A smart contract logic to reduce hoax propagation across social media

Franklin Tchakounté, Koudanbe Amadou Calvin, Ado Adamou Abba Ari, David Jaures Fotsa Mbogne

Journal of King Saud University – Computer and Information Sciences 34 (2022) 3070–3078

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A smart contract logic to reduce hoax propagation across social media

Franklin Tchakounté [a], Koudanbe Amadou Calvin [a], Ado Adamou Abba Ari [b,c,*], David Jaures Fotsa Mbogne [a]

[a] Department of Mathematics and Computer Science, University of Ngaoundere, P.O. Box 454, Ngaoundere, Cameroon
[b] LaRI Lab, University of Maroua, P.O. Box 814, Maroua, Cameroon
[c] LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, 45 Avenue États-Unis, 78035 Versailles cedex, France

ARTICLE INFO

Article history:
Received 5 May 2020
Revised 27 August 2020
Accepted 2 September 2020
Available online 9 September 2020

Keywords:
Block
Dissemination
Hoax
Reduce
Social graph
Smart contract
Trust index
Privacy

ABSTRACT

One of the main concerns of cybersecurity is the detection of hoaxes across social media. Hoaxers propagate such messages to mislead users and to promote violence. Several approaches exist in literature to address this issue. They are mainly limited to detect hoax activities by characterizing the message nature and detecting provenance of messages. However, unless hoaxes are detected, they continue to propagate across social media nodes. This work aims at reducing the dissemination of hoaxes across group of users. Relying on social graph structure, this research develops a mechanism based on smart contract logics to prevent a group to consume a fake post. To achieve this objective, we used a smart contract to exploit a trust index computed based on message characteristics and group features such as graph density, group status, group degree, group acceptability. Based on the value of trust index, the message is forwarded or blocked. Experiments realized on groups of different characteristics revealed that the proposed smart contract is even able to reactively block a fake post of the same nature than the group type. Results indicate that the proportion of targeted groups could be reduced even if their interests match with the message subject. This research is an important step forward to anti-promote hoaxes with the novelty of exploiting smart contract approach to contain their propagation.

1. Introduction

Nowadays, privacy is becoming a growing concern in the world (Ari et al., xxxx; Babaghayou et al., 2019). Government and companies track and monitor people in order to better control them by predicting their actions a well as intentions (Anshari et al., 2019; Shaffer et al., 2019). Furthermore, the Web is a place of unfeigned proliferation false information as reported by Kumar et al. (Kumar et al., 2016; Fraga-Lamas and Fernández-Caramés, 2020). A hoax is false, outdated or unverifiable information that is spontaneously spread by Internet users (Rahmat and Areni, 2019). Hoaxes are messages disseminated across social media by humans and robots, which aim to trigger positive or negative emotions in the user: virus alert, missing child, promise of happiness, and petition.[1] According to GDATA,[2] 59% of Internet users has already been in touch with a hoax. Their consequences are multiple: manipulating people, promoting war, degradation of the image of a person or a company, disbelief among others (Kumar and Shah, xxxx). Concerning the severe global threat COVID-19 pandemic, propagation of hoaxes is a huge concern (Frenkel et al., xxxx; Russonello, xxxx). Hoaxers share conspiracy stories about virus as being fabricated by China as a biological weapon and false medication against the virus. Other hoaxes related that this virus is inefficient to Africans (Pennycook et al., xxxx). As consequences, people are lured to under-follow prescribed measures and adopt ineffective and harmful remedies catalyzing the destruction of immune system.

Existing anti-hoax approaches include four orientations (Shu et al., xxxx): (1) analyzing and detecting fake news with fact-checking; (2) identifying quantifiable characteristics or features susceptible to discriminate hoaxes from benign ones; (3) studying how hoaxes propagate and spread on the social graph to detect hoaxes by assessing credibility of sources (Shu et al., 2017; Zubiaga et al., 2018; Guille et al., 2013; Hernandez et al., 2002). Although these proposals are somehow able recognize hoax traits, they are inefficient to stop hoax propagation. Unlike these proposals, this work intends to limit hoax dissemination across group of users. In distributed architecture such as social media, smart con-

* Corresponding author at: LaRI Lab, University of Maroua, P.O. Box 814, Maroua, Cameroon.
E-mail address: adoadamou.abbaari@gmail.com (A.A.A. Ari).

[1] Alexandre Pouchard, Delphine Roucaute, Adrien Sénécat and Agathe Dahyot. "Décodex: notre kit pour vérifier l'information á destination des enseignants." Le Monde.https://bit.ly/3b0djsL.

[2] What actually is a hoax?https://www.gdatasoftware.com/.

https://doi.org/10.1016/j.jksuci.2020.09.001
1319-1578/

tracts are proven to provide efficient decision making autonomously and without any intermediaries (Macrinici et al., 2018). Its lightweight and independence to input data, compared to mechanisms related to artificial intelligence, fact checking and propagation modelling, makes great virtue in facilitating decision making processing. We therefore associate user groups to the smart contract logic (Khedim et al., 2018) to intelligibly filter incoming messages to any group. Decision making is made relying on trust index computed based on the message features and group features such as graph density, group status, group degree, and group acceptability. Experiments on various social graphs revealed the pertinence of the proposed scheme: even hoaxes of the same type than the group interest could be blocked. In brief, this work provides two contributions: a model based on smart contract logic which filters incoming hoaxes; and a simulation process of different social graph structures and various types of messages, demonstrating that the proposed approach is able to block the propagation of hoaxes to group of consumers.

The rest of this document is organized as follows. Section 2 presents literature about fake news detection in general. Section 3 concerns the concepts about hoaxes, social graphs and smart contracts. Section 4 is dedicated to the proposed approach for filtering dissemination of hoaxes. Section 5 presents different experimentation and analyses of results. The paper ends with a conclusion and perspectives in Section 6.

