International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

An Improved Rumour Detection Block Chain Security Framework In Social Network

K. Lino Fathima ChinnaRani[1], Dr. M. Kasthuri[2]

[1]Department of Computer Applications, Bishop Heber College, Affiliated to Bharathidasan University, Trichy, Tamilnadu.
[2]Department of Computer Applications, Bishop Heber College, Affiliated to Bharathidasan University, Trichy, Tamilnadu.

Email: [1]linofathima.ca@bhc.edu.in, [2]kasthuri.ca@bhc.edu.in

Abstract: A blockchain is an interconnected chain of growing list of blocks. Blockchain technology is used in various domains such as crypto currency, financial services, risk management, internet of things (IoT) to public, social networks, etc. Block chain has various benefits such as decentralisation, persistency, privacy and auditability. In social networks there are various issues existing such as fake identities, no privacy, no security, exposing too much of information, spreading rumours, etc. Information that spreads across social networks can carry a lot of false claims. The development of online social networks along with the innovative media can even make rumour spreading more severe. Identifying rumour sources in social networks acting a significant task in limiting the damage caused by them through the timely quarantine of the sources. Additionally, identifying the rumour information in social network is a complex task. Therefore, this research paper proposed blockchain architecture for identifying rumours in social network using contract-based progression. This paper takes the initial step to recognise how the block chain technology can assist limit the spread of rumours.

Keywords: Blockchain, Rumour detection, security, Framework.

1. INTRODUCTION

Rumour has been prevailing for thousands of years in human history. Rumour often refers to a piece of unverified information such as clarification of events, media coverage and information exchange. Rumours are flowing from person to person or belong to an object, event, or issue of public concern. In the period of Internet, deeper connections between beings along with faster information transmission rate also activated speedy rumour propagation. It could cause more strong social anxieties and harmful effects. Earlier studies have put highlighting on both the exhibiting techniques of rumour spreading. Most of the existing studies cannot find the root of rumour explosion. There is no effective approach to eliminate rumour propagation.

The blockchain technology is suitable to overcome the existing rumour identification problem. This has stirred us to reshape the statistics interchange process in recent social networks. This is known as the pair-wise spreading style of rumour. The blockchain based contract to become a good solution for upcoming facts propagation and interchange platform.

In this work, we introduce architecture for smart contract-based design that is useful for identifying rumours in social media using blockchain technologies. By assigning a simulated gathered credit for each participant in the social network, an advanced methodology design constructed for information exchange. Such credits are a replication of the reliability of both social network followers and corresponding information[12].

The proposed architecture supports to avoid the large-scale circulation of fake news through the social network. To demonstrate that for peer-to-peer information exchange and propagation, individuals under blockchain are more vigilant about the genuineness of the information. The proposed model examined the propagation of information with and without the proposed architecture, and revealed that our proposed approach can successfully decrease the social and economic damage by rumour. From the literature review, this paper is the first work directing to utilize the features of blockchain technology to address and solve the rumour spreading problems in social networks[9].

This paper classified as follows: More than one dimensional view of various authors has discussed in Section 2. An overview of blockchain technology characteristics and its unique architecture has discoursed in Section 2. The proposed blockchain-enabled framework for information exchange, which can be integrated into the social network model described in Section 3. Section 4 and 5 has illustrated how such an existing rumour spreading model fused with blockchain-enabled framework can propel a trusted social network as a whole. Section 6 and 7 has elaborated the dynamics of existing as well as proposed model. section 8 concludes the paper.

2. REVIEW OF LITERATURE

M. Vinod Kumar et al.(2018) have presented a theoretical study on the blockchain technology and how various industries would get benefited by implementing this blockchain technology into their business . They compared traditional rice supply chain models, analysed and introduce a new block supply chain framework that helps in increasing the efficiency of rice supply chain. It provides a traceability system which backup all the measures happening within the rice supply chain. It monitors security and quality of the rice. Walid Al-Saqaf et al.(2017) have summarized a few principles of blockchain technology have relevance in several domains that could impact society at large. They also discussed few characteristics of blockchain technology such as Transparency, equality and autonomy that could facilitate progress in areas like online identity, human trafficking, corruption, fraud, democratic participation and freedom of expression. Here, they didn’t provide any framework model for intrusion detection.

