# Exploring Trust Dynamics and Key Player Roles in the BTC-Alpha Network: Implications for Cryptocurrency Privacy and Security

Gwendoline Hays-Valentin & Charaf Zguiouar

April 3, 2024

University Paris 1 Panthéon-Sorbonne

*This project investigates the trust dynamics within the BTC Alpha cryptocurrency network by analyzing transaction data to identify anomalies and predict potential drops in network confidence. Utilizing an Isolation Forest algorithm, anomalous transactions indicative of unusual trust-related behavior—were detected. Network features, such as average trust given and received, along with anomaly detection results, were used as inputs to a machine learning model aimed at predicting the likelihood of significant shifts in trust. This approach enabled the correlation of trust pattern anomalies with historical events known to affect network confidence, such as the Bitcoin hack of February 2014. The findings offer insights into the propagation of trust and its resilience in the face of adversarial actions within the network, providing valuable implications for the design of robust trust-based systems in decentralized financial networks.*

## Introduction

Cryptocurrencies, spearheaded by Bitcoin, have revolutionized the financial landscape by introducing a decentralized platform for financial transactions. Unlike traditional banking systems, cryptocurrencies operate without a central authority, thereby necessitating mechanisms to establish and maintain trust among its users. The Bitcoin Over-The-Counter (OTC) platform is one such environment where trust plays a pivotal role in facilitating transactions. Users on the Bitcoin OTC platform can anonymously buy and sell bitcoins while relying on a reputation system to assess the trustworthiness of their counterparts.

This study delves into the "who-trusts-whom" network of Bitcoin traders from the Bitcoin OTC platform, employing the BTC-Alpha network dataset. This dataset is the first of its kind to offer a weighted signed directed network for research, presenting an unparalleled opportunity to analyze the dynamics of trust and its influence on the behavior within cryptocurrency networks. Understanding these dynamics is crucial for enhancing the privacy and security of transactions in decentralized financial systems.

## Dataset Information

The BTC-Alpha network dataset encompasses interactions between 5,881 users, documented through 35,592 trust/distrust relationships. Each edge in this network is weighted, representing trust on a scale from -10 (total distrust) to +10 (total trust), with an intriguing 89% of these edges being positive. This dataset not only facilitates the exploration of trust dynamics but also offers insights into the behavioral spread and influence within the network.

In this study, we leverage this rich dataset to undertake a dual-pronged exploration. First, we aim to visualize and quantify trust relationships and their changes over time, employing a variety of network analysis techniques. Next, we concentrate on modeling trust dynamics in the face of network perturbations, focusing particularly on the repercussions of the Mt. Gox Hack—a significant event that shook the Bitcoin community and serves as a natural experiment for observing trust resilience.

# Contents



# List of Tables



# List of Figures

Chapter 1

# Descriptive Statistics

## 1.1 Descriptive tables of the dataset

The tables provided offer a detailed statistical overview of the datasets concerning nodes, edges, and a specific dataframe labeled 'Transactions' that includes dates, Sources, Targets and their relevant trust rating. These summaries are instrumental in shedding light on the underlying characteristics and distributions within the data, which is pivotal for a comprehensive analysis.

### Summary for 'nodes' Dataset

| Attribute | Description |
|---|---|
| Id | Unique identifier for nodes |
| Class | Classification of nodes |
| In/Outdegree | Number of incoming/outgoing connections |
| Degree | Total number of connections |
| Eccentricity | Maximum distance from any other node |
| Centrality Measures | Includes closeness, betweenness, eigencentrality, etc. |
| Component Numbers | Indicators for components and strong components |
| Modularity Class | Community structure classification |
| Clustering | The degree to which nodes cluster together |

### Summary for 'edges' Dataset

| Attribute | Description |
|---|---|
| Source/Target | Identifiers for the source and target of an edge |
| Type | Type of edge (Directed) |
| Id | Unique identifier for edges |
| Label | Optional label for edges |
| Timeset | Timestamp or time-related attribute for the edge |
| Weight | Weight of the edge, indicating strength or capacity |

### Summary for 'Transactions' Dataset

| Attribute | Description |
|---|---|
| SOURCE/TARGET | Identifiers for the source and target entities |
| RATING | Rating or transaction value between the source and target |
| TIME | Timestamp for when the rating or transaction occurred |

### Summary Statistics for 'nodes'

| Variable | Mean | STD | Min | Median | Max |
|---|---|---|---|---|---|
| indegree | 6.39 | 16.41 | 0.0 | 2.00 | 398.0 |
| outdegree | 6.39 | 18.29 | 0.0 | 2.00 | 490.0 |
| Degree | 12.79 | 34.45 | 1.0 | 4.00 | 888.0 |
| Number of Nodes: 3783 | | | | | |

In the *Summary Statistics for 'nodes'*, we observe an intricate portrayal of network connectivity through attributes such as indegree, outdegree, and Degree. The similar mean values for indegree and outdegree suggest a balanced level of interaction among the nodes, with a high standard deviation indicating significant variability in connectivity. This variability is further underscored by the maximum values, hinting at the presence of highly connected nodes or "hubs" within the network. The dataset comprising 3783 nodes presents a moderately extensive network, offering ample data for nuanced network analysis.

