Noname manuscript No.
(will be inserted by the editor)

A Blockchain-based Secured and Trusted framework for Information Propagation on Online Social Networks

Md Arquam[1], Anurag Singh[2] and Rajesh Sharma[3]

Received: date / Accepted: date

Abstract The online social networks facilitate to share information among the users based on their interests. The specific information being shared by a user may be legitimate or fake. Often, misinformation propagated by users and groups can create chaos and riots in the worst circumstances. Nowadays, a third party like ALT news and Cobrapost check the authenticity of the information, but it takes too much time to validate it. Therefore, there is a need to establish a new robust system to check the information authenticity within the network. In this paper, we envision a model for sharing the information securely at the peer level based on blockchain. In the proposed model, a chain is created by combining blocks of information. Each node in the network propagates the information based on its credibility against its peer nodes. The credibility of a node varies according to their respective information. Trust is calculated between sender and receiver using either of two ways, Local trust, and Global trust. We evaluate our model using real datasets from Facebook and Live journal as well as synthetic datasets generated by using E-R Network Model and BA Network Model. The proposed model achieves high accuracy on real-world Scale-Free networks. The simulation results validate that the model can detect misinformation (fake news or rumor), as well as the source of information propagating nodes using network parameters by applying blockchain technology without the involvement of third parties.

Keywords Blockchain, Information Dynamics, Social Network, Trust, Credibility

[1], [2]Depatment of Computer Science & Engineering,
National Institute of Technology Delhi, New Delhi, India-110040
Email: [1]arquam@nitdelhi.ac.in, [2]anuragsg@nitdelhi.ac.in
· [3]Institute of Computer Science,University of Tartu, Tartu, Estonia
Email: [3]rajesh.sharma@ut.ee

1 Introduction

Information spreading among humans is a natural phenomenon. A decade back, it happened mainly through offline interactions. However, with the web's advancement, information spreads mainly through online social media, and that too very fast as people are densely connected with each other [1]. Information that is spreading on a network may or may not be correct. Incorrect information may be termed as fake or misleading information [2]. Nowadays, social networks, like Facebook, Twitter have become popular platforms for discussion and communication among people for taking collaborative action, for example, the Arab spring uprising [3, 4] and London riots [5, 6].

Researchers have studied the dynamics of fake information spreading on social networks considering both the modeling technique as well as the mechanism to avoid fake information spreading [7]. One of the main directions in this domain is about studying the role of the online social network structure for the information spreading [8–10]. Therefore, the relationship between the dynamics of information and the structure of the underlying network is crucial in many real cases, e.g., the spreading of worms in a computer network (e.g., ransom virus on technological networks), information propagation in the online social network (e.g., rumor spreading [11, 12], opinion diffusion on social networks [13], Viral marketing on social networks. [14]).

People need correct, trusted, and authentic information on social networks. Therefore, it is important to find out the authenticity of the information. The blockchain-based methodology, which has been explored in various domains such as in biomedical [15, 16], secure data transmission in communication network [17, 18], smart energy grid [19] and most importantly developed for financial transactions of bitcoins with trusted and secured contract between two communicating parties at the peer level, can also be used for authentication and validation of the information.

1.1 Motivation

Social networks are developed mainly to provide a platform for exchanging various types of information among users. Most researchers have considered the development of information propagation model [20] and rumor spreading [11, 21] as separate topics. Due to the development of transmission media and the presence of various social networks, researchers are not able to propose an effective implicit method (that is, a method that exploits network parameters) to mitigate the dissemination of fake information in social networks. In addition, there is a void of work with respect to the exploration of a trust-based mechanism for stopping the spread of incorrect information.

Hence, a new technique is required to solve the problem of misinformation dynamics by considering verification and authentication of information and that too in the early stages of the information spreading in social networks so that immediate action can be taken to remove the unverified information. In addition, it is also important to find the source of information blast to take proper action against the misinformation originators.

There are many challenges with existing social networks, such as finding trusted friends or connections and the authenticity check of shared information, to name a few. In addition, information security and trust-based user credibility are two important aspects that need to be addressed for information propagation. A significant amount of data is published on these social platforms every day, and data privacy is becoming an important issue. Based on platforms' settings and common friends, friends' data can still be accessed by friends to some extent, which is often being added by users without any authenticity. For example, most social networking sites, such as Facebook and Twitter, rely on traditional methods to find a trusted mutual link based on mutual friendship. This method is not full proof to find trustworthy friends. Therefore, it becomes challenging for a user to trust which information is credible or not coming, being sent to them by their connections. They are on their own to find ways to check the credibility of the information. This problem becomes much more critical when the source of information is not known to the other.

1.2 Contribution

In this paper, we study the authenticity of the information propagating on social networks. To check the authenticity of the information, we proposed a blockchain-based method. The method propagates the information to its trusted peer nodes only. These peer nodes check the credibility of the information generating nodes before accepting the information. Based on credibility, information is classified as correct or incorrect. In addition, We apply the degree of the nodes as a network parameter of the underlying topology of the network to define the smart contract for a blockchain-based method rather than using the fixed virtual credit for each node. Using this methodology, we can also find the source of information generating nodes, which is very useful in case of misinformation propagation. We evaluated our approach on real-world network datasets: i) Facebook social network and ii) Live journal social network and the synthetic networks: i) E-R network model and, ii) BA model of a scale-free network.

The rest of this paper is organized as follows: Section 2 discusses the current state of arts regarding information dynamics on social networks and blockchain applications other than bitcoin. Section 3 explains the proposed methodology that includes blockchain in information propagation on the social network by cons. Section 4 presents the simulation and result analysis. In this section, we have simulated the model to get the result. Finally, Section 5 describes conclusions and outlines some of our future directions.

2 Related Work

In this section, we first present various works related to social networks, including trusts on social networks, the concept which is an integral part of our framework (Section 2.1), and later, we describe the related work of the blockchain technology and their application (Section 2.2). Finally, we have explored the application of blockchain beyond cryptocurrency (Section 2.3)

2.1 Social networks

Nowadays, many Online Social Networks (OSN) exist and observe the emergence of new online social platforms day by day. The primary reason for the presence of large social networks is due to the fact that they play a crucial role in personal and commercial online interactions, and most importantly, they play an important role in finding the source of information and knowledge [22]. In particular, OSNs such as Facebook, Twitter and, LinkedIn are popular platforms where people around the world get connected and share information with each other [23]

Each social network contains user profiles, a list of connected users called friends, and their topic of interests [24]. According to their interests, users share information on these online social platforms. Therefore, social networks provide a base to maintain social relationships among people around the world, find other users with similar interests, and find the content shared by other users [25]. Every person has a certain mindset for the propagation of information according to the topic of interest. Further, each user in a social network creates trust with its neighbors at a peer level before sharing the information. Trust is a measure of confidence in social networks, and it provides information about the neighbors with whom one may share/accept information [26]. Therefore, trust in social networks has attracted much attention to opinions formation [27], recommendation [26], viral marketing of products [28, 29].

Each node is connected to its peer nodes based on some common interests in the social networks. The information is propagated from one node to its peer nodes and furthermore. In this way, information is propagated in the social network based on connectivity [11]. Therefore, the study of underlying network topology is also important. The study of social networks includes both the dynamics on the network as well as underlying network topology [21]. It has been noted that most of the social networks are scale-free in nature [30] with long-tail degree distribution.

2.2 The Blockchain Technology

A blockchain is a collection of blocks connected in sequential order with respect to time, as shown in Figure 1. Each block carries the respective record of the transaction with a timestamp, as shown in Figure 2. This chain is created for the propagation of records of a node with other connected nodes in a peer-to-peer network. The design of blockchain prevents the modification of data and validates the records due to continuous hashing of blocks [31]. This block of the record is propagated based on the trust created in the blockchain.