Gokhan Sagirlar et al.(2018) have introduce a novel hybrid blockchain architecture for IoT, referred to as Hybrid-IoT. In Hybrid-IoT, subgroups of IoT devices becomes peers on Proof-Of-Work (POW) sub blockchains, connected with a BFT (Byzantine Fault Tolerant) inter-connector framework. They focus and analyse the design of the POW sub-blockchains, addressing IoT issues and dimensions that are translated to blockchain issues and dimensions. Kristoffer et al. (2017) have explain the new block chain technology into business provides a level of supply chain transparency that allows supply chain managers to obtain the information consumers are demanding and thus contribute to their companies competitive advantages. They introduce Unified Theory of acceptance and Use of Technology to expand the explanation of end user technology acceptance for blockchain traceability applications. This theory delivers a strong conceptual framework to describe these associations. It supports the development of blockchain tools.

Mehrdad Salimitari et al. (2019) have discussed the possibilities of using blockchain for securing and assuring data integrity in IoT networks. They focused on the currently used consensus methods and their practical applicability for resource constrained IoT devices and networks. they discussed the pros and cons of current consensus methods used in blockchain implementations. They also discussed how private blockchains and tangle can be a better alternative to public blockchains for IoT networks. Among the discoursed operations of blockchain, Hyperledger Fabric, and Ethereum appear more promising for IoT networks and applications subsequently they have met some of the current limitations of blockchain. They have addressed some of the limitations including throughput, latency, computational overhead, network overhead, scalability and privacy Yet, nothing has been effective in addressing all the limitations to a satisfactory grade.

A. Shanti Bruyn (2017) provided a general exploration of blockchain. After the research, it explores the significances of blockchain in a precise manner to unknown business people. The summary of this paper may provide a good general idea of Block chain This paper focusses in more detail on the Nakamoto blockchain, the original and the most commonly known for its use in Bitcoin.

The literature review reveals that blockchain technology useful in various fields such as online transaction, identity management, social network, notarization, etc. Scholars have applied blockchain based rules to construct a decentralized network. In this network, the third party is substituted by an automated access control manager, supported by the distributed blockchain system. Other researchers suggested implementing blockchain in supply chain management for an enhanced quality. Blockchain can resolve the traceability and trust-ability complications in this consequence. People also discover blockchain beneficial in power grid industry. Both services and users benefit from this technology by recording and authenticating the information on a distributed network reasonably and consistently. In the meantime, a combination of blockchain and the internet of things (IoT) upturn the operation of cloud storage.

3. BLOCKCHAIN TECHNOLOGY

A blockchain is an interconnected chain of growing list of blocks. Every block has its equivalent record and the timestamp. The blockchain is constructed with a peer-to-peer network. Here, each node transmits its records to further nodes [6]. This design inhibits invalidated alteration of data. The technical benefit of blockchain is decentralization, security; trustworthiness creates bitcoin in advanced currency [5].

3.1 CHARACTERISTICS OF BLOCKCHAIN

A blockchain is categorized by censorship conflict, immutability and worldwide usability [3]. It has a global network of validators called miners. They retain it through block payments, termed as crypto tokens. Decentralization guarantees fault tolerance, attack resistance and collusion resistance. This blockchain is decentralized on two of the three possible divisions in software decentralization:

- ➢ Politically decentralized - means that no one controls it
- ➢ Architecturally decentralized - no infrastructural significant point of disaster occurs[15]
- ➢ Logically centralized - there is one ordinarily granted state and the system performs similar to a single computer.

3.2 BLOCKCHAIN ARCHITECTURE

The blockchain is a categorization of blocks, which contains a wide-ranging list of transaction records. Each block plugs to the immediately next block through the reference that is fundamentally a hash value of the earlier block termed as parent block[1]. Children of the block's ancestors are termed as uncle blocks. Hashes would also be kept in Ethereum bockchain. The initial block of a blockchain is termed as genesis block. It has no parent blocks. Figure 1 shows general structure of blockchain technology.

