Network Analysis : Optimizing a Crypto-Currency Trading Platform by Predicting Untrustworthy Users.

Fragkiskos Malliaros

Mohamed Alami Chehboune
CentraleSupelec
Paris, France
m.alamichehboune@student-cs.fr

David Chamma
CentraleSupelec
Paris, France
david.chamma@student-cs.fr

Arthur Degonde
CentraleSupelec
Paris, France
arthur.degonde@student-cs.fr

David Kiskovski
CentraleSupelec
Paris, France
david.kiskovski@student-cs.fr

ABSTRACT

A Network of transactions of cryptocurrencies between users of the OTC trading platform was analyzed to determine the potential to set up a recommendation service associated to it. The degree distribution of users follows a power law as networks often do and the platform was found to be particularly sensitive to targeted attacks, as some users were indeed more influential than others. Predictions were made on missing transactions and their associated ratings, where individual nodes corresponded to a user, and the edge between them to the rating of the transaction giving by one or both of the users. Similarity graphical features and fairness-goodness estimates of ratings were used to train an SVM and the model attained an accuracy of 83,2% on missing transactions and a Root-Mean-Squared-Error of 0,35 for the ratings. Finally, community detection algorithms (Infomap, Louvain, Multi-Level..) were performed in order to maximize the modularity of the partition, considering the graph first as directed then as undirected. The maximum modularity was found to be 0.48 by considering the graph as undirected and splitting the partition into 20 communities, as opposed to 0,29 when keeping it undirected. Some communities were observed to comprise of more trustworthy users [6].

1 MOTIVATION AND PROBLEM DEFINITION

New technologies keep enabling payments to be made in increasingly efficient manners. Methods such as contactless payment and apple pay are very much implemented in our every day lives whilst new players keep finding innovative ways of efficiently and securely transferring money, making it a hot and growing market [15].

The past few years have also seen a rise in the trade of cryptocurrencies, which are digital assets designed to work as a medium of exchange that use strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Although once thought to only be used for illicit means (by criminals to make secure and untraceable payments to purchase drugs and weapons), cryptocurrencies received worldwide coverage as their potential to become a centralized currency and facilitate trading induced a drastic increase in their total value, equating nearly 700 Billion $ at its peak in January 2018 [16].

The focus of this project was on the most used cryptocurrency: the bitcoin [1]. Bitcoin is an important electronic and decentralized cryptographic currency system proposed by Satoshi Nakamoto [12]. It is based on a peer-to-peer architecture and there is no need for a central authority or central bank to control the money supply within the system. It relies on a proof-of-work system to verify and authenticate the transactions that are carried out in the network.

A Bitcoin can be defined as a chain of digital signatures. By transferring the electronic coin to the next user it gets digitally signed with a hash of the previous transaction and the public key of the next owner; adding these together to the end of the Bitcoin. The signatures can be verified by the payee to prove the chain of ownership. To provide some sort of anonymity, direct personally identiable information is omitted from the transaction. Therefore, the source and destination address are encoded in the form of public keys. Every public key that serves as a pseudonym has a corresponding private key which is stored in the electronic wallet. These are used to sign or authenticate any transactions [5].

Although its price has crashed to a seventh of its peak value (at the date this paper is written), the potential bitcoin and cryptocurrencies in general hold in tomorrow's economy is boundless. However, trades on them being done anonymously for security reasons, methods must be put in place to regulate fare trade and make sure no one can abuse the system and rob people of their money. These measures could enable the use of cryptocurrencies to become more widespread, and maybe, in time, take over from National currencies.

The objective of this project was to investigate the network of users exchanging bitcoins with each other and assigning a ratings to other users. Finding patterns amongst the transactions and associated ratings was the priority in order to determine which users should be prioritized to make trades with and which ones should be banned from the trading platform. This study could set the groundwork for a future recommendation service available on such trading platforms, in order to optimize user experience and finally make cryptocurrencies a trusted and fully efficient way of payment.

