



iTrustBD: Study and Analysis of Bitcoin Networks to Identify the Influence of Trust Behavior Dynamics

Md. Jahidul Islam^{1,2} · Md. Rakibul Islam² · Md. Abul Basar²

Received: 30 July 2023 / Accepted: 18 March 2024

© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2024

Abstract

The concept of cryptocurrency is a significant advancement in digital currencies. “Cryptocurrency” refers to a form of electronic or virtual currency that is secured through the application of encryption. It is a common practice to trade cryptocurrencies on decentralized exchanges where neither governments nor financial institutions can exert any form of authority over them. This being the case that cryptocurrencies are not regulated either by the government or financial institutions presents a potential risk for investors. Although a few nations have authorized cryptocurrency, the vast majority of nations, including Bangladesh, have not recognized it due to concerns over the safety of the cryptocurrency system. In this paper, we analyze cryptocurrency networks, “Bitcoin Alpha trust weighted signed network” and “Bitcoin OTC trust weighted signed network”. Following an investigation into the characteristics of the networks, we came to the conclusion that they are robust and reliable, as well as capable of withstanding any kind of attack. Additionally, we forecast the future condition of the trader’s conduct in terms of trustworthiness; as a consequence, we identified more trustworthy behaviors on the behalf of traders. As a result, this work has the potential to make a contribution to the process of legalizing cryptocurrency transactions.

Keywords Cryptocurrency · Network analysis · Epidemic spread · Behavior dynamics · Trusty

Introduction

Cryptocurrency is an electronic or digital resource that is used as a method of exchange. Cryptocurrencies are decentralized, which means they are not controlled by governments or financial institutions. The first and most well-known cryptocurrency, Bitcoin, was created in 2009. Cryptocurrencies are frequently traded on digital currencies and can be used to buy goods and services. Cryptocurrencies have many advantages compared to conventional fiat money.

They are increasingly publicly available, which means that anyone with internet access can use them. They are considered safer for their users because they are distributed, though they aren’t under the regulation of the government or financial institutions. Cryptocurrencies are also untraceable, which means that users can make transactions without disclosing their identity. But, cryptocurrencies also come with a variety of drawbacks. They are volatile, which means their value can fluctuate dramatically. They are also not widely accepted yet, which makes them difficult to use in everyday transactions. Notwithstanding their drawbacks, cryptocurrencies are becoming increasingly popular and are being used on a daily basis. Their popularity stems from a variety of advantages, including worldwide impact, confidentiality, and untraceability.

The United States, Japan, Singapore, the United Arab Emirates, and other central banks have recently formally acknowledged cryptocurrency. Although cryptocurrency trading is not allowed in Bangladesh, the Bangladesh Bank sent a letter to the Criminal Investigation Department of the police that, “Trading of cryptocurrencies cannot be considered a crime although virtual coins are illegal under the laws

✉ Md. Jahidul Islam
jahid.jabed@gmail.com

Md. Rakibul Islam
engrrkb@gmail.com

Md. Abul Basar
bashar7075@gmail.com

¹ Department of Computer Science and Engineering,
Chandpur Science and Technology University,
Chandpur 3600, Bangladesh

² Department of Computer Science and Engineering,
Bangladesh University of Engineering and Technology,
Dhaka 1000, Bangladesh

of the country.”¹ The banking regulator in Bangladesh still does not allow or support the trading of any cryptocurrency because of the following trust issues-

- Decentralized Structure.
- High Risk for Illegal Transaction.
- Absence of scope of monitoring

Considering current laws, policies, and future scopes, we are motivated to conduct a detailed study on a cryptocurrency network. Our works in this study include the following contributions-

1. Analysing the network metrics and properties to find out whether it provides trusty individuals.
2. Finding the trusty traders for future reference from the current state of cryptocurrency networks.
3. Preparing a behavior spread model with the help of news spread models including other state-of-the-art approaches.
4. Analysing how the roles of important individuals in the networks contribute to the dynamics of the cryptocurrency networks.

This section explains what this article is about and what research has been done on it. The work is discussed in detail in “[Methodology](#)” section and “[Result Analysis](#)” section. “[Literature Reviews](#)” section is about earlier works that are similar to this one and address the topic of the author’s interest. In “[Preliminaries and Backgrounds](#)” section, the background information and preliminary steps that need to be taken are included. “[Methodology](#)” section, includes the methods used in the research that is done for this work, such as the network metrics analysis and the network future behavior analysis. “[Result Analysis](#)” section, is about the results of the work along with an analysis of the results and what they mean. Lastly, “[Discussions and Conclusion](#)” section will wrap up the article by summarizing what are the outcomes of this work and what are the future scopes or aims.

Literature Reviews

Cryptocurrency research is still in its early stages and is constantly evolving. Much of the research is focused on understanding how cryptocurrencies work, their potential implications, and how they can be used in various ways.

The study of cryptocurrency networks is a rapidly expanding field with a wide range of tools and methods. Network topology, community detection, and centrality measures are a few popular network analysis techniques. New techniques and tools are consistently being developed in this discipline, where there is still considerable research to be done. However, there has been some progress made in recent years and there are now a few different approaches that can be used to analyze cryptocurrency networks.

In [1] authors give a thorough and systematic survey of the most recent research on network construction, network profiling, and network-based detection as well as analysis and mining of Bitcoin transaction networks. They present several potential research directions for future work on examining cryptocurrency transaction networks, including a brief overview of some benchmark data sources of cryptocurrency transaction networks and valuable guidance for brand-new researchers in this area. They also summarize the instructive and significant findings in the existing literature. The author of [2] analyzes the cryptocurrency market network during the COVID-19 pandemic financial crisis. The behavior of individuals during the financial crisis is included in the author’s research. The Social Network Analysis (SNA) parameters of degree, diameter, modularity, centrality, and path length are used in [3] for various cryptocurrency networks and their actual market price by crawling (data gathering) from Twitter. The authors also have shown that the popularity of cryptocurrencies is influenced by their market price and the social media activity of their actors. In [4], the authors examine how the COVID-19 epidemic has affected cryptocurrency markets by looking at cryptocurrency networks. The data is split up into temporal frames of indefinite size using Symbolic Time Series Analysis (STSA). To determine the statistical properties of the network, they also calculate the mutual information and correlation coefficient for pre- and post-COVID-19 outbreaks. Additionally, MST and PMFG are used by the authors to examine the topological dynamics and network behavior during and after COVID-19 outbreaks.

Cryptocurrency transactions are often thought to be safer than conventional transactions as they employ digital certificates and encrypted communications to secure the transfer of funds. However, there are still a few trust issues with cryptocurrency transactions. For example, it is difficult to verify the identities of the parties involved in the transaction, it is also difficult to ensure that perhaps the funds will be used for the intended purpose. An evaluation of a cryptocurrency network’s trustworthiness is done using a network trust analysis. This can be done by taking into account numerous elements such as the network’s hashrate, node number, degree of decentralization, and overall security. There are few research works found in the literature that use network analysis techniques to find

¹ The Daily Star, Jul 29, 2021, Bangladeshi newspaper, Available online—<https://www.thedailystar.net/business/news/cryptocurrency-trading-not-allowed-all-bangladesh-bank-2140141>.

the trustworthiness of cryptocurrency transactions. In [5], the article examines the hype surrounding the advent of decentralized systems for managing digital networks. According to this theory, people in this context are enamored with their connections to other networks. The inability to comprehend how ultra-modern digital networks disguise very classic consolidation of power and capital may be at the root of Bitcoin's failure as a currency (rather than as a hoarded asset in emerging inflation) and as an ideology. The growth and fall of Bitcoin are a cautionary story about how creative ideas that threaten the power and the centralization of capital are ultimately co-opted and colonized by capital in the digital age. The paper concludes with a consideration of some of the more altruistic applications of the digital technologies that Bitcoin has made feasible. The authors of [6] provide an overview of relevant studies on cryptocurrencies and trust in human-computer interaction (HCI) and evaluate its utility for comprehending the trust concerns in Bitcoin technology. Several limitations of the existing theories and models of trust are highlighted, and a research model is provided to investigate the unique trust difficulties posed by Bitcoin technology.

However, there are only a very small number of works in network analysis that use a network science and graph theoretical perspective. Due to the anonymity of Bitcoin dealers, it is critical to monitor each dealer's credit history in order to prevent fraud and other security risks. By using social network analysis techniques, such as small World, Page Rank, Density, Reciprocity, Centrality, Transitivity (Global and Local Clustering Coefficients), Link Analysis, Community Detection Algorithms, Weight Prediction, and others, the authors of [7] intend to address security issues within the Bitcoin trust network. Furthermore, this type of network analysis has a drawback in that it cannot guarantee changes in Bitcoin traders' behavior in the future, even while it gives traders a solid idea of how they would behave in situations involving trust. As a result, we intend to analyze the Bitcoin networks, using network analysis and taking future behavior changes depending on the spread of individual behavior to other neighboring or connected traders into consideration.

