

Social Trust-based Blockchain-enabled Social Media News Verification System

Riri Fitri Sari

(Department of Electrical Engineering, Faculty of Engineering, University of Indonesia, Depok 16424, Indonesia,

 <https://orcid.org/0000-0002-8841-8078>, riri@ui.ac.id)

Asri Samsiar Ilmananda

(Department of Information System, Faculty of Information Technology, University of Merdeka Malang, Malang 65146, Indonesia,

 <https://orcid.org/0000-0002-9469-2997>, asri.ilmananda@unmer.ac.id)

Daniela M. Romano

(Department of Information Studies, University College London, Foster Court, Gower Street, WC1E 6BT, United Kingdom,

 <https://orcid.org/0000-0001-5756-0146>, D.Romano@ucl.ac.uk)

Abstract: In the current digital era, information exchanges can be done easily through the Internet and social media. However, the actual truth of the news on social media platforms is hard to prove, and social media platforms are susceptible to the spreading of hoaxes. As a remedy, Blockchain technology can be used to ensure the reliability of shared information and can create a trusted communications environment. In this study, we propose a social media news spreading model by adapting an epidemic methodology and a scale-free network. A Blockchain-based news verification system is implemented to identify the credibility of the news and its sources. The effectiveness of the model is investigated by utilizing agent-based modelling using NetLogo software. In the simulations, fake news with a truth level of 20% are assigned a low News Credibility Indicator (NCI ± -0.637) value for all of the different network dimensions. Moreover, the Producer Reputation Credit is also decreased (PRC ± 0.213) so that the trust factor value is reduced. Our epidemic approach for news verification has also been implemented using Ethereum Smart Contract and several tools such as React with Solidity, IPFS, Web3.js, and Metamask. By showing the measurements of the credibility indicator and reputation credit to the user during the news dissemination process, this proposed smart contract can effectively limit user behaviour in spreading fake news and improve the content quality on social media.

Keywords: Social media, Blockchain, smart contract, epidemic model, scale-free networks, agent-based modelling

Categories: I.6.3, I.6.4, I.6.5, I.6.6, K.4.2

DOI: 10.3897/jucs.68692

1 Introduction

The Internet and social media allow information to spread quickly and easily. However, they are also the same platforms used for the dissemination of false information, fake news or hoaxes [Tambuscio et al. 2015]. Fake news is a statement where the truth is unknown or intentionally falsified [Nguyen 2017]. Viral circulation of fake news can

modify public perceptions and disrupt public opinions by obscuring truthful information [Reimche 2018]. The research on false information has been reviewed in [Kumar and Shah 2018], it categorized various social media platforms and showed that false information is spread with the intention of deception (providing misinformation and disinformation). Alternatively it simply represents the individual opinion of the spreader with no absolute grounds for truth and with the goal of influencing the readers' opinion. This behaviour is also reinforced by human-bias, where some categories of news consumers, e.g., less educated and low consumers of media, are more susceptible to false news [Kumar and Shah 2018]. They also presented several studies that showed that people are not very good at discerning false from true information and that this leads to the creation of 'echo-chambers', in which people polarize themselves into groups with comparable backgrounds, which increases the spreading of similar beliefs, and if untrue, of fake news, suggesting that effective techniques for breaking these echo-chambers are greatly needed [Kumar and Shah 2018]. Finally, they presented literature-based evidence to show that only a small number of very active users are responsible for the spread of hoaxes [Kumar and Shah 2018].

In the research literature, a number of researchers were attentive to this topic through the use of various techniques and approaches; some experiments focused on studying the rumour spreading characteristics and investigating how the spread of rumours occur [Cheng et al. 2013, Jin et al. 2013, Mazzoli et al. 2018]. Some methods were applied to identify fake news, i.e., fact-checking [Tambuscio et al. 2015], text classifications based on neural networks [Nguyen 2017], and topic and sentiment analyses [Carrera and Jung 2018]. A fake news detection research [Shu et al. 2017] provided a comprehensive review of the psychological and social theories for social-media fake news detection, the existing data mining algorithms, and the relevant evaluation metrics. However, no approach to date has considered using Blockchain technology for fake news detection, as proposed in this paper.

The Blockchain approach was inspired by the work of Chen et al., which proposed a trusted Blockchain-based social networking system [Chen et al. 2018]. They conduct numerical analyses and simulated a news spreading model that was designed based on the Poisson distribution theorem, the Susceptible-Infected-Recovered (SIR) epidemic model and the smart contract protocol. Blockchain technology has the ability to build trust in a safe and decentralized system [Xia et al. 2019] and can encourage trust from the edge of the communications chain, the social media users, allowing them to contribute by reporting false news. Therefore, many other unsuspecting users can be conscripted to selectively read and spread news. The model relies on social responsibility and social trust, as will be discussed in [Section 3].

NetLogo is an agent-based modelling environment developed in 1999 by Uri Wilensky [Bajwa 2018] that has the ability to observe the dynamics of individual agent behaviour, along with the interaction patterns that occur within a complex system [Wilensky 2001]. Each NetLogo agent independently executes the given instructions so that each agent can take different actions based on their perceptions [Bajwa 2018]. NetLogo, due to its ability to rapidly prototype community behaviour, has been chosen in this study as the agent-based modelling environment to simulate the news spreading process that occurs in social media. Previously, an agent-based model has also been used to study the urgent diffusion in social media [Rand et al. 2015].

In [Section 2], we review some of the relevant research literature. We also elaborate the correlation between social responsibility and social trust [see Section 3].

Subsequently, we propose a novel model for news spreading in social media, which adapts the power-law distribution theorem on scale-free networks and the Verifier-Spreader-Ignorant-Stifler (VSIR) epidemic model, integrating a social trust Blockchain-based news verification system [see Section 4]. The effectiveness of the model is tested through a multi-agent-based simulation using the NetLogo software [see Section 5]. The simulation results of the proposed model using Netlogo and the implementation possibilities in Ethereum platform are presented and discussed in [Section 6]. Finally, [Section 7] concludes this paper by showing the advantages of Blockchain-based solution and the future work recommendation.

2 Fake News, Social Media and Blockchain

In the era of digital communications, the Internet and social media have become part of the lifestyles of modern societies and centres for information exchanges [Smith and Anderson 2018]. Nevertheless, social media is very vulnerable to the spread of hoaxes, propaganda, and even conspiracy theories by certain parties who want to take advantage [Delmi 2018] of the social networks. The hoax is a phenomenon that has a long history in human societies. The previous research stated that a hoax often refers to information about an object or event that has no factual basis and has not been verified as truthful [Chen et al. 2018]. A hoax, or fake news, is easily concocted to undermine or fight something or someone, in support of the point of view of the stakeholders who fund the news' release [Allcott and Gentzkow 2017]. This can affect decision makers and cause confusion in society. A hoax is spread, relying on perceptual and emotional factors, which can easily influence the receiver's opinions in lieu of the actual facts [Reimche 2018]. Therefore, fake news articles or hoaxes can be shared frequently via social media. There are a number of reasons why someone would easily believe and spread fake news; these reasons include lack of education, lack of trust, indifference and manipulation [Delmi 2018].