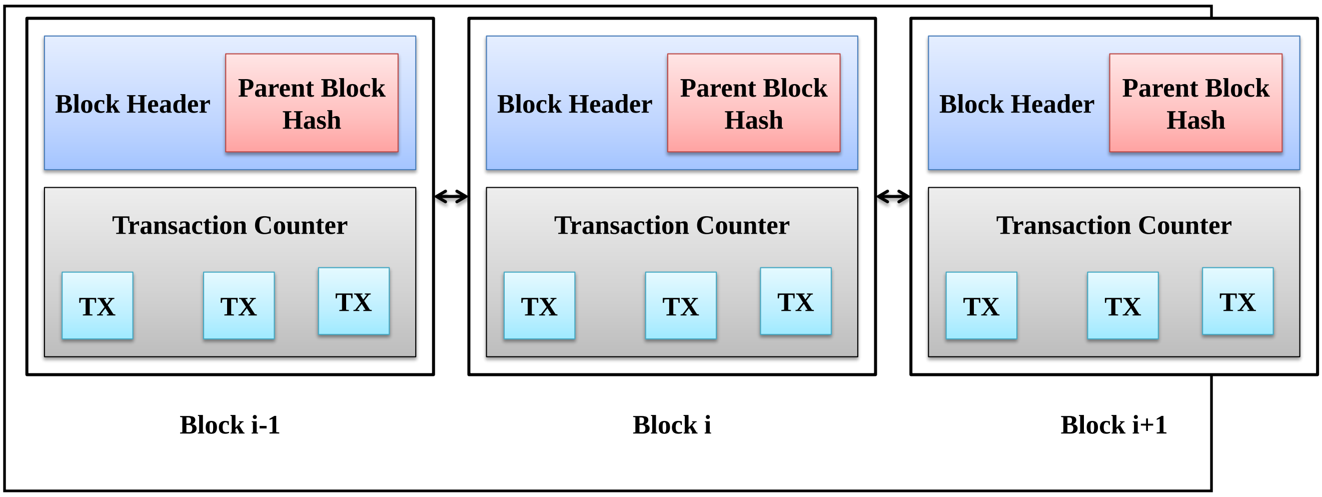

Fig.1. General Structure of Blockchain Technology

3.2.1 BLOCK

A block contains two parts such as block header and block body. Specifically, the block header includes:

(i) Block version: It specifies which set of blocks undergo authentication rules to follow.
(ii) Root hash: The hash value of entire transactions in the block.
(iii) Timestamp: Existing time as per seconds in universal time.
(iv) n Bits: target edge of a legal block hash.

(v) Nonce: A 4-byte field. It usually starts with 0 and rises for every single hash computation [4].
(vi) Parent block hash: It is a 256-bit hash value. It points to the former block.

Transaction counter and transactions are the extreme number of transactions that a block can comprise depends on the block size and the size of each transaction [8]. Blockchain practises an asymmetric cryptography mechanism to authenticate the verification of transactions. Digital signature established on asymmetric cryptography is used in an unreliable situation[7].