### Summary Statistics for 'edges'

| Variable | Mean | STD | Min | Median | Max |
|---|---|---|---|---|---|
| Weight | 1.46 | 2.90 | -10.0 | 1.00 | 10.0 |
| Number of Edges: 24186 | | | | | |

Moving on to the *Summary Statistics for 'edges'*, the focus narrows down to the Rating attribute of the network's edges. This attribute, reflecting the strength or capacity of interactions between nodes, ranges from -10 to 10. The mean and median values hovering around 1, with the presence of negative ratings introducing an element of adversarial or negative interactions into the network dynamics. The dataset includes 24186 edges, providing a clear picture of the network's density and its interconnectedness.

**Summary Statistics for 'Transactions' with Dates**

| Variable | Mean | STD | Min | Median | Max |
|---|---|---|---|---|---|
| RATING | 1.46 | 2.90 | -10 | 1.00 | 10 |
| DATE Range | | | 2010-11-08 | | 2016-01-22 |
| Number of Rows: 24186 | | | | | |

Lastly, the *Summary Statistics for 'Transactions' with Dates* details the transactions from which node they come and to which node they have gone. The specified DATE Range from November 8, 2010, to January 22, 2016, encapsulates the temporal bounds of the dataset. With an identical row count to the edges dataset.

## 1.2 EDA

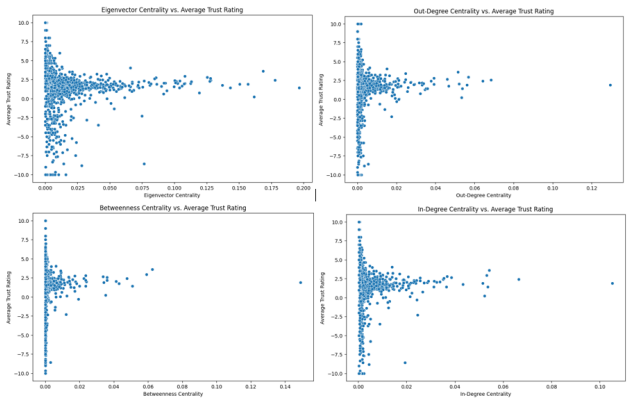


**Fig. 1.1:** Nodes' metrics versus the average rating

In plot (0,0) in Fig 1, the eigenvector centrality plot reveals that nodes with higher eigenvector centrality—those that are connected to well-connected nodes—tend to have a broad spectrum of average trust ratings. This indicates that being connected to influential nodes does not necessarily correlate with receiving higher trust ratings.

In plot (0,1) in Fig 1, focused on out-degree centrality, indicates a similar pattern to in-degree centrality. Nodes with a higher number of outgoing ratings (out-degree centrality) have average trust ratings that are less negative. This could suggest that nodes whose rate others more frequently are themselves rated more positively, or it might reflect that active participants in rating others are also more engaged and thus better trusted in the network.

In plot (1,0) in Fig 1. showing betweenness centrality versus average trust rating, there is a notable concentration of points toward the lower end of betweenness centrality, which indicates that many nodes with lower betweenness centrality scores have a wide range of average trust ratings. Interestingly, a few nodes with higher betweenness centrality also exhibit a range of trust ratings, from very high to very low. This suggests that nodes that

often act as bridges in the network, while critical to its connectivity, are not universally trusted or distrusted.

In plot (1,1) in Fig 1. depicting in-degree centrality against average trust ratings, also shows a diverse range of average trust ratings for nodes with lower in-degree scores. However, for nodes with higher in-degree centrality, the trust ratings tend to be less negative on average. This implies that nodes that receive more ratings (indicative of being rated by more peers) are generally trusted to a certain degree within the network.