This paper proposes a new model of social networking with Blockchain-based smart contract as a solution to limit the spread of hoaxes and to increase user's awareness of social media. Blockchain itself is a technology initiated by Satoshi Nakamoto in 2008 as the foundation to run the Bitcoin cryptocurrency system [Battistoni 2016]. Literally, Blockchains can be regarded as distributed databases that are managed by blocks of data (block) and are arranged sequentially (chain) [Delmi 2018]. A Blockchain is designed to ensure the security and reliability of data and to grow trust between interrelated parties for a particular transaction or contract agreement [Lee et al. 2018].

The Blockchain system runs on a network formed by a group of nodes or participants that are connected to each other [Bajwa 2018]. Communication is done through peer-to-peer (P2P) networks, which are the main elements in the Blockchain's decentralized system. In this network, there is no centralized server as the dominant authority, so trust in a transaction is built without needing a third party [Battistoni 2016].

Blockchains store all the records for a digital transaction in a public database called a public ledger [Chen et al. 2018]. Because the ledger is copied to some, or all, of the participant's devices that are spread over the network, the data is more difficult to hack, exploit, or lose [Lee et al. 2018]. When a number of new transactions have been

collected, a block will be created and linked to the previous block in the ledger. Each block will go through a validation process held by one of the selected participants who is qualified as a validator based on a certain consensus protocols [Battistoni 2016]. A modification, or any slight change of data in a block is almost impossible since it will affect all the records in the next block [Lee et al. 2018].

The consensus protocol creates a system of collective agreements [Delmi 2018], which regulates the management of transaction blocks, while ensuring the integrity of the information stored in them [Xia et al. 2019]. One of the commonly used consensus protocol methods is the Proof of Stake (PoS). PoS is a consensus method based on the proof of ownership of digital currency deposits [Delmi 2018]. A participant has the opportunity to become a validator and process a new block based on the percentage of coins owned or at stake. The validator who successfully validates the block and adds it to the ledger will receive a prize in the form of a digital currency or a certain token. PoS does not require a computational process, nor massive energy consumption, so it can save time and money [Battistoni 2016].

Through the Blockchain-based approach, the process of information exchange in social media no longer requires control from the platform provider, because the system itself can build trust and protect itself from attacks [Delmi 2018]. All the user activities will be recorded in the ledger blocks, allowing transparency, reliability and security of data [Chen et al. 2018]. A user can monitor the track record and reputation of the other users, so that both parties can build trust in each other [Bajwa 2018]. Users who intentionally want to spread hoaxes will damage their own reputation. Additionally, hoax spreading activities can be traced easily and can be legally proven because all the information will be permanently recorded in the ledger [Delmi 2018]. Thus, Blockchain technology is expected to provide an improved alternative communication system for social media networks.

3 Responsibility and Trust in Social Networks

Social networks are a culture-based method that can affect from people's behaviour to economic development [Fukuyama 1995]. The phenomenon in social communities can be explained through an old concept called social capital. The notion of social capital popularized by [Putnam et al. 1993] refers to connections between individuals that can increase the efficiency of society by facilitating cooperation and collective action for mutual benefit. The major elements of social capital include social networks, norms of reciprocity, and trustworthiness that arises from it. Meanwhile, [Lin 2001] defines the concept of social capital as an investment in social relations with expected returns. According to Lin, it is the members of the group who create the possibility of maintenance and reproduction of social network's assets.

Social networks have value and social contacts affect individual and group productivity [Putnam et al. 1993]. Putnam argues that, people who participate in social networks or voluntary organisations can form habits of cooperation, solidarity, and also encourage the development and spread of trust. This is also explained in [Lin 2001], where people who are involved in social networks can obtain certain benefits. To [Putnam et al. 1993], the most significant norm underlying social trust is reciprocity. It can generally be associated with continuing relationships and hopes with the possibility of relying on them in the future, e.g. friendships and mutually helpful relationships.

Matzat in [Kotarski 2015] explains that in online social communities, there are three main sociability issues: (i) the changeability of community members, (ii) free-riding on community resources without equitable reciprocity, and (iii) lack of trust. The information that a person discloses in a social group demands a certain level of trust towards others. This means that participants in a social networks may have different reactions to the information shared among them. Whether the information will be approved or will be opposed, depends on how trustworthy is the author of the information.

An analysis of social capital has been conducted by Bucholtz in [Kotarski 2015] for the Latvian social networking site Sviesta ciba based on measures of social networks, norms, and trust. The results showed that the broader the network of user connections and the more intense the interactions on the site, the more likely this person's trust in other users would be high. In addition, users who tend to trust others and are willing to engage in deep discussions, have a greater chance of receiving emotional support.

We propose to generalize the idea of social trust to social media networks, making a shift from the idea of physical neighbours to the idea of network neighbours. In a free society, such as those created on social media, social trust is an important form of capital that relies on social norms; the belief that those we deal with will conduct themselves in a socially accepted manner [Juola 2020]. Social capital is a strong indicator of a community's level of wellbeing. The more people involve themselves in voluntary networks, the more trust they have for others, and as a consequence, the more productive and happier are the participants in the community. Of course, there are many cases in which people are careless and do not make reasonable efforts to comply with the community norms or do not have the time or skills to comply. However, when people act for the social good, this enriches the community in which they operate, and increases the reciprocal social trust of others in that community.

4 Proposed Model

This research was conducted with the objective of investigating how a social-trust Blockchain-enabled solution can limit the spread of hoaxes in social media. To achieve this, a model of news spreading in social media has been implemented utilizing the agent-based modelling environment NetLogo.

In the model, it is assumed that the news producers and consumers (or network participants) have the same characteristics and transmission speeds. All participants are linked peer-to-peer to form a decentralized network. Each participant is identified by a unique identifier, equipped with a wallet containing tokens, and able to rate every news item they receive and spread it, or not spread it, to the network.

News is assessed based on the quality of its content, as either a fact or a hoax. This assessment depends on the perception and knowledge, social responsibility and social trust of each participant in the network. If a news item is rated with a low score, the reputation of the participant who has posted the item decreases, and if the news item receives a high score, the news producer's reputation increases. If a news item is spread, but not rated, the news producer's reputation increases only to a midpoint value. The credibility indicator of the news item is calculated based on the news' rating and the reputation credit obtained for the news s/he has generated by the other network

participants. The more a news item is reported, the higher the accuracy of the assessment results. In addition, it is possible to measure the social trust or credibility level of the network by combining the ratings of the news generated and the people participating in the network. A detailed description of the model is shown in the subsections below.

When a participant receives a message, it is assumed that the participant will receive additional information in the form of a News Credibility Indicator (NCI) and a Producer Reputation Credit (PRC) of the news' source. This additional information helps the users estimate the quality of the content of the news generated by a network, so that it can be used as a guide in considering whether the news can also be trusted across networks, or echo-chambers.

