Caution in the Wind: Using Preferential Attachment to Assess Bitcoin Networks

Tom Goon, Isabelle Hren, & Leda Liang

Washington University, St. Louis, 63130

July 14, 2022

Abstract

Bitcoin and cryptocurrency in general is touted for its decentralized nature and the ability for the network to function independent of large entities, such as governments. Champions of cryptocurrency argue that by removing these large entities, cryptocurrency is creating a more free world. There exists data from Bitcoin OTC (a platform which handles Bitcoin transactions) on the Stanford SNAP database [1]. The network data consists of nodes representing transactors and edges representing transactions with timestamps attached as well as weights representing a trust score. We identifiy if this network follows the preferential attachment model. If the Bitcoin transaction network is truly decentralized, we should expect to see little evidence of preferential attachment. However, our hypothesis is that users tend to be more willing to transact with parties who are perceived as more trustworthy, which may lead to preferential attachment. This in turn would suggest that cryptocurrency would potentially succumb to requiring trustworthy entities and regulators, which would weaken the decentralized nature of cryptocurrency to begin with. To investigate this hypothesis, we analyze any correlations between the trustworthiness of a party and certain network statistics using NetworkX. This could open a potential route to investigate the binary prediction of transactors as trustworthy or not based on those network statistics. Kumar et al. developed an algorithm, REV2, to assess the goodness, fairness, and reliability of actors in a network [2].We give a synopsis and an intuitive interpretation of this algorithm as well as discussing the practicality of this method. Additionally, we examine the degree distribution to identify hubs and then go back in time and use Gephi to visualize how these "trustworthy" transactors came to be.

Keywords— **Signed Network Analysis**, **Preferential Attachment**, **Temporal Network Analysis**

Code

Github team name: `isabelle-hren-tgoon-ledaliang`
https://github.com/cse416a-sp22/final-project-isabelle-hren-tgoon-ledaliang

1 Introduction

Bitcoin has seen a rapid increase in popularity and mainstream acceptance over the last decade. It was first introduced by Satoshi Nakamoto in 2008 and featured the revolutionary idea of decentralized banking [4]. Traditionally, a central bank is responsible for financial stability. For example, a particularly relevant example duty of a central bank is to control inflation. A decentralized currency, such as Bitcoin, follows a decentralized framework where the idea is that no party, or small subset of individuals, should hold a majority interest in the currency. One reason why many perceive this as favorable is that it allows users to transact over international borders without the hassle foreign exchange rates.

Preferential attachment is a phenomenon where vertices with higher degree are more likely to accumulate more edges. The reason why we choose to caution the reader against this type of phenomenon in a Bitcoin trading platform is that it suggests that large entities form and amass a great deal of transactions. Although there could be an entire separate analysis on the human behaviour of this network and others like it, our hypothesis hinges on a higher trustworthy score indicating higher trust. However, what we found is a much greater reliance on a transactor having more transactions. A similar paradigm exists in any market platform like Amazon: do you trust the vendor with only a handful of 5 star reviews or the vendor with thousands of reviews averaging 4 stars? Typically it is the latter, and the most popular and in turn the most "trustworthy" tend to corner the market. In the end, there is reason to believe (although no guarantee) that cryptocurrencies will inevitably rely on huge entities to maintain trustworthiness and some sort of trustworthiness scale akin to a credit score would emerge either explicitly or implicitly. Whether or not this is a good thing is left open to the reader, but it is certainly not the freeing vision of cryptocurrency that many proponents dream of.

To conduct our investigation, we focus on network statistics including the degree distribution and "trustworthiness" over time. A series of graphs are visualized using gephi to give the reader a way to personally resonate with what is suggested. Transactions are weighted and temporal, meaning that users rate a transactions on a scale of -10 to 10 in steps of 1 and each transactions is labeled with the time. For a given transactor and transaction, the transaction is either considered outgoing, in which case the transactor is the one sending Bitcoin, or incoming in which case the transactor is receiving Bitcoin. We first perform a great deal of visualization concerning the incoming-outgoing nature. This is followed by analyzing the trustworthiness of outgoing transactions over time. This is because incoming transactions are less likely to be viewed unfavorably as large entities seemed to "okay" tons of transactions the same mute way. Lastly, we compare these insights with Kumar's ideas of goodness/fairness.