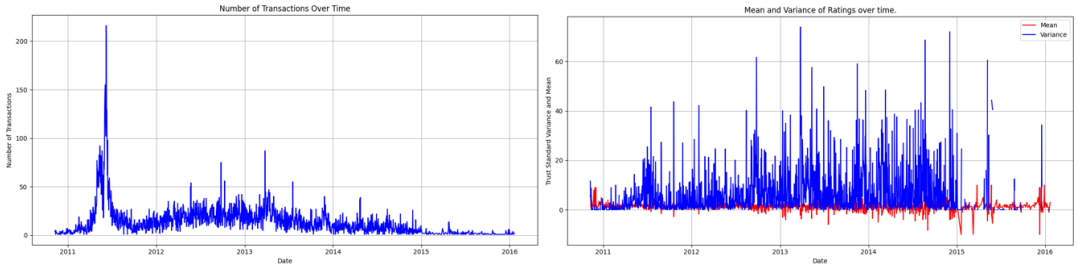


**Fig. 1.2:** The evolution of the number of transactions over time and the mean/variance of the ratings.

Fig 2. captures the and flow of the Bitcoin Alpha trust network's activity over time, showing the number of transactions and the average trust and variance expressed through ratings. A noticeable feature is the presence of sporadic spikes in transaction volume, which hint at moments when the network's activity surged significantly—potentially due to external influences or organic network growth. Accompanying this plot is a dual-line chart presenting both the mean and variance of ratings over time. The average rating, depicted in red, oscillates, reflecting the changing sentiment within the network, while the blue line indicating variance reveals the consensus (or lack thereof) among users. Periods of high variance suggest that users' perceptions were highly polarized, with some transactions being much more positively or negatively rated than the average. Drops of the average rating are correlated with jumps in variance, suggesting hightened levels of uncertainty.

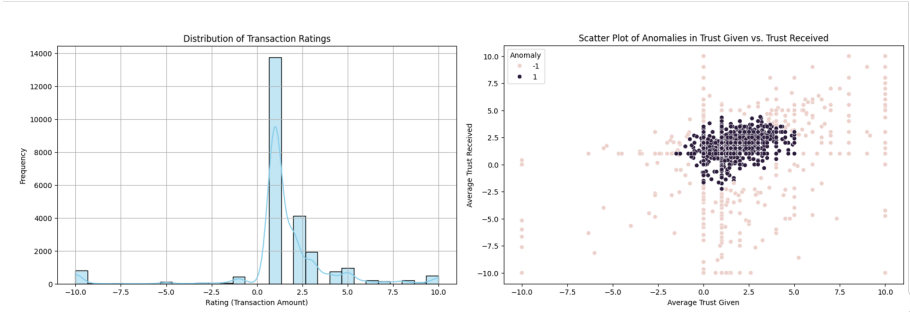


**Fig. 1.3:** The ratings distribution and a scatter plot of nodes that have similar levels of trust versus those who do not.

Finally, the third visualization focuses on the distribution of transaction ratings across the entire network, with a pronounced peak at the higher end of the positive ratings. This trend signals a general inclination toward trust among network participants, despite the

presence of negative ratings. Alongside the histogram, a scatter plot highlights anomalies in trust given versus trust received, identifying outliers in the dataset. These anomalies may represent individuals or entities whose rating behavior is atypical, either by rating others far more harshly or leniently than average, or by receiving such ratings themselves. These could be points of interest for further investigation, as they may indicate unique behavioral patterns, potential misuse, or nodes with exceptional circumstances within the trust network.

The data suggests that trust is not only multifactorial but also subject to the network's evolving interactions and perceptions, which are influenced by a myriad of underlying social and economic factors.

Chapter 2

# Network Plots

## 2.1 Visualisation of relationships of trust and mistrust

We decided to create a network highlighting the nodes and edges with the highest and lowest confidence weights.

### 2.1.1 Network plot & description

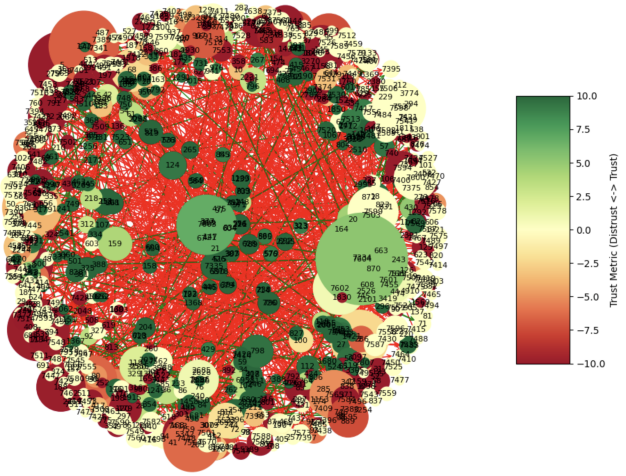


**Fig. 2.1:** High Trust and High Distrust Network with Color Scale for Nodes

The displayed network is a directed graph, reflecting a complex system of trust relations where each node represents a participant and each directed edge signifies a trust rating flowing from one participant to another. The visualization reveals a dense core, indicating a group of participants who are highly interconnected through trust or distrust relations. This core is surrounded by sparser areas, suggesting that a number of participants are central to the network's trust dynamics and that others are more peripheral with fewer connections.

