An analysis of the Bitcoin users graph: inferring unusual behaviours

Damiano Di Francesco Maesa, Andrea Marino and Laura Ricci

Abstract An increasing interest on cryptocurrencies has recently raised, in particular on bitcoin. A unique feature of this system is that the list of all the economic transactions is publicly available. This makes available a large amount of information that can be analysed to discover the topological properties of the transaction graph and to obtain insights in the behaviour of the users. In a previous work we have presented a first set of analyses of the bitcoin network. Among other properties of the network, these analyses have also revealed a set of unusual patterns in the bitcoin users graph. We conjecture that these topological patterns are due to artificial users behaviors, not strictly related to normal economic interaction. In particular, in this paper, we analyse the outliers in the in-degree distribution of the bitcoin users graph. The results of our analysis support our conjecture, i.e. they are due to artificial transaction patterns.

1 Introduction

The boost in the diffusion, during the last years, of bitcoin [12], the first true digital currency, together with the public availability of its blockchain makes it interesting and feasible to analyse the behaviour of the users of this peculiar economy. Even if bitcoin still represents a niche economy, it is no longer an experimental currency only for computer science specialists, and has reached a widespread usage. Therefore, the analysis of its blockchain may return interesting insights on the behaviour of the users of a cryptocurrency.

Our previous work [7] analysed several properties of the bitcoin users graph. In particular, we showed that the graph presents many features characteristics of the small-world phenomenon, but also some odd behaviours. As a matter of fact, while

Damiano Di Francesco Maesa (e-mail: damiano.difrancescomaesa@for.unipi.it)✉ · Andrea Marino (e-mail: andrea.marino@unipi.it)✉ · Laura Ricci (e-mail: laura.ricci@unipi.it)✉
Department of Computer Science, University of Pisa

H. Cherifi et al. (eds.), *Complex Networks & Their Applications V*,
Studies in Computational Intelligence 693,
DOI 10.1007/978-3-319-50901-3_59

the average distance between nodes is low, the graph presents a high value of the diameter. This highlights the presence of a few pair of nodes connected by long paths. Furthermore, the in-degree distribution of the nodes presents some relevant outliers. A possible conjecture is that these odd behaviors are caused by users exploiting bitcoin not only for ordinary transactions, but rather for other activities, like fund management and, possibly, attacks. In other words, our conjecture is that if we could distinguish and isolate the transactions representing ordinary economic interactions from the other ones, the resulting user graph would be a better representation of a small world.

This paper will focus on the analysis of the outliers present in the in-degree distribution of the users graph. Our analysis shows that the outliers are a consequence of particular anomalous chains of transactions, that we classify as PS-transactions (Pseudo-Spam transactions). We give different conjectures about the meaning of these transactions and analyze their features.

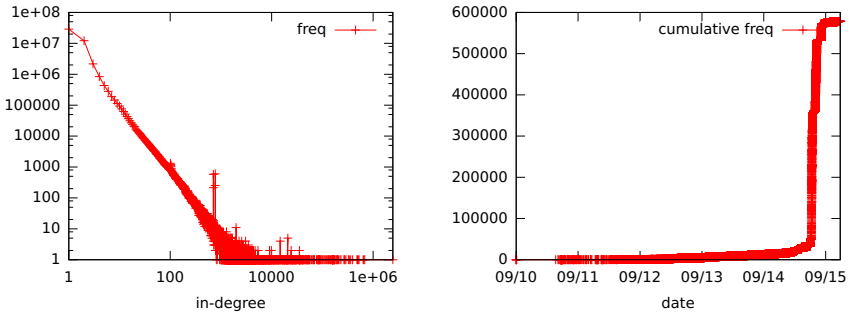
We are currently also investigating the anomalous network diameter and our preliminary results show that its unexpected high length is caused by the behaviour of a single user. So those chains can be further agglomerated in just one cluster significantly lowering the diameter length and hence obtaining a much shorter diameter as expected in a small world. However, due to space constraints, these results are not shown in this paper.

The paper is organized as follows: in Section 2 we report some related work. Section 3 presents our analysis inferring unusual behaviors of the users of the bitcoin network and our conjectures about such behaviors. Section 4, presents a refinement of our initial analysis which is exploited in Section 5 to prove our initial conjecture. Finally, Section 6 reports our conclusions.

2 Related Work

Several features of the bitcoin network have been recently analysed. Most analyses are based on a ”transaction graph” built from the blockchain, which is, in turn, transformed in the ”users graph” (multi-graph with sets of addresses as nodes and arcs derived from the transaction graph) through a well established heuristic rule. By applying this rule, all the input addresses of a multi-input transaction are considered as belonging to the same user [8, 12] (and we say that they are *clustered* in a *cluster* representing the user). This heuristic rule, possibly combined with other heuristic rules, has been used for several analyses [4, 9, 10, 11, 13].