Thus our objectives can be generally split into two. First, we aim to provide evidence of the preferential attachment model in order to caution the reader against promised claims of cryptocurrency. Second, we wish to visualize the network at key times to extract interesting or important features of the network to pave the way for future research or to commentate on the nature of typical transactions.

2 Related Works

There is previous work by Gervais et al. analyzing whether Bitcoin is truly a decentralized currency [5]. Their findings show that while Bitcoin is controlled by any government, it does appear that there are a small number of individuals who hold control the majority of computing power in Bitcoin. They have observed "pools" of users who coordinate their computing resources. In 2013, it was found that the top 6 pools of users controlled over 75% of computing power in Bitcoin. This is striking because Bitcoin transactions were designed to require verification by other parties in the network to prevent fraud. However, having a minority hold so much power can undermine the integrity of the network if they are able to collude. While they are related, this paper focuses on the computing power rather than the volume of transactions made by different users.

Kumar et al. study the ability to predict fraudulent users in rating platforms [2]. This work explores how to quantify trust and fairness across a network. However, this metric relies on having access to training data that includes user ratings. They propose a linear time algorithm, Rev2, that predicts fraudulent users. This work does not analyze the consequences that trustworthiness can have on the degree distribution of a network such as the Bitcoin transaction network.

3 Dataset and Network Statistics

Found in the Stanford Large Network Dataset Collection, the dataset used is described as a "Weighted Signed Directed Temporal Bitcoin OTC web of trust network." Bitcoin OTC stands for over-the-counter, and it is a marketplace used to trade Bitcoin. In general, Bitcoin keeps user identities anonymous, which can potentially be problematic, especially in regard to counterparty credit risk (CCR), since transactions occur directly peer-to-peer. This means that a user risks a counterparty not paying as committed during their Bitcoin transaction, since their is no mediation by the OTC platform or third party. "To mitigate this risk, you need to have access to your counterparty's reputation and trade history." [6] The "web of trust" data is formatted in a way such that the source node is the rater and the target is the ratee. According to the authors of the dataset, "Members of Bitcoin OTC rate other members in a scale of -10 (total distrust) to +10 (total trust) in steps of 1," and each rating is labeled with the time of the rating in seconds.

In this network of Bitcoin transactions on the Bitcoin OTC platform, there are 5,881 nodes (transactors) and 35,592 edges (transactions), where 89% of edges are positively weighted. Transactions fall in the years 2010-2016, essentially the early days of Bitcoin. This dataset was directly imported into NetworkX and required no scraping of any sort.

4 Network Visualizations

The overall network of transactions on Bitcoin OTC is depicted in Figure 1 and can be found on Page 6. Looking first at nodes, the nodes in the network are colored based on the percentage of positive trust scores for outgoing edges, and the sizes of the nodes are based on degree, increasing in size with increasing degree. The colors of the node label differentiate the top six highest-degree nodes labeled in green from the rest of the remaining nodes with pink labels. Looking now at edges, the coloring of the edges only applies to the top six highest-degree nodes, with red denoting the outgoing edges and blue denoting the incoming edges. For edges between nodes that are not of the top six highest-degree, the colors are grayscaled.

The two networks found in Figure 2 on Page 6 visualize the network up until the year 2010 and then up until the year 2011, and these networks follow the same color and size scale as the original network in Figure 1. In the 2010 network, there are 55 nodes (Transactors) and 143 edges (Transactions). Of the top six highest-degree nodes at the last timestamp, the only one present at this time is node 35. In the 2011 network, there are 1637 Transactors and 7903 Transactions, with now two hubs, node 35 and node 905, present.

The next two networks found in Figure 3 on Page 7 visualize the network at the years 2012 and 2013. In the network for 2012, there are 3162 Transactors and 17336 Transactions, but now all of the top six highest-degree nodes are present. We see the network growing over time, and, by 2013, there are 5161 Transactors and 30318 Transactions, with again all 6 hubs present. Although the time labels in the dataset range from 2010 through 2016, all 6 hubs are present and visually prominent starting around 2012 and growing as time progresses.