2. Related works

This section relies on recent and consistent surveys of researches around fake news. (Zhou and Zafarani, xxxx; Sharma et al., 2019). According to these studies, fake news can be split into four directions.

The first direction includes analyzing and detecting fake news with fact-checking. The manual fact-checking is achieved by known group of highly credible experts to verify the contents (Hassan et al., 2017), crowd-sourced individuals (Kim et al., 2018; Tschiatschek et al., xxxx), and crowd-sourced fact-checking websites such as HoaxSlayer.[3] The automatic fact-checking takes into consideration the volume of information generated in social media. It relies on reliable fact retrieval methods for further processing to deal with redundancy, incompleteness, unreliability and conflicts (Lao and Cohen, 2010). Once data is cleaned, knowledge is extracted under a graph form and fed into an exploitable knowledge base (Hoffart et al., 2013). Fact checking requires a huge collection of information from experts, online systems and people to prove veracity of the fact underlining a hoax. So reliable knowledge related to the fact is required. Expertise in our case comes from smart contract logic which has been proved robust and no subjective. The aim is no to check but to eliminate hoax flows.

The second direction concerns identifying quantifiable characteristics or features susceptible to discriminate hoaxes from benign ones (Pisarevskaya, 2015; Potthast et al., xxxx; Volkova et al., 2017). In this regards, authors investigate attribute-based language features and structure-based language features which characterize a post. They build machine learning-based strategies on structured information to derive classification and regression models (Ren and Ji, 2017; Shu et al., xxxx; Aboubakar et al., 2020). This direction is unreliable without consistent datasets of hoax and non–hoax samples, somehow hardly collected and accessible. Then considerable amount of tasks are to be realized to make these datasets exploitable. To avoid such constraints, this work opts to look for propagation features to limit hoax floods. Moreover, we suppose that hoaxes already exist and we want to make their dissemination as reduced as possible.

The third direction refers to study how hoaxes propagate and spread on the social graph. For that, one can make qualitative analysis of patterns to recognize fake news propagation (Du et al., 2014; Najar et al., 2012; Draper and Smith, 2014). Some proposals consisted on mathematical models for fake news propagation based on epidemic diffusion models (Kucharski, 2016) and game theoretical models (Shu et al., xxxx). The detection based on fake news propagation is achieved using supervised learning on cascade (a tree or tree-like structure representing the propagation of a hoax) features (Ma et al., 2018) or network-based propagation structures (Shu et al., 2017; Shu et al., 2019). Another option in this direction aims at using graph kernels to compute similarity between various cascades of posts (Vishwanathan et al., 2010). This information is then used as features to supervised learning algorithms to detect hoaxes (Wu et al., 2010). We take from this direction that it is possible to study propagation of fake news based on analysis of graph structure. Since we are working on dissemination, this feature has been borrowed and exploited. Unlike, It is not used for recognizing hoax propagation that we assume true in social media, but to contain this propagation across groups.

The fourth direction consists to detect hoaxes by assessing credibility related to hoax headlines (Pengnate, 2016), hoax sources and provenance (Fraga-Lamas and Fernández-Caramés, 2020; Esteves et al., xxxx), hoax comments (Dungs et al., 2018), and hoax spreaders (Shu et al., 2019). In this direction, authors aggregate different opinions to make a final decision about the post (Tchakounté et al., xxxx). However, there is an issue of fake comments and opinions which leads to biased results. Unlike, what we propose is independent from subjective comments and does not aim to identify the nature of any post. But we rely on message characteristics and group features to filter incoming messages.

All the aforementioned approaches have in common to capture information to identify hoax traits. However their detection does not block their dissemination and therefore the contamination continues to spread across social network nodes. This issue motivates our work, which intends to develop strategies to convince a group to stop an incoming hoax message. The overall effort made in different groups can contain dissemination of hoaxes. Therefore our work comes after identification of hoaxes.

3. Background

This section briefly presents some concepts about hoax, smart contract and social graph.

3.1. Hoax

A hoax is false, outdated or unverifiable information that is spontaneously spread by Internet users. Hoaxes concern any subject likely to trigger a positive or negative emotion in the user: virus alert, missing child, promise of happiness, petition (Assiroj et al., 2018). Hoaxes are in written form such as e-mail, message in a forum, etc. Unlike offline rumors, they are mainly exploited to psychologically influence users to propagate (Kumar et al., 2016). The initiator of the hoax (hoaxer) is the malicious person or a robot that is built by a third person. According to Vinz (Attention canularInfo ou canular, 2014), there are many types of hoaxes. An announcement hoax is to make a fake announcement of a service or an activity. An anti-promotion hoax aims to dirty image of a concurrent company. Anti-political hoaxes are about turning people against governmental opinions. A rumor hoax is dedicated to propagate a false rumor for a certain period about specific situation to analyze reactions and behaviors of people. Our work considers all these kind as

[3] Latest Email and Social Media Hoaxes – Current Internet Scams - Hoax-Slayer. http://hoax-slayer.com/.

hoax. Consequences of hoaxes are according to Bessi et al. (Bessi and Ferrara, 2016): over-flooding networks, disinformation, degradation of the image of an entity (company and personality), and disbelief to turn people to unconsciously work with the hoaxer. Their work assumes that an incoming message is hoax and aims to reduce propagation making fewer victims within the network.

3.2. Smart contract

Blockchains exploit smart contracts as procedures to manage interactions between entities on the network (Khedim et al., 2018; Suciu et al., 2018; Titouna et al., 2018). According to Bayon et al. (Bayón, xxxx), "A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code". Therefore, smart contracts operate as independent and autonomous entities, whose behavior is completely predictable (the same input will always produce the same output) (Christidis and Devetsikiotis, 2016). A smart contract is launched by messages/transactions sent to its address. They allow expressing business logic in code mainly in the form *if ... then* statements. They should describe all possible outcomes of the contract. A smart contract lives within a blockchain and its state is scrutinized by every network participant to know which action to take. Fig. 1 depicts a smart contract related to renting an apartment while paying in crypto-currencies.