The edges between the nodes are directed, which means they have a direction that shows from whom to whom the trust or distrust is flowing. This is crucial for understanding how trust is spread within the network.

The color scale is giving a clear reference for the trust metrics, ranging from -10 to +10, and allowing viewers to gauge the trust levels at a glance. The arrangement of the nodes and the pattern of connections can tell us about the network's structure, including which participants are trust hubs, who are more isolated, and if there are distinct communities or clusters where trust or distrust is particularly strong.

The insights drawn from these visual features will be further enriched by a subsequent analysis of statistical metrics. We will delve into specific network statistics such as the assortativity coefficient, average clustering coefficient, and network density. These will complement our visual analysis and enhance our understanding of the trust dynamics within the BTC-Alpha network.

### 2.1.2 Network Statistics and Exploration

| Metric | Value |
|---|---|
| Network Overview (Nodes, Edges) | (3783, 24186) |
| Average Degree | 3.326 |
| Density | 0.001987 |
| Transitivity | 0.0927 |
| Average Clustering Coefficient | 0.03651 |
| Assortativity Coefficient | -0.0550 |

**Table 2.1:** Key Network Statistics

The network is composed of **3783 nodes and 24186 edges**, indicating a substantial structure with multiple interactions among participants. This suggests a system where many agents interact, but the nature of these interactions requires further scrutiny. An average **degree** of 3.327 suggests that each node is connected to around 3 other nodes on average. In the context of social or trust networks, this implies that each participant on average evaluates or interacts with three others. This might reflect a certain hierarchy or specialization of roles within the network, with central actors playing key roles in connectivity.

The **very low density** of 0.001987 indicates that the network is largely underutilized compared to the total possible number of links. It signifies that the majority of participants do not trust or know each other, characteristic of a community where newcomers are frequent or distrust is widespread. A **transitivity of 0.0927** is low, indicating that participants in the network do not form tight-knit groups where everyone trusts each other mutually. The average clustering coefficient of 0.0365 supports this interpretation by showing that a given participant's neighbors are not inclined to trust each other, suggesting an absence of closed trust circles or cliques. An infinite average shortest **path length** suggests that the network contains disjoint components. This means there are groups of participants who are not connected by any path of trust or distrust, indicating the existence of isolated subgroups within the overall network.

With an **assortativity coefficient of -0.0550**, the network exhibits a non-assortative or disassortative tendency, meaning nodes tend to connect with other nodes dissimilar in degree terms. This could suggest interaction between very active participants and those less engaged, potentially reflecting a mentorship structure, hierarchy, or interactions between core and peripheral users.

The network appears to be characterized by a high degree of heterogeneity with areas of strong distrust, trust, and isolated subgroups. The low density and transitivity indicate that trust relations are specific and not widespread, which could be a sign of a network

where trust must be earned and is not lightly granted. Central actors may play a crucial role in facilitating or obstructing trust within the network, while the presence of disjoint components could indicate communication barriers or highly specialized subgroups.