To analyze these networks and their changes over time, it is important to note that the Bitcoin OTC marketplace states the following general disclaimers for counterparties:

1. Conduct due diligence on their counterparties.
2. Act in a prudent way to avoid falling prey to fraudulent users.
3. Do not rely on the ratings blindly.
4. Talk to other users on the platform first, make sure they are familiar with the user you're about to trade with, have traded with that user successfully in the past, etc. [6]

Preferential attachment can be defined as "the probability Π_i that a link of a new node connects to node i is proportional to the product of node i's degree k_i and its fitness η_i." [7]

$$\Pi_i = \frac{\eta_i k_i}{\sum_j \eta_j k_j}$$

Looking at this equation for preferential attachment, the dependence of Π_i on k_i highlights that a node with higher degree has more visibility, which in turn implies there is a higher chance of linking to that node. [7] This dependence can be seen in node 2028 which first appears in 2012 and grows in degree by 2013. We can infer from this and from the disclaimers that more transactions are occurring with node 2028 because more users have previously traded with or are at least familiar with node 2028.

Similarly, the dependence of Π_i on η_i highlights that a node with higher fitness than another node is more likely to be selected in the case when those two nodes have the same degree, where the property of fitness can be thought of as a node's ability to turn "each random encounter into a lasting social link." [7] Further, this "assures that even a relatively young node, with initially only a few links, can acquire links rapidly if it has larger fitness than the rest of the nodes." [7] This can be seen in node 35, which originally appears small in the network in Figure 2 due to its small degree in 2010. But, we see in 2012, node 35 has a much larger degree and remains a high-degree node through 2016 when the dataset concludes. The progression into a hub may stem from node 35's transactions with others, in that they were successful and positive, which in turn helped node 35's reputation and fitness. The Bitcoin OTC network appears to exhibit patterns that follow preferential attachment characteristics.

5 Further Exploration & Insights

Firstly, we do not go beyond 2013 for the sake of space and the reason that the majority of transactions have already occurred in this window. Instead, we shift our focus to when there are a quarter and half of transaction present. A quarter of transactions are present by March 2012 with 1800 transactors and 8899 transactions and half of transactions by January 2013 with 3241 transactors and 17797 transactions. Three-quarters is omitted for space but similar insights can be gleaned. Figure 4 shows both graphs respectively. The only thing that has changed is how the edges are colored; complete distrust (a score of -10) is deep rep while complete trust (a score of 10) is dark blue. Immediately, we notice an overwhelming sea of light blue. It is not just that 89% of edges are positive, the majority of users are just content with their transaction. A far cry from total trust, a whole study on human behaviour could be conducted to analyze the network as well.

The next Figure 5 shows us zoomed in perspectives on node 35 with its rating distribution while Figure 6 does the same for node 832. Node 35 is our top hub, the pillar of what someone would predict for being a "trustworthy" transactor - majority positive reviews and a lot of them. Contrast this with node 832 which from the picture alone can be see to be a shade of pink and having more colorful (strongly opinionated transactions) edges attached. If we fast forward to the half point of transactions, Figure 7 shows the rating distribution for nodes 35 and 832. Whereas our hub 35 more than doubled transactions from 292 to 677, node 832 merely gained 3, finishing with 169 from 166. While it is impossible to say the real reason, there is evidence from this node and others that generally speaking less "trustworthy" nodes are less preferable to future transactors.

However, there are indeed exceptions and questions that cannot be answered that deserve attention in future work. Figure 8 pictures the dark green node 2691 (as well as 2351) with 2691's rating distribution also shown. There are 41 transactions at this point in time with 2691, 38 which were rated a -10. The main question: why are users deciding to continue transacting with 2691? Are they the only option for a particular product or service? Is the person being retaliated against or review bombed? Is something shadier going on? Unfortunately we have no information to base an answer off of beyond the network itself and it is impossible to say the real reason.

6 Fairness, Goodness, and Reliability

6.1 Explanation

As with any other transaction, users are only willing to transact Bitcoin with others whom they perceive as trustworthy. While anonymity is a major selling point for Bitcoin, it is also the source if great risk to the individual user. Unlike other online marketplaces which allow users to leave reviews, there is no such system in place for Bitcoin transactions as it would contradict anonymity promises. Bitcoin OTC is a Bitcoin trading platform that allows users to rate others on a scale of -10 to 10. Kumar et al. have proposed an algorithm to predict fraud given such little information [2]. They propose that a measure of trustworthiness should rely on fairness, goodness, and reliability.