Although we are aware of very little study on Bitcoin networks that integrates the analysis from both graph theory and network science viewpoints in the present day, we have included relevant research on two recently publicly accessible networks. In [8], the authors introduced a Self-supervised Temporal-aware Dynamic Graph representation Learning framework (STDGL) that separates temporal shift embedding from temporal consistency embedding in dynamic graphs (BTC Alpha and BTC OTC), thereby addressing the shortcomings of previous methods. By using a self-supervised approach that takes into account both local and global connectivity modeling for nodes, STDGL

improves the interpretability of graph representations and outperforms state-of-the-art techniques while providing attractive interpretability and transferability from the disentangled node representations. The article [9] introduces DWSGCN, a directed weighted signed graph convolutional network, for community discovery. To overcome limitations, the authors suggest novel aggregation algorithms inspired by social psychological theories, implement a weighted adjacency matrix to represent link direction and weight and apply a modularity maximization loss to signed networks such as the BTC Alpha network. The community-oriented node embedding is achieved through the joint optimization of DWSGCN with a structural loss, resulting in end-to-end community identification. The research [10] explores the importance of network embedding and the constraints of existing graph neural networks (GNNs) in absorbing edge weight information in signed networks, particularly weighted signed BTC Alpha and BTC OTC networks. The proposed WSNN model aims to address these shortcomings by reconstructing link signs, link directions, and signed directed triangles at the same time, demonstrating its superiority over state-of-the-art algorithms in graph representation learning for signed networks via extensive experiments on real-world datasets. The criticism stems from a lack of particular details on the limitations of existing GNNs, as well as a lack of a comparative analysis with other proposed models in the field, which might provide a more comprehensive evaluation of WSNN's performance. Several works introduce the structural behavior of Bitcoin networks, such as extracting latent structural information [11], curriculum representation learning [12], balancing structure, and position information [13], that are not points of interest to the work we described in this manuscript.

In addition, the survey [14] explores the area of cryptocurrency transaction network embedding (CTNE). It explores upcoming trends in CTNE, assesses the effectiveness of commonly used methods, reviews publicly available Bitcoin datasets, and classifies recent advances in CTNE methodologies. By providing a thorough review of current CTNE techniques, the study hopes to stimulate more research in this important and developing field by addressing both static and dynamic perspectives. In order to investigate the dynamic perspective, the article [15] explores the field of adversarial social network analysis, focusing on the difficulty of avoiding FGA, an edge weight prediction technique intended for signed weighted networks. The study, which focuses on the theoretical underpinnings and computational characteristics of FGA, shows that, in contrast to many other tools, this approach is robust against adversarial actions and presents practical challenges for manipulation in addition to being difficult to manipulate optimally. The authors of [16] describe GCN_MA, a node representation learning framework that integrates Graph Convolutional Networks (GCN), Recurrent

Neural Networks (RNN), and multi-head attention for dynamic network link prediction. By combining global and local viewpoints and applying an algorithm known as Node Representation, which is based on the Node Aggregation Effect (NRNAE), this method successfully captures temporal evolution patterns and comprehensively represents structural properties. The efficiency of the suggested strategy is demonstrated by experimental findings on six datasets, where it outperforms the most advanced baseline methods in link prediction. In a similar work [17], authors tackle the problem of encoding the dynamics and sign semantics of dynamic signed networks found in real life, where edges have sign semantics that can be both positive or negative and change over time. Balance theory and ordinary differential equations (ODE) are incorporated into node representation learning in the proposed Dynamic Signed Network Embedding (Dyna-miSE) method to address the problem of over-smoothing in network dynamics learning. Through building a more complex dynamic signed graph neural network, DynamiSE seeks to efficiently represent the complex sign semantics resulting from positive and negative edges.

Furthermore, there is a noteworthy scarcity of literature addressing the reliability of Bitcoin networks. The scarcity of research in this area highlights the necessity for extensive studies on analyzing and comprehending the trust dynamics within Bitcoin networks. The authors of [18] investigate the improvement of adversarial attacks on the Fairness and Goodness Algorithm (FGA) and Review to Reviewer (REV2) in the context of trust prediction within signed graphs. The study focuses on the iterative trust dynamics processes in FGA and REV2, revealing strong and weak relationships within FGA as well as preferable pathways in REV2. The development of a novel vicinage attack capitalizes on these results to strategically target edges along influential pathways, advancing adversarial attack tactics and giving deeper insights into trust dynamics patterns in signed graphs. Some other studies, such as the application of recognizing fairness in financial services [19] and identification of influence maximization throughout temporal networks [20, 21], explore the dynamics of influence and fairness inside temporal networks, offering information on how these features evolve.

We intend to use some news spread models to identify the spread of behaviors of Bitcoin traders over the Bitcoin networks. The news spread model studies community information spread. The model assumes that new, exciting, and intriguing information will be shared more. This means that current or future news is more likely to spread. The model has been used to investigate political campaign information, natural disasters, and disease propagation. As the news spread model relies on people connectivity, there are many graph theory and network science studies on network analysis and news spread on networks. In [22] authors used a Value-weighted Mixture Voter (VwMV) model that

detects anti-majority opinionists. They add the anti-majoritarian tendency of each node as a new parameter to the value-weighted voter model and learn this parameter and the value of each opinion from a social network's observed opinion data. They also show theoretically that the local opinion share can be approximated by the average opinion share. Several pieces of literature use the Voter Model in the context of news spread in a network, such as [23–25].

We are ensembling disease spread models with news spread models to identify the behavior spread of Bitcoin traders. The disease spread models along with news spread models are used in literature for network dynamics predictions. On six classical networks, in [26] authors mimic the epidemic spreading experiment in accordance with the Susceptible-Infected (SI) model, the static attacking study, and the node differentiation experiment. For susceptible-infected (SI) disease spreading over a heterogeneous human interaction network, authors of [27] alter the degree-based compartmental model. The suggested model is based on the finding that state variables in the conventional model develop similarly for degree classes with equal degrees. As a consequence of other people's opinions, a person's beliefs may alter, which may have an impact on how they now feel. The authors of the work in [28] typically use a concept or point of view that is commonly purposely handed from one person to another. such as opinions in support or opposition to vaccination. In this paper, a variety of modeling techniques are examined in connection to the underlying interactions and updating process, including models like the Susceptible-Infected-Susceptible Model, Voter Model, and Bilingual Model.

We adopt and ensemble the Susceptible-Infected-Susceptible model, the Bilingual model, and the Voter model in our works to identify the dynamic of behavior spread over cryptocurrency networks. This is done for the purpose of determining the trustworthiness of Bitcoin traders and their influence on the trusty behavior of neighboring traders whom they nominated by voting. Additionally, we conduct a straight network analysis to determine trustworthiness in terms of network science and graph theoretical perspective. The method that we used in order to do this assignment will be dissected in the next part in excruciating depth.

Preliminaries and Backgrounds

To identify the influence of neighbors in the BTC-Alpha and BTC OTC networks in the behavior dynamics from trusty to suspicious or vice versa in case of analysis of cryptocurrency stability, we use network metrics analysis, as well as find future changes in behavior by using an ensemble of three news spread and epidemic spread models. The subsequent part of this section will discuss the definition of the problem of this work, the preliminaries required, and the associated background studies

that we employed in our work, but which will not be addressed in the methodological portion of this work.

Problem Definition

Our scope and interest in this study are illustrated briefly in the Definition 1 below. The symbols and preliminaries are discussed in “Preliminaries” section.

Definition 1 (*iTrustBD: influence of trust behavior dynamic*) Finding the trusty behavior (\mathcal{T}_B) and/or suspicious behavior (\mathcal{S}_B), from normal behavior (\mathcal{N}_B) of Bitcoin alpha networks, which consists of trusty traders (\mathcal{T}), normal traders (\mathcal{N}), and suspicious traders (\mathcal{S}).

Preliminaries

- μ_m : Mutation factor. The probability that random traders evolved trusty behavior.
- β_T, β_S : The rate at which trusty (\mathcal{T}) or suspicious (\mathcal{S}) neighbors influence normal (\mathcal{N}) neighbours, respectively.
- μ_T, μ_S : The rate at which originally normal (\mathcal{N}) neighbors go back to normality (\mathcal{N}_B) from trusty behavior (\mathcal{T}_B) or suspicious behavior (\mathcal{S}_B), respectively.
- σ_C^i : The proportion of neighbors of trader i in the class C , ($C \in \{\mathcal{N}_B, \mathcal{T}_B, \mathcal{S}_B\}$).
- $p_{C_j \rightarrow C_k}^i$: Transition probability of trader i from C_j to C_k .

Influence Analysis Models

In numerous ways, network nodes influence the behavior of their neighbors. One method is the spread of information. When a node exchanges information with its neighbors, it influences their behavior effectively. This is due to the increased likelihood that the neighbors will behave similarly to the node that supplied the information. The creation of links is a second means by which nodes impact their neighbors. When one node connects to another, it effectively establishes a link between their respective behaviors. This indicates that the likelihood of the nodes influencing one another's behavior has increased. In this work, we used the following spread analysis models used in networks.