2 DATASET DESCRIPTION

This study was conducted with the use of the first explicit weighted signed directed network available for research [7]. This is a who-trusts-whom network of people who traded using Bitcoin on a platform called Bitcoin OTC. Since Bitcoin users were anonymous, there was a need to maintain a record of users' reputation to prevent transactions with fraudulent and risky users. Members of Bitcoin OTC rated other members in a scale of -10 (total distrust) to +10 (total trust) in increments of 1. The characteristics of the network are represented on table 1.

Dataset statistics	
Nodes	5,881
Edges	35,592
Range of edge weight	-10 to +10
Percentage of positive edges	89%

Table 1 : Network properties

3 METHODOLOGY

This section describes the methods employed in the project and which algorithms were used in order to do so.

3.1 Degree distribution

The network structure and topology was first analyzed by studying the degree distribution of its nodes. This served to indicate the relative importance of some nodes compared to others, and hence the higher probability that edges will form from them when predicting missing transactions later on in the project. The degree distribution was first computed by plotting the graph as undirected to analyse the overall dynamic of the network. An important feature of this network how was that edges were directed and weighted. Hence each node was characterized by an out-degree k_{out}, representing the number of payments from one bitcoin holder to another, and an in-degree k_{in}, representing the number of other bitcoin holders that paid the selected node. The distinction had to therefore be made between the two degree distributions: the probability that a randomly chosen node sold Bitcoin (k_{out}, or p_{kout}) , and the probability that a randomly chosen node bought it (k_{in}, or p_{kin}) .

3.2 Robustness of the network

The sensitivity of the connectivity of the network to node removal was also investigated, in order to determine the the robustness of trading platform.
Two methods of removal were implemented : Targeted Attack, which is a removal of nodes in order of decreasing centrality (Eigenvector centrality was used in our case) [3], and Random Failure, a removal of node completely at random. This was done in order to verify how important the higher degree nodes were to the rest of the network and whether their removal would cause catastrophic consequences to the platform.

3.3 Link prediction

It was the aim of the project to be able to predict the weights of future edges of the network, meaning the ratings given by a user to one another for a transaction that had not happened yet. Future edges had to first be predicted, then a rating would be associated to each one. To do so, a few topological features were computed, and the graph was considered as undirected because it did not matter who was the rater or the ratedin the transaction, but rather simply if two users would work together or not. The following were used :

- **Neighborhood-Based Methods:** The amount of common neighbors between pairs of nodes were first found, constituting the most straight-forward feature. Indeed it was suspected that trustful users would want to exchange bitcoins among each other. These would in turn constitute trustful bitcoin exchange communities.
$$c(x, y) = |\Gamma(x) \cap \Gamma(y)|$$
- **Jaccard Coefficient:** Calculated for pairs of nodes. It corresponds to the fraction of common neighbours between the nodes to the total amount of neighbors both nodes possess. This corresponds to the probability that both nodes have common neighbors. Here again this feature may be representative of the membership of a community for the considered nodes.
$$c(x, y) = \frac{|\Gamma(x) \cap \Gamma(y)|}{|\Gamma(x) \cup \Gamma(y)|}$$
- **Preferential Attachment Coefficient:** Computed for each pair of users. This value represents the product of the degrees of each node. Indeed, this features may help to detect users that appears in many transactions. The highest

this value the higher were the chances that a transaction would occur between the nodes.

$$c(x, y) = |\Gamma(x)| \cdot |\Gamma(y)|$$

- **Adamic Adar Coefficient :** Also computed for each pair of nodes, this coefficient assigned large weights to pair of users that made a transaction with the same other user that had not made transactions with a large number of other users.

$$c(x, y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{log|\Gamma(z)|}$$

Data cleaning and feature engineering :
To be able to train a model, a new data set was created. Indeed, since our graph was directed, our initial data set was only constituted of existing edges between pairs of nodes, and not pairs of not which did not have an edge. New pairs of nodes labelled with "0" were created to train the model with nodes that did not share any edges, using hence a "0" when there were no edge, and "1" when there was one. The ratio of edges to no edges in the data was inputted to be 50% to avoid bias. The value of all the features were computed for each pair of nodes. This was done for both the training and testing set.