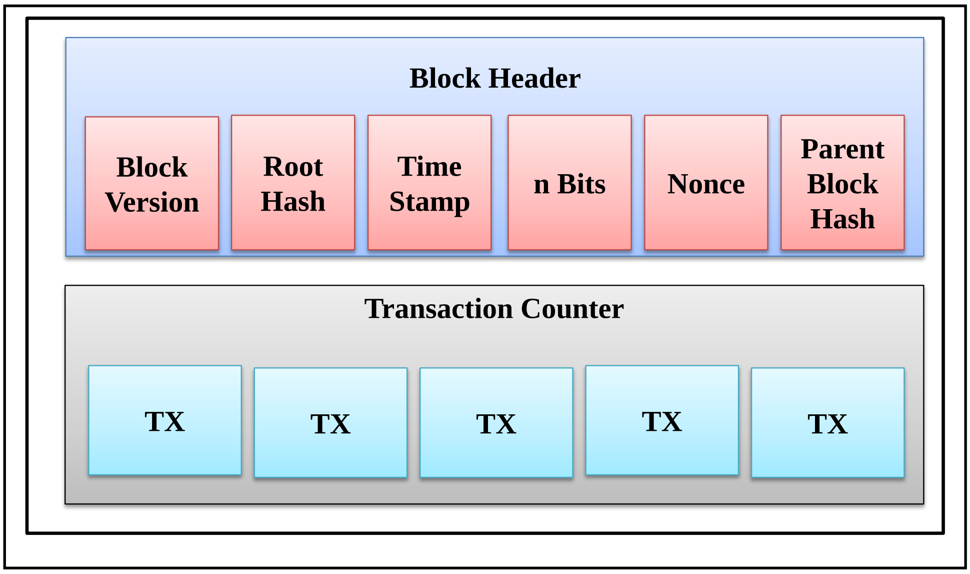

Fig.2. Components of a Single Block

4. RUMOUR SPREADING- EXISTING MODEL

A rumour is a part of unproven flowing of information. Previous studies explained that rumours involved in multidisciplinary determinations from physics, sociology and psychology. A number of methodologies to the sculpting of rumour scattering and control of its destruction were discussed. Classic rumour models viewed the diverse social networks as a graph where rumours circulated. The existing research used stochastic processes to virtualized rumour spreading. It was generated a better consideration of rumour spreading. In another research work, the authors detected more prominent propagators to be present on social networks. They had given higher possibilities for them to blowout the information in the framework of new types of social media and network like micro-Blogging. Spreading process is categorized as susceptible, infected, and recovered. The work is built on the supposition that ignorant are certainly subjective by the propagator, and that accordance with actuality will change the probabilities of altering a spreader into a stifler. Existing studies have revealed that the termination or explosion of rumours is generally connected to the stifling and fail to recall rectifying tools or methods for a specified network. New practises of social networks such as bidirectional information connections also developed. In this situation, the receiver could also have a stimulus on the spreader. Therefore, the proposed architecture is useful to identify rumours spreading in social network using blockchain technology.

5. PROPOSED ARCHITECTURE

In this section, first describe the proposed blockchain enabled architecture for information exchange, which can be integrated into the social network mode. Then illustrate how such blockchain enabled architecture can drive trusted social networks.

5.1 BLOCKCHAIN FOR RUMOUR SPREADING

To ensure both security and privacy of the information exchange process as well as avoiding a large scale spreading of rumours, the proposed architecture adopts the blockchain technology[2]. Enhanced blockchain architecture contains various phases such as API gateway, contract processing, operational analytics, data storage and data dictionary. Since the objective of this research work is to avoid the spreading of untrusted information and allocate an accumulated virtual information credit for each participant in the network. The following sections describe various phases existing in the proposed blockchain architecture for identifying rumours in the social network. blockchain architecture for identifying rumours in the social network.

Phase 1: Information origin
Phase 2: API gateway
Phase 3: Data Processing
Phase 4: Contract Processing
Phase 5: Operational Analytics
Phase 6: Block Chain

Phase 1: Information Origin

Data are scattered in various forms. The information is generated from social network, online forum, news aggregator and photos. This information is gathered from various resources and injected through API gateway.

Phase 2: API Gateway

An API gateway is programming that sits in front of an application programming interface (API) and acts as a single point of entry for a defined group of micro services. API receives information from various resources and passed to analytical processing[13]. This gateway acts like an interface between information origin layer and a processing layer.

API Gateway includes functions such as:

- Authentication
- Security Policy Enforcement
- Load Balancing
- Cache Management
- Dependency Resolution

Phase 3: Data Processing

Data dictionary is useful for collecting data from various databases and consolidating into a single source that can be easily and instantly evaluated. With the help of data discovery, the user searches for specific items or patterns in a dataset[14]. Visual tools make the process fast, easy-to-use, swift and intuitive. These tools used to create high fidelity presentations of data discovery.