## 2.2 Community detection over the time

### 2.2.1 Network plot & description

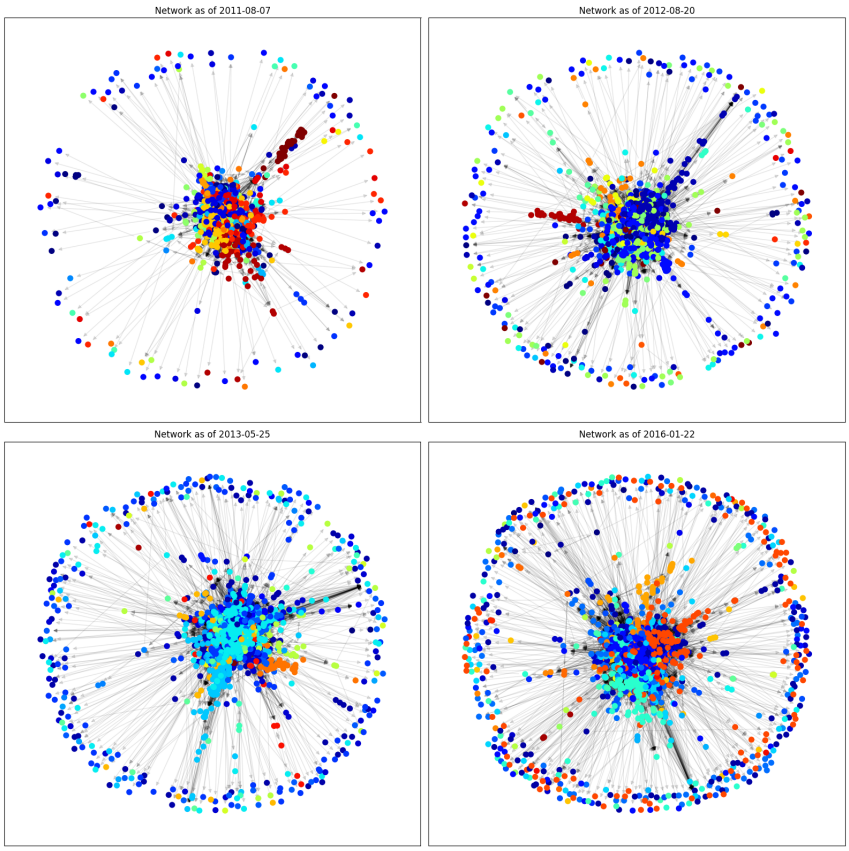


**Fig. 2.2:** Community detection over the time

The network visualization distinguishes distinct communities with a color-coded scheme, derived from the Louvain method. The idea was to provide four separate snapshots of a trust network at different points in time.

The network seems to be growing over time, with an increasing number of nodes (users) and edges (trust relationships) visible in later snapshots. This growth could imply more users participating in the platform or increased engagement over time.

Nodes are colored differently to represent different communities detected within the network. The distribution of colors across nodes shows how communities evolve. Early on, there are smaller, distinct clusters, but over time, one or two larger communities dominate, indicating consolidation or increased interconnectedness among users.

In the earlier networks, there are multiple central nodes (those with many connections) that serve as hubs, while in the later networks, we observe a tendency towards a more centralized structure, with a prominent core of highly interconnected nodes. This might suggest the emergence of influential users or central authorities within the network.

The increase in the network's density and clustering coefficient over time can be inferred from the visuals, suggesting that the network is becoming more tightly knit, with users tending to form more close-knit groups.

There are nodes on the periphery across all snapshots, some of which may have fewer connections or belong to smaller communities. Their persistent presence indicates that while some users become integrated into the larger structure, others remain on the outskirts of the trust network.

In some snapshots, particularly the later ones, we can observe nodes that appear to form bridges between communities (nodes that connect clusters of different colors). These bridge nodes are crucial for information flow and maintaining network cohesion.

While the overall size and density of the network appear to increase, the community structure (as indicated by color) seems to stabilize over time, with large, consistent communities forming. This may reflect a maturation of the network where user groups have established stable relationships.

These insights can be valuable for understanding social dynamics within the Bitcoin Alpha platform, such as how trust is built and how influence or authority emerges and consolidates within the community. Additionally, for stakeholders or analysts, understanding these patterns can help in making strategic decisions related to governance, community engagement, and platform design. We will now focus on the statistics.

### 2.2.2 Network Statistics and Exploration

| Date | Nodes | Edges | Avg Degree | Density | Avg Clustering |
|---|---|---|---|---|---|
| 2011-08-07 | 1300 | 5937 | 9.13 | 0.00352 | 0.0941 |
| 2012-08-20 | 2207 | 11807 | 10.70 | 0.00243 | 0.1247 |
| 2013-05-25 | 3044 | 17314 | 11.38 | 0.00187 | 0.1438 |
| 2016-01-22 | 3683 | 22650 | 12.30 | 0.00167 | 0.1671 |

**Table 2.2:** Network metrics for the Bitcoin Alpha trust network at four key timestamps.

The network grows in size over time, indicated by the increase in both the number of nodes (from 1,300 to 3,683) and the number of edges (from 5,937 to 22,650). This growth reflects an expanding system with more users and interactions. The average degree increases from around 9.13 to 12.30 over the observed periods, suggesting that, on average, users are forming more connections. This could imply stronger or more extensive trust relationships as the network matures.

Despite the growth in average degree, the network density decreases over time (from 0.0035 to 0.0017), which is typical for growing networks. As more nodes are added, the

potential number of connections grows quadratically, so unless the number of edges grows at the same rate, density tends to decrease. This decrease in density could also imply that the network's expansion is not fully dense and that there may be room for even more connections. The average clustering coefficient increases (from 0.094 to 0.167), which indicates a tendency for users to form tightly-knit groups. This might reflect growing trust within certain communities or user subsets, leading to more triangular connections (a sign of a robust social structure).

Visual observation suggested that the network structure became more centralized over time. This is somewhat supported by the increasing average clustering coefficient and average degree, which together could indicate that while users are forming more connections, they're doing so in a more cliquish or community-oriented manner. The increasing average degree and clustering coefficient in a growing network suggest that as the network matures, users tend to form more mutual connections and the trust relationships consolidate within communities.

The decrease in density alongside the increase in clustering may imply that it becomes harder for new users to integrate into the network as it grows, possibly needing to establish trust with well-connected individuals or nodes within established communities.

Together, the visual and quantitative analyses provide a comprehensive view of the network's development, highlighting the importance of both community structure and individual user behavior in the evolution of trust networks.