In this study, the mechanism for selecting a validator was created to represent a consensus protocol, which is the equivalent of social trust in the network or community to which one belongs. A validator is determined based on two criteria, namely, the number of tokens owned, and the reputation credit. Because the validator will receive an additional token as a prize, the participant will be encouraged to maintain his or her reputation in order to have a chance to become a validator. Participants sincerely consider whether they want to spread a hoax, so the quality of the social media content will increase.

The implementation of Blockchain technology in this study is focused on supporting a news verification system, so the block validation mechanisms and the data storage in the real ledger were not considered to simplify the model. The model's design framework was divided into three main stages, as shown in Figure 1.

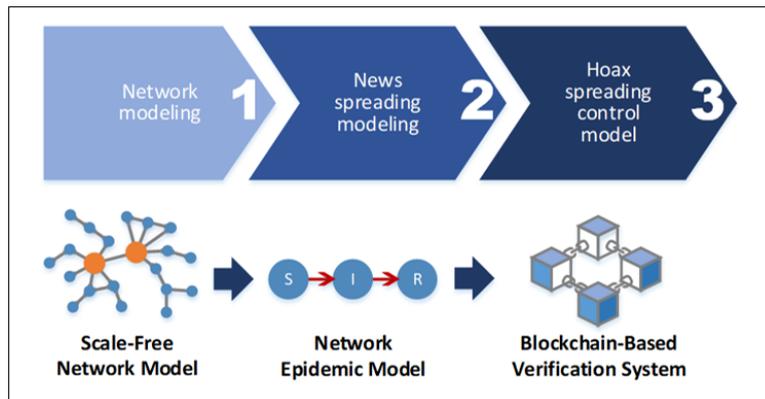


Figure 1: Design framework of the proposed model

4.1 Scale-free Network Model

The first stage of the design is done by modelling the network structure on social media. In this study, a scale-free network model was chosen because it is able to describe the characteristics of social media networks. In addition, a scale-free model also mimics the Blockchain's decentralized network features. Scale-free

networks have been used in several previous studies [Wang et al. 2015, Battistoni 2016] to model social media networks.

A scale-free network is a general model of a real-world network introduced by Barabási-Albert in 1999 [Doerr et al. 2012, Pastor-Satorras et al. 2015]. A scale-free network topology is arranged in a hierarchy, where a new node tends to form a link with a node that has the highest degrees or number of links [Barabási 2016]. In this case, some nodes will act as hubs, which have a high connectivity and are connected to many nodes simultaneously. However, most nodes will be connected to each other with lower degrees. Scale-free networks are formed based on preferential attachment rules [Pastor-Satorras et al. 2015], which state that the higher the degree of a node, the higher the probability of obtaining a connection with a new node.

In this model, the network is formed by a group of nodes, designated as participants. The friendship between two participants is indicated by a link. A communications line is described as an undirected network [Zhang and Yu 2018]. Based on the scale-free network concept, a network will have many participants with a low number of links and several participants with a high number of links. This exemplifies a real-world social media networks, which shows that the number of relationships an individual has with other individuals are influenced by their popularity or the number of friends they have [Baafi et al. 2017].

4.2 News Spreading Model

The next design stage is modelling the process of spreading news on social media. The way news spreads has similar characteristics with disease propagation, so it can be conceptually modelled as an epidemic model [Tambuscio et al. 2015, Yuan and Hu 2018]. Over the past few years, researchers have developed a number of information spreading models based on epidemiological studies i.e., the *Susceptible-Infected-Recovered* (SIR) epidemic model [Cheng et al. 2013, Yuan and Hu 2018], the *Susceptible-Infected-Susceptible* (SIS) model and the *Susceptible-Exposed-Infected-Sceptic* (SEIZ) epidemic model [Jin et al. 2013], and the *Emotion-based Spreader-Ignorant-Stifler* (ESIS) epidemic model [Wang et al. 2015]. The network epidemic model was chosen in this study to show the dynamics of participant behaviour in social media, specifically under what conditions a participant trusts or denies the news.

The epidemic model allows a mathematical approach that can describe the dynamics of a system based on certain assumptions [Baafi et al. 2017]. To illustrate the spreading of news on social media, our research model was developed by adopting an epidemic model, i.e., the *Verifier-Spreader-Ignorant-Stifler* (VSIR) model. In the VSIR model, N participants can switch their status between four conditions:

- *Ignorant* (I), which are participants who do not know about the news or have not yet received the news.
- *Verifier* (V), which are participants who have received the news and then make a decision to trust or deny the news after some period of time.
- *Spreader* (S), which are participants who believe in the content of the news and attempt to spread the news to their friends in the networks.
- *Stifler* (R), which are participants who refuse to believe the content of the news and do not want to be involved further with the news.

It is assumed that one participant will spread the news for the first time in the network, so that the initial status of the participants becomes:

$$I(0) = N - I; E(0) = 0; S(0) = I; R(0) = 0$$

Each participant will change status randomly by considering the parameters, as follows:

- The spreading rate (β), which determines the probability for an ignorant to receive the news from a spreader and turn into a verifier.
- The truth level of the news (γ), which determines the probability of a verifier deciding to change into a spreader or a stifler in accordance with the magnitude of trust the verifier has in the news.
- The recovery rate (δ), which determines the chance of a spreader or a stifler returning to an ignorant because of a forgetting mechanism.

A schematic diagram of the news spreading model is shown in Figure 2.

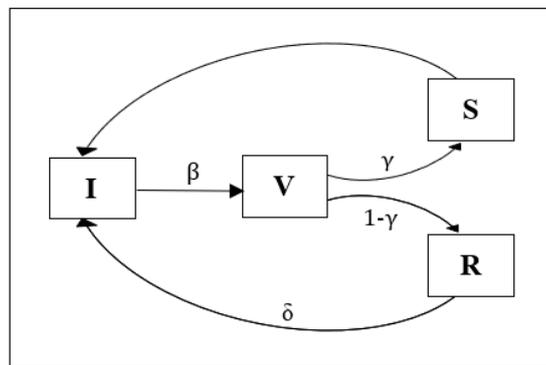


Figure 2: A schematic diagram of the news spreading model

During the news spreading process, there are three status transition phases:

- The spreading phase [*I becomes V*], where an ignorant can receive news from a spreader and turn into a verifier at the spreading rate of β .
- The verification phase [*V becomes S, V becomes R*], where the verifier can choose to be a spreader or a stifler after τ period of time. The magnitude of trust for the news is determined by the truth level of the news of γ .
- The forgetting/lost interest phase [*S becomes I, R becomes I*], where a spreader or a stifler can return to an ignorant state at the recovery rate of δ due to forgetting factors or losing interest in the news.