The predictions of the model were computed using Support Vector Machines(SVM) with a linear kernel which is one of the classifier that performs best for this task.

The aim of Support Vector Machine (SVM) with a linear Kernel is to find a hyperplane that separates two classes. In practice we have a training set $D = (x^1, y^1), ...(x^n, y^n)$ such that $x^i \in \mathbb{R}^p$, $y^i \in \{-1, 1$. We then assume that our data is linearly separable meaning that :

$$\exists\, (w, b) \in \mathbb{R}^p \times \mathbb{R}\ s.t. \begin{cases} \langle w, x^i \rangle + b > 0\ if y^i = 1 \\ \langle w, x^i \rangle + b < 0\ if y^i = -1 \end{cases}$$

Hence, the aim of the algorithm is to find (w^*, b^*) that defines the hyperplane with the maximum margin. However, on top of predicting links, predicting their associated ratings was also attempted. It is called weight prediction and is discussed in the next section.

3.4 Weight prediction

Weight prediction in weighted signed networks has already been studied and the "Fairness x Goodness" feature seems to be the most effective to predict the weight of an edge. [7]

Fairness Goodness Algorithm
The fairness and the goodness are two values attributed to a user that will help us predict the weights of the edges (the rating given by an user to another). "The fairness of a vertex is a measure of how fair or reliable the vertex is in assigning ratings"[...]"The goodness of a vertex specifies how much other vertices trust that vertex and what its true quality is" [7].
Fairness Goodness feature has shown to be more efficient for predictions than other features such as Tidal trust [17], Triadic Balance [4], Bias and Deserve or MDS (Multi Dimensionnal Scaling) [13]. That is why it was decided to use it in this project.

Input: A WSN $G = (V, E, W)$
Output: Fairness and Goodness scores for all vertices in V
Let $f^0(u) = 1$ and $g^0(u) = 1$, $\forall u \in V$
$t = -1$
do
  $t = t + 1$
  $g^{t+1}(v) = \frac{1}{|in(v)|} \sum_{u \in in(v)} f^t(u) \times W(u, v)$, $\forall v \in V$
  $f^{t+1}(u) = 1 - \frac{1}{2|out(u)|} \sum_{v \in out(u)} |W(u, v) - g^{t+1}(v)|$, $\forall u \in V$
while $\sum_{u \in V} |f^{t+1}(u) - f^t(u)| > \epsilon$ or $\sum_{u \in V} |g^{t+1}(u) - g^t(u)| > \epsilon$
Return $f^{t+1}(u)$ and $g^{t+1}(u)$, $\forall u \in V$

Figure 1 : Fairness Goodness Algorithm

Both fairness and goodness are mutually recursive and are updated until both the scores converge. The algorithm converges when the change between fairness and goodness scores in consecutive iterations for all vertices is less than an error bound ϵ, which was set to 0.001 and is described thoroughly in figure 1. The scores of fairness and goodness from the last iteration are the final scores.

Henceforth this algorithm was useful when predicting weights of transactions by using past transactions by the same users, looking at the rating they gave/were given in the past, and determining whether or not it is likely to be trusted by other users. A simple Linear Regression was then used to predict the weights of the edges.

3.5 Communities Detection

An important characteristic of the studied network is the communities composing it. Indeed, the platform was more than a random network consisting of vertices and edges representing different transactions, it was a social network where users rated each others. The users in turn probably, in time, formed trading communities within themselves. Finding these communities and under what criteria they appeared was determined to be essential to understanding the dynamics of this network, as user behaviour could be compared from one community to the next, to determine if one was more trustworthy than another.

To distinguish communities, several models were applied. All had for objective to maximize the modularity Q, a measure for assessing the strength of communities.

$$Q = \frac{1}{N} \sum_{i,j} (Ai, j - \frac{kikj}{2m}) \delta(Ci, Cj)$$

with :

- A is the adjacency matrix
- ki, kj are the degrees of nodes i and j respectively
- m is the number of edges in the graph
- Ci is the community of node i

- $\delta(.)$ is the Kronecker function: 1 if both nodes i and j belong to the same community (Ci = Cj), 0 otherwise.