Chapter 3

# Questions and Answers

## 3.1 Simulations using the Independent Cascade Model: What impact does a drop of 50% confidence have on the market?

### 3.1.1 Definition

The *Independent Cascade Model (ICM)* is a stochastic process used to model the propagation of influence through a network. In the context of social networks, it simulates how information, behaviors, or viruses spread from person to person. The process begins with an initial set of active nodes (individuals) known as 'seed nodes'. At each discrete time step, active nodes have a single chance to activate their inactive neighbors, with a success probability predefined for each edge in the network. Activation means changing the state of a node from inactive to active, representing the adoption of information or behavior. The model iterates until no further activations occur, providing insight into the dynamics of spread within the network structure.

### 3.1.2 Trust Dynamics and self-fulfilling crises

Trust crises can be induced by external factors, but also endogenously by market participlants themselves.

> The evidence that large market moves occur on days without identifiable major news casts doubts on the view that price movements are fully explicable by news... (Cutler-Poterba-Summers, 1989) → "Excess volatility puzzle" (R. Shiller)

This observation suggests a significant role for endogenous factors in financial volatility, aligning with Shiller's Excess Volatility Puzzle, which posits that market prices exhibit more volatility than can be justified by changes in fundamental values alone. The phenomenon of endogenous jumps underscores the complexity of market dynamics, where participant behaviors can induce volatility independently of external news events. Such dynamics can erode trust in financial markets, as investors may perceive these movements as unmoored from fundamental economic indicators, leading to a feedback loop that exacerbates volatility. Understanding these endogenous mechanisms is vital for assessing market stability and the integrity of financial systems.

We can then rightly ask, how would a sharp instantaneous drop in confidence impact the network's structure? Which nodes would leave the network and become inactive?

### 3.1.3 Simulation of 50 percent drop of confidence using the ICM:

We use the ICM to simulate how a 50 percent drop in trust

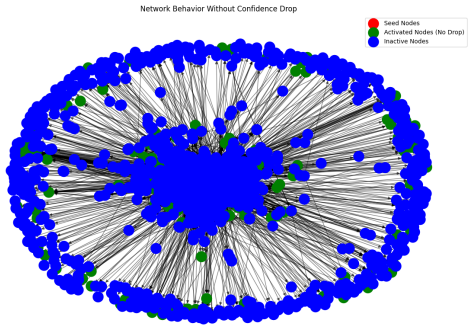


**Fig. 3.1:** Network Graph before the drop.

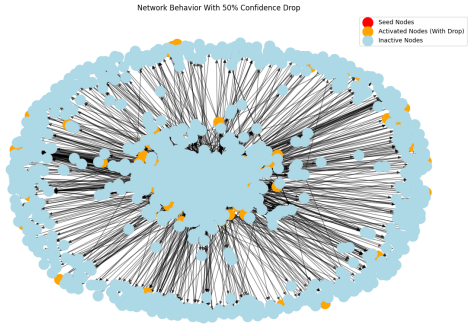


**Fig. 3.2:** Network Graph adfter the drop.

## Analysis of Activated Nodes

In the context of the Independent Cascade Model applied to our network, the term *activated nodes* refers to the nodes that have been influenced through the propagation process initiated by a set of seed nodes. Initially, the network exhibited a total of 924 activated nodes. This number represents the extent of the trust or influence spread across the network, starting from the seed nodes. The significant count of activated nodes signifies a robust level of trust propagation, indicating a strong and interconnected network where the nodes are highly influential and receptive to the spread of trust.

Following the 50% drop in confidence, there was a noteworthy decline in the number of activated nodes, which decreased to 592. This substantial reduction by approximately 36% is indicative of the heightened sensitivity of the network to variations in trust levels. The diminished propagation shows the impact of confidence levels on the network's structure and behavior.

The observed decrease in activated nodes from 924 to 592 shows that the network's dynamics are considerably affected by trust. Such a reduction in trust propagation can

lead to reduced transactions both in volume and number.

## 3.2 Machine learning algorithm : How likely is it that a node will leave its community in times of crisis or doubt?

The primary aim of this study is to investigate the likelihood of a node leaving its community in times of crisis or doubt, with a specific focus on the Mt Gox Hack as a pivotal crisis event. We plan to approach this by analyzing a dataset representing user relationships in the context of the Bitcoin Alpha network, identifying community structures before and after the crisis, and applying machine learning techniques to predict community changes in response to the crisis.