It can also be written simply into differential equations as follows:

$$\frac{dI(t)}{dt} = -\beta \frac{S(t)}{N} I(t) + \delta(S(t) + R(t))$$

$$\frac{dV(t)}{dt} = \beta \frac{S(t)}{N} I(t) - \omega V(t); \text{ where } \omega = \text{frequency} = \frac{1}{\tau}$$

$$\frac{dS(t)}{dt} = \omega \gamma V(t) - \delta S(t)$$

$$\frac{dR(t)}{dt} = \omega(1 - \gamma)V\delta R(t)$$

4.3 Blockchain-based News Verification System

The final design phase consists of implementing the Blockchain-based smart contract to control the spread of hoaxes in social media. The news verification process will be conducted by all participants with a verifier status. After a certain period of time, the verifier can decide to trust or deny a news item and give a rating according to their perception of the news. The news assessment values consist of the following:

- *The News Rating (NR)*, which is the news rating value given to the news by each verifier receiving the news. The higher the participant's trust level of the news, the greater the rating obtained.
- *The Producer Reputation Credit (PRC)*, which is the credit value that determines how much a network participant can be trusted. This credit will increase when the news posted and spread by a participant is a fact and it will drop when the news is a hoax.
- *The Network Social Trust/News Credibility Indicator (NCI)*, which is the value that states the quality of a news item.

These parameters are calculated through the following equations:

$$NR = \frac{\sum_{i=1}^m NR_i}{n}; m = \text{number of participants who receive the news}$$

$$PRC = \frac{\sum_{j=1}^m RC_j}{n}; m = \text{number of reports}$$

$$NCI = NR + PRC$$

The specification of the news assessment is shown in detail in Figure 3. The participant's trust level for the news is categorized from low, medium (implicit) to high. Each level has its own criteria, so it causes different impacts on the dynamic change of the participant's status in the network.

At the start, the values of NR, PRC and NCI are initialized to 0. NR is an integer value that ranges from -2 to 2. When the trust level is low, participants will rate the news with the value of -1 or -2, and the PRC value will be increased by 0 points. Based on this condition, the value of NCI will be less than 0. At the implicit trust level, a participant will not rate the news, and the PRC value will go up by 0.5 points. If the news obtains a high trust value from the participant, the news will be rated with the value of 1 or 2. The PRC value will be increased by 1 point, so the NCI will reach a positive value.

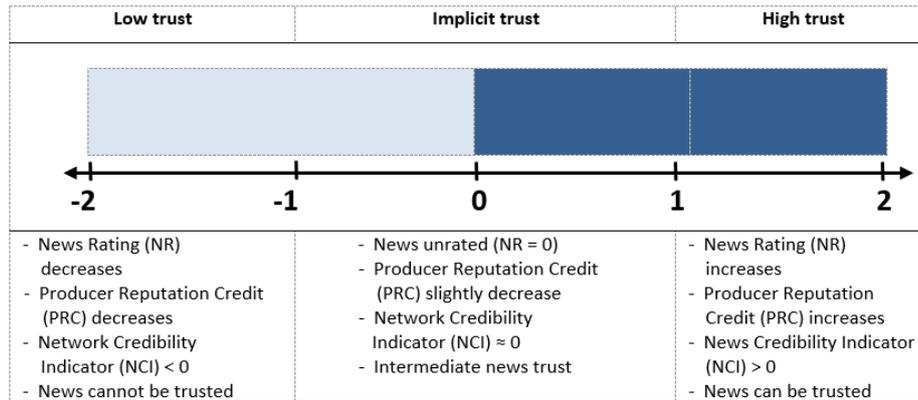


Figure 3: News assessment specification

The flow of the news assessment is shown in Figure 4. This assessment will start every time a verifier has ended his/her evaluation period of τ . The evaluation period represents the time needed by a verifier to indicate whether s/he will rate the news or not. If the verifier is convinced that the news is true, then the trust level will be high. His/her status will be changed to spreader, which will expand the news spread in the network. Otherwise, the trust level will be low when the verifier determines that the news has a likelihood of being fake. At this state, the verifier’s status will be changed to stifler. The value of the NCI will be calculated based on all the received reports and will be updated in every cycle.

In general, when the NCI is low, the participant’s awareness will increase and they will tend not to believe in the news. This can cause a decrease in the number of spreaders in the network, so that the spread of hoaxes in the social media is controlled.

5 Simulation Scenario

A simulation is conducted in order to observe the participant behaviour in the network during the news’ dissemination. In this study, three network dimensions are formed by 1000, 10000 and 100000 participants. The participant with the highest degree (maximum links) is initialized as the news source to optimize the news dissemination. A validator is selected at each time step or *tick* based on the weight calculated by the following equation:

$$Weight = token \times reputation\ credit$$

To mimic real-world behaviour, this model is simulated at two different truth levels of news (γ): a 20% level representing fake news and an 80% level representing true news. The other parameters are set at a constant value, including a spreading rate (β) of 29% and a recovery rate (δ) of 1%. The evaluation period (τ) is random from 1 to 5 *ticks*. The simulation is run in 3 cycles of 60 *ticks* and repeated 30 times to obtain data stability.

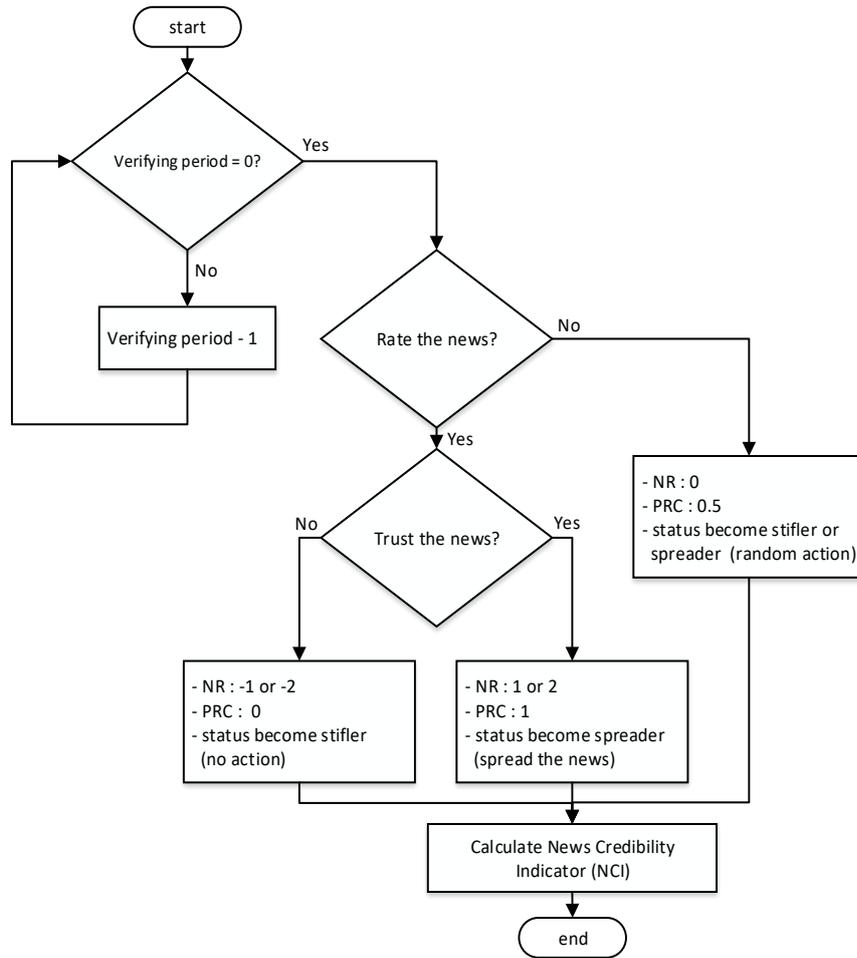


Figure 4: News assessment flow

6 Result and Discussion

In the simulation, a verifier can have a random level of perception and trust. The lower the truth level of the news, the greater the chance of the news to be identified as a hoax. The experimental results of the news spreading simulations are summarized in Figures 5. Each shows the end state of the simulation in the different network dimensions.