The trust mechanism of blockchain is dependent on a smart contract. Smart contracts are self-executing contracts having certain conditions among peer users. Once those conditions are met, the terms of the agreement are automatically executed. In particular, smart contracts increase the trust within blockchains due to Immutability and Distribution [32,33]. Due to this immutability, a block cannot be tempered. More specifically, the issue of developing a distributed storage system for timestamped documents in which no party can tamper with the data or timestamps without be-

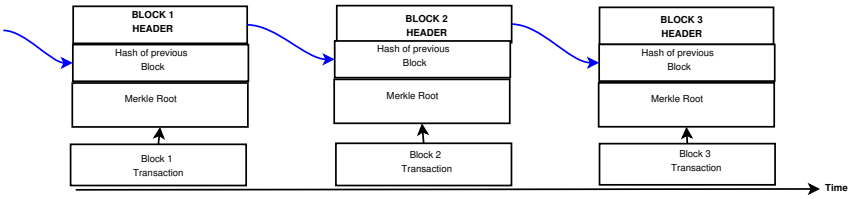

Fig. 1 Structure of Blockchain used in Bitcoin

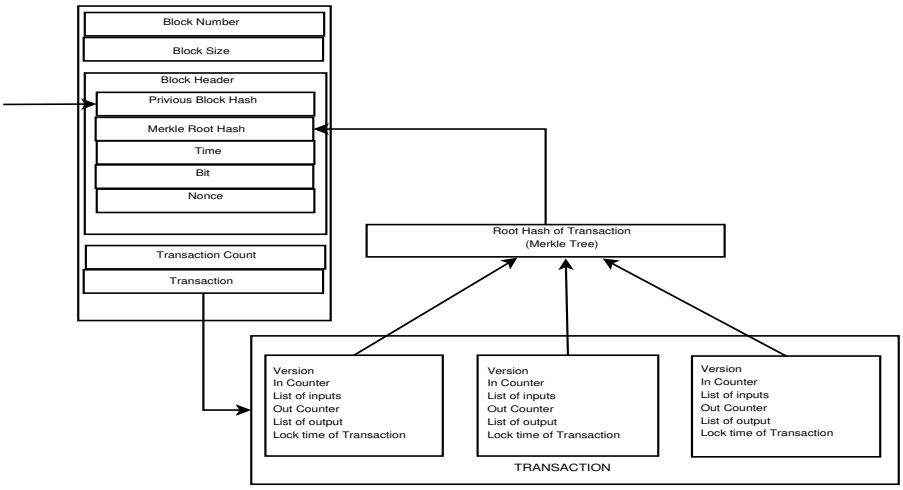

Fig. 2 Structure of Block which contains the information about the transaction used in Bitcoin Blockchain [37]

ing detected. The timestamp, however, needs confidence in the party who signed the document. Time is of the essence in financial transactions, and other types of legal contracts and the order of such financial transactions must be independently certified in order to be auditable [33, 34].

Researchers have investigated the blockchain to create a decentralized network. In such types of networks, there is no need for a third party for authentication and validation. An automated access control manager is used instead of a third party. The access manager is enabled by distributed blockchain system [35]. Also, researchers have applied the concept of blockchain in the utilization of cloud storage by combining blockchain and IoT (Internet of Things) [36]. The other area of applications of the blockchain other than an online transaction is identity management and notarization [35].

In [38], authors presented centralized blockchain architecture to tackle the spreading of fake news. Each block is used as an object in their architecture, and inside each block, related information is stored. This object is shared with each source. They maintained transparency to users through this type of structure, ensuring that the host cannot change the information stored in the blockchain. Their work did not explore

the trust among neighbors by considering the underlying network topology. In a different work, researchers provided a review and direction on implementing blockchain on social media to build trust and prevent fake news [39]. Jing et al. proposed a theoretical framework to use the blockchain technique in social networks for trusted and credible news propagation. They applied the AI-based plugin for social networks to use blockchain technology to authenticate the news. The authors also explained the various challenges to build trust to prevent fake news using blockchain [40].

Akshada et al. have used the immutability and security feature of blockchain to trace the originator of news. By using the immutability of the blockchain, no one can change the identity of the originator of news. They develop the system to help the news channels to provide authentic articles [41]. In a different work [42], authors studied the tracing of the source of news by using the information stored on the distributed, decentralized, and other features of the blockchain. They combined the consensus algorithm and intelligent contract with the traditional data tracing technology to analyze the tracing of the news source. Qayyum et al. explored the various design issues of the blockchain-based framework for fake news prevention. They highlighted the techniques used to detect and mitigate fake news by using the blockchain-based framework [43]. Anik et al. proposed a secure news trading technique on the network by using blockchain-based privacy. They used pseudonymity, fault-tolerance, immutability, and the distributed structure of blockchain to develop a system named NEWSTRADCOIN to share the news [44].

2.3 Application of blockchain in other domain beyond cryptocurrency:

Researchers have used the trust mechanism of blockchain by considering applications dependent parameters in various applications. We discuss some applications below

A) Supply Chains: In supply chain management, the blockchain is used by suppliers to store the origins of materials that they have purchased. Along with popular labels like ”Organic,” ”Local,” and ”Fair Trade,” this enables businesses to check the authenticity of their goods. [45–47].

B) Health care: In data privacy and protection, blockchain models are used in electronic health record systems (EHRS), where patient data is processed using blockchain security [48, 49].

C) Energy Sector: The current energy infrastructure for mass production is primarily based on the premise that access to knowledge about the sources, allocation, and energy consumption is prohibitively costly. However, in recent years, the movement towards more decentralized energy solutions has accelerated, and sensor data collection has become more affordable. For these reasons, researchers have developed many energy system paradigms considering blockchain-based trust mechanism [50, 51].

D) Bank and Insurances: In this use case, blockchain and smart contracts are exploited to increase the speed of claim processing as well as to reduce the costs (and mistakes) associated with the manual processing of claims. From this perspective, a smart contract could encode the rules for enabling the transfer of refund from the company to the insured [52, 53].

E) E-Government: Bitcoin satisfies most of the fundamental criteria for an information system, putting it in a strong position to influence future digital innovation. Using the blockchain to store and secure certificates is a cost-effective method of doing so. This is true for certificates, but it may also be a promising technology for all forms of permanent or semi-permanent public records. Given its information technology capability, other examples may include various types of contracts (e.g., procurement contracts), licenses (e.g., driver's licenses), and several more [54, 55].

3 Proposed Methodology

In this section, first, we describe the network model as a decentralized network and evaluate the trust values of the nodes by considering the degree of a node as a network parameter. If the trust value is high, then the reputation of the node will be more, and it will be considered as reputed and unharmful. The trusted node will provide a safe and reliable environment for others. Based on the trust, we define the credibility score for each node according to the topic of interest of the information type. A credible node may be trusted and will be influential with a good reputation among other nodes. Finally, we explain blockchain-based information propagation. In the proposed work, we consider social networks as decentralized networks. Let, an agent **A**, has limited interests in various topics. For example, **A** is very good in science and technology-related subjects in combination with other subjects; hence, he shares most of the time science-related information to other individuals in the network. Simultaneously, **A** is a movie-loving individual also. Then he has a specific association with some other movie-loving users. Further, **A** also talks about religion. Therefore, he has a connection with religious users. It clearly shows the different forms and contexts of **A**, and **A** effortlessly glides from one to the other.

We consider the network as an undirected graph, $G = (V, E)$, where V is set of n nodes, such that $V = \{V_1, V_2, ...V_n\}$, each node is attached through a set of limited connections with other nodes, which represents its neighbors. E is the set of edges, where each edge $e_{ij} \in E$, connects a node V_i with the node V_j. I and C are used to represent a set of information type and credibility set of nodes, such that, $I = \{I_1, I_2, ...I_4\}$ and $C = \{C_1, C_2, ...C_n\}$, where $C_j = \{I_{j_i}, V_j\}$. Each node V_j has a particular credibility $C_{(I_{j_i}, V_j)} \in C$. It has global impact on network and different from trust.

3.1 Trust Relationship

A blockchain-based secured and trusted framework for information propagation on online social networks model is proposed. We consider trust relationships among the users. The aim of introducing trust among the nodes is to find a suitable user to validate or invalidate the information in order to propagate the information. Each user, V_i, keeps track of a trust value T_{V_i,V_j} with each of its neighboring users, V_j. Trust may be considered in two ways; one is a local trust (or private trust) between two communicating nodes and, the other is the global trust (or public trust), in which a

source node broadcasts the information in the network about the type of information which he has. Local trust is defined in the form of a Pearson correlation coefficient by using the network parameter. In global trust, credibility score is used for authentication of information. The trust value between the nodes is changing with time. Here, in this paper, the initial (at time $t = 0$) value of the trust is calculated through local trust, and then it will be used for global trust calculation.