Moreover, Smart contracts have many advantages (Cuccuru, 2017; Jean and De Filippi, xxxx):

1. *Reliability:* It is virtually impossible to shut down the entire computers participating in the blockchain simultaneously. As a result, this database is always online and its operation never stops.
2. *Removal of intermediaries:* smart contracts make it possible to automate a process, while eliminating intermediaries.
3. *Unstoppable:* The entire code of the smart contract is immutable, in the sense that its code is published and therefore written in a transaction making the application unassailable and unstoppable.
4. *Borderless:* smart contracts do not depend on a supervisory authority i.e the borders, physical location and jurisdiction of the country.
5. *Open source:* It means that source code of the smart contract should be accessible and verifiable to the community.
6. *Autonomous:* Once a smart contract has been created and published, it becomes accessible to the other members of the blockchain. It belongs to any point of the blockchain which can add its own rules and conditions.

In addition, smart contract is of interest due to these properties which give a smart contract ability and flexibility to ease decision making. This work relies on the smart contract logic without deploying the whole environment of blockchains. Its role is to help making decision whether the group should consume or not an incoming hoax.

3.3. Social graph

A social graph is connectivity between people in a social network characterized by relationships between entities (humans and objects) (Ugander et al., xxxx). Any social network can be mathematically represented as a graph $G = (V, E)$, where V is the set of vertices, E is the set of edges of the graph. V can be seen as individuals, group of individuals or non–human objects (shared images, videos) (Kirichenko et al., xxxx). Relationships in a network can be directional or nondirectional. There are mainly two types of relationships: relatives (people are familiar with each other) and interests (people are included in one group having the same interests). A social graph has some key features (Kirichenko et al., xxxx). Centrality shows how a node within a specific network is influential. Density defines the ratio between the number of connections of a node and the total possible connections of a node. Closeness is a measure of information dissemination in the graph from one node to the others. Fig. 2 illustrates a social graph with vertices as people and edges, their relationships. In this case, relationships are directional (Ed to Albert) or bidirectional (Ed to Doris). In this example of graph, the underlined structure of the graph can be represented with centrality, density and closeness to show how a group behavior towards a message can influence the other group reaction to the same message. They can therefore be essential for decision making concerning the hoax issue.

4. Proposed approach

The overall process is depicted in Fig. 3. It is summarized as follows. The hoaxer sends the hoax to the group. It arrived to the smart contract which computes, based on the group characteristics, an index determining whether to transmit the message to the gateway or not. In case it is transferred to the gateway (index greater than 2), the latter checks whether to broadcast to other members or to block the message. In case, clauses are not respected (index lower than 2), the smart contract blocks the message. The process flow includes two processes. The first process, the determination of confidence index, is the responsibility of the smart contract. It takes as input the incoming message with its characteristics with the characteristics of the target group. It then calculates a value called confidence index which depends on several features (explained later in this section) and which is used by the smart contract to block or accept hoax messages based on a certain threshold. The second process which is the result from threshold comparison includes two tasks which can be done exclusively. Either, the first task discards the message or the second task lets the message comes into the group towards to the administrator of the group. In the following, details for the overall process are provided.

4.1. Formalisms

This section formalizes key concepts required to perform activities in the process. Objects involved in the process are described hereinafter and highlighted in Fig. 4.

- *Group*. A group is a set people who adhered because of a specific interest. A group has an identity, a status, a type and a set of members.
- *Graph*. The social graph considers groups of members as vertices and group interconnections as edges. Several groups can be interconnected due to the simultaneous membership in several groups and inter relationships between members.
- *Messages*. The incoming message is assumed to be a hoax within the scope of that work. Based on social media architecture, the message has three attributes such as message = "id"; "type"; "recipient". The id identifies the message and it is generated by the social media system. The type indicates a subject category related to the content such as football, politics, and heath. The recipient attribute is a structure which identifies the message destination.
- *Gateway*. The gateway of a group is an intermediary between the contract and the members. It is one member or a set of members from the group that is selected based on some scenarios. As shown in Fig. 4, there are two gateways that act between

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Fig. 1. Smart contract for renting (Rosic, xxxx).

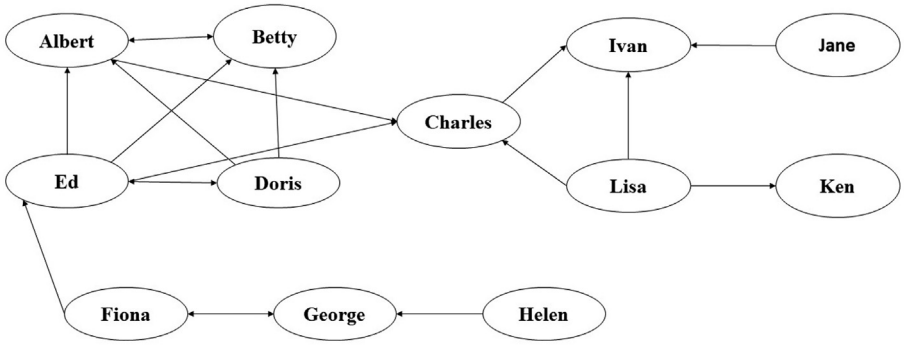

Fig. 2. Social graph.

members and one contract. This structure shows that each group has a point of contact when the message arrives. This contact is the contract and it is independent (explained later). It collaborates with the group's contact namely the gateway that forwards the post to the other members or blocks the message based on investigations made by the contract.