The fairness of a user should reflect whether a user provides unbiased ratings. We should expect that a trustworthy user should give good ratings to good other good users and bad ratings for bad users. On the contrary, a user who rates good users negatively and bad users positively should be seen as fraudulent.

Goodness is a measure of the most likely rating a fair user would give. We should expect that a good user would receive good ratings from fair users and a fraudulent user should receive bad ratings from fair users.

Finally, reliability indicates the trustworthiness of a given rating.

The recursive definitions of Fairness, Goodness, and Reliability lead us to the five following axioms proposed by Kumar et al.

1. Better products get higher ratings
2. better products get more reliable positive ratings
3. Reliable ratings are loser to goodness scores
4. Reliable ratings are given by fair users
5. Fairer users give more reliable ratings.

Now that we have laid out how we expect each metric to behave, we can define formulas for computing each score. We will use u when referring to a user and p for some user that was transacted with. $Out(u)$ represents the set of outgoing edges from user u, or the set of users u has transacted with where they sent money to another user. Likewise, $In(u)$ is the set of incoming edges of a user u, or the set of users from which they received transactions. $Score(u, p)$ is the rating given for that particular transaction, which is given in the data set from Bitcoin OTC.

The fairness of a user, $F(u) \in [0, 1]$, is 1 for a 100% trustworthy user and 0 for a completely untrustworthy user. The fairness score is essentially the average of reliability scores of outgoing edges of user u.

$$F(u) = \frac{\sum_{(u,p)\in Out(u)} R(u, p)}{|Out(u)|}$$

The goodness of a transaction, $G(p) \in [-1, 1]$, where -1 signifies a terrible transaction and 1 for a good transaction. The goodness of a user is the average of all ratings a user has received that is weighted by the reliability of each review.

$$G(p) = \frac{\sum_{(u,p)\in In(p)} R(u, p) score(u, p)}{|In(p)|}$$

The reliability of a rating, $R(u, p) \in [0, 1]$, where 0 shows an untrustworthy rating of a transaction and 1 is a trustworthy rating. Finally, the reliability score can be interpreted as a mixture between the goodness and fairness scores.

$$R(u, p) = \frac{\gamma_1 F(u) + \gamma_2 \left(1 - \frac{|score(u,p) - G(p)|}{2}\right)}{\gamma_1 + \gamma_2}$$

γ_1 and γ_2 are hyperparameters that can be tuned in instances where labeled data is present.

6.2 Analysis

The first piece is the fairness of users, which once again describes if a user gives out "fair" ratings. Although we did visualize and compute fairness, we exclude them from our report because according to this Kumar metric, nearly all users are fair. At the quarter point, there is a mean fairness rating of 0.950 with the median being skewed further right at 0.968. At the mid point, they are slightly lower with the mean being 0.941 and median 0.965. The lowest fairness score is still positive at all points in time, and thus we did not find it rewarding to try to delve too much into this category for this particular network.

More interesting is probably the implications of goodness. Overall, the network at the mid point has a mean goodness score of 0.111 and median 0.0987. This is reflected in Figure 9 with nearly all visible nodes being a light pink with the same green-purple scale for goodness. Using Kumar's metrics combined with our previous insight comes with an interesting conclusion. Most users do not worship others - they simply have no reason to leave a stellar review for a standard transaction. In truth, users do not need to trust each other whole- heartedly, but really they just need a history of reliable transactions.

7 Conclusion

All in all, there were many insights into the behaviour of the Bitcoin OTC network. Although we have evidence to support our hypotheses, we do not go as far to say that our word is truth. The network shows strong evidence of having hubs and following the preferential attachment model. More interestingly, combining our work with the Rev2 algorithm developed by Kumar we can form the conclusion that while our original hypothesis is true that users with perfect reviews and many transactions will garner more and more transactions, trust is less important than we believed. What is more important it is a large history of “okay” reviews from fair users. This large dependence on degree fits the preferential attachment model and is far more important than having complete confidence in a user. To summarize, we believe a better analogy to the true behaviour of the network is the question every Amazon customer faces: Do I trust the vendor with a handful of 5 star reviews or the vendor with thousands of reviews averaging 4 stars?

References

[1] J. Leskovec and A. Krevl, “SNAP Datasets: Stanford large network dataset collection.” https://snap.stanford.edu/data/soc-sign-bitcoin-otc.html, June 2014.