Suceptible-Infected-Suceptible (SIS) Model [29]

The SIS model of an epidemic has two states: susceptible and infectious. The model is used to examine disease propagation and epidemic circumstances. SIS is a simple model for studying the transmission of infectious illnesses. The model can be used to explore the effect of contact rate, infectiousness, and recovery rate on the epidemic spread. The model can also be used to examine intervention effects

on the epidemic spread. The model can be used to examine vaccination's effect on the epidemic's spread. The continuum equation characterizing the SIS model's network dynamics can be described using Eq. (1).

$$\frac{di_k}{dt} = \beta(1 - i_k)k\Theta_k t - \mu i_k \quad (1)$$

where β is the infection rate, i_k is the k -degree infected node, $\Theta_k(t)$ represents the infected neighbors of a susceptible node k , μ is the recovery rate, and the term μi_k indicates the presence of recovery procedures. The total fraction of infected nodes grows with time, based on the SIS model as the Eq. (2).

$$i = i_0 \left(1 + \frac{\langle k \rangle^2 - \langle k \rangle}{\langle k^2 \rangle - \langle k \rangle} \left(e^{\frac{t}{\tau^{SIS}}} - 1 \right) \right) \quad (2)$$

where i_0 is the number of initially infected individuals and τ^{SIS} represents the characteristics time for the spread of the pathogen that is described by the Eq. (3).

$$\tau^{SIS} = \left(\frac{\langle k \rangle}{\beta \langle k^2 \rangle - \mu \langle k \rangle} \right) \quad (3)$$

For a scale-free network, the epidemic threshold of the SIS model is described using Eq. (4).

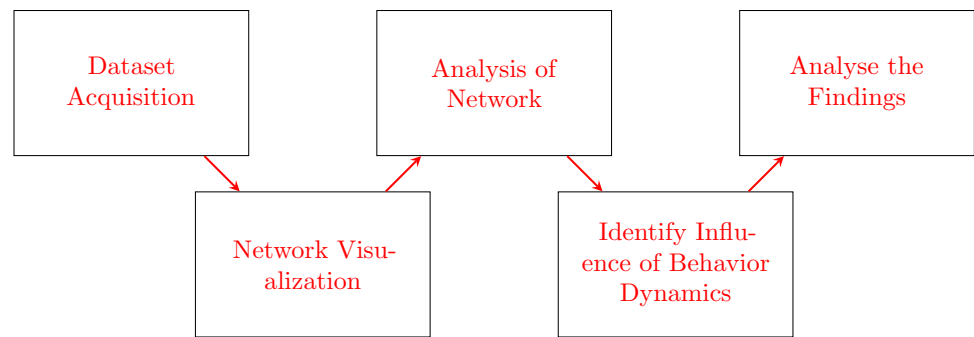
$$\lambda_C = \frac{\langle k \rangle}{\langle k^2 \rangle} \quad (4)$$

Bilingual Model [28]

The bilingual model considers neutral nodes as bilingual individuals, that are able to communicate with both parties. A monolingual can decide to adopt the opposing language and become a bilingual if it has the incentive to communicate with some of its neighbors. A bilingual can be induced to abandon one of the two languages if it has not necessary to know it to speak to its friends.

Voter Model ([30])

A straightforward model of the dynamics of opinion in social networks is the voter model. It is predicated on the notion that people's opinions are impacted by those in their immediate surroundings. The model is used to research how ideas circulate on social media and how they might be swayed by outside forces like marketing or the media. The approach can be applied to research how social media affects public opinion. In the traditional voter model, one voter resides at each of the N nodes in a random static graph. Picking a voter uniformly at random, having that voter adopt the state of a

Fig. 1 The brief workflow of iTrustBD**Table 1** Summary of Bitcoin datasets in terms of their format and statistical properties

<i>Dataset statistics</i>		
Properties	BTC Alpha	BTC OTC
Nodes	3783	5881
Edges	24,186	35,592
Range of edge weight	– 10 to + 10	– 10 to + 10
Percentage of positive edges	93.00%	89.00%
<i>Dataset format</i>		
Heads	Descriptions	
SOURCE	Node id of source, i.e., rater	
TARGET	Node id of target, i.e., ratee	
RATING	The source's rating for the target, ranging from – 10 to + 10 in steps of 1	
TIME	The time of the rating, measured as seconds since Epoch	

random neighbor, and repeating this process until consensus is necessary is how opinions evolve.

Methodology

The methodology, to identify the influence of trust behavior in a cryptocurrency network, used in this research project adheres to the workflow described in Fig. 1. A detailed description of the workflow is included in the subsequent part of this section, and the data, other information, and codes are available.²

Dataset Acquisition

We use a cryptocurrency traders' network, which is a who-trusts-whom network of Bitcoin traders on a platform called Bitcoin Alpha³ and Bitcoin OTC.⁴ Because Bitcoin users are unknown, it is necessary to keep track of their reputation

in order to avoid transactions with fraudulent or hazardous individuals. Members of Bitcoin AlphaOTC assess other members on levels on a scale of – 10 (complete distrust) to +10 (complete trust). These are the first specified weighted signed directed network that is available for study, called “Bitcoin Alpha Trust Weighted Signed Network”⁵ and “Bitcoin OTC Trust Weighted Signed Network”⁶ [31, 32].

Dataset Statistics and Format

The dataset consists of the following statistical properties and the format illustrated in Table 1.

Dataset Acquisition Process

To acquire both Bitcoin networks in its present form we need the following minor edition-

- Class: The class of each trader (node).

² <https://dataparadox.github.io/iTrustBD/>.

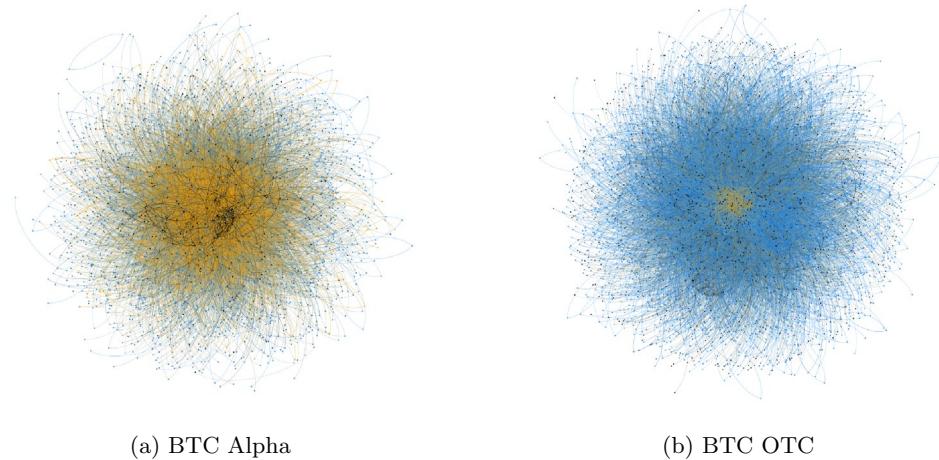
³ <https://www.btc-alpha.com/en>.

⁴ <https://www.bitcoin-otc.com/>.

⁵ <https://snap.stanford.edu/data/soc-sign-bitcoin-alpha.html>.

⁶ <https://snap.stanford.edu/data/soc-sign-bitcoin-otc.html>.

Fig. 2 Initial state of the Bitcoin networks found from both datasets



- Trusty Class (\mathcal{T}): +1
 - Normal Class (\mathcal{N}): 0
 - Suspicious Class (\mathcal{S}): -1
- The class label of the node v is calculated using Eq. (5).

$$v_{Class} = \begin{cases} -1 & \text{if } deg^{w-}(v) < 0 \\ +1 & \text{if } deg^{w-}(v) \geq \frac{2L\langle w \rangle}{N} \\ 0 & \text{Otherwise} \end{cases} \quad (5)$$

where $deg^{w-}(v)$ represent the weighted in-degree of node v , L is the number of edges in the network, N is the number of nodes in the network, and $\langle w \rangle$ represents the average weight of the network.

Network Visualization

The network generated from our BTC Alpha dataset is visualized in Fig. 2a. The orange node in the network represents trusty (\mathcal{T}) class, individuals. The network has 36.48% of trusty individuals. 54.96% of the individuals are normal (\mathcal{N}) in the class label, which is represented here using the blue color. Rest 8.56% are the suspicious (\mathcal{S}) individuals who are represented in the network using black nodes. The edges have adopted the color of the source nodes. For the BTC OTC dataset, the percentage of individuals with normal (\mathcal{N}) behavior is 84.14 %, trusty (\mathcal{T}) behavior is 2.02 %, and suspicious (\mathcal{S}) behavior is 13.84 %, which are marked with the colors blue, orange, and black respectively in Fig. 2b .

Analysis of the Bitcoin Networks

The section includes network metrics analysis and the network degree distribution analysis of the BTC Alpha and BTC OTC networks to find their types. The following parts of this section discuss that analysis.

