard deviation varying the number of iterations.

The results presented in Fig. 5 show a small difference in accuracy by varying the number of times the algorithm was executed. The most significant difference considering the number of fact samples is equal to seven, can only be observed between 10 and 100 interactions. From these values, the reliability assignments

based on the logarithmic scale do not influence any significant difference in the final execution result of the truth finder algorithm.

4.2 Contract Linkage

To enable the implementation of our architecture, in the smart contract development process, we attempted to link the trustability level of each source in the creation of each new smart contract regarding a new object. We choose to use this type of architecture in order to our application be as much decentralized as possible, eliminating the need for third-party service for storing data regarding the trustability level of each news source. Algorithm 1 illustrates the code function developed to ensure this functionality.

Algorithm 1. Contract Linkage Function

```
1: procedure GENERATE CHILDREN(address pChildren, address Contract)
2:     addres nC = new NewsLedger()
3:     NewsLedger pC = NewsLedger pChildren
4:     for i=1 to pChildren.size do
5:         for j=1 to newChildren.size do
6:             if nC.dataframe[j].source equals dataframe[i].source then
7:                 nC.dataframe[j].trust = pC.dataframe[i].trust
8:             end if
9:         end for
10:    end for
11:    Contract = nC
12: end procedure
```

As seen in Algorithm 1, the function that generates new child contracts belongs to the truth finder contract code. A list of addresses of these subsequent agreements is stored in it. The function, based on the address of the previous contract, generates an instance of the new contract, crossing both contracts, searching similar sources that if found, have their reliability attribute modified.

4.3 Contract Cost

Considering that our proof of concept used the Ethereum blockchain, we evaluated in our tests the contract gas cost for the proposed architecture. For the evaluation of the gas cost of each contract, we vary the functions present in the contract for the standard and pure types. For standard functions, the network allows the storage of data in the blockchain and the use of it as a source of processing. Pure functions use the Ethereum network only as a processing source. Table 2 shows the gas cost of the contract for the two types of function.

As can be seen in Table 2, we developed four contracts versions. In each version, we changed the number of functions of the pure type and the standard

Table 2. Precision variation.

Contract version	Standard functions	Pure functions	Contract cost (gas)
1	18	2	0.241581
2	17	3	0.241581
3	16	4	0.241581
4	15	5	0.241581

type in order to reduce the gas cost of the contract. None of the versions tested presented cost variation. Most of the implemented functions modify states in the contract and have interdependence among them, not allowing a test where all of them were modified to pure. Because of this, there was no difference in the results.

We evaluated the contract cost by the number of sources, and this factor has a significant impact on the contract cost since it is necessary to store what each source reports about a specific object. Therefore, we also evaluated the contract cost by varying the number of sources that publishes a particular news item. Figure 6 shows the results obtained.

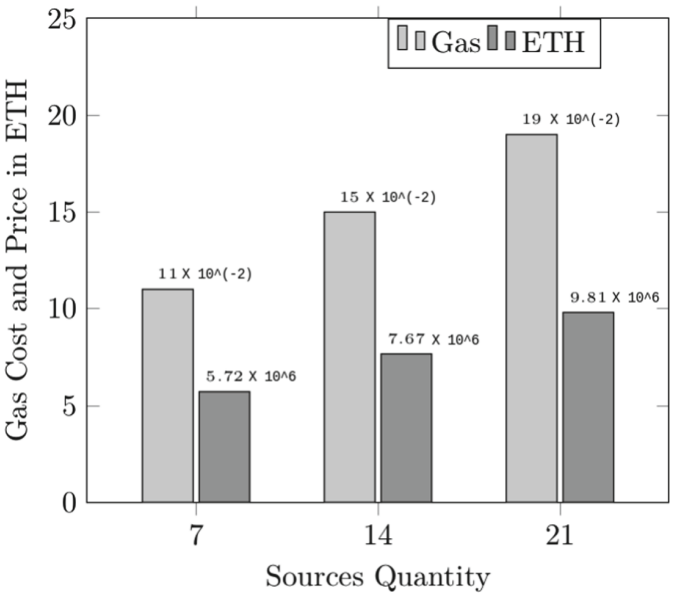

Fig. 6. Gas cost varying sources quantity.

In this test, we varied the number of sources to observe the impact on the gas cost and the price in ETH. The adopted samples were of 7, 14, and 21

news in order to evaluate a possible linear growth based on the tests carried out in Python by [12]. Thus, the results corresponded to the expected values and adopted a continuous growth format.

4.4 Overall System Evaluation

After the performance evaluation of the proposed architecture we did a test to verify the effectiveness of the system for a real situation. We performed the simulation of the proposed architecture by executing three smart contracts, wherein each contract different news items were published. We developed the test with seven, fourteen, and twenty-one news sources. Table 3 shows the values obtained by the tests performed and the expected values.

Table 3. Overall system result.