Our previous work [7], has highlighted several properties of the bitcoin network, detected by studying the time evolution of the network in the last years. We have observed a small average distance and we have characterized the network as a small-world. Moreover, we have computed also the diameter by using the algorithm in [6]. Surprisingly, we have observed an high diameter and the presence of several outliers in the in-degree distribution of the nodes. We found that the most central nodes in the network (according to harmonic centrality [5]) are also the ones with highest degree. Finally, we verified the rich get richer conjecture, both from the point of view



(a) Indegree distribution.

(b) Time Stamp Cumulative Distribution of PS-transactions.

Fig. 1

of the balance of each node and from the connectivity point of view. The analyses we conducted revealed the presence of unusual patterns in the bitcoin graph. The goal of the following sections is to study one of these anomalous patterns.

3 Analyzing Indegree Outliers and Detecting PS-transactions

As observed in [7], the indegree distribution of the nodes of the users graph follows a power law, as expected in a small world network. For the sake of completeness we report this in indegree distribution in Figure 1(a) (note the log-log scale). In [7] we also observed that the exponent of this distribution is stable over time. (i.e. the exponent for the distribution of the indegrees of the graph obtained from the blockchain at discrete time intervals). In this paper, we aim to verify the following conjecture.

Conjecture 3.1. The small world theory discrepancies, as the indegree distribution outliers, are caused by artificial users behavior.

Restricting ourselves to the indegree distribution analysis only, we want now to verify the hypothesis by proving that such distribution outliers are in fact a consequence of long chains of special transactions.

In order to select the indegree outliers to be analyzed, we consider all the degrees having the following property (with 10 as value of the parameter k).

Property 3.1. Let $y = I(x)$ be the indegree distribution, where $I(x)$ is the number of nodes of the users graph with indegree x, and let Δ be the maximum indegree in the graph and $k \in \mathbb{N}$ a parameter. For every $k < x \leq \Delta$, x is a *suspicious outlier* if $I(x)$ is at least one order of magnitude greater than the average $I(x-i)$ with $1 \leq i \leq k$, i.e. if $I(x) > 10 \cdot \frac{\sum_{i=1}^{k} I(x-i)}{k}$.

The only spikes satisfying the Property 3.1 are the ones corresponding to indegree 708, 709, 771, and 772.The corresponding $I(x)$ values are between two and three

order of magnitude above the value expected. We have analyzed the nodes of the network corresponding to these peculiar degrees.

To analyze the selected outliers, we started from a manual inspection of them. To do so we retrieved in the graph the clusters with indegree 708, 709, 771 and 772 and isolated their neighborhood and transactions history. This provided us with 1647 clusters to analyze. We noticed that many of them had almost consecutive identifiers in our graph. That happened because the oldest addresses contained in each of those clusters appeared for the first time in the blockchain together as destination of a payment in a unique transaction.

Looking for the first appearance of a sample of those addresses in the blockchain we noticed some peculiar transactions. One of these, for instance (Transaction hash `35dead89c059e846e2013a06a70cd84a7ba0f80da7741c283d6efd573e0a7319`) has one input and 101 outputs paying 0.00001 BTC to each one of the outputs except one, that is filled with the change (minus the fees). The address containing the change is then used to perform an analogous transaction leaving the change in a new address and so on. Basically the behavior of the transaction creator is to create a chain of transactions, where a transaction at each step pays a constant amount of 0.00001 BTC to some addresses and leaves the change in an intermediary address used as input for the next hop in the chain. A chain ends either when the funds in the last change address are used for a transaction without this particular structure or when the input funds are completely spent and no change address is used in the last transaction of the chain. We also noted that the output addresses receiving 0.00001 BTC were addresses for the most part identifiable with users from the `bitcointalk` forum (indeed, the forum users had specified those addresses in their signatures). This suspicious transactions chain led us to define a new classification for transactions, labeling all the transactions with this peculiar behavior as *pseudo-spam* transactions (PS-transactions).

Definition 3.1. Let A be the set of all addresses present in the blockchain. Given a transaction t modeled as a tuple $(In, Out, InAmount, Fees)$, where:

- $In \subseteq A$;
- Out is a multiset of couples (o,b) where $o \in A$ and $b \in \mathbb{R}$, where b corresponds to the amount payed to address o by In;
- $InAmount \in \mathbb{R}$;
- $Fees \in \mathbb{R}$;

we say that t is a *pseudo-spam transaction* (PS-transaction) if it satisfies the following properties:

- $|In| = 1$;
- $|Out| \geq 2$;
- $|\{(o,b) \in Out \ : \ b \neq 0.00001\}| \leq 1$.