Network Metrics Analysis

The properties of the networks for some important metrics are shown in Table 2. The robustness of the network is reflected by the average degree and weighted average degree. For both networks, the average and weighted average degrees are relatively high given their density. For a variety of reasons, the average degree is crucial for network robustness. The average degree is a measurement of how many connections each node in the network has to other nodes. A high average degree increases the likelihood that a node will be connected to certain other nodes in the network and hence be capable of communicating with them. As a result, they are therefore less likely to be cut off from the rest of the network. The average degree, which measures redundancy in the network, is the second factor. Because redundancy ensures that other nodes can step in if one fails, it is crucial for a network's robustness. The likelihood that the network will be able to continue to operate even if one node fails as a consequence. The network's robustness is measured by

Table 2 Network properties of Bitcoin datasets

Metrics	BTC Alpha	BTC OTC
<i>Average degree</i>	6.393	6.052
<i>Average weighted degree</i>	9.360	6.125
<i>Diameter</i>	10	11
<i>Average path length</i>	3.679	3.719
<i>Density</i>	0.002	0.001
<i>Clustering coefficient</i>	0.078	0.177
<i>Weakly connected components</i>	5	4
<i>Strongly connected components</i>	540	1144
<i>Modularity</i>	0.724	1.421
<i>Number of communities</i>	130	126
<i>Average clustering coefficient</i>	0.156	0.149
<i>Degree correlation coefficient</i>	-0.086	-0.083

the average degree, which is the last factor. The network's robustness is its capacity to bounce back after a failure. A network with a high average degree is more likely than a network with a relatively low degree to be able to recover from a failure. The robustness of this network indicates the stability of the cryptocurrency network and its trustworthiness.

Diameter is essential in network robustness because it measures the longest and shortest path among any two nodes in a network. A network with a big diameter is more resilient because it can continue to function even if some nodes are not linked to the rest of the network. In both BTC Alpha and BTC OTC, the diameters are greater on a wide scale compared to the average path length.

The degree to which a network of nodes tends to cluster together is quantified by the clustering coefficient. Nodes seem to be more likely to establish connections to adjacent nodes when the clustering coefficient is high, whereas nodes are far more likely to connect to distant nodes when the clustering coefficient is low. Since nodes are more likely to be able to identify alternate paths if one path is blocked, high clustering coefficients are sometimes regarded as an indicator of network robustness. On the other hand, low clustering coefficients might be viewed as an indication of fragility because they suggest that a single node loss could result in significant disruptions. Comparatively speaking, the clustering coefficients of both BTC Alpha and BTC OTC are not that high, but it is enough for the network robustness which provides the stability of the cryptocurrency transaction based on our selected networks.

Modularity is essential in network durability because it provides for the recognition of smaller, more connected groupings within the network. This can be advantageous in two ways. First, if one or more of these groups becomes disconnected from the rest of the network, the others can continue to operate independently. Second, if the network as a whole is attacked or fails, these small communities can provide some redundancy and allow the network to function. Similarly, connected components play a role in network robustness. This happens because they determine which sections of the network are linked and which are not. This data can be used to identify which areas of the network are more sensitive to attack or failure, and which are more likely to continue functioning. In addition, community structure plays a significant role in network robustness. This is due to its ability to determine which areas of the network seem to be more tightly connected to one another. This data can be used to determine which areas of the network are more vulnerable to an attack or failure and which ones are more likely to remain operating. In our networks, the number of strong clusters and communities with high modularity values represents the high robustness of the network structure.

Since the degree correlation coefficient (r) for both BTC Alpha and BTC OTC networks are negative in value, both networks are disassortative. Disassortativity is a measure of how closely nodes in a network are linked to nodes that are significantly different from them. A disassortative network has nodes that are more likely to be connected to nodes that are significantly different from them, whereas an assortative network has nodes that are more likely to be connected to nodes that are similar to them. It has been discovered that disassortativity is important for network robustness. This is due to the fact that disassortative networks are even less likely to be adversely affected by the removal of a small number of nodes because the nodes that are removed are less likely to be similar to each other and thus less likely to be connected.

Because the BTC Alpha, as well as BTC OTC networks, has been found to be robust based on their network properties and metrics, we can assert that both networks are capable of resisting attacks and providing the trustworthiness of the cryptocurrency transaction system. As a consequence, the stability of the cryptocurrency system increases which is dependent on the network structure's robustness.

Network Distributions Analysis

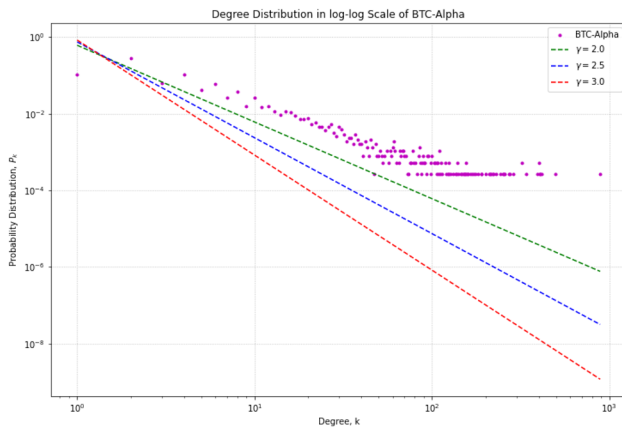
We have done a study on the degree distribution of both BTC Alpha and BTC OTC networks to determine their kind before continuing our investigation into their attributes. The findings of this degree distribution provided the answers to two significant research questions that will be covered in this section.

ResearchQuestion 1. *Is there any network behavior that the BTC Alpha and/or BTC OTC dataset adheres to?*

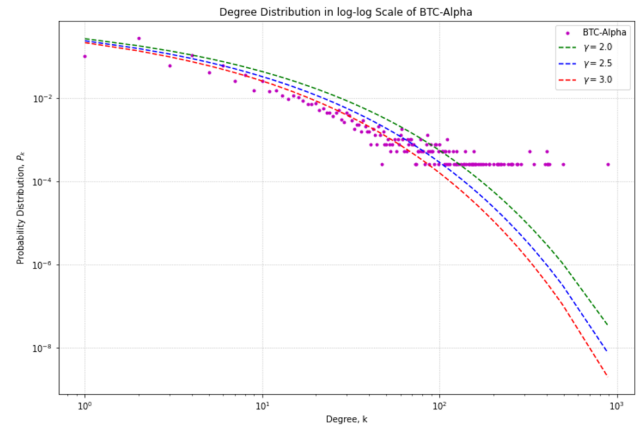
Calculating the degree distribution of both Bitcoin networks is one way that we attempt to address research question 1. The findings indicate that each network represented by both BTC Alpha and BTC OTC datasets is not consistent with the power laws equation that is presented in Eq. (6). However, our investigation revealed that it had the characteristics of a scale-free network. Therefore, we investigate the characteristics of equations based on power laws using a stretched version of the one found in Eq. (7). The output of the degree distribution was appropriate for the stretched power level's characteristics. Figure 3 presents the probability degree distribution for both the direct power law and the stretched power low exponent. As a result, we are in a position to assert that both BTC Alpha and BTC OTC networks demonstrate the characteristics of a scale-free network.

$$\rho_k = \frac{k^{-\gamma}}{\zeta(\gamma)} \quad (6)$$

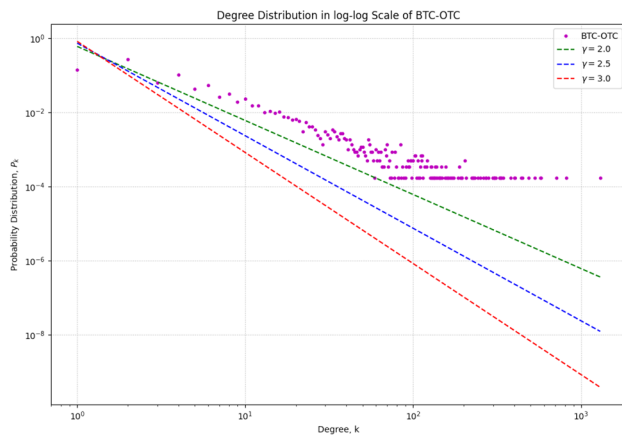
where $\zeta(\gamma)$ is the Riemann-zeta function.



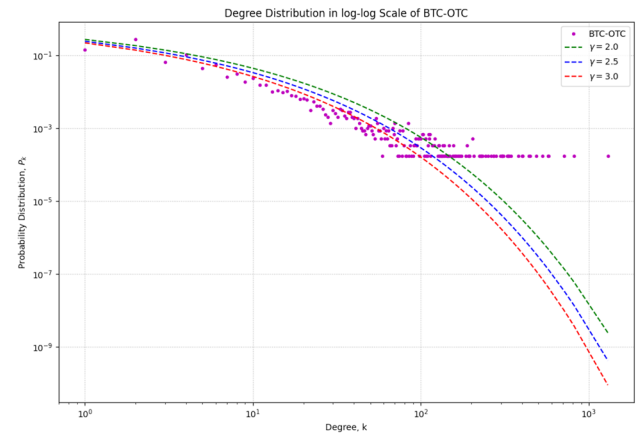
(a) Degree Distribution on BTC Alpha



(b) Stretched Degree Distribution on BTC Alpha



(c) Degree Distribution on BTC OTC



(d) Stretched Degree Distribution on BTC OTC

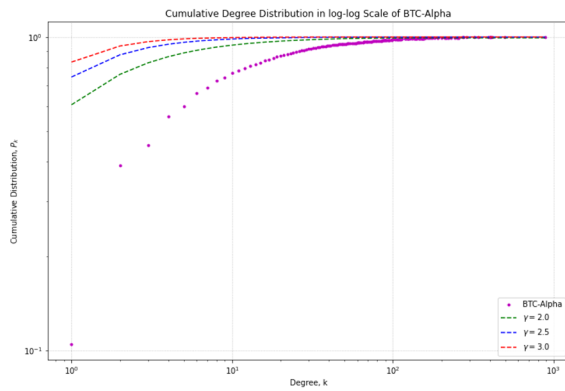
Fig. 3 Degree distributions of the Bitcoin networks with power-law degree distribution

$$\begin{aligned}
 P(x) &= e^{(-\gamma x)^\beta} \\
 P\{x\} &= Cx^{B-1} e^{(-\gamma x)^\beta} \\
 C &= \beta\gamma^\beta
 \end{aligned}
 \quad (7)$$

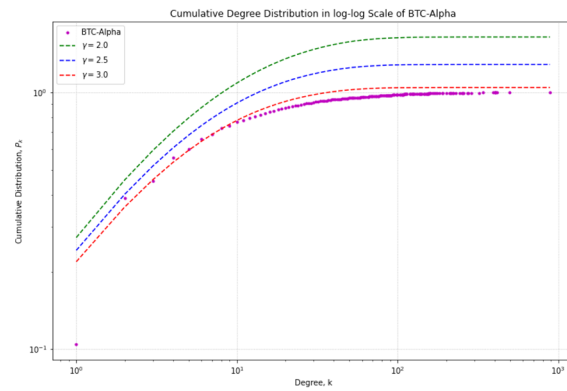
where $\beta = 0.38$, which is the stretching exponent.