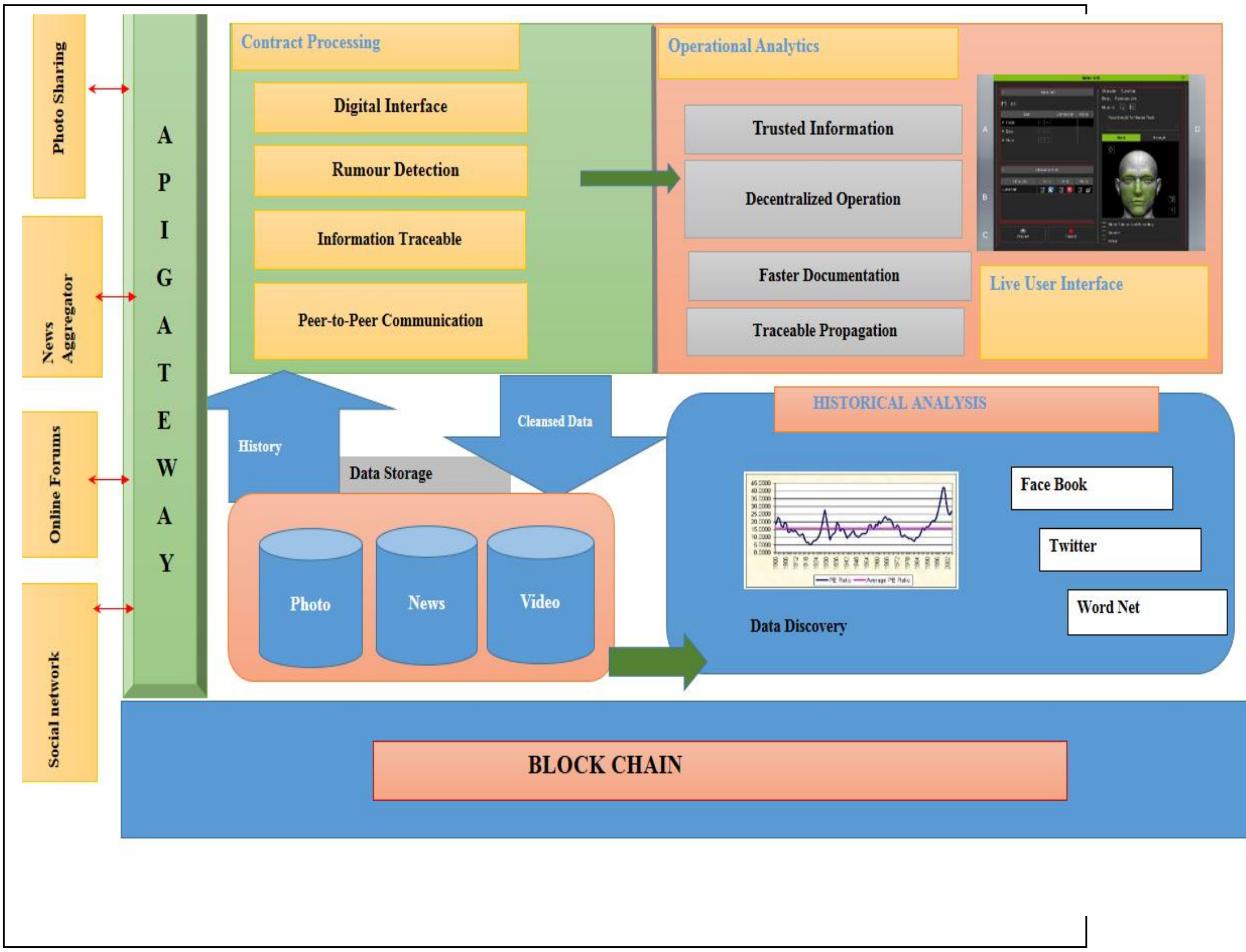

Figure 3. Proposed Blockchain Architecture for Identifying Rumours in Social Network

It has the following steps:

Data acquisition: Integrate relevant data. These can be a relational database, a data warehouse, or Big data.

Data storage: The data can be stored in the database and the user can view the data by various graphical representation**.**

Data preparation: Usually, to merge different data sets to get valuable insights. The real insights are found by correlation of different data[10]. The output of data preparation is frequently in the form of files with multiple rows and columns. These files can be used for further analysis.

Exploratory data analysis: The user uses the integrated and prepared data to spot rumour and new insights[17]. For the better implementation of above methods, investigate how rumours are propagated through the network, adopt a rule-based classification method that dividing the vertices into three convertible sets such as the spreader, the ignorant, and the stifler.

The dynamics of these three classes are as follows:

The Spreader: A spreader is contributing to the propagation of rumour.

The Ignorant: The ignorant are similar to susceptible individuals who has no interests in the rumour anymore.

The Stifler: A stifler is contributing to the final elimination of the rumour.

convertible sets such as the spreader, the ignorant, and the stifler.