3.1.1 Local Trust

The local trust exists only among current neighbors of a node in the network. Local trust is based on the physical properties of the network, where a node makes a connection with a similar type of node. The value of local trust between two nodes has been evaluated with the help of degree-degree correlation (DDC). The DDC is a network property that measures the tendency of the nodes to connect with other nodes based on similarity or dissimilarity. The correlation coefficient's value decides the structural similarity (or dissimilarity) of the nodes in the network. The Pearson correlation coefficient is used to calculate local trust and is given by,

$$T_{s,r}^{(0)} = \frac{\sum_k (A_{ik} - \langle A_i \rangle)(A_{jk} - \langle A_j \rangle)}{\sqrt{\sum_k (A_{ik} - \langle A_i \rangle)^2} \sqrt{\sum_k (A_{jk} - \langle A_j \rangle)^2}} \tag{1}$$

where, $T_{s,r}$ is Pearson coefficient,
$\sum_k A_{ik}$ is k number of neighbors of i
$\sum_k A_{jk}$ is k number of neighbors of j
$\langle A_i \rangle = \frac{1}{n} \sum_k A_{ik}$
$\langle A_j \rangle = \frac{1}{n} \sum_k A_{jk}$
The value of parameter $T_{s,r}$ lies strictly in the range of $[-1, 1]$. This Pearson correlation coefficient is used as local trust because it gives the node similarity in the network. To propagate information, we select the information generating node as V_s. The value of the local trust helps to decide whether the information should be propagated or not. The detailed description is provided in Algorithm 1.

Algorithm 1: Information propagation through local trust

```
Result: Peer nodes will accept or reject information
Input: T^0_{s,r}, V_s, where, V_s is information generating node ;
while (k! = Ne(V_s)) do
    if (T_{s,r} < 0) then
        return False;   # information will not be accepted by peer node;
    else
        makeBlock(message);   # information block is created;
        chain.append(makeBlock)   # Chain is created by adding block;
        propagate(message);   # information will be accepted by peer node;
    end
end
```

3.1.2 Global Trust

The global trust of the nodes is updated based on some parameters: the nodes involved in the information propagation, the type of information propagated, and the node's credibility score. Information propagated with credibility is used as proof of a contract to all available nodes of the information exchange, which is used for decision-making.

An information generating node V_s propagates information according to its credibility and interest in the topic. Suppose an information with credibility $C^t_{(I_{s_i},V_s)}$ is created to propagate at time t. If a node has k neighbors, then this information is reached to all k neighbors. However, all the neighbors do not have the same interest in the topic of information propagated. Only those nodes will validate the information who have the same interest topic-wise. Therefore, a threshold value of the credibility score is set to validate the information, and only the correct information will be propagated. When information is propagated, decisions about information are taken to propagate or block, based on the credibility of nodes and topic of interest. When a source node V_s generates information i a block of information $Block_i(t)$ is created at each time t, which contains information propagated to each neighboring nodes $Ne(V_s)$ with its credibility $C_{(I_{s_i},V_s)}$

$$\forall i : Block_i(t) = C^t_{(I_{s_i},V_s)} \tag{2}$$

Where, $Block_i(t)$ is the block of information , $C^t_{(I_{s_i},V_s)}$ is a particular type of information generated at time t by . A global trust between sender (s) and receiver (r) nodes can be defined as [56],

$$T_{s,r} = T^0_{s,r} + \frac{\sum_{j\in Ne(j)|T_{s,j}} T_{r,j}T_{j,s}}{\sum_{j\in Ne(j)|T_{r,j}} T_{r,j}} \tag{3}$$

Where $T_{s,r}$ is a trust between sender and receiver nodes, $T^0_{s,r}$ is the initial value of trust of a sender node. The Eq. 3 is used to calculate the trust between two communicating nodes; if the information is validated, then $T^0_{s,r}$ is updated, and the trust value of the source node is increased. Each receiver node repeats this process to know the depth of the current node from the source. If information is not validated, then the trust value will be negative and decreased as in Eq. 4,

$$T_{s,r} = T^0_{s,r} - \frac{\sum_{j\in Ne(j)|T_{r,j}} T_{r,j}T_{j,s}}{\sum_{j\in Ne(j)|T_{r,j}} T_{r,j}} \tag{4}$$

Finally, validation of information is done by the peer nodes by considering their average credibility for the information. Therefore, the credibility of a node changes according to validation. For the set of nodes $Ne(V_s) \in V$ used for the validation, the

credibility score $C_{(I_{s_i},V_s)}$ of source node V_s according to information of interest I_i changes by considering from source to each node at peer level,

$$C^{t+1}_{(I_{s_i},V_s)} = \frac{\sum_{j \in V_n} T_{s,j} * C^{t}_{j(I_{s_i},V_s)}}{\sum_{j \in V_n} T_{s,j}} \tag{5}$$

Where, $C^{t+1}_{(I_{s_i},V_s)}$ is the new credibility score of a source node with respective information I_i. This credibility score will be constant until the next propagation. If the credibility of this information is greater than the threshold, then the information will be propagated else blocked. A threshold value of the credibility will be calculated by considering the average credibility score of neighbors interested in the similar topic of interest of a propagating node, which is used to validate the information at the peer level, where, $Avg\_cred = \sum_{j \in Ne(V_s)} \frac{C_{j_{(I_{s_i})}}}{|Ne(V_s)|}$

Based on global trust, algorithm 2 is used for information authentication and propagation:

Algorithm 2: Global Trust based information validation

```
Result: peer nodes will authenticate or validate the information
Input: C^t_(I_si,Vs), I_i, information generating nodes V_s ;
while (j! = |V_n|) do
    if (C^t_(I_si,Vs) ≥ Avg_cred) then
        return True;  # information will be validated by peer node;
    else
        return False;  # information will be blocked by peer node;
    end
    checkChain(chain);
    checkBlockHash(block);
    update C^{t+1}_(I_si,Vs);
end
```

3.2 Blockchain based Information Propagation in Social Network

This section explains the information propagation in social networks through the blockchain method. In the social network, information can be propagated from one node to another through direct or indirect connection. However, the information may not always be right. It may be modified or wrong or maybe a rumor. Hence, it is required to check the authenticity of the information. Nowadays, a third party like Alt news or Cobrapost generally checked the information authenticity on the social network. The authentication process through the third party is itself a time taking process for a large-scale network.

Therefore, a system is required which checks the authenticity of the information implicitly on the network. To do this, we have taken the idea from blockchain technology used in a financial transaction without using any third party. In our approach,

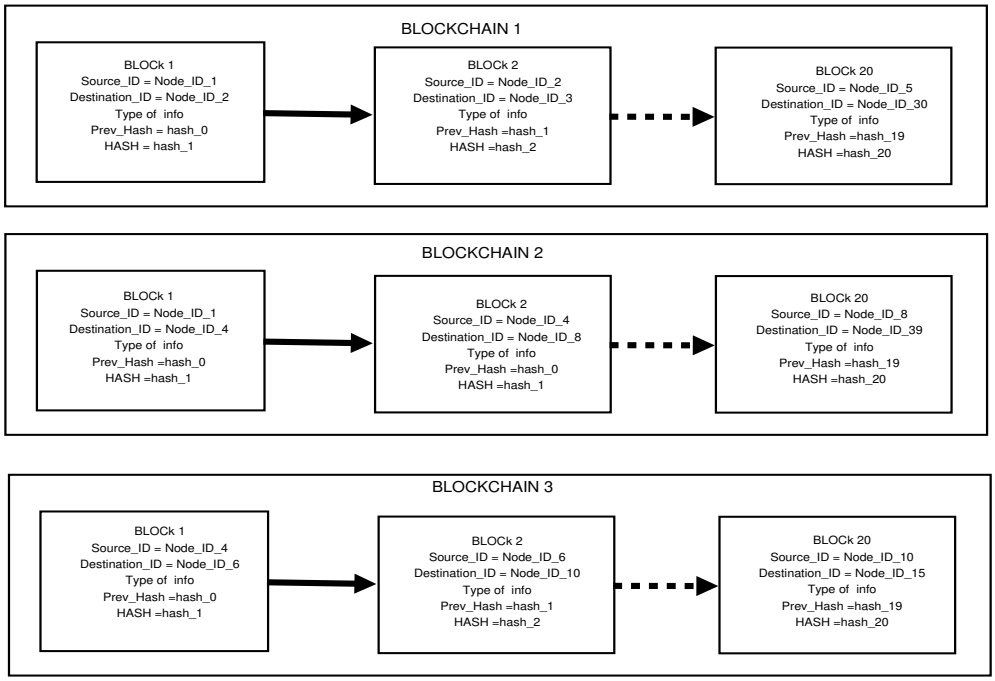

Fig. 3 Blockchain based Information Propagation where each block carries type of information with hash of previous block to form a chain of 20 blocks. Each block contains hash of previous block. In this way we can trace the root source of information generation.

each user in the network is assigned some resources, i.e., information propagated in the form of blocks, as shown in Figure 3. Each block has three main parts, i.e., type of information, message, and lock time of propagation, as shown in Figure 4.