[2] S. Kumar, B. Hooi, D. Makhija, M. Kumar, C. Faloutsos, and V. Subrahmanian, “Rev2: Fraudulent user prediction in rating platforms,” in *Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining*, pp. 333–341, ACM, 2018.

[3] S. Kumar, F. Spezzano, V. Subrahmanian, and C. Faloutsos, “Edge weight prediction in weighted signed networks,” in *Data Mining (ICDM), 2016 IEEE 16th International Conference on*, pp. 221–230, IEEE, 2016.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, p. 21260, 2008.

[5] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, “Is bitcoin a decentralized currency?,” *IEEE security & privacy*, vol. 12, no. 3, pp. 54–60, 2014.

[6] “bitcoin-otc marketplace.” https://www.bitcoin-otc.com/. Accessed: 2022-04-14.

[7] A.-L. Barabási and M. Pósfai, *Network Science*. Cambridge: Cambridge University Press, 2016.

A Figures

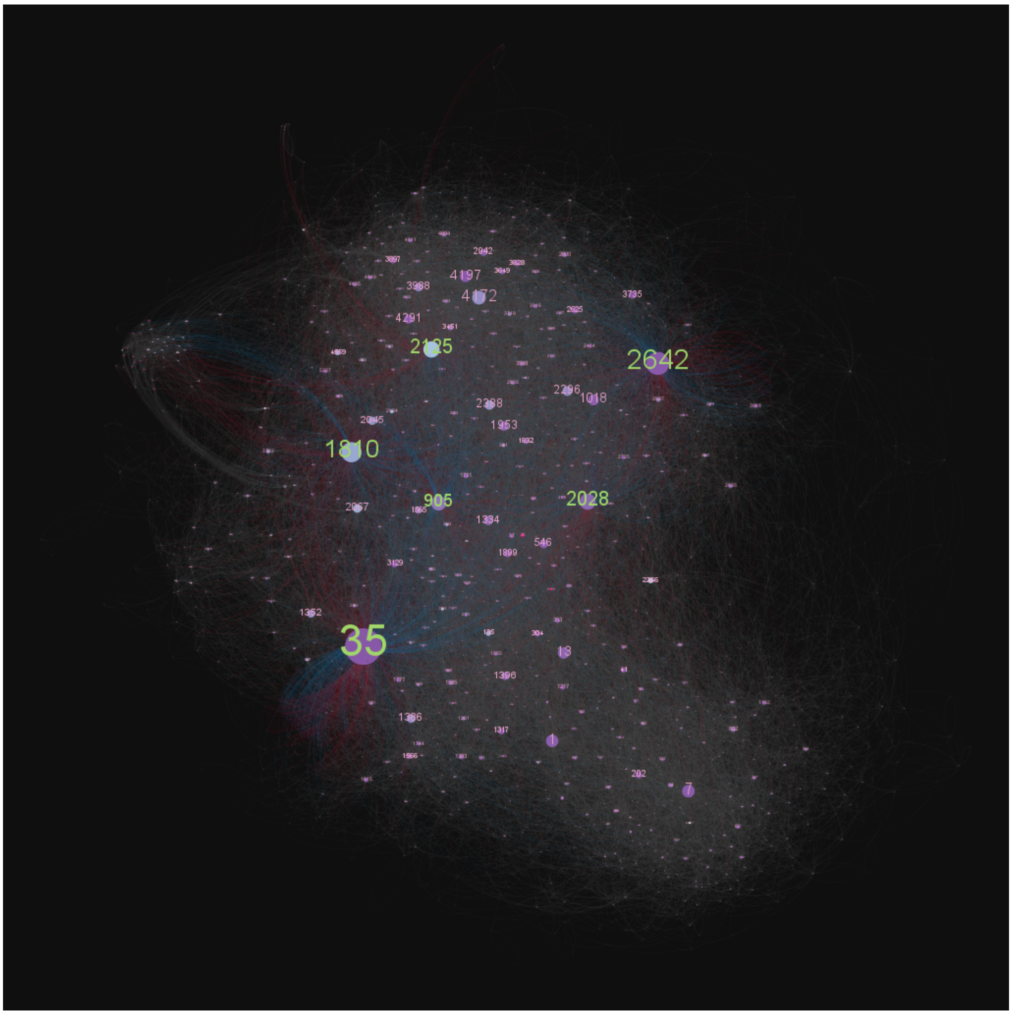

Figure 1: The online social network of Bitcoin transactions on the Bitcoin OTC platform.