The power-law distribution function of a network's nodes is the characteristic that defines the scale-free nature of a network. This indicates that a small number of nodes have a significant number of connections, whereas the majority of nodes have just a small number of connections. Two different aspects of a network's resilience are influenced by its scale-free nature. To begin, the network is more robust to random failures when it has a smaller number of nodes that have a greater number of connections between them. This is due to the fact that there are always a select few nodes that have a high number of connections and are therefore able to

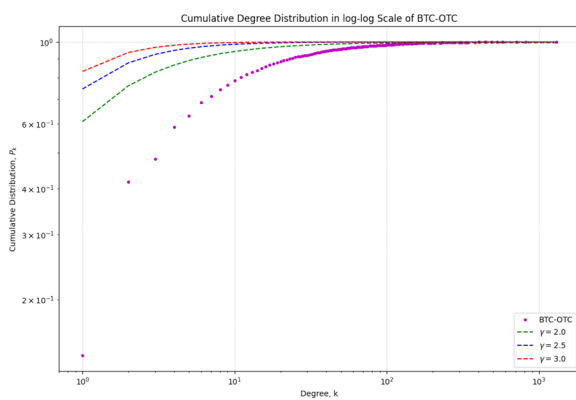
function as backups for other nodes in the network. Second, the fact that a network is scale-free makes it more immune to attacks that are specifically aimed at it. This is due to the fact that it is extremely challenging to single out all of the nodes that have a high number of connections in order to stop the network. The number of hubs in the network is enough due to the fact that the network can expand without restriction. The capacity of a network to survive structural damage is one of the most important factors in determining its robustness. Networks that include a small number of nodes that are extremely well linked to one another, often known as hubs, are more resistant to structural damage than networks that do not have hubs. As both BTC Alpha and BTC OTC networks have scale-free nature, they have more hubs. When a hub is removed from the network, the connectivity of the network decreases, and the network's ability to tolerate harm also decreases. If, on the other hand, the hub is changed



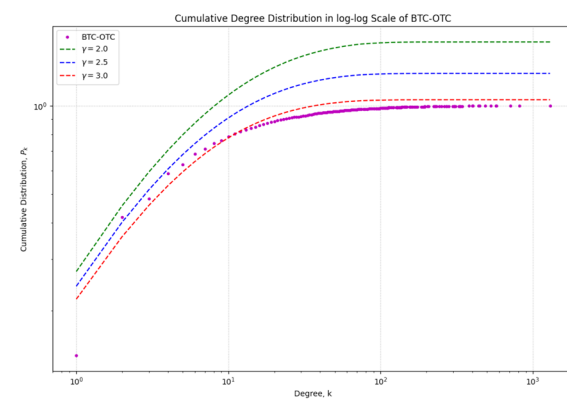
(a) Cumulative Degree Distribution on BTC Alpha



(b) Cumulative Stretched Degree Distribution on BTC Alpha



(c) Cumulative Degree Distribution on BTC OTC



(d) Cumulative Stretched Degree Distribution on BTC OTC

Fig. 4 Cumulative degree distributions of the Bitcoin networks with power-law degree distribution

out for another node in the network, the robustness of the system will rapidly return to where it was before. Therefore, if we consistently observed traders in BTC Alpha and BTC OTC networks that had more connections, cryptocurrency transactions would be more risk-free, and it would aid in the system's ability to continue.

ResearchQuestion 2. *Do the news spread or epidemic spread models provide promising inferences in the BTC Alpha and/or BTC OTC datasets?*

We draw the cumulative degree distribution of our works against the degree of each individual. The results show that the green dashed line of standard behavior dynamics of scale-free networks is approximately fitted by our works illustrated in Fig. 4 with blue dots for both BTC Alpha and BTC OTC networks. The standard curve in our work follows the scale-free networks curve that was analyzed before, such as collaboration networks, the sex web, etc. The curves are drawn based on the power laws theorem shown in Fig. 4a for BTC Alpha and Fig. 4c for BTC OTC networks, and stretched exponential power laws shown in

Fig. 4b, and Fig. 4d for BTC Alpha, and BTC OTC networks respectively.

The sole network metrics study only gives the robustness of a static network. Using static metrics analysis of the network, one cannot discover any information regarding future predictions or dynamical changes in the behavior of nodes. Because of this, we make use of epidemic, and news spread models to determine the changes in behavior on the network, which are explained in the next section.

Identify Influence of Behavior Dynamics

The identification of the influence of neighbors in the Bitcoin networks based on the behavior of individuals is mimicked using the Algorithm 1. The network is divided into the following compartmentalization groups discussed below, to identify the influence of trusty-worthiness dynamics throughout the networks.

Algorithm 1 iTrustBd: An algorithm for identification of the influence of trust behavior dynamics.

```

1: dataset  $\leftarrow$  Bitcoin dataset
2: t  $\leftarrow$  0
3: repeat
4:   t  $\leftarrow$  t + 1
5:   behaviorSpreadNeighbor(dataset)  $\triangleright$  Adopt behavior from Neighbors at a
      certain rate.
6:   behaviorSpreadMutate(dataset)  $\triangleright$  Homogeneous mixing with certain
      mutation rate.
7:   Start selectRandom  $\triangleright$  Models are chosen at random to remove the bias
      caused by factors in a particular model.
8:     modelSIS(dataset)
9:     modelVoter(dataset)
10:    modelBilingual(dataset)
11:   End selectRandom
12: until we run out of time or found promising inference

```

Compartmentalisation

The network is classed based on an individual's status during a deterministic time step of the identification process. Based on the epidemic modeling, the simplest categorization implies that an individual can be in one of three states or compartments, such as -

- Susceptible (S): Healthy people who have not yet come into touch with the virus.
- Infectious (I): Contagious persons who have come into touch with the disease and can thereby infect others.
- Recovered (R): Individuals who have previously been affected but have recovered from the sickness and are hence not infectious.

We aim that in our model of influence dynamic there is no recovered state based on the properties of the network. In our works, we map the epidemic model in our task of behavior dynamics based on the following techniques in the next part of this section.

Behavior Spread

Trusty (\mathcal{T}) and Suspicious (\mathcal{S}) traders are thought of as infectious nodes in our work. An infectious trader can share the behavior with some Normal (\mathcal{N}) neighbors (susceptible), making them change state to infectious behavior. We assume that the initial infectious nodes (i_0) remain infectious state forever, hence, we represent them as extreme infectious traders. An infectious but extreme trader will remain

infectious forever; hence, the only admitted transition is from normal to infectious.

Homogeneous Mixing

The homogeneous mixing hypothesis holds that each person has the same probability of coming into touch with an infected (trusty or suspicious) individual. This concept reduces the requirement to identify the exact contact network via which the disease spreads. That led to the conclusion that anyone can infect anyone else. In iTrustBD, we used the notion of mutation factors in behavior dynamics to test this theory, which states that 1% of individuals can be randomly changed to a new behavior from another behavior.

Behavior Spread Based on Neighbors

In our work, only traders with normal behavior are influenced by infectious traders based on their infectious neighbors. We assume 5% random influence in behavior spread from each trader's neighbors outside of model influence.

Susceptible-Infected-Susceptible (SIS) Model

The SIS model, often known as the contact process model, is an epidemiological model. A population of N people are divided into two divisions in a SIS model: susceptible (\mathcal{S}) and infected (\mathcal{I}). Only when a susceptible person comes into contact with an infected person does the disease spread. The SIS model is adopted in our work as follows and can be described using the model equations in Eq. (8).