We define two entities for authentication and propagation of information in the network.

- Node Property(NP) is defined in the form of a vector having the identity of the node, $Node\_ID$, credibility score, $Credibility$, and type of the information, $Info\_Type$
  $NP = \Big([Node\_ID, Credibility, Info\_Type]\Big)$
- Node service(NS) is defined as the available information and local trust
  $NS = \Big([Information, Local\_Trust]\Big)$

Blockchain-based information dynamics proposes a new method to propagate information and node identity to peer nodes, allowing each component of the network to verify the information about nodes in the network. Blockchain-based information dynamics link cryptographic keys with each NP and NS in the network. We are using the same model of Bitcoin to identify an NP or NS among the network.

We consider each propagated information as an event like "transaction in bitcoin," providing information about the status of a NP and its cryptographic information

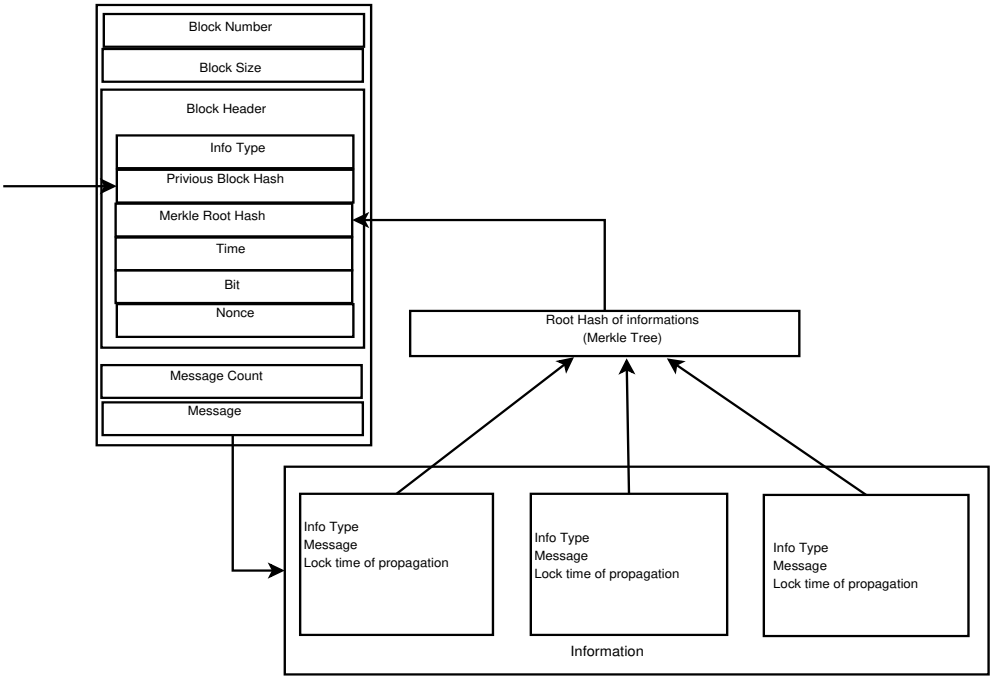

Fig. 4 Structure of Block used in Information Propagation in which each block contains type of information and time of information generation along with other detail shown in Figure 3 and 5

containing NS. When a node propagates the information, it submits the credibility score and information type in the network also. When a node wants to propagate information in the network with his NP for the first time, it generates a specific information block $(SIMB)$ containing NP to all nodes. An authentication request is approved when an authenticated NP includes the $(SIMB)$ in a valid block. The credibility score of the nodes can be updated as per their NS by $Verify\_MB$ and $Block\_MB$. There are four types of information block used in this approach for information propagation, as shown in Figure 5.

- SIMB: This information block is used when a node wants to share information in the network.
- Minor MB: This information block is used to validate the blocks to be in the chain.
- Verification MB: This information block is used for verification of information.
- Blocking MB: This information block tells about the misinformation generated by a node.

Note that when information is not authenticated and blocked, a NP/NS must provide a new credibility score to those nodes that have generated the information in the network. Neighbor nodes, those are involved in authentication, also called Minor nodes in bitcoin, will try to include $Block\_MB$ and new credibility score in the same block to ensure continuity of node status in the network. If a node wants to propa-

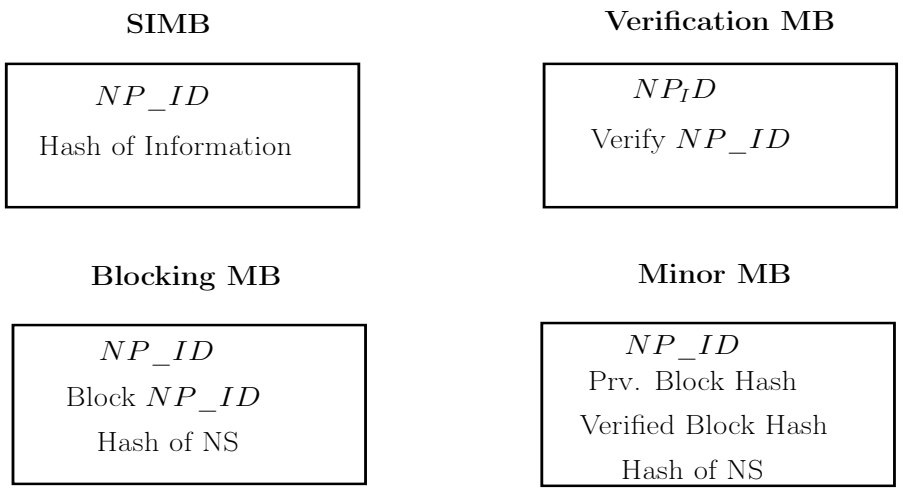

Fig. 5 Different types of Information Block used for verification and validation.

gate information without further verification, every node will generate its information block in the network. This will create ambiguity to identify the source node of the information propagation. To overcome this issue, every information block must have a hash block with NP in its entry.

The root of information generation can be traced using blockchain through the time stamp services and connection between blocks. In the blockchain, each block has two parts, header, and body. The block body contains the content of the current block and stores the information through the hash. The header contains the current block header hash and previous block header hash with other details. This header helps to trace the root of information generation. The blocks are chained in sequential order according to the time stamp. When information is not authenticated, then the chain is examined by block number. Due to continuous hashing, no one can change the identity of the information generating node. Once block one is reached, the root of information generation is found. We have calculated the average level of detection of each false information. The average level of detection is calculated using the level of detection of each fake information divided by the total number of nodes generating fake information.

4 Result and Analysis

In this section, we first explain our experimental settings, and next, we discuss the results of our simulations performed using *blockchain-based information propagation* considering various underlying network topologies.

4.1 Analysis on Real World Datasets

We have taken two real-world network datasets that is Facebook dataset [57] and LiveJournal social network [58], describe in Table 1. Both of these networks show scale-free property. For interest assignment, we relied on a survey conducted by **PEW Research Center**, which has reported that 66% of social media user discuss politics, 58% share and talk about the movie, 53% user argue about research, 68% user share information about science and technology. [22]. Taking inspiration from this **PEW Research Center** report, the distribution of topics among nodes followed by using the same pattern. For each node's interests, the initial credibility value is assigned randomly between [0,1]. For example, a person might be more interested in information about movies compared to information related to R&D. Thus; his credibility will be high for movies-related information as compared to R&D. In addition, we have taken 100 seed nodes which are used as originators of the information.

We perform the simulations to illustrate the proposed model for secure and trusted information propagation on the above two mentioned real social network datasets.