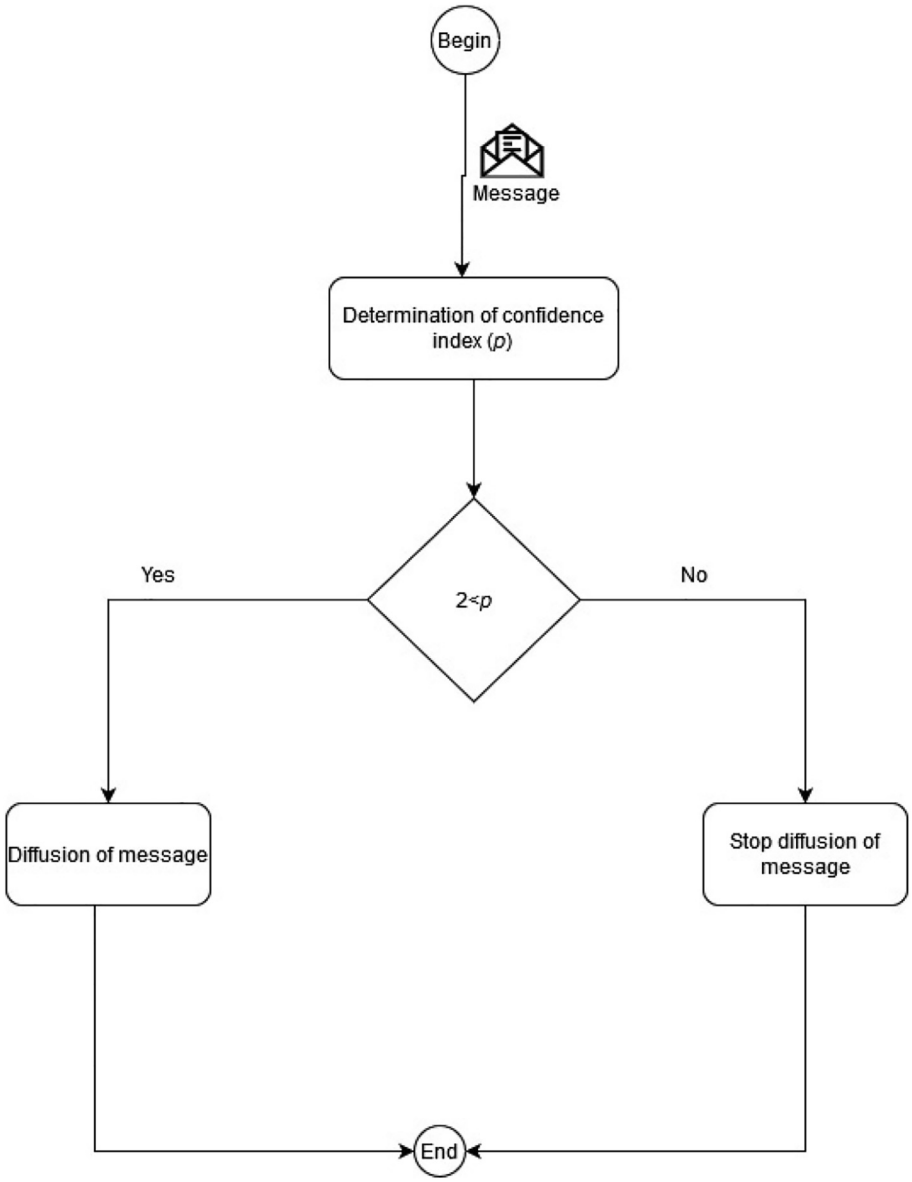

Fig. 3. Process flow.

1. The gateway is (set of) the natural creator(s) of the group in case they are publicly active. In this case, we talk about natural gateway.

2. In case the natural gateway leaves, the gateway designation is entirely managed by the group members. Some studies proposed to elect the most influential members (Ahajjam et al., 2015).

- *Contract.* It is created and bound after the group creation and the contract is triggered every time a message incomes in the group. Also, the contract is responsible to intercept to filter incoming message.

There are several features exploited by the smart contract to make the filtering decision.

1. Density of graph (Dg): This feature represents the proportion of edges existing in the graph i.e. the number of edges in the graph divided by the maximum number of edges that can exist (Lemmouchi, 2012). Its expression is given in Eq. (1).

$$Dg = 2 \times \frac{m}{n \times (n-1)}; \quad 0 \leqslant Dg \leq 1 \tag{1}$$

where n is the number of nodes in the group and m is the number of edges in the group. At best, $Dg = 1$ at worst $Dg = 0$.

2. Status of group (Ds): This feature represents how a member can join a group. In our model, a group can have the following status: open, semi-open and closed. A group is open when everyone can join without any preconditions. A group is semi-open when one member is connected to a member of another group. A group is closed when only the gateway is responsible to manage inside members, to manage incoming messages and to management joining requests. Its formula is given as in Eq. (2).

$$Ds = k; \quad 0 \leqslant k \leq 1. \tag{2}$$

where k is obtained according to the status of group.

- *0* if the group is open;
- *0.5* if it is semi-open;
- *1* if it is closed.