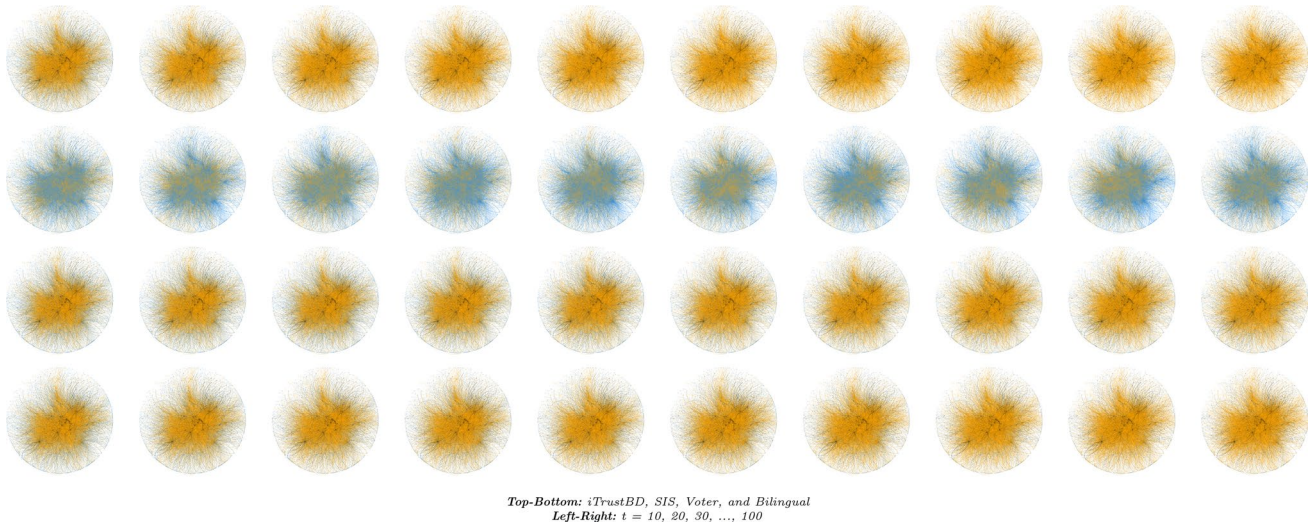


Fig. 5 Network visualization over time for BTC Alpha network

- Trusty (\mathcal{T}) and Suspicious (\mathcal{S}) traders are Infected individuals.
- Normal (\mathcal{N}) traders are Susceptible individuals.

$$\begin{aligned}\mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{T}_B}^i &= \sigma_{\mathcal{T}_B}^i \beta_{\mathcal{T}} \\ \mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{S}_B}^i &= \sigma_{\mathcal{S}_B}^i \beta_{\mathcal{S}} \\ \mathcal{P}_{\mathcal{T}_B \rightarrow \mathcal{N}_B}^i &= \mu_{\mathcal{T}} \\ \mathcal{P}_{\mathcal{S}_B \rightarrow \mathcal{N}_B}^i &= \mu_{\mathcal{S}}\end{aligned}\quad (8)$$

Bilingual Model

The bilingual model considers neutral nodes to be bilingual individuals who can communicate with both parties. If a monolingual has the incentive to communicate with some of their neighbors, he or she may elect to adopt the opposing language and become a bilingual. A bilingual can be persuaded to abandon one of the two languages if it is not required to know it to interact with friends. The Bilingual model is adopted as the following based on the Eq. (9)-

- Trusty (\mathcal{T}) and Suspicious (\mathcal{S}) traders are monolingual.
- Normal (\mathcal{N}) traders are bilingual.

$$\begin{aligned}\mathcal{P}_{\mathcal{S}_B \rightarrow \mathcal{N}_B}^i &= \sigma_{\mathcal{T}_B}^i \beta_{\mathcal{S}} \\ \mathcal{P}_{\mathcal{T}_B \rightarrow \mathcal{N}_B}^i &= \sigma_{\mathcal{S}_B}^i \beta_{\mathcal{T}} \\ \mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{S}_B}^i &= (1 - \sigma_{\mathcal{T}_B}^i) \mu_{\mathcal{S}} \\ \mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{T}_B}^i &= (1 - \sigma_{\mathcal{S}_B}^i) \mu_{\mathcal{T}}\end{aligned}\quad (9)$$

Voter Model

In the conventional voter model, N voters reside at the nodes of a random static network, with one voter per node. The development of opinion is simple itself, since -

- Randomly selects one individual voter.
- This voter adopts a random neighbor's state.
- Repetition is required until consensus is attained.

The voter model is adopted in our work as illustrated in Eq. (10), which consider following-

- Trusty (\mathcal{T}) and (\mathcal{S}) traders act as random neighbors.
- Normal (\mathcal{N}) traders are voter.

$$\begin{aligned}\mathcal{P}_{\mathcal{S}_B \rightarrow \mathcal{N}_B}^i &= \sigma_{\mathcal{N}_B}^i \beta_{\mathcal{S}} \\ \mathcal{P}_{\mathcal{T}_B \rightarrow \mathcal{N}_B}^i &= \sigma_{\mathcal{N}_B}^i \beta_{\mathcal{T}} \\ \mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{S}_B}^i &= \sigma_{\mathcal{S}_B}^i \mu_{\mathcal{S}} \\ \mathcal{P}_{\mathcal{N}_B \rightarrow \mathcal{T}_B}^i &= \sigma_{\mathcal{T}_B}^i \mu_{\mathcal{T}}\end{aligned}\quad (10)$$

In our research, we use these three models with homogeneous mixing and neighbor influence to predict the future state of the cryptocurrency network using the BTC Alpha and BTC OTC networks. The results are thoroughly examined in the following section.