The dynamics of these three classes are as follows:

The Spreader: A spreader is contributing to the propagation of rumour.

The Ignorant: The ignorant are similar to susceptible individuals who has no interests in the rumour anymore.

The Stifler: A stifler is contributing to the final elimination of the rumour.

Phase 4: Contract Processing

This phase hides the insights without being explicitly programmed. Contract processing is helpful to determine the blocks or information that is transmitted between nodes in the network. This contrast processing phase uses data analysis methods in order to detect the rumours through the tracing of information. The developer has to integrate the analytic model into real time event processing to automatically monitor real time transactions and trigger actions like rumour detection. This phase can reveal suspicious activity while performing fraud, security and compliance investigation [19].

To ensure both security and privacy of the information exchange process as well as avoiding a large scale spreading of rumours, the proposed architecture adopts the blockchain technology and design. A protocol comprising of both private contract and public contract. The private contract for content exchange is compromised and it can be contracted between **the spreader and the receiver**. Since our objective is to avoid the spreading of untrusted information, the proposed architecture allocates an accumulated virtual information credit for each participant in the network, and use such credits to motivate the propagation of trusted information.

The public contract is updated at every time step to record the links of information propagation as well as the credit flows throughout the social network [11]. It serves as the public ledger for all information transactions. This contract also makes the highest transaction credit, public to all existing participants of the information exchange, which is available for decision-making in each private contract.

Phase 5: Operational Analytics

Blockchain has the potential to play a major role in establishing trust on the internet[16]. This phase includes two parts to implementation, machine-to-machine automation and enablement of human interactions. This proposed architecture uses various machine learning methods in order to stimulate faster documentation. These methods are operational in nature and it included transactions and block updates per second. This phase is using a **configurational window (UI) that provides a method to start, stop, pause and mute operations[9]**. The main key feature is to import various forms of data, then define their relationships. When the system approaches to the final states, there are only ignorant and stiflers left in the network, while spreaders will perish out.

6. RUMOUR SPREADING DYNAMICS

The above proposed architecture model has been characterizing the social networks rumour spreading dynamics with a static number of members, here the introduction of Blockchain technology can play the latent roles to diminishes the spreading of rumours.

6.1 Model Set-Up

Consider an undirected graph G= (V.E), where each node in the social network considered as a vertices and E represents a set of social interactions. Consider that the social network has a static group of homogeneously assorted population and the degree of node distribution in Graph(G) confirms to Poisson distribution:

$$P(k) = \frac{e^{-\bar{k}}\,\bar{k}^{k}}{k!'} \quad \text{-------------}\ 1$$

Where $\underline{k}$ – degree for Graph (G)

P(k)represents the probability of observing k degrees for v ϵ V.

For better Clarification, rumours are circulated via the network and therefore the adoption of rule-based classification method has been used which can be further divided into 3 sets [20].

The spreader set S b. The ignorant set I, and
c. The stifler set R.

The dynamics of these three classes are as follows:

- **Ignorant with Density I(t).** The ignorant are like to vulnerable entities in classic models where Time t > 0, an ignorant has a probability λ Here, to turn out to be a spreader when it reaches with a spreader who is relatively certain rumour reality. Subsequently, it’s eagerly to spread the rumour in the succeeding time phases. In the meantime, the ignorant has probability η to convert as a stifler, who has no interests in the rumour anymore.
- **Spreader with Density S(t).** A spreader plays a major role to circulate of rumour inside the graph(G). The spreader contribute in a pair-wise consultation tries to “contaminate" other entities with the acknowledged rumour. Therefore, at time t > 0, when a spreader interacts with a stifler, the spreader has a probability γ to alter a stifler. In addition, assume that at a certain time, a spreader itself has forgotten the rumour and then converts into a stifler at rate δ.
- **Stifler with Density R(t).** A stifler is acting as an initiator of rumour elimination. In wide-ranging purpose, it is a fascinating state in our model, and are gathering its density by converting both ignorant and spreaders into stiflers.