Source	Trustworthiness	Fact	Object	Fact confidence
A	0.95256	Einstein	Special Relativity	0.95256
A	0.95256	Newton	Univ. Gravitation	0.95256
A	0.95256	Einstein	Special Relativity	0.95256
A	0.95256	Newton	Univ.Gravitation	0.95256
B	0.95256	Einstein	Special Relativity	0.95256
B	0.95256	Galilei	Heliocentrism	0.95256
B	0.95256	Galilei	Heliocentrism	0.95256
B	0.95256	Galilei	Heliocentrism	0.95256
C	0.88077	Newton	Special Relativity	0.88077
C	0.88077	Galilei	Univ. Gravitation	0.88077
C	0.88077	Einstein	Heliocentrism	0.88077
C	0.88077	Galilei	Special Relativity	0.88077
D	0.87954	Newton	Univ. Gravitation	0.95256
D	0.87954	Einstein	Special Relativity	0.95256
D	0.87954	Galilei	Special Relativity	0.88077
D	0.87954	Einstein	Heliocentrism	0.88077
D	0.87954	Einstein	Univ. Gravitation	0.73103
E	0.84334	Newton	Special Relativity	0.88077
E	0.84334	Einstein	Heliocentrism	0.88077
E	0.84334	Galilei	Univ.Gravitation	0.88077
E	0.84334	Newton	Heliocentrism	0.73103

In Table 3, we can observe the results after generating three contracts. We calculated the reliability of each source in the final result according to the grades assigned in previous contracts, and they are in ascending order in Table 3.

In tests done, only ten relationships entered in Table 3 are correct. The results show that the highest grades, considering the reliability of source and fact, were attributed to real facts, propagated mainly by sources A and B, which have a higher reliability index. Considering this, the sites that propagated fake news information, such as C, D, and E, were below the table, even if occasionally they could deliver truthful information.

For the tests, the initial values of Dampening Factor and Influence Related attributes were 0.8 and 0.6, respectively. In the algorithm, Dampening Factor is used as a way to prevent excessively high-reliability indexes. Influence Related, on the other hand, denotes how much information with similar facts can help with reliability. These settings, as well as the samples, were based on the Python language-adapted code.

Regarding the implementation of the Truth Finder algorithm in Solidity, there was only one function of the original algorithm in Python that was not implemented. The Implication function works based on the logic of facts about the same objects that could be conflicting or supportive, which would not cause a significant perturbation in the results, besides an increase in accuracy.

5 Related Work

Song et al. [11] describe the use of blockchain to ensure the authenticity of publications on social networks. The authors mention that blockchain cannot identify the veracity of the data stored in its blocks. Considering this situation, Song et al. suggest the use of a digital signature on information posted by users, thus ensuring the authenticity that someone has verified the information stored in the blockchain. In their model, the social media service provider (i.e., Facebook or Instagram) generates a digital signature through Public Key Infrastructure on each publication done by users and stores the digital signature in the blockchain. In a given moment, when a user wants to check the authenticity of a publication, the public key of the social media service provider is used to verify the authenticity of a publication. The authors report that their system is fraud-proof because only the social media service provider has the private key for the encryption of digital signatures.

Shang et al. [9] present a blockchain architecture to ensure transparency in the process of publishing, disseminating, and tracking news on social media networks. The authors suggest storing information concerning the content of the news, category, and other data about it when the news is published. Regarding the dissemination of the news, the authors indicate storing the information about the time and hash of the news published, thus creating the block structure of the blockchain. When a reader wishes to read a news item, through the information stored in the blockchain, it can verify the origin and path of the news during the publication and dissemination process.

Huckle and White [2] detail an architecture to identify the publication of fake news on social networks. Their solution uses a tool to extract the metadata of an image published in news sites. The metadata is divided into four entities,

being copyright, event, object, and agent. Each of these entities is responsible for storing a part of the image metadata. The authors use the blockchain to store the hash of the original image and the metadata of the image. Thus, when a user wants to check if an image is real, it checks in blockchain whether the hash of the image exists.

Table 4 shows a comparison of the related works with our architecture. In the comparison, we listed the year of publication of the paper, the main functionality of the blockchain for the architecture proposed in each of the works, and the advantages and disadvantages of each solution.

Table 4. Related work comparison.

Work	Year	Blockchain functionality	Advantage	Disadvantages
[11]	2019	Digital signature storage	Authenticated information	Centralized architecture
[9]	2018	Information storage	Scratch information	Unauthenticated information
[2]	2017	Hash/metadata storage	Authenticated information	High cost
Our work	2019	Algorithm processing	Reliability e authenticity	Require a significant amount of sources

As can be seen in Table 4, all related works use the blockchain for data storage, but none of the authors mention how to treat the issue of the storage cost of the information in the blockchain since this type of operation has a high cost. In our work, we used blockchain as the processing source for the truth-discovery algorithm, reducing the cost of data storage.