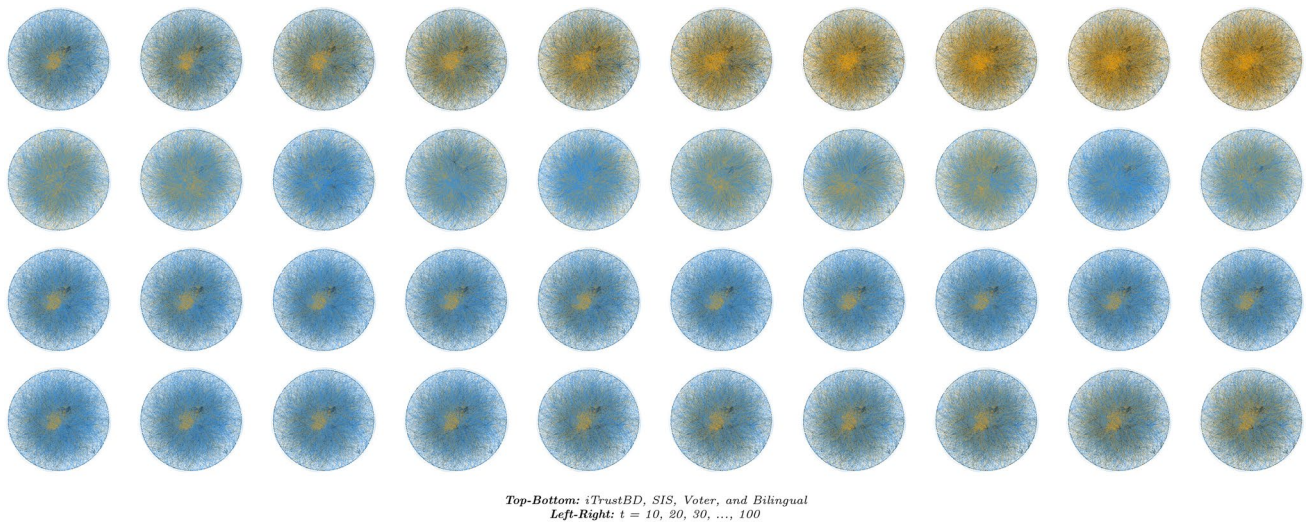


Fig. 6 Network visualization over time for BTC OTC network

Table 3 Percentage of individuals' behavior on Bitcoin networks

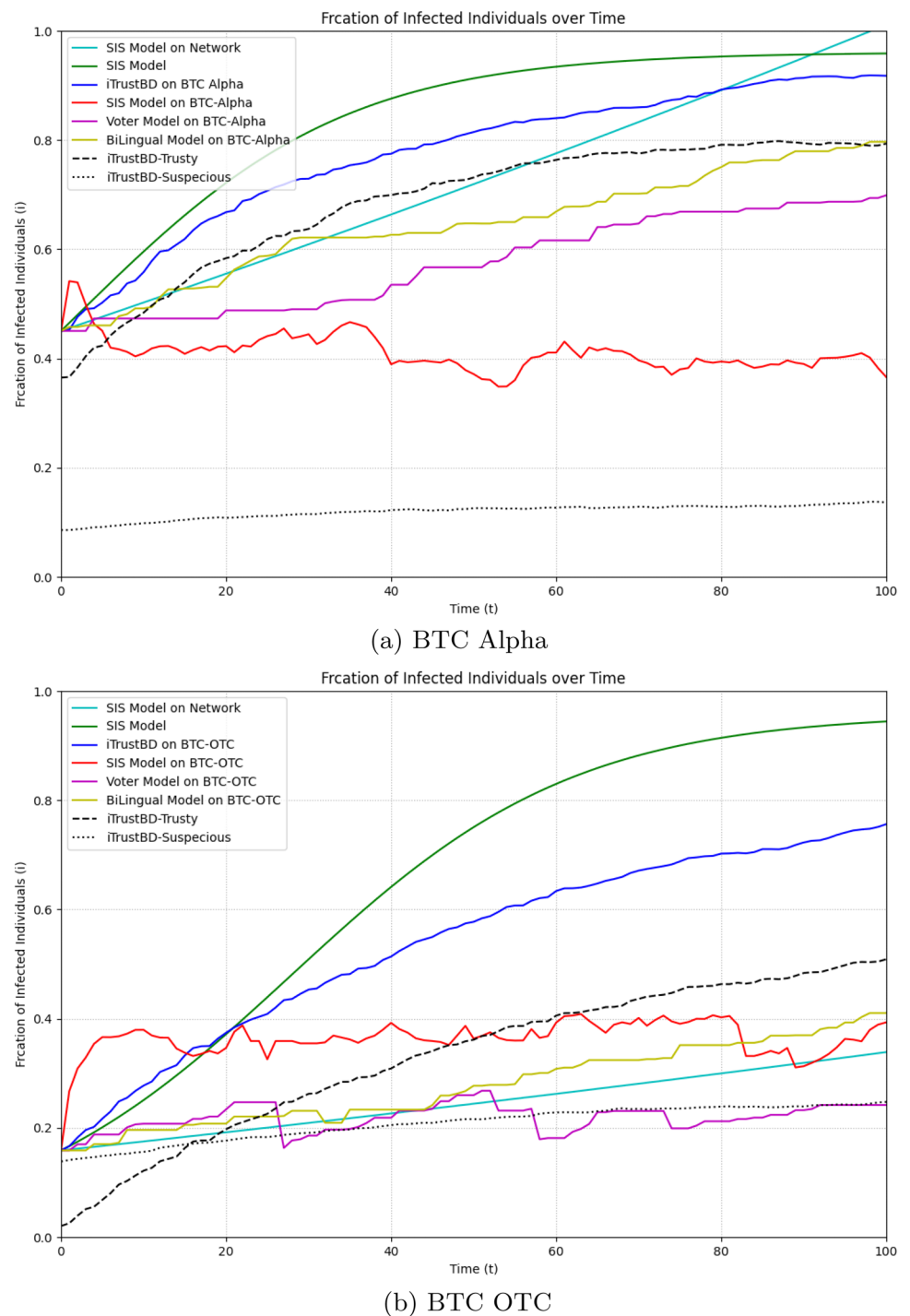
Datasets	Epoch (t)	iTrustBD			SIS			Voter			Bilingual		
		N (%)	T (%)	S (%)	N (%)	T (%)	S (%)	N (%)	T (%)	S (%)	N (%)	T (%)	S (%)
BTC Alpha	0	54.96	36.48	8.56	54.96	36.48	8.56	54.96	36.48	8.56	54.96	36.48	8.56
	10	44.20	46.18	9.62	59.08	37.35	3.57	52.68	38.59	8.72	50.83	40.07	9.09
	20	33.20	56.60	10.20	57.73	39.25	3.01	51.20	40.05	8.75	45.28	44.75	9.97
	30	27.09	61.91	11.00	55.56	41.37	3.07	50.99	40.18	8.83	37.85	51.31	10.84
	40	22.52	65.64	11.84	61.06	35.98	2.96	46.50	44.44	9.07	37.35	51.70	10.94
	50	18.53	69.20	12.27	62.86	34.02	3.12	43.30	47.45	9.25	35.26	53.74	11.00
	60	15.99	71.56	12.45	58.92	37.99	3.09	38.38	52.02	9.60	33.10	55.96	10.94
	70	14.01	73.33	12.66	60.35	36.61	3.04	35.29	54.67	10.04	29.82	59.24	10.94
	80	10.76	76.55	12.69	60.56	36.48	2.96	33.12	56.70	10.18	24.95	63.94	11.10
	90	8.62	78.51	12.87	61.01	35.98	3.01	31.46	58.18	10.36	22.05	66.30	11.66
BTC OTC	100	8.22	78.40	13.38	63.42	33.54	3.04	30.11	59.45	10.44	20.33	67.94	11.74
	0	84.14	2.02	13.84	84.14	2.02	13.84	84.14	2.02	13.84	84.14	2.02	13.84
	10	72.27	12.14	15.59	62.05	30.91	7.04	79.26	6.16	14.59	80.39	5.02	14.59
	20	62.59	19.74	17.67	65.36	28.41	6.22	76.62	8.45	14.93	79.24	5.95	14.81
	30	54.68	26.24	19.08	64.53	20.61	10.68	81.41	4.17	14.42	76.87	7.74	15.39
	40	48.63	30.88	20.49	60.77	31.71	7.52	78.15	6.85	15.00	76.67	8.37	14.96
	50	42.27	36.13	21.59	63.65	30.06	6.29	74.02	10.20	15.78	72.28	11.87	15.85
	60	36.63	40.55	22.82	60.72	32.55	6.73	81.87	3.74	14.39	69.19	14.22	16.60
	70	32.89	43.63	23.48	59.87	33.46	6.67	76.91	8.03	15.07	67.59	15.30	17.11
	80	29.77	46.34	23.89	59.77	33.85	6.38	78.80	6.16	15.05	64.85	17.53	17.62
	90	27.73	48.36	23.91	68.71	22.89	8.40	76.77	7.70	15.52	63.05	18.57	18.38
	100	24.38	50.88	24.74	60.67	31.90	7.43	75.82	8.20	15.98	58.97	22.48	18.55

N (%): Percentage of individuals with normal behavior

T (%): Percentage of individuals with trustworthy behavior

S (%): Percentage of individuals with suspicious behavior

Fig. 7 Fraction of infected individuals over time on Bitcoin networks



Result Analysis

As demonstrated in Fig. 5 for the BTC Alpha dataset and Fig. 6 for the BTC OTC dataset with epoch time $t = 10, 20, 30, \dots, 100$, the outcome of the conventional SIS model without any modification demonstrates that the effects of any individual's behavior in networks to other neighbor individuals have random impact. Though both Voter and Bilingual

models in BTC Alpha and BTC OTC datasets show better dynamics to the influence of neighbor behavior, the dynamics are very slow in influencing its neighbor. However, our research utilizing iTrustBD demonstrates a smooth increase and decrease in individual behavior dynamics in terms of Bitcoin trading shown in Fig. 5, and Fig. 6 for both BTC Alpha and BTC OTC dataset respectively, including

trustworthiness, normality, and suspiciousness, which represent a good scale of dynamics of behavior across the network.

According to the conventional SIS, Voter, Bilingual models, and the iTrustBD, the change in behavior class throughout the network is depicted in Table 3. The iTrustBD model in our work gives solid guesses that can roughly match any epidemic spread or news spread model, whereas the conventional SIS model predicted behavior changes that were random in nature. Though, both Voter and Bilingual models provide better results than the SIS model, the behavior dynamics applying them are slower than the behavior dynamics of iTrustBD.

The results of our research are represented graphically in Fig. 7 utilizing the trusted individual's changes through time as an epoch number to represent the changes of the infected individual for both BTC Alpha and BTC OTC datasets. The straight cyan lines in Fig. 7a, b illustrate the percentage of infected behavior over time for any network with a large number of users as described by "Suceptible-Infected-Suceptible (SIS) Model [29]" section. The conventional SIS model described by Eq. (11) is depicted by the curvature of the continuous green lines. The blue continuous line in Fig. 7b represents the results of our study using the iTrustBD which provides a close approximation to the conventional SIS model in the BTC Alpha network. We found similar performance on the BTC OTC network illustrated by the continuous blue curve shown in Fig. 7b. The results we found by applying Voter and Bilingual models on both Bitcoin networks are shown by continuous magenta and yellow colors, those representing both Voter and Bilingual models have produced slower dynamics in behavior changes of neighbors than our iTrustBD model. The black dashed line represents trustworthy individuals, while the black dot lines represent suspicious individuals. When we display both infected individuals, trusty and suspicious individuals separately, they both exhibit identical properties of the conventional SIS model's curve. In our Bitcoin datasets, we evaluated the traditional SIS model without making any assumptions or fabrications. However, the conventional SIS model's curves on our Bitcoin networks are red continuous lines indicating the random variations in behaviors over time.

$$\frac{di}{dt} = \beta \langle k \rangle i(1-i) - \mu i$$

$$i = \left(1 - \frac{\mu}{\beta k}\right) \frac{Ce^{(\beta \langle k \rangle - \mu)t}}{1 + Ce^{(\beta \langle k \rangle - \mu)t}} \quad (11)$$

where the initial condition $i_0 = i(t=0)$ gives $C = \frac{i_0}{1-i_0 - \frac{\mu}{\beta \langle k \rangle}}$.

On the basis of our Bitcoin networks, it is therefore acceptable to state that the outcome of the iTrustBD gives the future dynamics that indicate the stability of the cryptocurrency network. Additionally, because both Bitcoin

networks we use are scale-free in nature, they also provide hubs immunization (thinking of the reverse process of real immunization as the infected individuals, trusted or suspect, are beneficial for the Bitcoin networks). The security will improve if we take control of the hubs since they have an impact on how most network users behave due to the scale-free network's ultra-small world characteristics. If hubs can be made to appear trustworthy, the impact of suspicious people will be reduced since the hubs will encourage trustworthy conduct among all of the neighbors. As a result, it is feasible to regulate Bitcoin networks globally, including Bangladesh, using just hubs and not all individuals.