To summarize all the dynamics considered above, we derive a nonlinear system consisting of the following differential equations for I(t),S(t) and R(t), respectively.

$$dI(t)/dt =(\lambda+\eta)\, \bar{k}I(t)S(t) \text{ ----------------------------- } 2$$

$$dS(t)/dt = \lambda\bar{k}I(t)\, S(t) - \gamma\bar{k}S(t)(S(t)+R(t)) - \delta S(t) \text{ ----------- } 3$$

$$dR(t)/dt = \eta\bar{k}I(t)S(t) + \gamma\bar{k}S(t)(S(t)+R(t)) - \delta S(t) \text{ ---------------} 4$$

7. BLOCKCHAIN TRUSTED MODEL DYNAMICS

This section elaborates the dynamics under the proposed blockchain architecture model. It has assisting to resist the rumour spreading on social network. The proposed model has an authorized blockchain enables trust contract. The difference between existing and proposed model is that the proposed model has a group of social network participants who have signed(authorized) trust contract.

For definition,

I_B - Initial members density of trust contract
I_N – Initial members who have not signed the contract
λ_N - Probability of converting ignorant to a spreader
η_N – Probability of converting ignorant to a stifler

Every time, if there is an information exchange occurred between two entities belongs to the trusted network, then they are eligible to execute the consistent consensus protocol to reach an agreement on the predetermined virtual members credit under the **I_B**. Subsequently, **I_B** members has a right to access the public data generated by current blockchain contracts. The trusted network members (I_B) have a diverse estimation of virtual credits of information exchange. Thus, I_B has different dynamics when it is related to I_N and the probabilities are defined as λ_B and η_B respectively. The dynamics of $I_N(t)$, $I_B(t)$, S(t) and R(t) on the blockchain-enabled social networks are as follows:

$$\frac{dI_B(t)}{dt} = -(\lambda_B + \eta_B)\, kI_B(t)S(t), \text{ --------------- } 5$$

$$\frac{dI_N(t)}{dt} = -(\lambda_N + \eta_N)\, kI_N(t)S(t), \text{ -------------------- } 6$$

$$\frac{dS(t)}{dt} = \lambda_B kI_B(t)S(t) + \lambda_N kI_N(t)S(t) - \gamma kS(t)(S(t) + R(t)) \text{ --}7$$

$$\frac{dR(t)}{dt} = \eta_B kI_B(t)S(t) + \eta_N kI_N(t)S(t) + \gamma kS(t)(S(t) + R(t)) \text{ --}8$$

7. ANALYSIS AND DISCUSSION

7.1 Rumour spreading rate:

When a member signed under a trusted contract through blockchain protocols, the additional record generated from the blockchain transactions which contains the list of trusted information inside the entire network. This yields an extra estimation “value” when an information transaction calculated by assembled credits, therefore, it can make an improved validity information decision which is based on the threat of drop down the credit values in definite transaction.

Commonly, when the private contract transaction between two entities has touched a greater virtual credit value, then the IB members are strictly authenticated on the current information transaction. Hence IB members are in less risk when revealing to a rumour. In the meantime, they lost an interest in a rumour and directly they are turn out to be a stifler.

Consequently, In the signed blockchain-enabled contract, I_B ignorant have restricted contributions to the spreader S consequently additional contributions to the stifler R:

$\lambda_B < \lambda_N, \eta_B > \eta_N$ ----------------------- 9

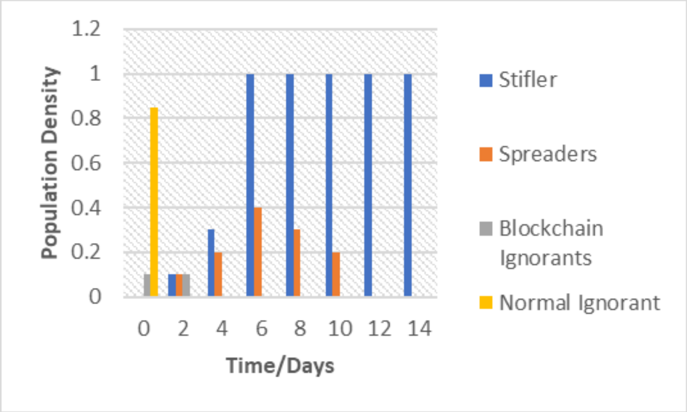

Figure 4. Temporal dynamics of the proposed blockchain-enabled system

8. CONCLUSION

This research paper proposed enhanced blockchain architecture for identifying rumours in social network using contract-based progression. In the recent years, large amount of information spread across internet and social media. In today's world huge number of rumours spread using social network. Rumour propagates Social networks plays a vital role in our society and is one of the essential mechanisms for the information distribution in the networks. We firstly introduced the architectural model setup for social networks. We then illustrated how to incorporate the blockchain contract into peer-to-peer information exchange process by employing virtual exchange of information. The designed blockchain architectural rumour spreading model demonstrated that blockchain technology would help in avoiding large-scale rumour spreading. The problem of fake news can be handled effectively by traceability, transparency and decentralization. The blockchain allowed platform can deliver online readers with a consistent way of authenticating the information and its source. To observe the architectural model as the number of initial blockchain contractors increases, the number of spreaders drops significantly. Such model setup and simulation consequences would motivate us to design trust-based information exchange system with blockchain technology enabled. In the future work, Contracts designed for extreme conditions and large-scale social networks may be designed and considered

9. REFERENCES

[1] M. Vinod Kumar and Dr. N. Ch. S. N. Iyengar, "A Framework for Blockchain Technology in Rice Supply Chain Management Plantation" Advanced Science and Technology Letters Vol.146 (FGCN 2017), pp.125-130,2018.

[2] Walid Al-Saqaf and Nicolas Seidler,”Blockchain technology for social impact: opportunities and challenges ahead”, JOURNAL OF CYBER POLICY, 2017.

[3] Gokhan Sagirlar_, Barbara Carminati_, Elena Ferrari, “Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things – PoW Sub-blockchains”. arXiv:1804.03903v3 [cs. DC], 2018.

[4] Kristoffer Francisco and David Swanson, “The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency”,2017.

[5] Mehrdad Salimitari and Mainak Chatterjee,"A Survey on Consensus Protocols in Blockchain for IOT networks” arXiv:1809.05613v4 [cs.NI] 2019.

[6] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,IEEE Transactions on industrial informatics”, vol. 10, no. 4, pp. 2233–2243, 2014.

[7] O. Bello and S. Zeadally, “Communication issues in the internet of things (iot),” in Next-Generation Wireless Technologies. Springer,2013, pp. 189–219.

[8] S. Tayeb, S. Latifi, and Y. Kim, “A survey on iot communication and computation frameworks: An industrial perspective,” in Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual. IEEE, 2017, pp. 1–6.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,”Future generation computer systems, vol. 29, no. 7, pp. 1645–1660,2013.

[10] F. Restuccia, S. D’Oro, and T. Melodia, “Securing the internet of things in the age of machine learning and software-defined networking,” IEEE Internet of Things Journal, 2018.

[11] C. Bekara, “Security issues and challenges for the iot-based smart grid,”Procedia Computer Science, vol. 34, pp. 532–537, 2014.

[12] B. Carminati et al., “Enhancing user control on personal data usage in internet of things ecosystems” in Services Computing (SCC), 2016 IEEE International Conference on. IEEE, pp. 291–298,2016.

[13] G. Sagirlar et al., “Decentralizing Privacy Enforcement for Internet of Things Smart Objects,” ArXiv e-prints, 2018.

[14] J. Wu et al., “R-osgi-based architecture of distributed smart home system,” IEEE Transactions on Consumer Electronics, vol. 54, no. 3, 2008.

[15] Shanti Bruyn ,” Blockchain -An Introduction”, University Amsterdam,2017.

[16] F. Tschorsch et al., “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[17] Gilad, Yossi, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich,”Algorand: Scaling byzantine agreements for cryptocurrencies.” In Proceedings of the 26th Symposium on Operating Systems Principles, pp. 51-68. ACM, 2017.

[18] Zamani, Mahdi, Mahnush Movahedi, and Mariana Raykova,” RapidChain: Scaling blockchain via full sharding.” In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931-948. ACM, 2018.

[19] Hanke, Timo, Mahnush Movahedi, and Dominic Williams.” Dfinity technology overview series, consensus system.” arXiv preprint arXiv:1805.04548,2018.

[20] Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things –A survey of topics and trends”, Information Systems Frontiers, vol. 17, pp. 261–274, 2015.