The results show that when the truth level of news is low ($\gamma = 20\%$), the number of ignorant participants still dominates the network at approximately 95% of all the participants (Figure 5 (a) (b) (c)). It can be seen that fake news or hoaxes tend to have a low level of trust, so the proportion of spreaders is less than that of the stiflers, at a

1% and 4% rate, respectively. In this situation, the news spreading process can be stopped quickly and the distribution range decreases.

Meanwhile, when the truth level of the news is high ($\gamma = 80\%$), the proportion of spreaders is 50%, which is greater than that of stiflers, which is 14% (Figure 5 (d) (e) (f)). This indicates that true news or facts tend to have a high level of trust. The number of ignorant participants decreases prominently, until it reaches approximately 36% of all the participants, as long as the news is spread. These conditions are consistent across all network dimensions.

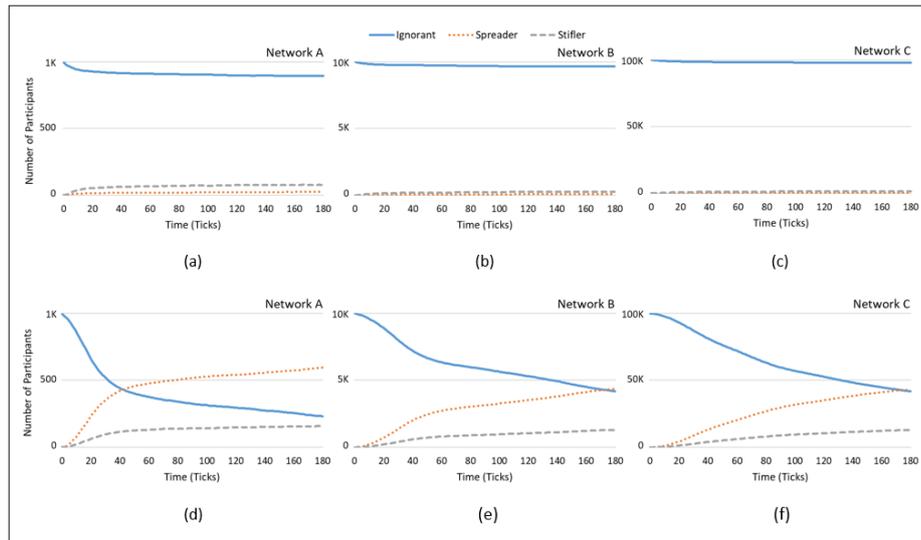


Figure 5: Status of participants with $\gamma = 20\%$ (a,b,c) and $\gamma = 80\%$ (d,e,f), Network A for 1000 participants, Network B for 10000 participants and Network C for 100000 participants

During the simulation, a news assessment is conducted by calculating the News Rating (NR) and the Producer Reputation Credit (PRC) to obtain the News Credibility Indicator (NCI). The average calculation results for all the network dimensions are shown in Figures 6 (a) and (b). Both pictures show that, the higher the truth level of the news, the greater the value of NR obtained. This is because true news has a larger chance of obtaining a high rating than fake news.

Similar to NR, the value of PRC is also influenced by the truth level of the news. This means that when a participant posts a hoax, his/her reputation credit will decrease and vice versa. Therefore, the credit reputation could be used to determine whether a participant is trusted.

The value of NCI is obtained by adding up the NR and the PRC from all incoming reports. When the truth level of the news is low ($\gamma = 20\%$), the value of the NCI decreases until it reaches $NCI \pm -0.637$, with $NR \pm -0.850$ and $PRC \pm 0.213$. In this case, the participants tend to avoid the news because they assume the news is not trustworthy. In contrast, when the truth level of the news is high ($\gamma = 80\%$), the value of the credibility indicator increases up to $NCI \pm 1.583$, with $NR \pm 0.814$ and $PRC \pm$

0.769 of 1. In this situation, the news is more trusted by the participants because the indicators have a positive assessment.

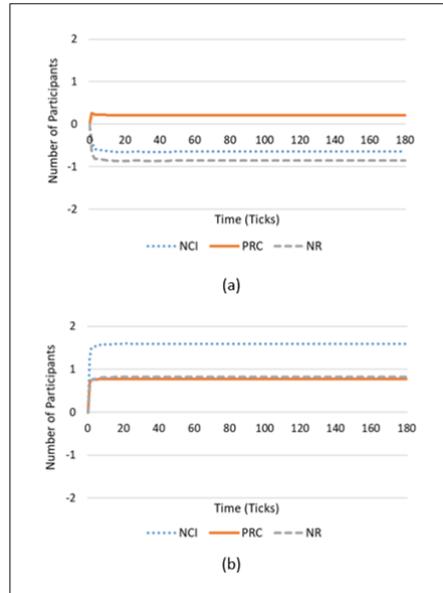


Figure 6: Average calculation result of NR, PRC and NCI for (a) $\gamma = 20\%$ and (b) $\gamma = 80\%$

Furthermore, the value of the PRC also affects the possibility of the participant being selected as a validator. The validator selection process is based on the number of the participant’s tokens in the wallet. The greater the weight of the participant, the higher the chance of being selected as a validator. When the participant posts a news item that is trusted, then the PRC will increase. Thus, the possibility of being chosen as a validator and increasing the number of tokens in the wallet will be even greater. Otherwise, if the participant posts a fake news item, s/he will receive a low PRC and have a smaller possibility of being selected as a validator. As a result, s/he will have difficulty in increasing the number of tokens in the wallet.

News dissemination is simulated in 3 cycles of 60 ticks. Figure 7 shows how many participants were influenced by the news for all the network dimensions. Figure 7 (a) with $\gamma = 20\%$ shows that the number of untrusted-participants starts to grow for the first 60 ticks, whereas the trusted-participants and the implicit-participants have low numbers until the final state. At the third cycle, the graphs are close to the steady state as the results have not changed significantly.

Different from Figure 7 (a), the graphs in Figure 7 (b) with $\gamma = 80\%$ have a high number of trusted participants. This starts increasing in the first 60 cycles and still grows slowly for the next two cycles. The number of untrusted-participants and implicit-participants are low. Both have less of an impact on spreading the news.