Discussions and Conclusion

Utilizing news spread models to infer the behavior spread model is the key contribution of our research. The new behavior may need more time to get established before it spreads, though. Therefore, rather than using the iteration period for real reflection, we need to define the time period. Our efforts do not take into consideration the addition or deletion of nodes or links. Consequently, in the framework of future scopes, we may think about the temporal frame as well as the addition or deletion of nodes and linkages.

Both BTC Alpha and BTC OTC networks are robust and capable of withstanding attacks, according to the examination of their network parameters. Because of these network characteristics, it increases their reliability. Hence, both Bitcoin cryptocurrency systems are more risk-free and reliable. For more successful inference in the future, we might consider the ensemble of models in logically specified ways. This investigation and analysis of the Bitcoin networks may aid in the process of approving cryptocurrencies for use in Bangladesh and other countries. The regularized ensemble of three behavior spread models discussed here can halt the equilibrium state of the individual model and the bias induced by the individual model. It could facilitate the process of creating the best-anticipated network that we need. Additionally, using three models rather than just one eliminates any bias that could be carried through the choices of influence factors utilized in a single model. Finally, if cryptocurrency is legalized in other countries including Bangladesh, our work provides the anticipated reliable traders for future transactions.

Acknowledgements The authors would like to express their gratitude to Prof. Dr. Md. Nasim Akhtar, Department of Computer Science and Engineering, Dhaka University of Engineering and Technology, for his contributions to the validation, formal analysis, and investigation during the revision process of this article, and helping in writing - review & editing. Additionally, they acknowledge Prof. Dr. Md. Saidur Rahman, Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology and Abu Wasif, Associate

Professor, Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology for their guidance, supervision, valuable suggestions, and insightful comments throughout the time line of this work.

Author Contributions Md. Jahidul Islam: Conceptualization, Methodology, Formal analysis, Investigation, Data collection, Writing - original draft, Writing - review & editing. Md. Rakibul Islam: Validation, Formal analysis, Investigation, Writing - original draft. Md. Abul Basar: Validation, Formal analysis, Investigation, Writing - original draft.

Funding No funds, grants, or other support was received.

Data Availability The authors mentioned this in the Methodology section of this manuscript.

Declarations

Conflict of interest The authors declare no Conflict of interest.

Competing interest The authors state that none of the work described in this publication appears to have been influenced by any known competing financial interests or personal relationships.

Consent to Participate Not applicable.

Consent to Publish Not applicable.

Ethical Approval Not applicable.

Informed Consent Not applicable.

Statement Regarding Research Involving Human Participants and/or Animals Not applicable.

References

- Wu J, Liu J, Zhao Y, Zheng Z. Analysis of cryptocurrency transactions from a network perspective: an overview. *J Netw Comput Appl*. 2021;190: 103139.
- Vidal-Tomás D. Transitions in the cryptocurrency market during the covid-19 pandemic: a network analysis. *Finance Res Lett*. 2021;43: 101981.
- Setyono JC, Suryawidjaja WS, Girsang AS. Social network analysis of cryptocurrency using business intelligence dashboard. *High-Tech Innov J*. 2022;3(2):220–9.
- Hong MY, Yoon JW. The impact of covid-19 on cryptocurrency markets: a network analysis based on mutual information. *PLoS ONE*. 2022;17(2):0259869.
- Baldwin J. In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Commun*. 2018;4(1):1–10.
- Sas C, Khairuddin IE. Exploring trust in bitcoin technology: a framework for HCI research. In: *Proceedings of the annual meeting of the Australian Special Interest Group for Computer Human Interaction*. 2015. p. 338–42.
- Chang V, Hall K, Xu QA, Wang Z, et al. A social network analysis of two networks: adolescent school network and bitcoin trader network. *Decis Anal J*. 2022;3:100065.
- Liu L, Wen G, Cao P, Yang J, Li W, Zaiane OR. Capturing temporal node evolution via self-supervised learning: a new perspective on dynamic graph learning. In: *Proceedings of the 17th ACM International Conference on Web Search and Data Mining (WSDM '24)*. Association for Computing Machinery, New York, NY, USA, 2024;443–451. <https://doi.org/10.1145/3616855.3635765>
- Cheng H, He C, Liu H, Liu X, Yu P, Chen Q. Community detection based on directed weighted signed graph convolutional networks. *IEEE Trans Netw Sci Eng*. 2023;11(2):1642–1654. <https://doi.org/10.1109/TNSE.2023.3328637>
- Lu Z, Yu Q, Li X, Li X, Yang Q. Learning weight signed network embedding with graph neural networks. *Data Sci Eng*. 2023;8(1):36–46.
- Zhang Z, Wan S, Wang S, Zheng X, Zhang X, Zhao K, Liu J, Hao D. Sga: a graph augmentation method for signed graph neural networks. 2023. arXiv preprint [arXiv:2310.09705](https://arxiv.org/abs/2310.09705).
- Zhang Z, Liu J, Zhao K, Wang Y, Han P, Zheng X, Wang Q, Zhang Z. Csg: curriculum representation learning for signed graph. 2023. arXiv preprint [arXiv:2310.11083](https://arxiv.org/abs/2310.11083).
- Hoang TL, Ta VC. Balancing structure and position information in graph transformer network with a learnable node embedding. *Expert Syst Appl*. 2024;238: 122096.
- Zhou Y, Luo X, Zhou M. Cryptocurrency transaction network embedding from static and dynamic perspectives: an overview. *IEEE/CAA J Autom Sin*. 2023;10(5):1105–21.
- Lizurej T, Michalak T, Dziembowski S. On manipulating weight predictions in signed weighted networks. 2023. arXiv preprint [arXiv:2302.02687](https://arxiv.org/abs/2302.02687).
- Mei P, Zhao Y. Dynamic network link prediction with node representation learning from graph convolutional networks. *Sci Rep*. 2024;14(1):538.
- Sun H, Tian P, Xiong Y, Zhang Y, Xiang Y, Jia X, Wang H. Dynamise: dynamic signed network embedding for link prediction. In: *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE; 2023. p. 1–2.
- Bu Y, Zhu Y, Geng L, Zhou K. Unleashing the power of indirect attacks against trust prediction via preferential path. 05 November 2023, PREPRINT (Version 1) available at Research Square. <https://doi.org/10.21203/rs.3.rs-3511555/v1>
- Song Z, Zhang Y, King I. Towards fair financial services for all: a temporal GNN approach for individual fairness on transaction networks. In: *Proceedings of the 32nd ACM international conference on information and knowledge management*. 2023. p. 2331–41.
- Mohammadi S, Nadimi-Shahraki MH, Beheshti Z, Zamanifar K. Fuzzy sign-aware diffusion models for influence maximization in signed social networks. *Inf Sci*. 2023;345:119174.
- Xiang N, Liu H, Tang X, Ma X. Information entropy-based node attribute influence maximization algorithm in signed networks. In: *2023 8th international conference on intelligent computing and signal processing (ICSP)*. IEEE; 2023. p. 1190–3.
- Kimura M, Saito K, Ohara K, Motoda H. Detecting anti-majority opinionists using value-weighted mixture voter model. In: Elomaa T, Hollmén J, Mannila H, editors. *Discovery science*. Berlin, Heidelberg: Springer; 2011. p. 150–64.
- Kimura M, Saito K, Ohara K, Motoda H. Opinion formation by voter model with temporal decay dynamics. In: Flach PA, De Bie T, Cristianini N, editors. *Machine learning and knowledge discovery in databases*. Berlin, Heidelberg: Springer; 2012. p. 565–80.
- Yamagishi Y, Saito K, Ohara K, Kimura M, Motoda H. Learning attribute-weighted voter model over social networks. In: *Asian conference on machine learning*. PMLR; 2011. p. 263–80.

25. Li Y, Chen W, Wang Y, Zhang Z-L. Voter model on signed social networks. *Internet Math.* 2015;11(2):93–133. <https://doi.org/10.1080/15427951.2013.862884>.
26. Ai J, He T, Su Z. Identifying influential nodes in complex networks based on resource allocation similarity. Available at SSRN 4203549. 2022.
27. Kandhway K. Susceptible-infected epidemics on human contact networks. In: *Proceedings of the 2022 fourteenth international conference on contemporary computing*. 2022. p. 514–9.
28. Lenti J, Ruffo G. Ensemble of opinion dynamics models to understand the role of the undecided about vaccines. *J Complex Netw.* 2022;10(3):cnac018. <https://doi.org/10.1093/comnet/cnac018>.
29. Barabási A-L, Márton P. *Network science*. Cambridge: Cambridge University Press; 2012.
30. Redner S. Reality-inspired voter models: a mini-review. *CR Phys.* 2019;20(4):275–92.
31. Kumar S, Spezzano F, Subrahmanian V, Faloutsos C. Edge weight prediction in weighted signed networks. In: *2016 IEEE 16th International Conference on Data Mining (ICDM)*. IEEE; 2016. p. 221–30.
32. Kumar S, Hooi B, Makhija D, Kumar M, Faloutsos C, Subrahmanian V. Rev2: fraudulent user prediction in rating platforms. In: *Proceedings of the eleventh ACM International Conference on Web Search and Data Mining*. ACM; 2018. p. 333–41.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.