3. Degree of group (Dc). It is the average of number of connections per group. Its expression is given in Eq. (3).

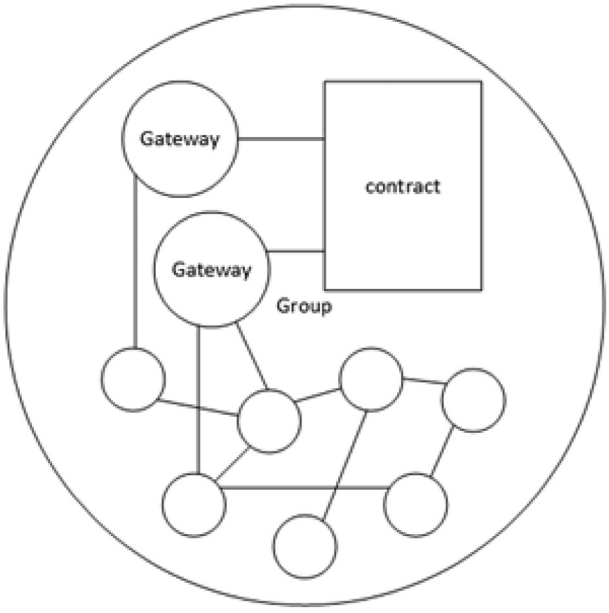

Fig. 4. Gateway.

$$Dc = \frac{\sum_{i}^{n} degre(i)}{n}; \quad 0 \leqslant Dc \leq 1. \tag{3}$$

where, *degre(i)* is the number of neighbors of node i in the group and n number of Nodes. Thus a totally dense community will have an average degree of *1* in this case all nodes are interconnected. Otherwise a non-dense group has a degree close to *0* because the number of nodes will be much smaller than the number of nodes.

4. Acceptability of group (Da): This feature measures the ability to accept or reject hoaxes. This element helps to know the state of a group in its behavior according to the hoax messages already received. It is given in Eq. (4).

$$Da = \frac{\sum Cv}{\sum transaction}; \quad 0 \leqslant Dg \leq 1. \tag{4}$$

Where cv is the number of transactions accepted in the group; *transaction* is the number of transactions performed by the contract.

5. Group interest (Tg): This feature refers to the type of subject to be addressed in the group (sport, health, politics etc...). Indeed, so a hoax about sports is supposed to target a group with the same interest. Tg equals 1 if topic of discussion in the group matches with the type of message and 0 otherwise. The group interest indicates that the gateway selects people with a certain expertise.
6. Confidence index: Confidence index is made up of the previous features. Its formula is given as in Eq. (5).

$$\rho = Dc + Ds + Da + Tg - Dg; \quad -1 \leqslant \rho \leqslant 4. \tag{5}$$

The comparative value of ρcompared to the contract will thus be set at $\frac{\rho}{2} \leqslant \rho$ if we consider the capacity to accept or reject hoax is equitable, the confidence index is an probability thus, it will be the average of ρ.

4.2. Decision making

This section specifies actions executed by the smart contract concerning filtering hoaxes. These actions are included in the algorithm described in Fig. 5. The algorithm takes as parameters the targeted group in the social graph (G) with the set of vertices (V) and the set of edges (E) as well as the incoming message. Lines 2 to 4 declare variables. Lines 6 to 10 consist to evaluate each feature presented in Section 4.1. The smart contract determines the trust index on that features (Line 11). In case this value is greater than 2, a link is established between the message source and the targeted group (line 13) and the message is transferred to the gateway (Line 15) and the connection state is saved. In case this condition is not verified (line 16), the message is blocked by the contract (line 17) and the connection state is saved (line 18).

5. Experimental validation

This section describes the conducted experiments on different structures of social graph.

5.1. Environment

Experiments have been conducted on an Intel(R) Core (TM)2 Duo CPU L9400 @1.86, 1867 MHz, 2 cores, 2 processors with 4 GigaBytes of DDR 2 memory. The artifact used to simulate different scenario of the experiments has been built with MatLab whereas the smart contract code has been written in Python. MS Excel has been exploited to structure groups into matrices. All the three elements are coupled to provide ability to test the proposed approach. All scripts are available in the GitHub at https://github.-com/calvinkda/smart_contrat.

5.2. Experiments, results and discussions

Two experimental cases were conducted, each provided with specific social graph structure including the following key elements.

- Nodes: They are groups with an identity, a status, a type and a set of members more or less interconnected to represent in our model by a matrix.
- Messages: we assume that incoming messages are hoaxes. They have a nature such as political, football, travel and a set of target groups.
- Trust index and the contract of each group: smart contract intercepts incoming message calculate its confidence index and filters based on the algorithm described in Fig. 5.

5.2.1. Experiment 1

This experimentation case aims to determine how the proposed model reacts while receiving a hoax message in case of social graph where nodes are not interconnected. This case is depicted in Fig. 6a.

This experiment includes 405 members in 10 groups as described in Table 1. The hoax is type "football" and targets all the groups. Once all the features are defined, the smart contract computes the confidences index to either accept or reject the hoax. The column labeled "smart contract result" provides such decisions. For example, the smart contract accepts the hoax and transfers it to the gateway of group 1. Table 1 shows that five groups such as group 1, group 2, group 5, group 9 and group 10 receive the hoax and the remaining ones accepts the hoax. Fig. 6b depicts the social graph obtained after applying smart contract filtering.

We discuss results in two aspects. The first aspect includes cases when the hoax is accepted. In this case, groups 1, 9 and 10 have the same type of the incoming message. The model supposes that members belonging to those groups have enough expertise to filter hoaxes. Groups 2 and 5 have different types but are closed

```
1   Algorithm decision ((G=V,E),m)
2   VARIABLES density, degree, status, acceptability, type
3             Destination belongs to V
4             Connection: the set of connections targeting G with its state
5   BEGIN
6      Density=getDensity(G)
7      degree=getDegree(G)
8      status= getStatus(G)
9       acceptability = getAcceptability(G, message[])
10     type=getType(G, m.type)
11     rho= (∑ density, degree, status, acceptability) - type
                        //calculation of the confidence index
12     If (rho>2) then // if Rho is good
13     E=E U {(m.source,G)} // message accepted
14     Connection = Connection U {(m.source,G,accepted)}
15     sendMessage(contract.object,G.gateway)
16     else
17     blockMessage(contract.object)
18     Connection = Connection U {(m.source,G,rejected)}
19     Endif
19  END
```

Fig. 5. Algorithm decision.