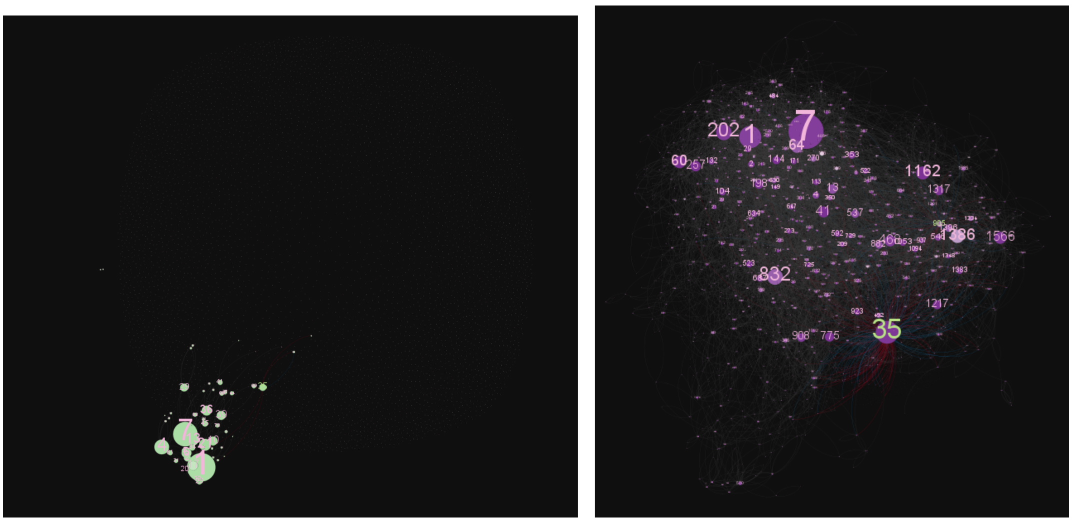

Figure 2: (Left) 2010 (Right) 2011

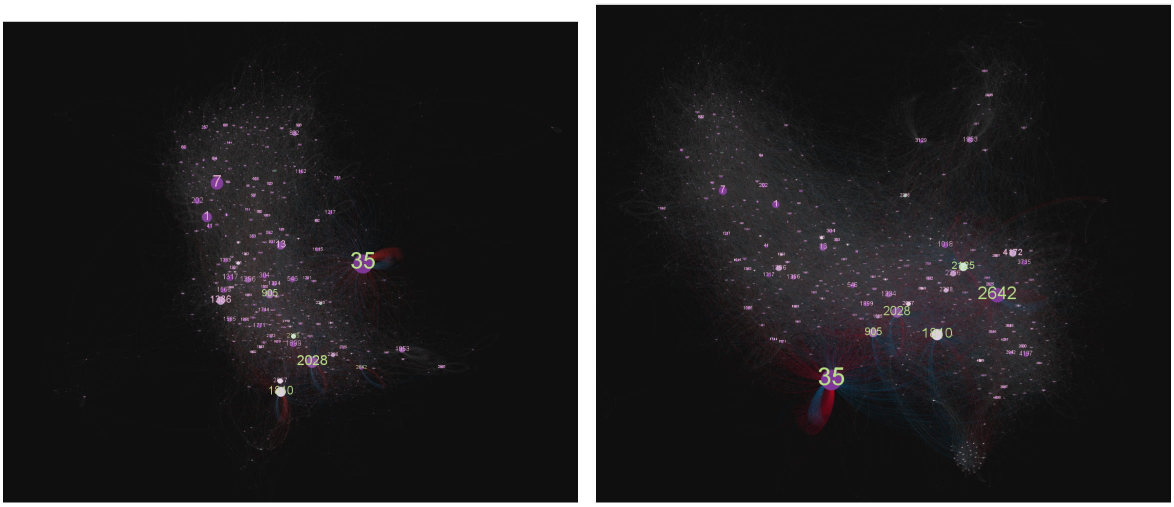

Figure 3: (Left) 2012 (Right) 2013

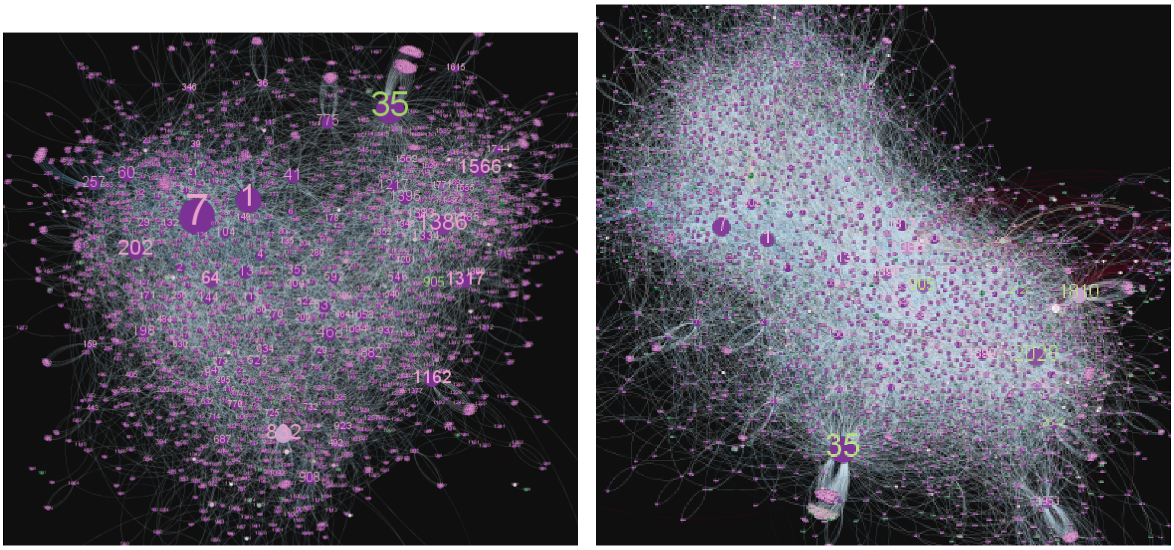

Figure 4: (Left) Quarter of Transactions (Right) Half of Transactions