### 3.2.1 The case of Mt Gox Hack

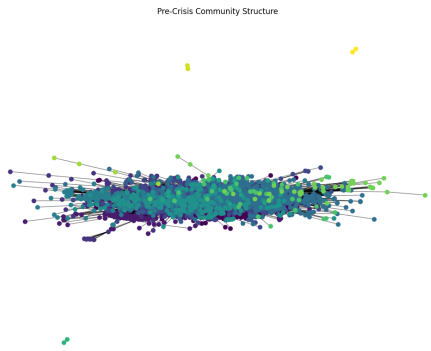


**Fig. 3.3:** Network Before the Crisis

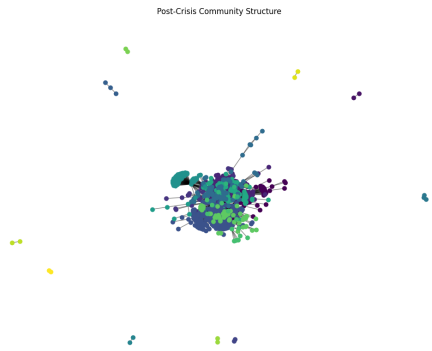


**Fig. 3.4:** Network After the Crisis

Figure 2.3 shows the network prior to the Mt Gox Hack, where nodes represent individuals or entities, and edges signify interactions. The diverse coloration corresponds to different communities, indicating a heterogeneous yet interconnected network structure. In contrast, Figure 2.4 captures the aftermath, where the redistribution of connections and the emergence of new clusters signal the network's response to the crisis. The transformation is noticeable, with some nodes relocating to new communities, possibly seeking stability or alignment with new allies in the face of uncertainty.

These visualizations are pivotal to understanding the nature of the question at hand: "How likely is it that a node will leave its community in times of crisis or doubt?" They underscore the need for a robust machine learning approach to predict potential shifts in allegiances and associations—shifts that could have far-reaching implications in the network's resilience and functionality.

### 3.2.2 Using an ML model : XG Boost

In response, we use an XGBoost model to delve deeper into the data. Beginning with an exploratory analysis to decipher the patterns within the pre-crisis network, we transition to detecting and predicting community changes as a result of the crisis. The algorithm's adeptness at handling class imbalance through SMOTE and its ability to fine-tune decision thresholds offers us a lens through which to gauge the probabilities of nodes transitioning between communities under stress. Our model's predictions, refined through meticulous optimization, aim to quantify the likelihood of such transitions, shedding light on the network's adaptability in the face of adversities like the Mt Gox Hack.

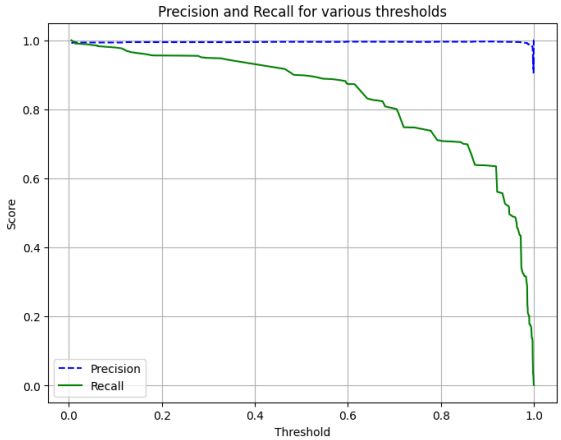


**Fig. 3.5:** Precision and Recall for various tresholds

The resulting model exhibits a nuanced capability to discern nodes that maintain their community allegiance with precision. However, the model demonstrates challenges in correctly identifying nodes that transitioned between communities, as indicated by the modest recall for the minority class. Upon optimizing the decision threshold to enhance the balance between precision and recall, we pinpoint a threshold value of approximately 0.031. This calibration improved the model's discernment between community stability and community change, culminating in a final precision of 0.75 and a recall of 0.18 for nodes that altered their community affiliation.

The adaptation we observed through the model's lens—while contending with the aftermath of the Mt Gox Hack—underscores the resilience and adaptability of the network's structure. Despite the crisis, the network's capability to sustain its cohesion while also permitting the flexibility of community reconfiguration stands evident.

Figure 2.5 presents the Precision-Recall curve, delineating the trade-off between the two metrics across various threshold values. The curve highlights the chosen threshold that yields the optimal F1 score for the minority class, marked distinctly for visual emphasis.

Table 2.1 contains the classification report, offering a tabulated view of the model's performance metrics post threshold adjustment. The accuracy and weighted average scores shows to the model's overall efficacy, whilst the macro average scores reveal the equilibrium between the recognition of community constancy and fluidity.

| Class | Precision | Recall | F1-score | Support |
|---|---|---|---|---|
| 0 | 0.04 | 0.55 | 0.08 | 20 |
| 1 | 0.99 | 0.85 | 0.92 | 1715 |
| Accuracy | | 0.85 | | 1735 |
| Macro avg | 0.52 | 0.70 | 0.50 | 1735 |
| Weighted avg | 0.98 | 0.85 | 0.91 | 1735 |

**Table 3.1:** Model result

### 3.2.3 Explanation for the low number of observations in the "0" class :

During the February 2014 hack, there has certainly been a noticeable drop in trust for a few days in the network. However, we postulate that such a drop has lead nodes for a few days to lower the number of transactions but not to fully leave their respective communities, and that probably they have chosen those communities in the first place because they trusted them, and that in times of stress their trust has not dropped dramatically due to this selection bias.