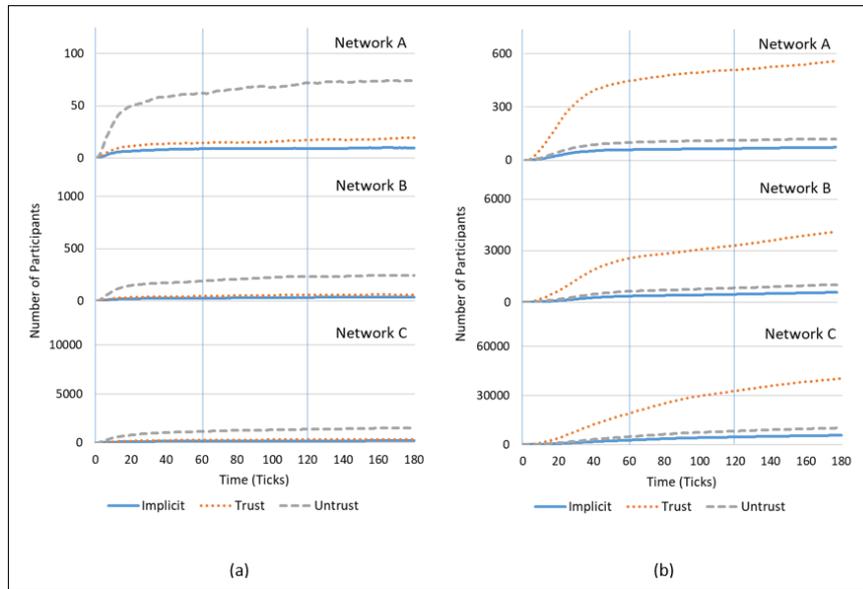


Figure 7: Trust in the news by participants when the truth level of the news
 (a) $\gamma = 20\%$ and (b) $\gamma = 80\%$, Network A has 1000 participants,
 (b) Network B has 10000 participants and Network C has 100000 participants

Based on our research results, the proposed smart contract has been designed to be implemented into a real social networking platform. Blockchain technology allows a revolution in how content or news is produced and distributed via the Internet. [Takayar 2018] explained that a platform that supports Blockchain have the following benefits:

- **News transparency**, the transparent nature of Blockchain allows news to be verified. News can be categorized as real or fake news by checking the specific criteria defined in the smart contract, so as to build trust among users. In our proposed design, each news item has specific information attached to it, namely the credibility indicator of the news itself and the reputation credit of the news source.
- **News traceability**, a news that is shared on a Blockchain-enabled application that can be traced for authenticity to prevent users from reading fake news. Even if the news has been changed, it will be possible to trace what changes have occurred and who changed the news from its original state to the present.
- **Decentralized approach**, decentralized platform approach allows for a relationship of trust to be built together. In addition, the absence of a centralized server to store data prevents the occurrence of a single point of failure (SPOF) which can cause the entire system to crash.
- **Immutable approach**, information stored on the Blockchain which could be in the form of news content, videos or images, cannot be changed, altered, or deleted so as to ensure data integrity. This allows social media users to share their news in an immutable and secure way.

In general, a Blockchain-based social networking platform divides users into three main roles:

- **Author** or news writer, the person who write and upload news to be published on social media. In our simulation model, an author is a participant who acts as the news producer. Unlike news agencies, every social media user can act as an author, even if they are an editor or an auditor.
- **Editor**, the person who verify and publish news on social media, and store them on the Blockchain. A specialized expert with broad knowledge, or a professional editor from a news publisher, has a higher likelihood of becoming a validator because of their reputation. Our simulation model represents the editor as the validator selected by consensus protocol.
- **Crowd auditors**, the people who will approve the news and may share it, or mark it as fake news. Crowd auditors are decisive in the assessment process of a news. In our simulation model, the crowd auditor is the other participants who can be in four different statuses, i.e. ignorant, verifier, spreader or stifler.

The news verification system has been set using smart contract on a social networking platform that supports Blockchain . It can be described in a diagram as shown in Figure 8. All actors, both author, editor and crowd auditors, register on the platform and create profiles according to their real identities. The personal data that is required such as name, email ID, identity card number, contact number, work experience and certificate of expertise. The Personal Identification Information (PII) will then be saved in the form of a document, with the address hashed and stored on the Blockchain. A third party background check may be required to verify the profile of the editor.

After registering with the platform, an author can upload news or other contents to share on social media. The news is equipped with the hash address of the author as a digital signature to provide information of who made it, where and when. The rules built into smart contract will put the news on a "waiting list" and will help assign an editor to it. The assigned editor will check the source and content of the news, then determine whether to publish it or not. News that is approved for publication will be rated for the first time, which is called News Rating (NR). Afterwards, the smart contract will trigger a rule to calculate the News Credibility Indicator (NCI), based on the value of NR and also the author's reputation credit named Producer Reputation Credit (PRC). The news then stored on the Blockchain along with the hash address of the editor. From this process, both author and editor can receive rewards in the form of tokens which will be accumulated in the wallet.

When the validation process is successful, the news uploaded by author will be distributed and published on social media. People connected on the network will be able to view and read the news according to their preferences. The news content is stored on the Blockchain's ledger. This make it impossible for someone to delete or change the content, even the author himself. Every time an author edits or modifies a news content, smart contract will trigger to record its detailed information changes and save it again in a different version. Thus, it will be easier to identify whether a story is original, edited or reused.

Determining the high and low rating of a news item is an important task for the crowd auditors. Crowd auditors may randomly or periodically assess content and decide to mark it as real or fake news. They evaluate the content of the news by considering

two factors: (i) NCI, the more auditors who make the assessment, the more reliable the calculation results of NCI, and (ii) PRC, the higher the reputation credit of the author, the higher the level of trust in the news. When an auditor assigns a rating to a news (NR), the smart contract will trigger a recalculation of NCI and PRC, update its value, and store it on the Blockchain. If the rating given is low, or the news is declared fake, then the NCI and PRC will tend to fall, and vice versa. For their contribution in assessing the news, token prizes should also be given to auditors.