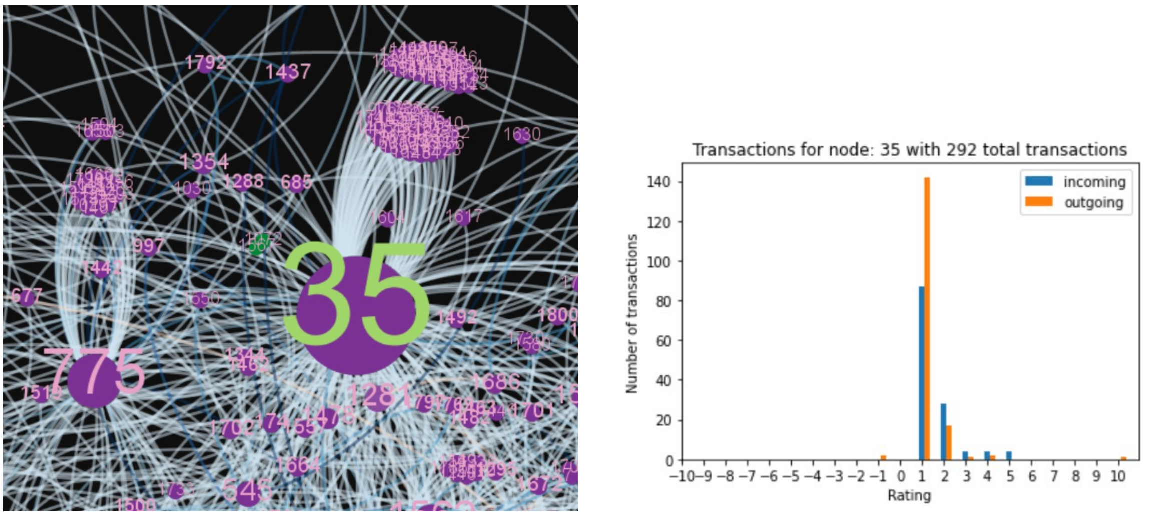

Figure 5: Quarter of Transactions Zoom on 35 and rating distribution

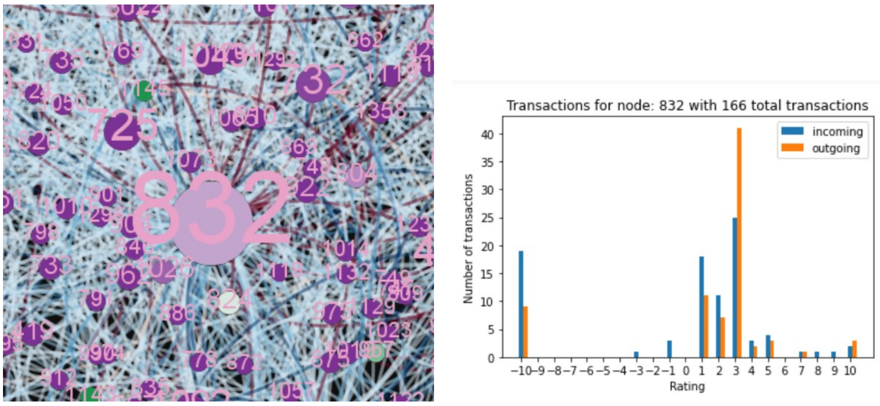

Figure 6: Quarter of Transactions Zoom on 832 and rating distribution

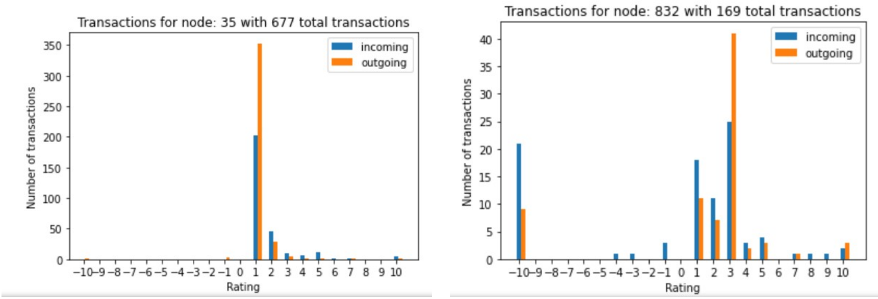