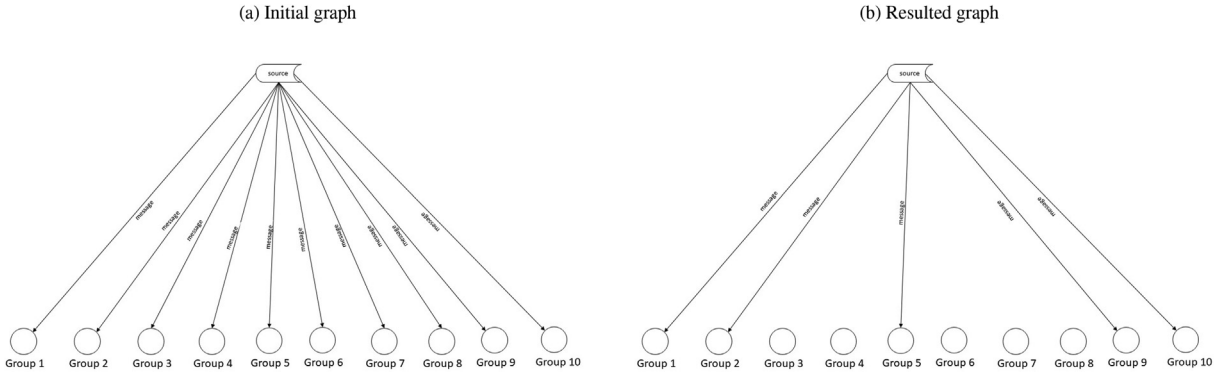

Fig. 6. Experiment 1.

Table 1
Experiments and output of results.

Group	Type	Status	Members	Density	Smart contract result	
					E1	E2
1	Football	Open	20	NTI	A	A
2	Handball	Closed	30	NTI	A	A
3	Any	Open	50	TI	R	R
4	Football	Open	70	NTI	R	A
5	Biology	Closed	20	TI	A	A
6	Handball	Semi-open	20	NTI	R	A
7	School	Closed	120	NTI	R	R
8	Politics	Open	15	NTI	R	R
9	Football	Semi-open	35	TI	A	A
10	Football	Open	25	NTI	A	A

NTI = Not totally interconnected, **TI** = totally interconnected,**A** = accepted,**R** = refused.

meaning that only getaway (administrator) selects the members of groups. The smart contract refuses the hoax because members and message management belong to the administrator who is supposed to have enough knowledge to filter. The second aspect includes cases where the hoax is rejected. In this aspect, groups 3, 6, 7, 8 have different type than the message subject. This property gives to the smart contract a reason to reject the message because it thinks members have not ability to understand the

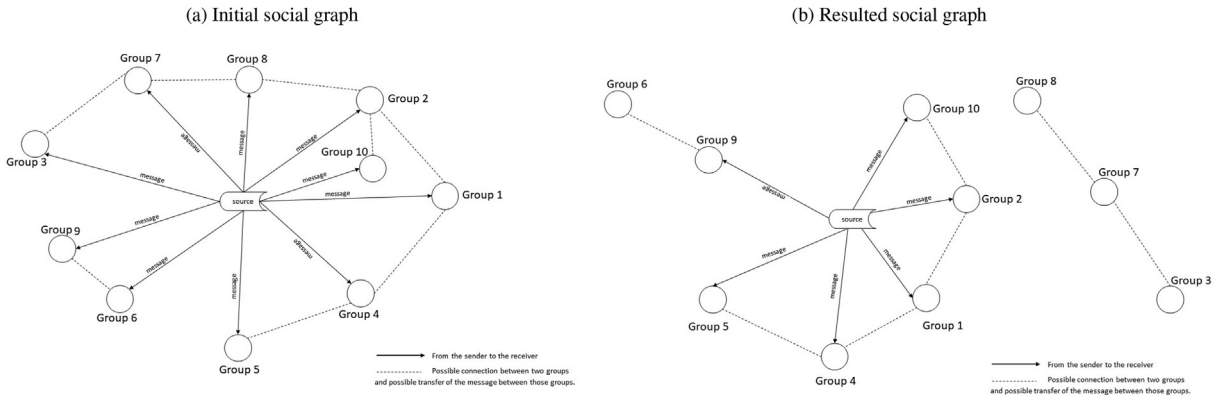

Fig. 7. Experiment 2.

nature of that message. Additionally, groups 3, 6 and 8 are open and not totally interconnected. A member can therefore join randomly those groups and with some connections with other outside from which they can get hoaxes. An interesting result is that the proposed model is able to refuse hoaxes to groups with the same interest message subject. This is the case of group 4. This decision in related to the number of members within a group. The determination of the old value depending on the number of the members remains an issue.

5.2.2. Experiment 2

This experimentation is realized on a social graph with the same nodes as in experimentation 1 but with a social graph with potential interconnection between groups. A connection means that a member of group belongs to different groups through intermediaries to exchange message. The group features are presented in Fig. 7a and the decision making from smart contract is available in column E2 in Table 1.

There are two cases excerpted in Fig. 7b. The first case concerns groups that accept the hoax. Group 1, 2, 4, 5, 6, 9 and 10 are involved in the case. The justification about group 1, 2, 5, 9 and 10 is similar as in experimentation 1. However, the model reacts specifically on groups 4 and 6. Since group 4, is connected to group 1 and 5, it is likely that group 4 gets the message. This situation is provided by the smart contract understand that group 6 an group 9 includes common members, so it let the message entering. The second case concerns groups that refuse the hoax group 3, 7 and 8 are involved in that case. The smart contract refuse hoax to these groups because of their types which are different from the message subject. Additionally, according to the social graph structure, they are not connected to any other groups susceptible to receive the message. This knowledge is determined by the smart contract.