Modularity is the most widely used measures for community detection, and has been successfully applied for detecting meaningful groups in a wide variety of real-world systems. The network could be said to show presence of communities if the value of modularity ranged form 0.3 to 0.7.

Different ways of partitioning the graph to maximize the modularity were attempted.
First, the directionality of the network was conserved. Community detection is still a very young topic in network sciences and there is not much literature on optimizing modularity [11] [9] for directed graphs however some algorithms exist. The Infomap algorithm was applied to obtain communities [8]. Given a network partition, the map equation specifies the theoretical modular description length of how concisely the trajectory of a random walker guided by the possibly weighted, directed links of the network could be described.
The Infomap algorithm aims to minimize the map equation over possible network partitions. This algorithm is relatively similar to the Louvain method [2].
First, each node was its own module. Then, neighboring nodes were joined into modules in order to get the largest decrease of the map equation. If no move resulted in a decrease of the map equation, the node stayed in their original module. This procedure was then repeated in a new random sequential order until no more movements induced a decrease in the map equation. [10]

4 RESULTS AND INTERPRETATION

4.1 Degree distribution

On figure 2 are observed the degree distribution of nodes in the network. A logarithmic scale was used to better fit the data, as it followed a power law, like random networks often do. This indeed went to show that some nodes were connected to many compared to others.

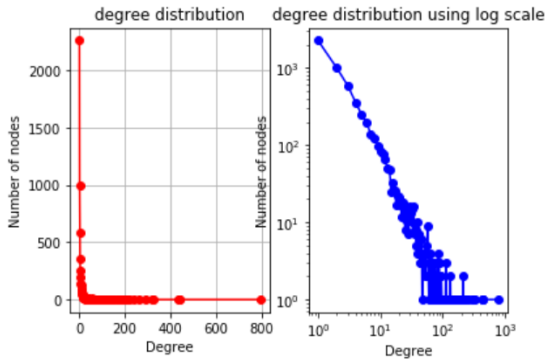

Figure 2 : Degree Distribution of nodes of the network

The degree of the power law computed was also computed and a coefficient of alpha = 3.45 was found.

The out-degree and in-degree distributions were also found and plotted. They both also followed a power law signifying that indeed some nodes where at the origin and the target of more ratings. Hence forth some users were by definition more active in the sense that they not only sold more but also bought more cryptocurrencies.

4.2 Robustness of the network

The fragmentation of the network under random failures and attacks was plotted in figure 3.

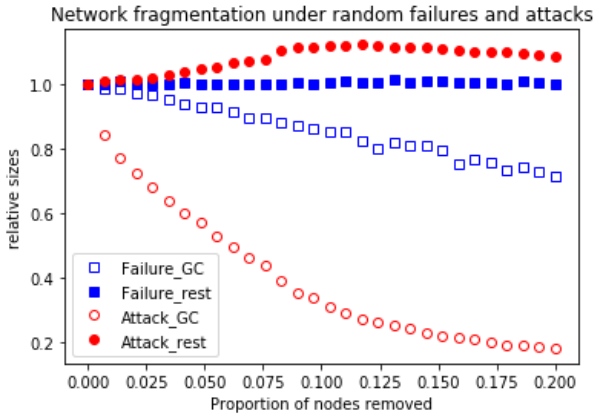

Figure 3. Here, both the diameter and size of Giant Component were plotted compared to a baseline of 1 which represented the initial values. This was done to emphasise on the impact of targeted attacks

Several things were deduced from the graph :

- The network is highly sensitive to targeted attacks. Indeed the size of the giant connected component decreased very fast with the proportion of removed nodes. The number of connected component increased, showing that some nodes became isolated. This result demonstrates the importance of a highly regulated and safe platform, as if prominent and important users lose interest or worse, get robbed, the whole network may crumble, which would heavily impair any potential recommendation service associated to it. This result hence reiterated the importance of distinguishing trustworthy users from the rest.