Figure 7: Half of Transactions rating distribution for 35 and 832

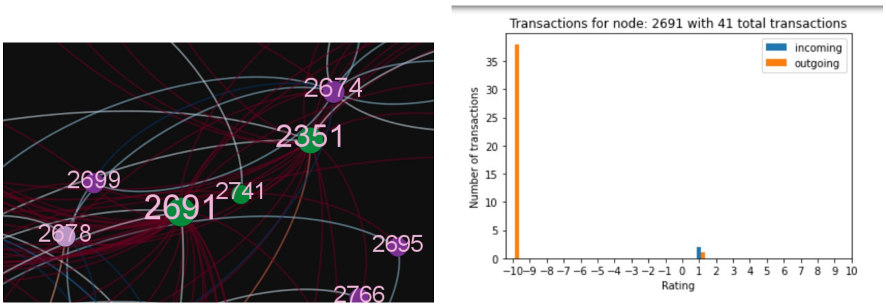

Figure 8: Half of Transactions zoom on 2691 with rating distribution

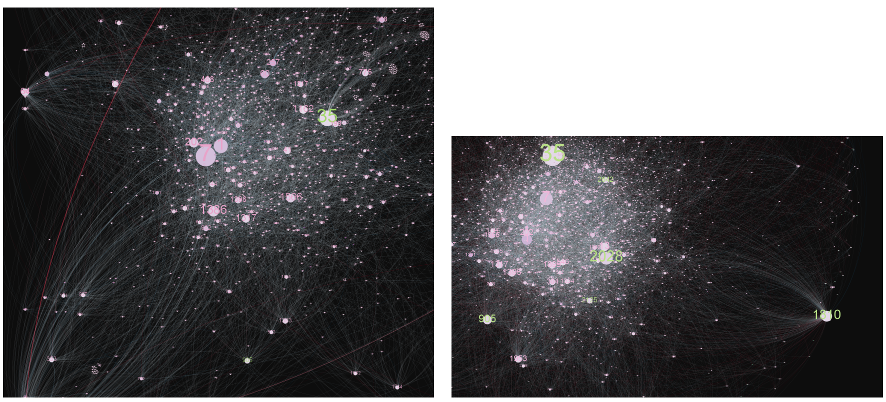

Figure 9: Quarter (Left) and Half (Right) Point of transactions with Goodness