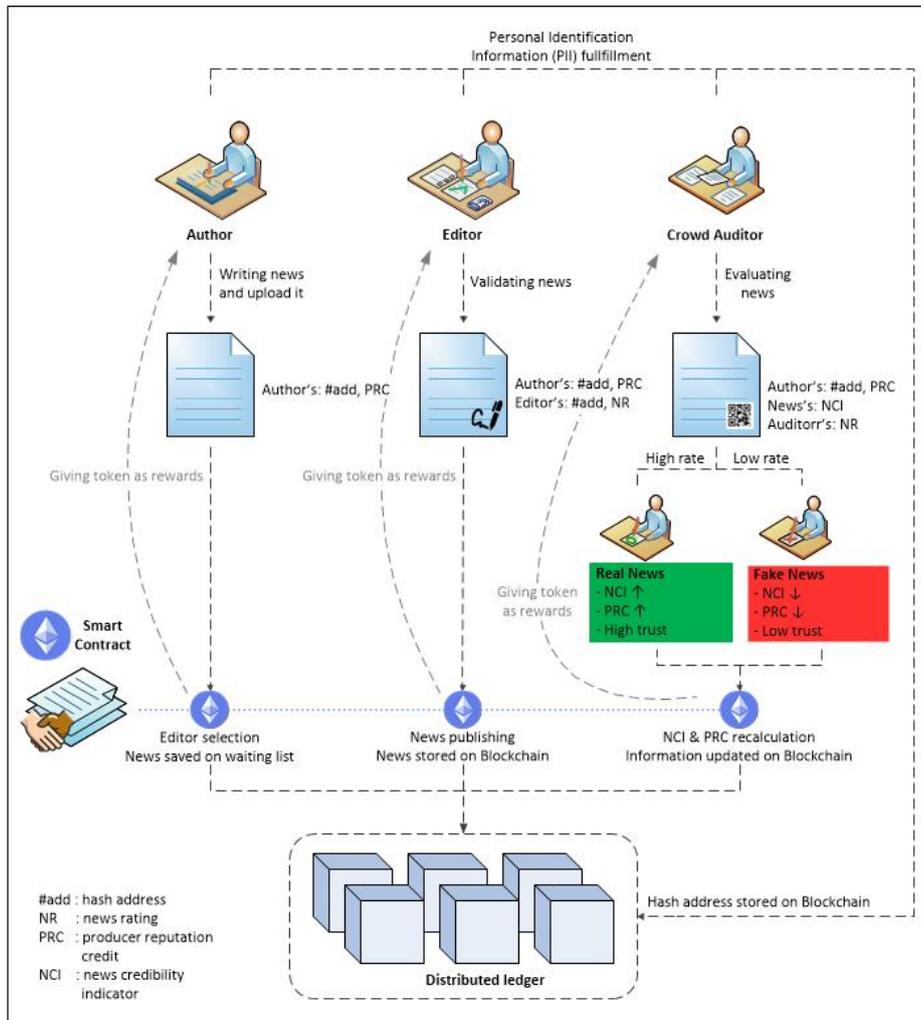


Figure 8: Blockchain-based smart contract on social networking platform

Each published news content is provided with complete news details, including the values of NCI and PRC, which can be displayed in the QR Code. By scanning the QR Code, the auditor can view the information needed to help make a decision whether a

news is real or fake and conducted an assessment to it. In addition, this information can also help the auditor to track when the news was written, published, edited or modified. This is possible with Blockchain, in which all of user information and activities are stored in a distributed ledger that is accessible to people on the network.

This Blockchain technology solution for social media networks can be further developed using the Ethereum platform, as was done in [Jianjun et al. 2020] to build an integrated data sharing platform. In [Hasan and Salah 2019], Ethereum was also used to provide a smart contract solution for tracing and tracking the provenance and history of digital content especially video. The front-end components may include mobile applications for authors and crowd auditors, as well as a web portal that can be accessed by editors. In its implementation, several tools have been used to run the system as follows:

- Inter Planetary File System (IPFS): Tools used as a Peer-to-Peer Decentralized Database which is a special network of files or files that are stored and distributed via a peer-to-peer network. IPFS is also compatible with all digital file formats such as images, video streams, databases, and documents. The data is chopped into small units and distributed to network nodes in which each node will store some files including the fingerprint of the file. This process is useful for making it easier for other users to read the file. The bigger the news stored in the IPFS, the more expensive the cost required to run the function. [Ramadhan et al. 2021].
- React with Solidity: Tools used to create a user interface in the form of a JavaScript library. This tool can be used as a platform for the front-end of the Blockchain by configuring and developing smart contract on Ethereum.
- Web3.js: A collection of libraries that allow programmers or clients to interact with on-chain components on the Ethereum networks.
- MetaMask: Tools used as a cryptocurrency wallet that can be used via a browser in the form of an extension file. This tool is also a bridge between users or accounts with the Ethereum Blockchain.

We have implemented the proposed smart contract on Ethereum platform and made it available on https://github.com/haekalhbz/News_Verification/tree/master. The solution works for reputation and credibility scoring. In this solution, there are four entities namely Journalist, Validator, Smart Contract and IPFS. The Smart Contract connects the application with the Ethereum Environment. It stores the received data from the Blockchain such as the rating given by the validator and the hash code from the file stored in the IPFS. IPFS will store the news created by the journalist. The news stored can be accessed by the application using a hash code that is generated by IPFS. Each function in the Ethereum Smart Contract has an execution cost for it to be executed. The Rating Functions have the same execution cost for each Smart Contract, while this is not the case with the Submit Function.

Overall our researched have applied the blockchain technology for a social trust-based social media platform, simulating predetermined scenarios employing NetLogo as an agent-based modelling software. Subsequently this NetLogo simulation have been proceeded with Smart Contract implementation using Ethereum, and have been presented, despite of some limitations on the credentials of the validator to ensure the trustworthiness of the validation process.

7 Conclusion

Trust is an important element in relationships among individuals, which also applies to social media network. Users who are likely to be positively involved in various activities in social media will get better emotional support and higher level of trust. Moreover, those who have a high level of trust will be able to encourage joint collaboration and foster an ecosystem of trust in the community. This mutual trust can help create meaningful interactions between users, where they can freely share personal problems and other urgencies. In this case, verifying the truth of information is very important, as well as to obtain the information of who made the news, where and when.

In this study, Blockchain technology was implemented in a model through a news verification system as a solution to control user behaviour in spreading fake news. The news assessment process generates a News Credibility Indicator (NCI), which is determined by the News Rating (NR) and the Producer Reputation Credit (PRC). The NR accumulates the rate of the news from all the incoming reports. The PRC measures the positive influence a participant has in the network. Thus, the value of NCI could affect a participant's decision of whether or not the news is trustworthy.

This model is scalable; for different network dimensions, a consistent-similar result is obtained. The results of the news assessment are observed based on the values of NR, PRC and NCI. When the values of NCI and PRC are low, the participant will increase their awareness and tend to avoid the news. The intensity of the hoaxes distributed in the network will decrease. Therefore, the spreading of hoaxes on social media can be controlled. The lower the PRC of a participant, the smaller the possibility of s/he being chosen as a validator, and s/he will also gather fewer tokens. Therefore, the participant will be incentivized to preserve their reputation by being more judicious in spreading news, and the content quality in social media will be improved.

The proposed blockchain smart contract which has been implemented using Ethereum can play important role in building trust for social media networks. Through the transparency, traceability and decentralization nature of Blockchain technology, the line between fake and authentic news is no longer blur. People will feel safe in the community, since trusting others has become their default behaviour. Disclosing personal information is no longer a major concern on online community, even if it is shared to someone who may not be or recently known. Furthermore, reciprocal relations also occur between users through the mechanism of news assessment as well as gift awarding in tokens. The whole processes are really depend on the user's reputation in social media. When people are required to participate actively, it could prevent free-riding, which is one of the most common problems in social networking.