In other words, a PS-transaction is such that the only input address pays all the others (at least two) 0.00001 BTC except one which can be the recipient of an arbitrary amount. We call this particular address *change address*, i.e. a is a change

address if a is s.t. $(a,b) \in Out_i$ and $b \neq 0.00001$. We call *common output* any output containing an address that is not a change address. Of course in each PS-transaction can exist at most one change address.

3.1 On the Economical Meaning of PS-transactions

Artificial transactions are not uncommon in the blockchain. Since they target what, at first glance, seems like a random selection of addresses in the blockchain, some users in the past have noticed receiving unexpected payments from such transactions and some interest has sparked around them. Unfortunately, there is no clear explanation of the goal of such transactions. In particular, in the following we explore some possible existing conjecture, showing that none of them is able to fully explain the purpose of our PS-transactions.

It is possible that these transactions are part of an attack on users pseudonymity, as an attempt to link addresses ownership. In fact the amounts sent are so tiny that in order to be spent they must be first combined with other funds in a multi-input transaction. This would potentially reveal new linking for the multi-input clustering heuristic (see Section 2) increasing its effectiveness. Even if this theory sounds reasonable, it does not seem to be applicable to our observed real use case. In fact the targets of our manually observed suspicious transactions are not picked at random from the blockchain but derived from a very close set of users belonging to the `bitcontalk` forum, and the transactions pay the same amount to any address multiple times. For an attacker it would make little sense to send funds (hence spending them) to the same address a lot of times and would be more efficient to send those funds to different addresses instead, because this would increase its probability of triggering a funds consolidation while minimizing the cost of the attack.

Another possible conjecture is that those transactions are used as part of a spam attack, to fill the blockchain space with useless data. But this is arguably not true since most of those transactions pay a regular fair fee to be included in the blockchain and so they have the same right to be included as any other transaction. Note that we perform a transaction analysis based on the blockchain information, so we only consider the permanent effect of transactions. The kind of transaction observed can be effectively used to perform a live spam attack to rapidly fill the users pending transactions lists, as historically really happened during the flooding attack of July 2015 [1]. But live spam attacks by themselves leave little to no sign on the blockchain.

Another possible interpretation would be that this transactions are used for advertising. By using vanity addresses or inserting human readable messages in the transactions it is possible to use a transaction to cheaply save an advertisement message in the blockchain forever. By including in such transactions the largest possible number of outputs one may attempt to increase the message visibility.

A famous example of these transactions arose to popularity during the Sochi Olympics, because two addresses (`1SochiWwFFySPjQoi2biVftXn8NRPCSQC` and `1Enjoy1C4bYBr3tN4sMKxvvJDqG8NkdR4Z`) started sending thousands of transactions paying exactly 1 satoshi (0.00000001 BTC) to what seemed like

random addresses read directly from the blockchain. Those transactions payed no fees and so only few of them were actually saved in the blockchain but they remained for hours in the users wallets as unconfirmed transactions, gaining a lot of visibility [2, 3]. It seems difficult to think that this was part of a deanonymization attack since most of the transactions never became part of the blockchain and so could not be spent to possibly reveal addresses linking. It might have been considered a spam attack but only limited to the live network (by filling the unconfirmed transaction lists of the users with useless data) but it had very little effect on the blockchain since few transactions were actually included. So the most plausible theory seems to be that it was part of a temporary spam advertising campaign, and a successful one since most bitcoin users received the message to "Enjoy Sochi" with very little cost. The cost was so little since very few transactions were accepted in a block (hence actually spending the used funds) and the 0.00000001 BTC payments carried so little value to do not matter anyway.

Whatever is the reason for this kind of transactions, it is obvious that they should be considered artificial transactions anyway, since the transaction purpose is to obtain some kind of side real world effect rather than to transfer value between addresses. This is clearly obvious for the Sochi example where the fair fees cost of a transaction would exceed the value effectively transferred. The same can be said for our manual inspected transactions were the fee was 0.0007184 BTC, hence seventy times the single amounts transferred and 41.8% of the total value actually spent by the transaction. This is the reason why we have labeled this kind of transactions as "pseudo-spam" even if we do not know neither want to imply that they are part of a spam attempt.