Table 1 Facebook and Live Journal Network Dataset statistics

Name of Parameter	**Facebook**	**Live Journal**
Nodes	46952	3997962
Edges	876,993	34681189
Average clustering coefficient	0.0851	0.2843
Mean Shortest Path	5.7	6.5
Number of triangles	122,852	177820130

We generate the block of information in the same manner as in bitcoin methodology, where a block is created once a transaction is initialized in the bitcoin blockchain. We restricted the creation to a maximum of 20 blocks for each information-generating node. Each block contains the nodes ID, credibility score, info type, and message along with the hash. Every block is added to the chain once it is authenticated. In this course of the simulation, the number of fake information generation nodes is detected at various levels depending on the underlying network topology based on credibility. The number of nodes which is detected as fake information generating node is listed in Table 2.

Table 2 Analysis of Fake Information on Real World Network Datasets

Network Type	Network name	Number of Node Detected
Real World Network Datasets	Facebook	17
	Live Journal	11

Finally, we analyze the authenticity of the information considering the underlying network topology of the Facebook dataset, and 83% of information is found correct, which includes all four types of categories considered in our simulations. We got the

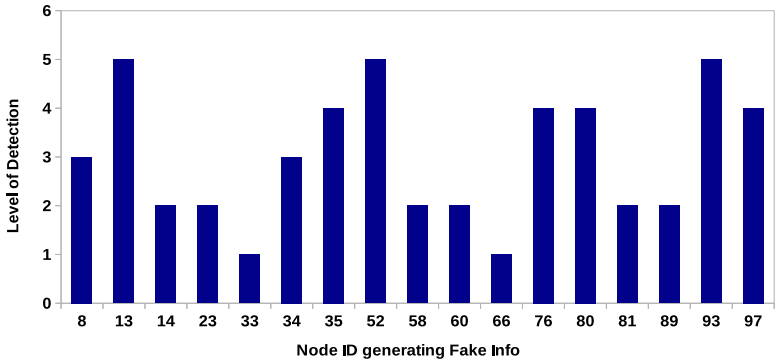

Fig. 6 Level of Detection of Fake Information generated by various nodes considering Facebook Dataset. Here, Node_ID is represented on X-axis while the level of detection is shown on Y-axis.

best results for movies, followed by politics, research-related information, and finally technology-related information. Among all the information, mostly fake information is related to politics and research. Our proposed model is also able to identify the originators of the information as it is not feasible to change the identity of the block generated by a particular node due to the continuous hashing of blocks in the chain.

We check the authenticity of information up to 6^{th} hop from the information generated nodes. If the authenticity of information is checked up to 6^{th} hop, then information is classified as valid otherwise invalid. We also found the level of detection for the authenticity of information generated by nodes at various levels, as shown in Figure 6. This result explains the detection of the source of fake information propagating nodes at various levels. The average level of detection is also listed in table 3. This table shows that the movie-related information is checked at the maximum level, and the technology-related information is checked as early as possible. The average level of detection for political and research-related information is the same, that is detected at level 3. Technology-related information is detected at level 2, while the level of detection of movies related information is 4.

Table 3 Average Level of Detection of Fake Information and Number of Nodes generating fake information ((Facebook Dataset)

Info Type	**Average Level of Detection**	**Number of Nodes generating fake information**
Politics	3	6
Technology	2	1
Research	3	6
Movie	4	4

We have plotted the frequency of nodes generating all four types of categories of information considered in our simulations, shown in Fig. 7. Total nodes, which are detected as fake information generating nodes, are seventeen. Movie-related fake

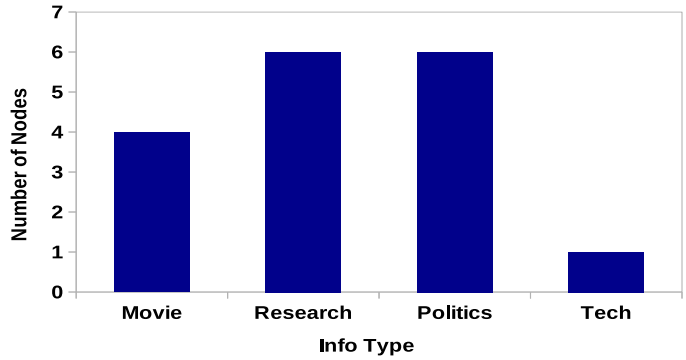

Fig. 7 Number of Nodes detected for the generation of Fake Information considering Facebook Dataset. Here, the number of nodes is represented on Y-axis while information type is shown on X-axis. It is used to explain the number of nodes that indulge in a particular type of fake information propagation.

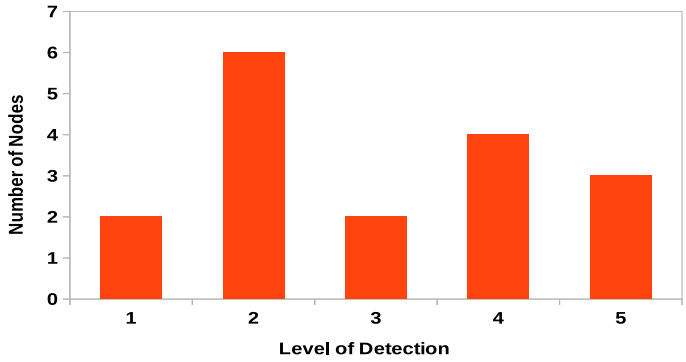

Fig. 8 Number of Nodes detected for the generation of Fake Information considering Facebook Dataset. Here, the level of detection is represented on X-axis while the number of nodes is shown on Y-axis. It is used to explain the number of nodes detected at various levels during fake information propagation.

information generating nodes is 4, research-related and politics related to fake information is propagated by six nodes, and technology-related information is propagated by one node. We have plotted to explain the number of nodes detected at various level. 2 nodes are detected at level 1 and 3 while six nodes are detected at level 2. 4 nodes are detected at level 4, and 3 nodes are detected at level 5 during fake information propagation, shown in Fig. 8.

We also analyze the information authenticity by using Live journal social network as underlying topology and found that 89% information is checked correctly that includes different types of information the level of detection for the authenticity of information at the various level as shown in Figure 9. This result shows that the movies and politics-related information are checked at the maximum level, and the technology-related information is checked as early as possible. The average level

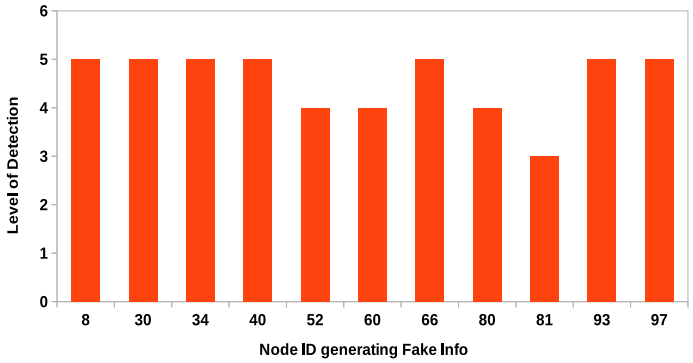

Fig. 9 Level of Detection of Fake Information considering Live journal Dataset. In this figure, Node_ID is represented on X-axis while level of detection is shown on Y-axis. It is used to explain that mostly nodes are detected at 5^{th} level.

of detection is also listed in table 4. The average level of detection for political and movies related information is the same, that is detected at level 5. Technology-related information is detected at level 4, while research-related information is correctly passed up to 6^{th} hop.