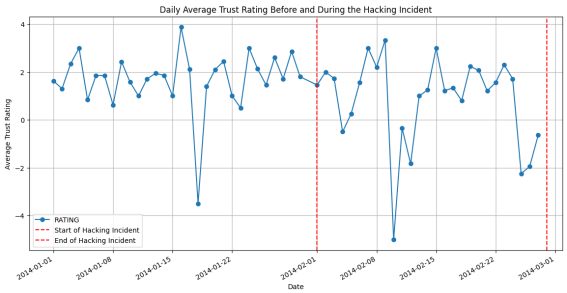


**Fig. 3.6:** The drop in the average trust recieved and given during February 2014.

### 3.2.4 Conclusion and Implications

Our study has illuminated the intricacies of predicting community transitions within networks during crisis scenarios. We've discerned that, although challenging, certain predictive markers can somewhat forecast a node's propensity for community shift. The model's precision in identifying the minority class suggests that distinct patterns signal impending changes, yet the comprehensive capture of these dynamics eludes us, as evidenced by the lower recall.

To accurately model the likelihood of nodes migrating between communities in times of uncertainty has proven to be a complex task. However, our findings indicate that social and transactional networks do exhibit preliminary indicators preceding such shifts, triggered by external disturbances.

It is imperative to acknowledge the study's limitations. The results hinge on the availability and quality of data, as well as the appropriateness of the selected features. Moreover, the inherent imbalance in the class distribution poses a significant challenge, potentially skewing the model's predictive capacity.

Moreover, extending this research to encapsulate diverse crises could unveil universal network behaviors during tumultuous episodes, thereby enriching our understanding of network resilience and adaptability in the face of adversity.

In sum, while our current model lays the groundwork for predictive analysis in network dynamics during crises, it also underscores the need for continuous refinement and expansion of scope to capture the nuanced fabric of community interaction and evolution.

Chapter 4

# Conclusion

This comprehensive study of the BTC-Alpha network has provided an insightful analysis into the multifaceted nature of trust within a decentralized financial system. Through an intricate examination of network plots, the simulation of trust dynamics under the Independent Cascade Model, and the application of machine learning algorithms, we have gained a nuanced understanding of the behavioral patterns and the robustness of trust in the wake of crises like the Mt. Gox Hack.

Our exploration began with visualizing trust and mistrust relationships within the network, revealing an evolving landscape of connections, community formations, and individual roles in the trust network. Quantitative measures such as network density, clustering coefficients, and centrality indices contributed to a richer picture of the network's anatomy over time, indicating a tendency towards more tightly-knit trust groups as the network matured.

Delving into the mechanics of trust dynamics, we applied the Independent Cascade Model to simulate the effect of a sharp drop in confidence, We have found that 50 percent drop in confidence induces A 36 percent drop in activated nodes. In trust-dependent networks, endogenously or exogenously induced drop are relevant, however given the evolving complex nature of such networks, trust chocs could emerge from within, it would interesting and worthwhile to study in advance how such crises emerge.

The use of an XGBoost machine learning model allowed us to predict community shifts, highlighting the model's adeptness at discerning nodes that maintain community ties and its struggle to identify those transitioning between communities. This dichotomy between precision and recall encapsulates the core challenge of predicting complex social behaviors under crisis conditions.

The study, while thorough, is not without its limitations. The predictive power of our models was constrained by the data available and was further complicated by the inherent class imbalance present within the network. These factors underscore the importance of continuous refinement of our methods and the expansion of the dataset for future research endeavors.

Looking ahead, this research paves the way for broader investigations into network behaviors during crises, which could inform the design of more resilient trust-based systems. By extending our analysis to a variety of crisis scenarios, we could better understand the universal patterns of trust dynamics and network adaptability—a pursuit that holds significant promise for enhancing the security and privacy of decentralized financial networks.

In closing, this study highlights the imperative need for robust analytical tools to navigate the ever-changing landscape of digital finance. The insights gained have improved our understanding how important trust can be in human networks and how the lack thereof in times of stress and severe uncertainty impacts the relationships between individual nodes and the overall structure of the network.

## 4.1 Contributions

We both worked on the project equally. First we drew up the plan together, then we used collaborative working solutions (Google Colab  Overleaf) to work on the different parts of the project. We each worked on the different parts of the project so that we could integrate our different points of view into the project. The report was also written by the two of us.