This new Blockchain-based social media model has the potential to change the way information is produced and distributed, so as to provide a reliable way to verify news content and source. Not only that, the Blockchain-based approach also has the capability to improve online communication by providing emotional, informational and material support, along with appropriate norms and trust both for individuals and society. For the future work, Ethereum could be escalated to be a feasible Blockchain-supported platform to further build this solution and tackle disinformation in social media.

Acknowledgements

We thank the University of Indonesia for financial support for this research under the PITQ1Q2 Grant number NKB-0321/UN2.R3.1/HKP.05.00/2019.

References

- [Allcott and Gentzkow 2017] H Allcott and M Gentzkow. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*. American Economic Association.
- [Baafi et al. 2017] Baafi et al. Vaccination as a Control of Infectious Diseases. *J. Appl. Comput. Math.* 06(03), 2017. doi: 10.4172/21689679.1000357.
- [Bajwa 2018] N K Bajwa. Modelling and Simulation of Blockchain based Education system. Concordia University, 2018.
- [Barabási 2016] A-L Barabási. *Network Science*. Cambridge University Press, 2016.
- [Battistoni 2016] L Battistoni. Emerging cryptocurrency trust in an agent-based model. 2016.
- [Carrera and Jung 2018] B Carrera and J-Y Jung. SentiFlow: An Information Diffusion Process Discovery Based on Topic and Sentiment from Online Social Networks. *Sustainability*. 10(8):2731, August 2018. doi: 10.3390/su10082731.
- [Chen et al. 2018] Y Chen et al. Towards trusted social networks with blockchain technology. *arXiv*. arXiv.
- [Cheng et al. 2013] J J Cheng et al. An epidemic model of rumor diffusion in online social networks. *Eur. Phys. J. B*. 86(1), 2013. doi: 10.1140/epjb/e2012-30483-5.
- [Delmi 2018] D Delmi. *Democratizing Blockchain with New Generation Social Network and The First Federated Byzantine Proof-Of-Identity Protocol*. 2018.
- [Doerr et al. 2012] B Doerr et al. Why rumors spread so quickly in social networks. *Commun. ACM*. 55(6):70–75, June 2012. doi: 10.1145/2184319.2184338.
- [Fukuyama 1995] F Fukuyama. *Trust: The Social Virtues and the Creation of Prosperity*. Free Press, New York, 1995.
- [Hasan and Salah 2019] H R Hasan and K Salah. Combating Deepfake Videos Using Blockchain and Smart Contracts. *IEEE Access*. 7:41596–41606, 2019. doi: 10.1109/ACCESS.2019.2905689.
- [Jianjun et al. 2020] S Jianjun et al. Research and application of data sharing platform integrating Ethereum and IPFs Technology. *Proceedings - 2020 19th Distributed Computing and Applications for Business Engineering and Science, DCABES 2020 (Oct.-2020)*, 279–282.
- [Jin et al. 2013] F Jin et al. Epidemiological modeling of news and rumors on Twitter. *Proceedings of the 7th Workshop on Social Network Mining and Analysis, SNA-KDD 2013 (2013)*.
- [Juola 2020] P Juola. Authorship Studies and the Dark Side of Social Media Analytics. *J. Univers. Comput. Sci.* 26:156–170, 2020.
- [Kotarski 2015] H Kotarski. *Pragmatics of social and cultural capital*. Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszow, 2015.

- [Kumar and Shah 2018] S Kumar and N Shah. False Information on Web and Social Media: A Survey. 2018.
- [Lee et al. 2018] K Lee et al. Generating synthetic bitcoin transactions and predicting market price movement via inverse reinforcement learning and agent-based modeling. *JASSS*. 21(3), June 2018. doi: 10.18564/jasss.3733.
- [Lin 2001] N Lin. *Social Capital*. Cambridge University Press, January 2001.
- [Mazzoli et al. 2018] M Mazzoli et al. Agent Based Rumor Spreading in a scale-free network. *arXiv*. arXiv.
- [Nguyen 2017] T N Nguyen. A Comprehensive Low and High-level Feature Analysis for Early Rumor Detection on Twitter. *arXiv*. arXiv.
- [Pastor-Satorras et al. 2015] R Pastor-Satorras et al. Epidemic processes in complex networks. *Rev. Mod. Phys.* 87(3), August 2015. doi: 10.1103/RevModPhys.87.925.
- [Putnam et al. 1993] R D Putnam et al. *Making Democracy Work Civic Traditions in Modern Italy*. 1993.
- [Ramadhan et al. 2021] H F Ramadhan et al. News Verification using Ethereum Smart Contract and Inter Planetary File System (IPFS). (2021).
- [Rand et al. 2015] W Rand et al. An agent-based model of urgent diffusion in social media. *JASSS*. 18(2):1–24, 2015. doi: 10.18564/jasss.2616.
- [Reimche 2018] R Reimche. Comparison of the diffusion of real and fake news in social networks. Technische Universität Kaiserslautern, 2018.
- [Shu et al. 2017] K Shu et al. Fake news detection on social media: A data mining perspective. *arXiv*. arXiv.
- [Smith and Anderson 2018] A Smith and M Anderson. Social Media Use 2018: Demographics and Statistics | Pew Research Center. <https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/>, 2018. Accessed: 2021-02-23.
- [Takyar 2018] A Takyar. How can Blockchain solve the fake news problem. <https://www.leewayhertz.com/blockchain-fake-news/>, 2018. Accessed: 2021-05-04.
- [Tambuscio et al. 2015] M Tambuscio et al. Fact-checking effect on viral hoaxes: A model of misinformation spread in social networks. *WWW 2015 Companion - Proceedings of the 24th International Conference on World Wide Web* (May.-2015), 977–982.
- [Wang et al. 2015] Q Wang et al. ESIS: Emotion-based spreader-ignorant-stifler model for information diffusion. *Knowledge-Based Syst.* 81:46–55, June 2015. doi: 10.1016/j.knosys.2015.02.006.
- [Wilensky 2001] U Wilensky. Modeling nature’s emergent patterns with multi-agent languages. *Proc. EuroLogo*. 1–16, 2001.
- [Xia et al. 2019] Z Xia et al. Research on Fair Trading Mechanism of Surplus Power Based on Blockchain. *J. Univers. Comput. Sci.* 25:1240–1260, 2019.
- [Yuan and Hu 2018] S Yuan and J Hu. A Stochastic Information Diffusion Model in Social Networks Based on SIR Epidemic Model. *DEStech Trans. Comput. Sci. Eng.* (wcne), March 2018. doi: 10.12783/dtcese/wcne2017/19836.
- [Zhang and Yu 2018] J Zhang and P S Yu. Broad Learning. *ACM SIGKDD Explor. Newsl.* 20(1):24–50, May 2018. doi: 10.1145/3229329.3229333.