Table 4 Average Level of Detection of Fake Information and Number of Nodes generating fake information (Live Journal Social Network)

Info Type	**Average Level of Detection**	**Number of Nodes generating fake information**
Politics	5	4
Technology	4	2
Movie	5	5

We have plotted the frequency of nodes generating all four types of categories of information considering the Live journal network with the Node ID, shown in Fig. 10. Total nodes, which are detected as fake information generating nodes, are 11. Movie-related fake information generating nodes are 5, politics related to fake information is propagated by four nodes, and technology-related information is propagated by two nodes. We have plotted to explain the number of nodes detected at various levels. One node is detected at level 3 while, seven nodes are detected at level 5. Three nodes are detected at level 4 during fake information propagation, shown in Fig. 11

One important finding is that when the number of nodes is large enough, the accuracy level is increased, but the average level of detection is also increased. The average level of detection is 5 in the case of live journal network as underlying topology as compared to Facebook network in which the average level of detection is 3. The increase in detection level in the live journal network is due to the Mean Shortest

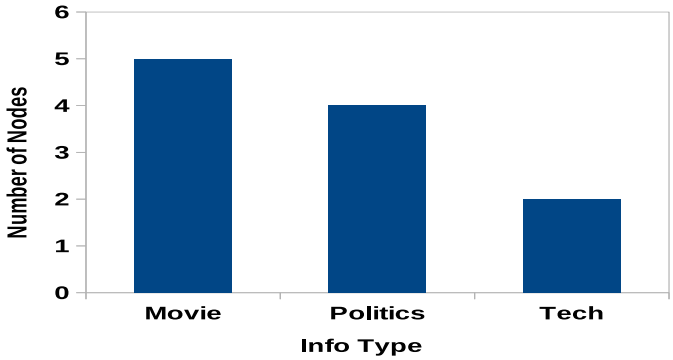

Fig. 10 Number of Nodes detected for generation of Fake Information considering Livejournal Dataset. In this figure, number of nodes are represented on Y-axis while information type is shown on X-axis. It is used to explain about the number of nodes indulge in particular type of fake information propagation.

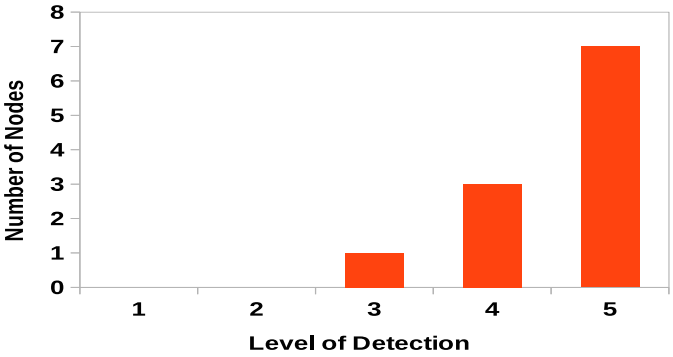

Fig. 11 Number of Nodes detected for the generation of Fake Information considering Livejournal Dataset. In this figure, the level of detection is represented on X-axis while the number of nodes is shown on Y-axis. It is used to explain the number of nodes detected at various levels during fake information propagation.

Path of the network, which is 6.5 compared to Facebook, where, Mean Shortest Path is 5.7.

4.2 Analysis on Synthetic Network

We also perform experiments on two synthetic networks considering the random network and BA model of a scale-free network. To generate a random network and scale-free network, we consider various parameter as listed in Table 4

We analyze the information authenticity by considering the scale-free network as underlying topology using 2000 nodes with 100 nodes as seed nodes, which is

Table 5 Simulation Parameter for Synthetic Network

Name of Parameter	**Value**
Nodes	2000
$Cred\_Score$	random (0-1)
$Info\_type$	[Politics, Technology, Movie, Research]
Connecting probability (p) (for E-R model)	0.2
Number of edges to attach from a new node to existing nodes (m) (for BA Model)	10

used as the originator of the information. We create blocks of information, consisting of the nodes ID, credibility score, info type, and message along with the hash. We restricted the creation to a maximum of 20 blocks for each information-generating node. Blocks are added in the chain after authentications. In these experiments, the number of fake information generation nodes are detected at various levels depending on the underlying network topology based on credibility. The number of nodes which is detected as fake information generating node is listed in Table 6.

Table 6 Analysis of Fake Information on Synthetic Network as Underlying Network Topology

Network Type	Network name	Number of Node Detected
Synthetic Network Datasets	Scale-Free Network	11
	E-R Random Network	23

Furthermore, we found that 89% information is checked correctly up to 6^{th} hop or level. If the information is validated up to 6^{th} hop, then information is classified as correct otherwise incorrect. In addition, we also found the level of detection for the authenticity of information generated by the source node at various levels, as shown in Figure 12. This result shows that the movies related information is checked at the maximum level, and the other types of information are checked as early as possible. The average level of detection and Number of fake information generating nodes are also listed in table 7. The average level of detection for technical, political, and research-related information is the same, that is detected at level 2, while the level of detection of movies related information is 4.

We plot the frequency of nodes generating all four types of categories of information considering the BA model of scale-free network with the Node ID, shown in Fig. 13. Total nodes, which are detected as fake information generating nodes, are 11. Movie-related fake information generating nodes are 2, research-related and politics related to fake information is propagated by four nodes, and technology-related information is propagated by one node. We have plotted to explain the number of nodes detected at various levels. 2 nodes are detected at levels 2 and 3 while four nodes are detected at level 4. Three nodes are detected at level 5 during fake information propagation, shown in Fig. 14

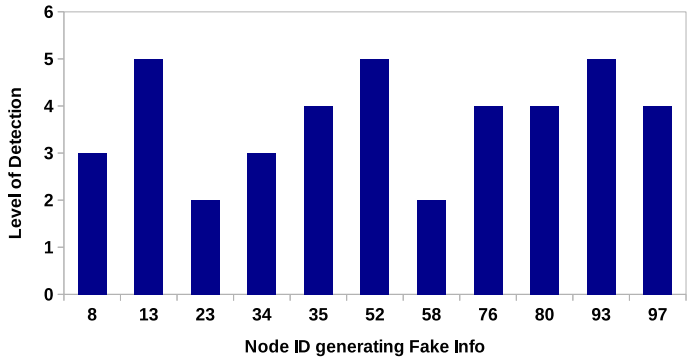

Fig. 12 Level of Detection of Fake Information considering BA model of Scale-Free Network of 2000 Nodes. In this figure, Node_ID is represented on X-axis while the level of detection is shown on Y-axis. This explains that most nodes are detected after 4^{th} level.

Table 7 Average Level of Detection of Fake Information and Number of Nodes generating fake information (BA model of Scale-Free Network)

Info Type	**Average Level of Detection**	**Number of Nodes generating fake information**
Politics	4	3
Research	3	5
Movie	4	4

We also analyze the information authenticity by considering the random network as underlying topology by using 2000 nodes with 100 seed nodes and found that 77% information is checked correctly to 6^{th} hop. If the information is validated up to 6^{th} hop, then information is classified as correct otherwise incorrect. We also investigate the level of detection for the authenticity of information at various levels, as shown in Figure 15. This result shows that the movies and politically related information is checked at the maximum level, and the technology and research related information is checked as early as possible. The average level of detection is also listed in table 8. The average level of detection for political and movies related information is detected at level 4, while technology and research-related information are the same, is detected at level 3.

We have plotted the frequency of nodes generating all four types of categories of information considering the ER model of random network with the Node ID, shown in Fig. 16. Total nodes, which are detected as fake information generating nodes, are 23. Movie related to fake information generating nodes is 7. Research related and politics related to fake information are propagated by 5 and 9 nodes, respectively, while technology-related information is propagated by two nodes. We have plotted to explain the number of nodes detected at various levels. One node is detected at level 1 while four nodes are detected at level 2. 8 and 7 nodes are detected at level 3

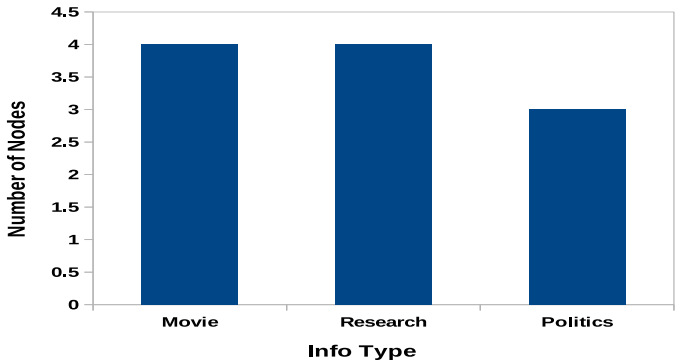

Fig. 13 Number of Nodes detected for the generation of Fake Information considering BA model of Scale-Free Network of 2000 Nodes, where only three types of information propagating nodes are detected that are Movie, Research, and Politics related information. In this figure, the number of nodes is represented on Y-axis while the information type is shown on X-axis. This is used to explain the number of nodes involve in a particular type of fake information propagation.