5.3. Limitations

There are some limitations to consider despite the fact that proposed model is able to learn social graph and group structures to efficiently filter the incoming hoax.

- This work only applies filtering to one group and does not deal with multiple intersected groups. That means, a hoax accepted within a group can bypass the filter of another group through multiple memberships.
- There are cases where the smart contract accepts hoaxes while relying on expertise of members and gateway. This is a limitation because expertise is not effective and the smart contract will therefore be subject to false identification.

6. Conclusion

Hoaxes spread like a disease through population. Those who are immunized are saved, new patients suffer from the disease and many other people can be agents of transmission. This dissemination context is applied in social networks where fake posts maintain instability among users. To deal with this issue, proposals capture information related to hoax traits and network structure to identify malicious users. The problem remains because hoaxes continue to spread across social media. This work proposed an approach based on group structure to reduce diffusion of hoaxes with him a group. More specifically, we designed a mechanism based on smart contract logic to limit hoax flows. Experiments made demonstrated that it is able to reduce the number of groups susceptible to receive hoaxes depending on social graph structure and node structure. As future work, we intend firstly to give to smart contract a global view of the social graph, which will augment its ability to reduce propagation. Secondly, we intend to consider adversarial members in social graph nodes.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aboubakar, M., Kellil, M., Bouabdallah, A., Roux, P., 2020. Using machine learning to estimate the optimal transmission range for RPL networks. In: NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, pp. 1–5.

Ahajjam, S., El Haddad, M., Badir, H., 2015. LeadersRank: Towards a new approach for community detection in social networks. In: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), IEEE, pp. 1–8.

Anshari, M., Almunawar, M.N., Lim, S.A., Al-Mudimigh, A., 2019. Customer relationship management and big data enabled: personalization & customization of services. Applied Computing and Informatics 15 (2), 94–101.

Ari, A.A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroui, A.M. Enabling privacy and security in cloud of things: architecture, applications, security & privacy challenges, Applied Computing and Informatics.

Assiroj, P., Hidayanto, A.N., Prabowo, H., Warnars, H.L.H.S., et al., 2018. Hoax news detection on social media: a survey. In: 2018 Indonesian Association for Pattern Recognition International Conference (INAPR), IEEE, pp. 186–191.

Attention canularInfo ou canular, avant dalerter tes amis, vérifie!, http://www2.ac-lyon.fr/etab/lycees/lyc-69/bernard/IMG/pdf/FP_canular.pdf, 2014.

Babaghayou, M., Labraoui, N., Ari, A.A.A., Gueroui, A.M., 2019. Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles. International Journal of Strategic Information Technology and Applications (IJSITA) 10 (4), 33–54.

Bayón, P.S. Key legal issues surrounding smart contract applications. KLRI Journal of Law and Legislation.