The works presented on [11] and [2] ensure the authenticity of the information, the work of [9] guarantees the readability of the published information. Our architecture guarantees both conditions because the truth discovery algorithm allows to discover the truthfulness of a fact (authenticity) and to update the reliability level of a source based on the news published by it.

Although the work of [11] uses blockchain, it uses a centralized architecture since only one entity can authenticate the information published on the platform. In the work of [9], while ensuring the path of information, the work does not guarantee that the information is correct. In the architecture described in [2], the main disadvantage observed was the cost of the application, since storing an image and its metadata in a blockchain becomes expensive (the solution presented by the authors uses the Ethereum Platform, which has a high cost of information storage). In our work, the main disadvantage observed is the number of news sources to determine the truth of a fact. If there are a small number of news sources, the value of the information's veracity calculation may be false-negative.

6 Conclusion and Future Work

In this paper, we have presented a blockchain architecture focused on fake news detection. Our architecture defines each block as an object, and inside each block is stored what each source knows about this object. Even using a centralized blockchain, our architecture ensures transparency to users through this type of structure, ensuring that the host cannot change the information stored in the blockchain. An advantage of our architecture is the truth-discovery consensus algorithm, which is used to validate and achieve consensus among users, rewarding users who publish real news and punishing those who post fake news.

With the proof of concept developed, we proved the feasibility of implementing the proposed architecture. The smart contract developed proved to be efficient in terms of fake news detection. The simulation of a real situation showed the effectiveness of the proposed architecture. In comparison to related work, our architecture is different because it can show users the reliability index of each news source present in the system through a system of reliability level.

As future work, we intend to improve the smart contract developed to act in a similar way to the PoS algorithm, guaranteeing democratization in the block mining process. We will also develop a data mining module aimed at obtaining the metadata of every social media article. Regarding the blockchain, we intend to develop the same tests on Hyperledger blockchain, considering its focus for business applications. We also intend to develop tests in the NEM blockchain since the advantage of using this blockchain refers to scalability issues.

Although our architecture is promising, it is necessary the study of data mining techniques and blockchain, since both themes are current and lack references that show an implementation focused on the chosen scenario.

Acknowledgment. This work was financed by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001 and Fundação de Amaparo à Pesquisa e Inovação do Estado de Santa Catarina – Brasil (FAPESC) – Grant No. 2019TR169. This research has been partially supported by the Portuguese Research Council (Fundação para a Ciência e Tecnologia), under the FCT Project UID/EEA/50008/2019.

References

1. Chalaemwongwan, N., Kurutach, W.: State of the art and challenges facing consensus protocols on blockchain. In: 2018 International Conference on Information Networking (ICOIN), pp. 957–962, January 2018. https://doi.org/10.1109/ICOIN.2018.8343266
2. Huckle, S., White, M.: Fake news: a technological approach to proving the origins of content, using blockchains. Big Data **5**(4), 356–371 (2017). https://doi.org/10.1089/big.2017.0071. pMID: 29235919
3. Kshetri, N., Voas, J.: The economics of "fake news". IT Prof. **19**(6), 8–12 (2017). https://doi.org/10.1109/MITP.2017.4241459
4. Li, Y., et al.: A survey on truth discovery. CoRR abs/1505.02463 (2015). http://arxiv.org/abs/1505.02463

5. Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R.: A brief survey of cryptocurrency systems. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 745–752, December 2016. https://doi.org/10.1109/PST.2016.7906988
6. Nakamoto, S.: Bitcoin (2008). https://bitcoin.org/bitcoin.pdf. Accessed 07 May 2019
7. Parikh, S.B., Atrey, P.K.: Media-rich fake news detection: a survey. In: 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp. 436–441, April 2018. https://doi.org/10.1109/MIPR.2018.00093
8. Rouhani, S., Deters, R.: Performance analysis of ethereum transactions in private blockchain. In: 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 70–74, November 2017. https://doi.org/10.1109/ICSESS.2017.8342866
9. Shang, W., Liu, M., Lin, W., Jia, M.: Tracing the source of news based on blockchain. In: 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), pp. 377–381, June 2018. https://doi.org/10.1109/ICIS.2018.8466516
10. Shu, K., Sliva, A., Wang, S., Tang, J., Liu, H.: Fake news detection on social media: A data mining perspective. CoRR abs/1708.01967 (2017). http://arxiv.org/abs/1708.01967
11. Song, G., Kim, S., Hwang, H., Lee, K.: Blockchain-based notarization for social media. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–2, January 2019. https://doi.org/10.1109/ICCE.2019.8661978
12. Takeshi, I.: Truthfinder (2018). https://github.com/IshitaTakeshi/TruthFinder. Accessed 10 May 2019
13. Times, T.N.Y.: Fake news is poisoning Brazilian politics. Whatsapp can stop it (2018). https://www.nytimes.com/2018/10/17/opinion/brazil-election-fake-news-whatsapp.html. Accessed 07 May 2019