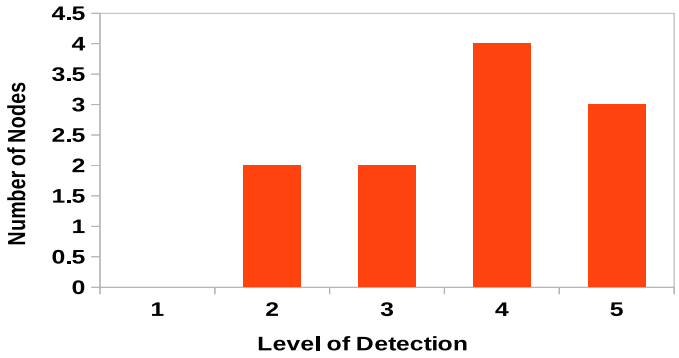

Fig. 14 Number of Nodes detected at various levels during fake information propagation considering BA model of Scale-Free Network of 2000 Nodes. Here, the level of detection is represented on X-axis while the number of nodes is shown on Y-axis. It is used to explain the number of nodes detected at various levels during fake information propagation.

and 4 respectively while, two nodes are detected at level 5 during fake information propagation, shown in Fig. 17

The most important finding we get by using the random network and the scale-free network is that detecting false information in the random network is difficult compared to the scale-free network due to homogeneity in the degree distribution of nodes in the random network. Due to the homogeneous degree distribution of nodes in the random network, all nodes have the same local trust with neighbors. Hence, each node propagates its information to its peer nodes and so on.

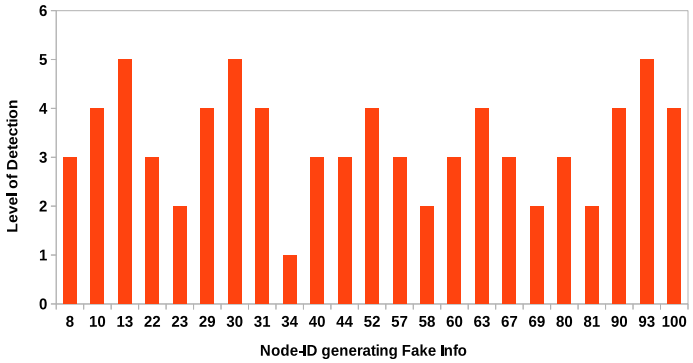

Fig. 15 Level of Detection of fake Information considering ER model of Random Network of 2000 Nodes. In this figure, Node_ID is represented on X-axis while the level of detection is shown on Y-axis. This explains that most nodes are detected after 3^{rd} level.

Table 8 Average Level of Detection of Fake Information and Number of Nodes generating fake information (ER model of Random Network)

Info Type	**Average Level of Detection**	**Number of Nodes generating fake information**
Politics	4	9
Technology	3	2
Research	3	5
Movie	4	7

5 Conclusion

The traditional methods of fake information detection are unable to find the source of the information generator in social networks. In this work, we proposed a blockchain-based approach for information propagation. In our proposed model, we have created the contract based on network parameters. When nodes at the peer level agree with local trust calculated by using the Pearson correlation coefficient, then information is accepted by peer nodes. Based on this local trust, we have derived global trust for the validation of information by peer nodes. If the global trust meets the criteria of validation of information, it is further propagated; otherwise, information is discarded and assumed as fake or rumor. Our proposed model can be used to stop rumor and fake information propagation without involving third parties The experiments show that it is impossible to change the information generator's source due to the hash. Once information is propagated, its' authenticity is checked implicitly by using the network parameter. Therefore, we no longer require a third party for information verification. We have simulated our approach using a real Facebook dataset and Live Journal Social Network, on which we achieved an accuracy of 83% and 89%, respectively. In addition, we have also simulated our approach using the synthetic networks of the E-R network model and BA model of a scale-free network, on which we achieved an

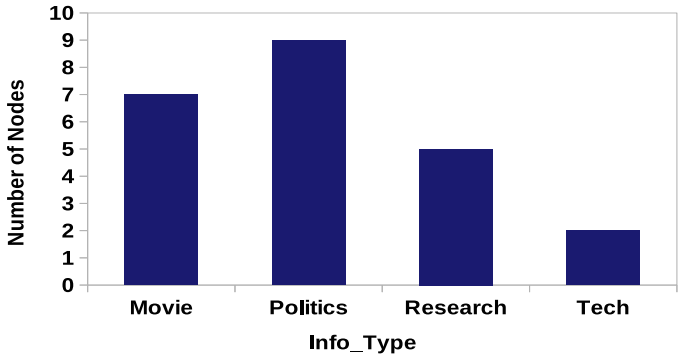

Fig. 16 Number of Nodes detected for the generation of Fake Information considering ER model of Random Network of 2000 Nodes. In this figure, the number of nodes is represented on Y-axis while the information type is shown on X-axis. This explains the number of nodes that indulge in a particular type of fake information propagation, where most nodes are involved in politics-related fake information propagation..

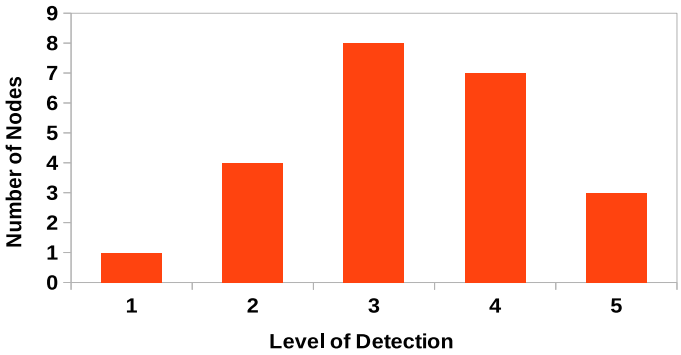

Fig. 17 Number of Nodes detected generating Fake Information considering ER model of Random Network of 2000 Nodes at various level. In this figure, the level of detection is represented on X-axis while the number of nodes is shown on Y-axis. This is used to explain the number of nodes detected at various levels during fake information propagation.

accuracy of 77% and 89%, respectively. Simulations based on realistic datasets are performed in order to get a better understanding of the blockchain-based secure and trusted framework for information propagation.

We plan to include various future directions for this work. A significant addition is to consider a more realistic scenario by considering the different interactions between nodes such as modular networks and dynamic networks [59, 60]. Another direction could be to understand the propagation behavior of information in the social network using various larger network datasets. We will work to find the propagation behavior of information in a directed social network like Twitter. The mobility and spatial distribution of the host population [61] on information propagation may also be ex-

amined. In the future, we are planning to develop a prototype of OSN considering the proposed framework, which is based on blockchain.

6 Acknowledgments

This work is supported by H2020 framework project, SoBigData++, and CHIST-ERA project SAI.