- However, as expected, the network was quite robust against random failures. Even if the size of the giant component decreased, the number of connected component did not increase. The overall structure of the network remained the same. This goes to show the importance of a select amount of users.

This graph showed that most of users tend to buy from the same users. That is why when the big users were removed from the network, many nodes become isolated.

4.3 Link prediction

The results of the trained SVM were obtained and are observed on table 3 :

Classifier	Train Accuracy	Test Accuracy
SVM	0.8350	0.8324

Table 2 : Results of SVM Classifier

Good results were obtained when focusing only on topological features. Also, even though the features were computed assuming an undirected graph, the predictions were nonetheless relatively accurate. Hence, as suspected, users were more likely to exchange between trusted users. These initial results imply the construction of communities, avoiding exchanging bitcoins with other, more untrustworthy users. This explains why using topological similarity leads to such good results for link predictions.

Link prediction may be useful to ensure security for this kind of trading platform. Indeed, unexpected links (a transaction between users that should not normally get in contact) could be analyzed to detect fraudulent behaviour. Moreover, it could also be used to predict the evolution of the network's size. This would help plan servers maintenance and enhancement.

4.4 Weight prediction

The results of the linear regression are the following :

Classifier	Train RMSE	Test RMSE
Linear Regression	0.3641	0.3531

Table 3 : Results of Linear Regression Classifier

RMSE (Root Mean Squared Error) obtained is low and approaches the value obtained in [7], even if the exact ratings were not predicted, the right behavior of the users (trustworthy, untrustworthy) are indeed found more often than not. Indeed, the RMSE could have been highly influenced by ratings of never seen users, which would give extreme ratings. Also, for each pair of nodes/users, the fairness of one user (the one who gave the rating) and the goodness of the other (the one who gets attributed a rating) was computed. Using those parameters to fit the linear regression, the actual behavior of the users were simulated. If the first user was fair, the given rating should be quite close to the actual goodness of the second. The difficulty lies in predicting the rating whenever the first user is unfair, because the user that is the source of the transaction may be attributing ratings at random.

The trading platform could be improved thanks to weight prediction. Indeed, the platform could suggest users to buy from according to the rating that would be given if the link was created. Also the platform could prevent unfair users from giving false ratings.

4.5 Communities

The main characteristic of the network was that it was directed and its weighted edges were signed. These attributes were essential when it came to detecting communities as it held important information about the network's structure; information that, at least in principle, could allow a more accurate partition of the communities to be made. Several previous studies [14] [**?**] have touched on this problem in the context of other analyses of directed network data. To tackle this problem, the infomap algorithm described above was chosen.

Infomap modularity maximization resulted in a score of 0.36 on the network.
Then, directionality was ignored and the network transformed to be undirected. The modularity was then maximized using two algorithms : community leading eigen vector and community multi-level.
The first led to a modularity of 0.39 while the second scored a 0.48 which was the highest score obtained. Hence, the remainder of the analysis was done using the partition obtained from the community multi-level algorithm. It partitioned the data into 28 clusters with varying lengths (going from 2 nodes to 1407 nodes) and average ratings from intra-structure transactions.

However, the vast majority of the research done on the subject has always ignored the directed characteristic and simply transformed the networks they studied into undirected ones. Both methods were used and their results were compared. The resulting modularities are observed on table 4. Surprisingly, it

Algorithm	Directed/Undirected	Maximum Modularity
Infomap	D	0.36
Louvain	U	0.19
Community Leading Eigen Vector	U	0.39
Community Multi-Level	U	0.48

Table 4 : Modularity obtained according to partitions realised with different community detection algorithms

appeared that, the maximum modularity had been achieved by using a Community Multi-Level algorithm, that considers the network as undirected. It was therefore considered as the best partition and analysis was conducted using it. Moreover, the object of the study was to analyze how users interacted with each other and who traded with whom; hence, the presence of an edge could be considered as the most important feature to take into account, as opposed to its direction. Given the obtained partition, a representation of the network where each node represented a community and the nodes distribution by community were computed and found on figure 4:

Figure 1: A graph of the different communities

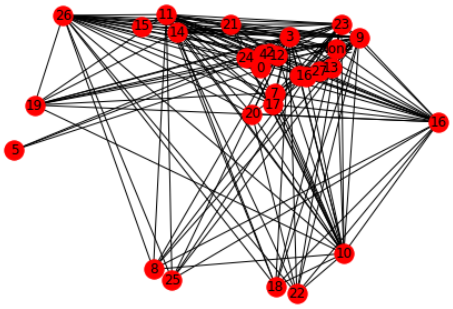

Figure 4 : Graph of communities

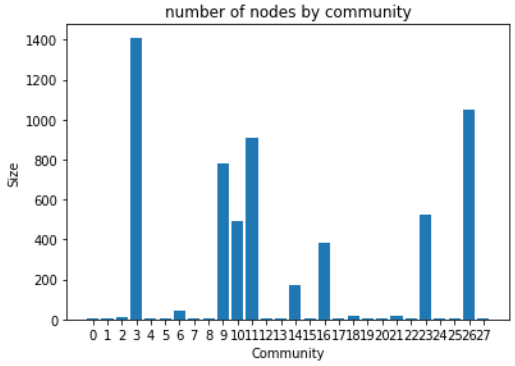

Figure 5 : Size of communities formed

it appeared that 8 communities were significantly bigger than the others and contained more significant patterns. Therefore the focus of the study was place on those communities, analyzing how they interacted with each other. A simpler representation of the network is plotted on figure 6.

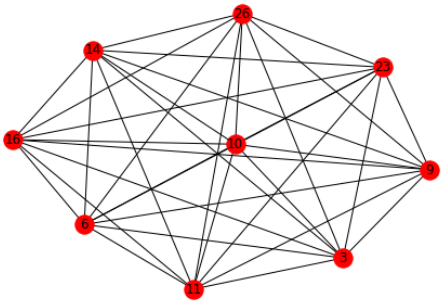

Figure 6 : Graph of connectivity of large communities

The questions tackled here were: "why do users decide to trade to others and why do they group in communities? What is the main criteria for them to be in a community or another? How to discriminate between good and bad communities?"

4.5.1 *Studying communities through their users rating*.

One first hypothesis could be that trustworthy users tend to do business together. Figures 7 are charts showing the mean rating by community and its standard deviation.

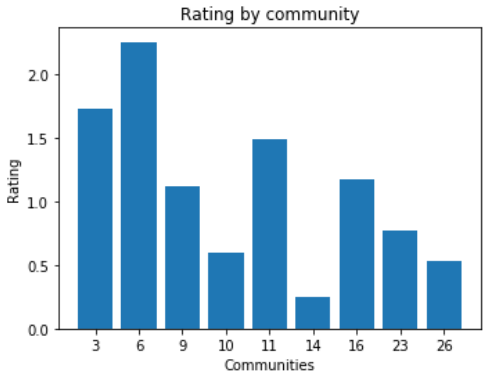

Figure 7: Mean rating that nodes give other nodes in the community

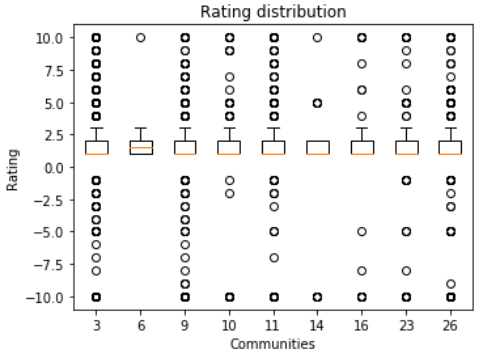

Table 8 : Representation of statistical components of large communities in graph

As observed, the ratings were quite well balanced. However, the standard deviations are high, which showed that the ratings were highly dispersed around the mean. That suggests that users ratings of the same community do not lie in the same range. Therefore, joining a community is not an insurance against frauds. Good and bad users may be part of the same community.