3.2 Chaining PS-*transactions*

Applying Definition 3.1 to our dataset we labeled 578 316 transactions as PS-transaction, out of the 99 602 440 multi-input multi-output transactions contained in our database. The transactions vary a lot (considering most of the transactions features as the number of outputs or the fees payed), but an interesting behavior can be seen analyzing the timestamps cumulative distribution among those transactions. As shown in Figure 1(b) we can see a steep step during July 2015 showing that most of those transactions were performed at that time. This is consistent with our observations, since the transactions of our case study take place during July 2015 as well, and with the existence of an historically recorded flooding attack happened during the same period [1].

As we've previously said, the interesting behavior is not only about the transactions themselves, but rather about their use as links in a chain. For this reason, we define a "pseudo-spam chain" (PS-chain) as follows.

Definition 3.2. A *pseudo-spam chain* (PS-chain) is a sequence of PS-transactions in which the unique input address of the i-th transaction is the change address of the $(i-1)$-th transaction and the amount in input of the i-th transaction is the value payed to the change address in the $(i-1)$-th transaction.

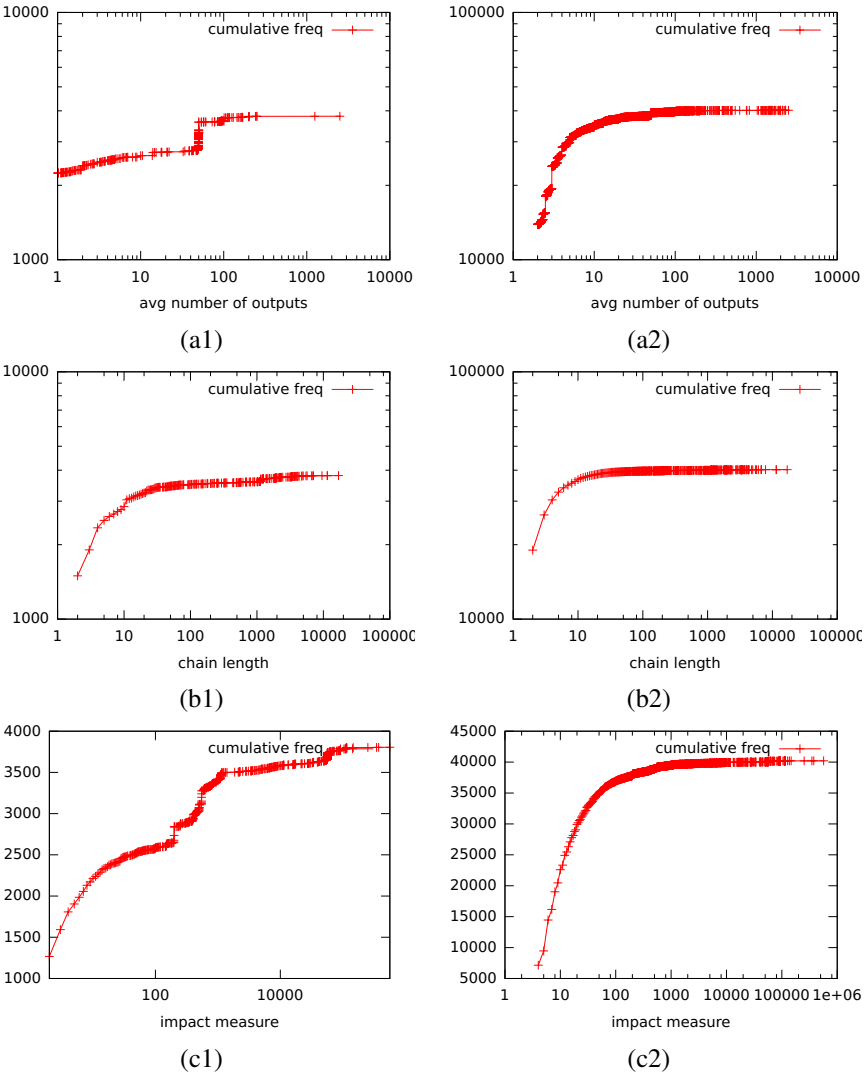


Fig. 2: PS-chains statistics (a1,b1,c1) and almost PS-chains statistics (a2,b2,c2)

Given a set T of PS-transactions, not always there exists just one pseudo-spam chain candidate including all the PS-transactions in T. We consider the smallest partition of T in PS-chain, i.e. whenever two PS-chains can be merged we merge them.

Considering as T the set of all the PS-transactions, we merged the PS-transactions in chains obtaining 24 381 PS-chains. To prune the PS-chains multiset from false positives we eliminated from the multiset all the singletons, hence discarding all the pseudo-spam transaction candidates that were not part of any chain. This left us with

3 805 PS-chains. In the following we report some basic statistics of the PS-chains we have found.