References

1. Yasuko Matsubara, Yasushi Sakurai, B Aditya Prakash, Lei Li, and Christos Faloutsos. Rise and fall patterns of information diffusion: model and implications. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 6–14. ACM, 2012.
2. Xinyi Zhou, Reza Zafarani, Kai Shu, and Huan Liu. Fake news: Fundamental theories, detection strategies and challenges. In *Proceedings of the twelfth ACM international conference on web search and data mining*, pages 836–837, 2019.
3. Habibul Haque Khondker. Role of the new media in the arab spring. *Globalizations*, 8(5):675–679, 2011.
4. Gadi Wolfsfeld, Elad Segev, and Tamir Sheafer. Social media and the arab spring: Politics comes first. *The International Journal of Press/Politics*, 18(2):115–137, 2013.
5. Emma Tonkin, Heather D Pfeiffer, and Greg Tourte. Twitter, information sharing and the london riots? *Bulletin of the American Society for Information Science and Technology*, 38(2):49–57, 2012.
6. Kimberly Glasgow and Clayton Fink. Hashtag lifespan and social networks during the london riots. In *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction*, pages 311–320. Springer, 2013.
7. Fang Jin, Edward Dougherty, Parang Saraf, Yang Cao, and Naren Ramakrishnan. Epidemiological modeling of news and rumors on twitter. In *Proceedings of the 7th Workshop on Social Network Mining and Analysis*, page 8. ACM, 2013.
8. Damon Centola. The spread of behavior in an online social network experiment. *science*, 329(5996):1194–1197, 2010.
9. Benjamin Doerr, Mahmoud Fouz, and Tobias Friedrich. Why rumors spread so quickly in social networks. *Communications of the ACM*, 55(6):70–75, 2012.
10. Xiaoyang Liu, Daobing He, and Chao Liu. Information diffusion nonlinear dynamics modeling and evolution analysis in online social network based on emergency events. *IEEE Transactions on Computational Social Systems*, 6(1):8–19, 2019.
11. Maziar Nekovee, Yamir Moreno, Ginestra Bianconi, and Matteo Marsili. Theory of rumour spreading in complex social networks. *Physica A: Statistical Mechanics and its Applications*, 374(1):457–470, 2007.
12. JY Lin and M Li. The competition dynamics of information propagation in complex network. In *Software Engineering and Information Technology: Proceedings of the 2015 International Conference on Software Engineering and Information Technology (SEIT2015)*, pages 46–49. World Scientific, 2016.
13. Haibo Hu. Competing opinion diffusion on social networks. *Royal Society Open Science*, 4(11):171160, 2017.
14. Saumik Bhattacharya, Kumar Gaurav, and Sayantari Ghosh. Viral marketing on social networks: An epidemiological perspective. *Physica A: Statistical Mechanics and its Applications*, 525:478–490, 2019.
15. Marko Hölbl, Marko Kompara, Aida Kamišalić, and Lili Nemec Zlatolas. A systematic review of the use of blockchain in healthcare. *Symmetry*, 10(10):470, 2018.
16. George Drosatos and Eleni Kaldoudi. Blockchain applications in the biomedical domain: a scoping review. *Computational and structural biotechnology journal*, 17:229–240, 2019.
17. Geetanjali Rathee, Ashutosh Sharma, Rajiv Kumar, and Razi Iqbal. A secure communicating things network framework for industrial iot using blockchain technology. *Ad Hoc Networks*, 94:101933, 2019.

18. Wei Liang, Mingdong Tang, Jing Long, Xin Peng, Jianlong Xu, and Kuan-Ching Li. A secure fabric blockchain-based data transmission technique for industrial internet-of-things. *IEEE Transactions on Industrial Informatics*, 15(6):3582–3592, 2019.
19. Alessandra Pieroni, Noemi Scarpato, Luca Di Nunzio, Francesca Fallucchi, and Mario Raso. Smarter city: smart energy grid based on blockchain technology. *Int. J. Adv. Sci. Eng. Inf. Technol*, 8(1):298–306, 2018.
20. Jihong Wan, Xiaoliang Chen, Yajun Du, and Mengmeng Jia. Information propagation model based on hybrid social factors of opportunity, trust and motivation. *Neurocomputing*, 333:169–184, 2019.
21. Yamir Moreno, Maziar Nekovee, and Amalio F Pacheco. Dynamics of rumor spreading in complex networks. *Physical Review E*, 69(6):066130, 2004.
22. *PEW Research Centre*, 2018. `http://www.pewinternet.org/`.
23. DA Williamson. Social network demographics and usage. *eMarketer, May*, 2010.
24. Amanda Nosko, Eileen Wood, and Seija Molema. All about me: Disclosure in online social networking profiles: The case of facebook. *Computers in human behavior*, 26(3):406–418, 2010.
25. Alan Mislove, Massimiliano Marcon, Krishna P Gummadi, Peter Druschel, and Bobby Bhattacharjee. Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 29–42. ACM, 2007.
26. Frank Edward Walter, Stefano Battiston, and Frank Schweitzer. A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems*, 16(1):57–74, 2008.
27. Daron Acemoglu and Asuman Ozdaglar. Opinion dynamics and learning in social networks. *Dynamic Games and Applications*, 1(1):3–49, 2011.
28. Jiyoung Woo and Hsinchun Chen. Epidemic model for information diffusion in web forums: experiments in marketing exchange and political dialog. *SpringerPlus*, 5(1):66, 2016.
29. Ling Zhang, Manman Luo, and Robert J Boncella. Product information diffusion in a social network. *Electronic Commerce Research*, 20(1):3–19, 2020.
30. Lun Li, David Alderson, John C Doyle, and Walter Willinger. Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4):431–523, 2005.
31. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
32. Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. business & information systems engineering, 59 (3), 183–187. *DOI: http://dx. doi. org/10.1007/s12599-017-0467-3*, 2017.
33. Karl Wüst and Arthur Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.
34. Massimo Di Pierro. What is the blockchain? *Computing in Science & Engineering*, 19(5):92–95, 2017.
35. Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.
36. Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy. Towards blockchain-based auditable storage and sharing of iot data. In *Proceedings of the 2017 on Cloud Computing Security Workshop*, pages 45–50. ACM, 2017.
37. Axel Moinet, Benoît Darties, and Jean-Luc Baril. Blockchain based trust & authentication for decentralized sensor networks. *arXiv preprint arXiv:1706.01730*, 2017.
38. Iago Sestrem Ochoa, Gabriel de Mello, Luis A Silva, Abel JP Gomes, Anita MR Fernandes, and Valderi Reis Quietinho Leithardt. Fakechain: A blockchain architecture to ensure trust in social media networks. In *International Conference on the Quality of Information and Communications Technology*, pages 105–118. Springer, 2019.
39. Wee Jing Tee and Raja Kumar Murugesan. Trust network, blockchain and evolution in social media to build trust and prevent fake news. In *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, pages 1–6. IEEE, 2018.
40. Tee Wee Jing and Raja Kumar Murugesan. A theoretical framework to build trust and prevent fake news in social media using blockchain. In *International Conference of Reliable Information and Communication Technology*, pages 955–962. Springer, 2018.
41. Akshada Babar, Aakash Shukla, Nalini Jagtap, Prachi Chaudhari, and Akshata Mithari. News tracing system using blockchain.
42. Wenqian Shang, Mengyu Liu, Weiguo Lin, and Minzheng Jia. Tracing the source of news based on blockchain. In *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, pages 377–381. IEEE, 2018.
43. Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher. Using blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional*, 21(4):16–24, 2019.

44. Anik Islam, Md Fazlul Kader, Md Mofijul Islam, and Soo Young Shin. Newstradcoin: A blockchain based privacy preserving secure news trading network. In *IC-BCT 2019*, pages 21–32. Springer, 2020.
45. Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang. A blockchain-based supply chain quality management framework. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pages 172–176. IEEE, 2017.
46. Horst Treiblmaier. The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, 2018.
47. Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7):2117–2135, 2019.
48. S Angraal, HM Krumholz, and WL Schulz. Blockchain technology: Applications in health care. circulation. cardiovascular quality and outcomes, 10 (9), 2017.
49. Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6):1211–1220, 2017.
50. Simon Albrecht, Stefan Reichert, Jan Schmid, Jens Strüker, Dirk Neumann, and Gilbert Fridgen. Dynamics of blockchain implementation-a case study from the energy sector. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.
51. Taneli Hukkinen, Juri Mattila, Juuso Ilomäki, and Timo Seppälä. A blockchain application in energy. Technical report, ETLA Report, 2017.
52. Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, and Víctor Santamaría. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, 10(2):20, 2018.
53. Hossein Hassani, Xu Huang, and Emmanuel Silva. Banking with blockchain-ed big data. *Journal of Management Analytics*, 5(4):256–275, 2018.
54. Svein Ølnes. Beyond bitcoin enabling smart government using blockchain technology. In *International conference on electronic government*, pages 253–264. Springer, 2016.
55. Heng Hou. The application of blockchain technology in e-government in china. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–4. IEEE, 2017.
56. Jennifer Golbeck. Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web (TWEB)*, 3(4):12, 2009.
57. Facebook wall posts network dataset – KONECT, April 2017.
58. Jaewon Yang and Jure Leskovec. Defining and evaluating network communities based on ground-truth. *Knowledge and Information Systems*, 42(1):181–213, 2015.
59. Navin Gupta, Anurag Singh, and Hocine Cherifi. Centrality measures for networks with community structure. *Physica A: Statistical Mechanics and its Applications*, 452:46–59, 2016.
60. Rimjhim Agrawal, Md Arquam, and Anurag Singh. Community detection in networks using graph embedding. *Procedia Computer Science*, 173:372–381, 2020.
61. MD ARQUAM and ANURAG SINGH. Epidemic spreading in geometric network with mobile agents. *Acta Physica Polonica B*, 51(9), 2020.