Even if the ratings were dispersed, it did not say much on the proportion of dispersion due to the fact that the mean ratings were low and that a rating with a range of 20 possible values was not interpreted in the same way by every user. For instance, a user could estimate that a grade of 3 was a good representation of trustworthiness, while an equivalent rating (in terms of signal) could be 6 for another user. Therefore, the range of possible ratings was narrowed by creating 4 categories:

- total distrust: from -10 to -6
- distrust: from -5 to -1
- trust: from 1 to 5

- total trust: from 6 to 10

Figure 9 shows the distribution of those categories within community 3 while Figure 10 shows the number of "trustworthy" nodes in each community. According to these charts and to the subjective categories that were defined, the community was globally trustworthy. However, the "total trust" category seemed to be relatively rare and could have been more discriminant between communities but unfortunately, after a careful consideration, it was not the case.

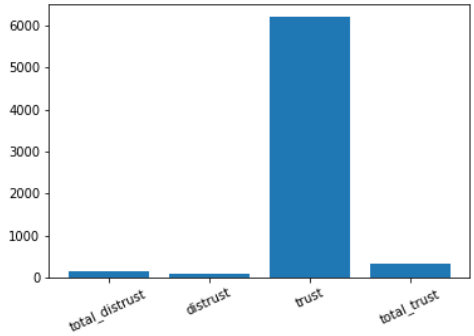

Table 9 : Trustworthiness distribution of community 3

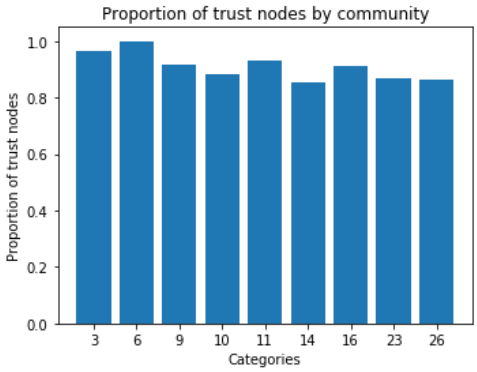

Table 10 :Proportion of trustworthy users in the different communities

4.5.2 *Studying communities through their users fairness/goodness*.

whilst the communities did not bundle up the best rated users, they may however have gathered the fairest ones, those that were honest and played the game as it should be played. Indeed, many "trolls" could have created multiple accounts, giving themselves high grades. Therefore, it could be possible that trustworthiness in each community is highly overestimated.

A first approach was to see how communities rated each other. This way, any kind of rivalry between communities could be monitored. The simple idea that if the users of some community were fair with the users of another community, they may as well be fair with themselves was employed. Moreover, a good indicator of the fairness of a community was added by computing the difference between the mean rating every community gave to another (r_{out}) and the mean rating the nodes of the considered community gave between themselves (r_{in}) (figure 11).

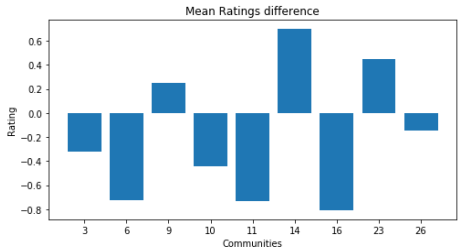

Table 11 :Difference between the mean rating every community gives to a given one and the mean rating the considered community gives to itself.

It appeared that communities 6, 10, 11 and 16 rated themselves more highly than the mean grade granted by the other communities. However, it was still impossible to determine if these communities were actually unfair or if it was the other communities rating them that were biased. That was why the fairness/Goodness metric was implemented.