Bessi, A., Ferrara, E., 2016. Social bots distort the 2016 US Presidential election online discussion. First Monday 21 (11-7).
Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.
Cuccuru, P., 2017. Beyond bitcoin: an early overview on smart contracts. International Journal of Law and Information Technology 25 (3), 179–195.
Draper, N.R., Smith, H., 2014. Applied Regression Analysis, vol. 326, John Wiley & Sons. doi 10 (2014) 9781118625590.
Du, N., Liang, Y., Balcan, M., Song, L., 2014. Influence function learning in information diffusion networks. In: International Conference on Machine Learning, 2016–2024.
Dungs, S., Aker, A., Fuhr, N., Bontcheva, K., 2018. Can rumour stance alone predict veracity?. In: Proceedings of the 27th International Conference on Computational Linguistics, pp. 3360–3370.
Esteves, D., Reddy, A.J., Chawla, P., Lehmann, J. Belittling the source: trustworthiness indicators to obfuscate fake news on the web, arXiv preprint arXiv:1809.00494.
Fraga-Lamas, P., Fernández-Caramés, T.M., 2020. Fake news, disinformation, and deepfakes: leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. IT Professional 22 (2), 53–59.
Frenkel, S., Alba, D., Zhong, R. Surge of virus misinformation stumps Facebook and Twitter, The New York Times.
Guille, A., Hacid, H., Favre, C., Zighed, D.A., 2013. Information diffusion in online social networks: a survey. ACM Sigmod Record 42 (2), 17–28.
Hassan, N., Arslan, F., Li, C., Tremayne, M., 2017. Toward automated fact-checking: detecting check-worthy factual claims by ClaimBuster. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1803–1812.
Hernandez, J.C., Hernandez, C.J., Sierra, J.M., Ribagorda, A., 2002. A first step towards automatic hoax detection. In: Proceedings. 36th Annual 2002 International Carnahan Conference on Security Technology. IEEE, pp. 102–114.
Hoffart, J., Suchanek, F.M., Berberich, K., Weikum, G., 2013. YAGO2: A spatially and temporally enhanced knowledge base from Wikipedia. Artificial Intelligence 194, 28–61.
Jean, B., De Filippi, P. Les Smart Contracts, les nouveaux contrats augmentés?.
Khedim, F., Labraoui, N., Ari, A.A.A., 2018. A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks. Journal of Network and Computer Applications 123, 42–56.
Kim, J., Tabibian, B., Oh, A., Schölkopf, B., Gomez-Rodriguez, M., 2018. Leveraging the crowd to detect and reduce the spread of fake news and misinformation. In: Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining, pp. 324–332.
Kirichenko, L., Radivilova, T., Carlsson, A. Detecting cyber threats through social network analysis: short survey, arXiv preprint arXiv:1805.06680.
Kucharski, A., 2016. Study epidemiology of fake news. Nature 540 (7634). 525–525.
Kumar, S., Shah, N. False information on web and social media: A survey, arXiv preprint arXiv:1804.08559.
Kumar, S., West, R., Leskovec, J., 2016. Disinformation on the web: Impact, characteristics, and detection of wikipedia hoaxes. In: Proceedings of the 25th international conference on World Wide Web, pp. 591–602.
Lao, N., Cohen, W.W., 2010. Relational retrieval using a combination of path-constrained random walks. Machine Learning 81 (1), 53–67.
Lemmouchi, S., 2012. Study of the robustness of emerging social graphs, Theses, Université Claude Bernard - Lyon I, https://tel.archives-ouvertes.fr/tel-00944441.
Macrinici, D., Cartofeanu, C., Gao, S., 2018. Smart contract applications within blockchain technology: a systematic mapping study. Telematics and Informatics 35 (8), 2337–2354.
Ma, J., Gao, W., Wong, K.-F., 2018. Rumor detection on twitter with tree-structured recursive neural networks. Association for Computational Linguistics.
Najar, A., Denoyer, L., Gallinari, P., 2012. Predicting information diffusion on social networks with partial knowledge. In: Proceedings of the 21st International Conference on World Wide Web, pp. 1197–1204.
Pengnate, S.F., 2016. Measuring emotional arousal in clickbait: Eye-tracking approach. In: Human-Computer Interaction (SIGHCI).
Pennycook, G., McPhetres, J., Zhang, Y., Rand, D. Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy nudge intervention, PsyArXiv Preprints 10.
Pisarevskaya, D., 2015. Rhetorical structure theory as a feature for deception detection in news reports in the Russian language. In: Artificial Intelligence and Natural Language & Information Extraction, Social Media and Web Search (AINL-ISMW) FRUCT Conference, Saint-Petersburg, Russia.
Potthast, M., Kiesel, J., Reinartz, K., Bevendorff, J., Stein, B. A stylometric inquiry into hyperpartisan and fake news, arXiv preprint arXiv:1702.05638.
Rahmat, M.A., Areni, I.S., et al., 2019. Hoax web detection for news in bahasa using support vector machine. In: 2019 International Conference on Information and Communications Technology (ICOIACT). IEEE, pp. 332–336.
Ren, Y., Ji, D., 2017. Neural networks for deceptive opinion spam detection: an empirical study. Information Sciences 385, 213–224.
Rosic, A. Smart Contracts: The BlockchainTechnology That Will Replace Lawyers, https://blockgeeks.com/guides/smart-contracts/,????.
Russonello, G. Afraid of coronavirus? That might say something about your politics, The New York Times.
Shaffer, G., Fernback, J., 2019. Cell phones, security and social capital: examining how perceptions of data privacy violations among cell-mostly internet users impact attitudes and behavior, security and social capital: examining how perceptions of data privacy violations among cell-mostly internet users impact attitudes and behavior (July 12, 2019).
Sharma, K., Qian, F., Jiang, H., Ruchansky, N., Zhang, M., Liu, Y., 2019. Combating fake news: a survey on identification and mitigation techniques. ACM Transactions on Intelligent Systems and Technology (TIST) 10 (3), 1–42.
Shu, K., Sliva, A., Wang, S., Tang, J., Liu, H., 2017. Fake news detection on social media: a data mining perspective. ACM SIGKDD Explorations Newsletter 19 (1), 22–36.
Shu, K., Bernard, H.R., Liu, H., 2019. Studying fake news via network analysis: detection and mitigation. In: Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining, Springer, pp. 43–65.
Shu, K., Wang, S., Lee, D., Liu, H. Mining disinformation and fake news: concepts, methods, and recent advancements, arXiv preprint arXiv:2001.00623.
Shu, K., Wang, S., Liu, H. Exploiting tri-relationship for fake news detection, arXiv preprint arXiv:1712.07709.
Suciu, G., Nădrag, C., Istrate, C., Vulpe, A., Ditu, M.-C., Subea, O., 2018. Comparative analysis of distributed ledger technologies. In: 2018 Global Wireless Summit (GWS), IEEE, pp. 370–373.
Tchakounté, F., Faissal, A., Atemkeng, M., Ntyam, A. A reliable weighting scheme for the aggregation of crowd intelligence to detect fake news, Information 11 (6), ISSN 2078-2489, doi: 10.3390/info11060319, https://www.mdpi.com/2078-2489/11/6/319.
Titouna, C., Ari, A.A.A., Moumen, H., 2018. FDRA: Fault detection and recovery algorithm for wireless sensor networks. In: International Conference on Mobile Web and Intelligent Information Systems. Springer, pp. 72–85.
Tschiatschek, S., Singla, A., Gomez Rodriguez, M., Merchant, A., Krause, A. Detecting fake news in social networks via crowdsourcing, arXiv preprint arXiv:1711.09025.
Ugander, J., Karrer, B., Backstrom, L., Marlow, C. The anatomy of the facebook social graph, arXiv preprint arXiv:1111.4503.
Vishwanathan, S.V.N., Schraudolph, N.N., Kondor, R., Borgwardt, K.M., 2010. Graph kernels. Journal of Machine Learning Research 11 (Apr), 1201–1242.
Volkova, S., Shaffer, K., Jang, J.Y., Hodas, N., 2017. Separating facts from fiction: Linguistic models to classify suspicious and trusted news posts on twitter. In: Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers), pp. 647–653.
Wu, G., Greene, D., Cunningham, P., 2010. Merging multiple criteria to identify suspicious reviews. In: Proceedings of the fourth ACM conference on Recommender systems, pp. 241–244.
Zhou, X., Zafarani, R. Fake news: A survey of research, detection methods, and opportunities, arXiv preprint arXiv:1812.00315.
Zubiaga, A., Aker, A., Bontcheva, K., Liakata, M., Procter, R., 2018. Detection and resolution of rumours in social media: a survey. ACM Computing Surveys (CSUR) 51 (2), 1–36.