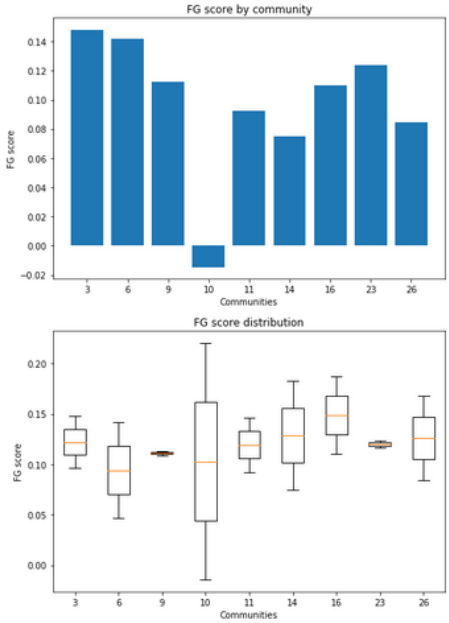

Table 12: Fairness Goodness score by community

The community 10 had the lowest fairness goodness score as observed in figure 12. Therefore, to summarize, this community rated itself better than the other communities rated it; moreover all the other communities had a better Fairness Goodness score, which meant that there ratings were more reliable.

Finally, comparing the Fairness Goodness score and the difference between r_{out} and r_{in} explicited which community was

unfair and which ratings were biased, therefore minimizing the objective value of all the ratings in the network. In such a business and social network, trust is key, hence the admins of the network should ban the unfair users of community 10 (which represents roughly 10% of all the users of the network) or at least hide ratings their give to other users.

5 CONCLUSION

Link predictions were performed based on graphical features and community detection algorithms were used to maximize the modularity of a partition of the total graph. Conclusive results were obtained as the link predictions were shown to have a high accuracy, hence it could be used for numerous applications in user recommendations and fraud detection. The community partitions were slightly tougher to interpret as there did not seem to be many specificities to each community observed after the preliminary analysis that was performed in the report. Presence of a 'parasitic' community was nonetheless observed.

Further work could be put in observing the characteristics of the communities, as find more underlying information they contain on users to always improve the recommendation service. Work could also be done comparing this network to another similar platform in order to detect if similar patterns appear in communities.

REFERENCES

[1] *Bitcoins.* Available online on: http://www.economist.com/topics/bitcoins.

[2] A. Fernandez A. Arenas, J. Duch and S. Gomez. In *Size reduction on complex networks preserving modularity*, 2013.

[3] Phillip Bonacich. In *Some unique properties of eigenvector centrality*, 2007.

[4] D. Cartwright and F. Harary. In *Structural balance: a generalization of heider's theory.*, 1956.

[5] Adi Shamir Dorit Ron. In *Quantitative Analysis of the Full Bitcoin Transaction Graph*, 2013.

[6] Ryan Farell. In *An Analysis of the Cryptocurrency Industry*, 2015.

[7] Srijan Kumar, Francesca Spezzano, VS Subrahmanian, and Christos Faloutsos. Edge weight prediction in weighted signed networks. In *Data Mining (ICDM), 2016 IEEE 16th International Conference on*, pages 221–230. IEEE, 2016.

[8] Andrea Lancichinetti and Santo Fortunato. In *Community detection algorithms: A comparative analysis*, 2009.

[9] Nees Jan van Eck Ludo Waltman. In *A smart local moving algorithm for large-scale modularity-based community detection*, 2007.

[10] C.T. Bergstrom M. Rosvall, D. Axelsson. In *The European Physical Journal Special Topics, Volume 178.*, 2009.

[11] M.E.J.Newman and E.A.Leicht. In *Mixture models and exploratory analysis in networks.*, 2007.

[12] Satoshi Nakatomo. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Available online, 2008.

[13] Y. Qian and S. Adali. In *Foundations of trust and distrust in networks: Extended structural balance theory.*, 2014.

[14] M.Sales-Pardo R.Guimer and L.A.N. Amaral. In *Module identification in bipartite and directed networks.* arXiv:physics/0701151, 2007.

[15] Roger Clews James Southgate Robleh Ali, John barrdear. In *Innovations in Payment Technologies and the Emergence of Digital Currencies*, 2014.

[16] Lawrence H. White William J. Luther. In *Can Bitcoin Become a Major Currency?*, 2014.

[17] Y.KatzandJ.Golbeck. In *Social network-based trust in prioritized default logic*, 2006.