Average Number of Outputs. We have observed the cumulative distribution of the average number of outputs (excluding the change address linking to the next link in the chain) in each chain, which is shown in Figure 2(a1). We can notice how a large number of chains (i.e. 2 240) has exactly one single output address (excluding the change address). If we consider the cumulative distribution ignoring this special case, hence ignoring single output chains, we can notice a steep increase around 50: this value seems to be the preferred average number of outputs of the chains. The transactions we have manually examined had 100 outputs excluding the change address. We have seen that a good percentage of the PS-chains found share this behavior (approximately 7% if we don't count the single output ones).

Chain Lengths. If we consider the distribution of the lengths of the PS-chains found, shown in Figure 2(b1), we can notice very high initial values as well. More precisely, the chains of length two are 39.3%, while the chains of length at most three are already more than 50%.

Chain Impact. The small average number of output and the short length of many chains show that we found a lot of chains with a very low overall number of outputs. We define the *impact* of a chain as its average number of outputs times its length, or in other words the total number of outputs (excluding change addresses used as intermediary chain links) of all the transactions included in the chain. The cumulative distribution of this new measure is shown in Figure 2(c1). The higher this value is, the more "disruptive" the chain can be considered for the graph. From the plot we can immediately observe as 33.3% of all the chains have the minimum value, it means that one third of all the chains has length two and only one output is not a change output in each of its two transactions. We think that there is an high chance that these chains are normal and not artificially intended. Hence, for small values of this new measure we cannot label those chains as artificial since they may as well result from a lot of "normal" use cases. Even if those chains are not naturally occurring but deliberately created, their impact on the network is limited and not statistically relevant (since they represent 0.026% of all the multi-input multi-output transactions). We can chose a threshold for the chain impact measure, below which the chain are to be considered indistinguishable from legitimate transactions chains and we can prune the PS-chains set accordingly.

4 From the case study to generic chains

In the previous section we have defined what is a PS-transaction and a PS-chain starting from manual observations. The definition of a PS-transaction was given keeping into account our practical observation that such transactions payed an amount equal to 0.00001 BTC to each output, but we can easily observe that the amount payed as output is not the distinctive feature of the chains we're trying to model, their structure rather is. Taking into account this observation, we consider different

transactions sharing a similar structure to the PS-transactions but having arbitrary amount spent by the common outputs.

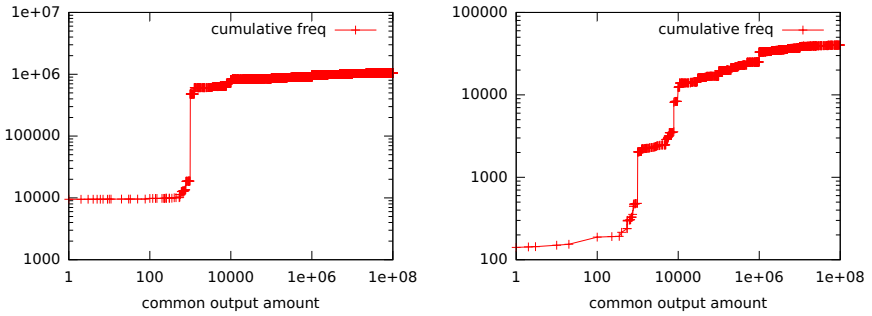
Definition 4.1. Given a transaction t we say that $t = (In, Out, InAmount, Fees)$ is an *almost* PS-*transaction* if it satisfies the following properties:

- $|In| = 1$;
- $|Out| \geq 3$;
- $|\{(o,b) \in Out \ : \ b \neq a\}| \leq 1$, for some $a \in \mathbb{R}$.

It is worth observing that not all the PS-transactions are almost PS-transactions. Indeed, we point out that we need to consider transactions of at least three outputs to be able to distinguish between the regular outputs and an eventual change address. Moreover, we also further restrict ourselves to only consider almost PS-transactions with common output value smaller than 1 BTC because high value transactions are more likely to be considered not spam.

We then define an almost PS-chain exactly as in Definition 3.2 but using almost PS-transactions instead. Applying our classification to the blockchain we found 1 050 783 almost PS-transactions that could be joined in 149 328 almost PS-chains. Among these, 40 208 almost PS-chains were not singletons.

If we perform the same analyses on some basic statistics of the almost PS-chains found as we did before for the PS-chains in Section 3, we obtain similar results. The plot of the cumulative distribution of chain lengths shown in Figure 2(a2) and number of outputs (excluding change addresses) shown in Figure 2(b2) show the same behavior as in Section 3, with 47.3% of the chains having length two and 34.6% of the chains having the minimum number of outputs. This suggests that our case study was a good approximation of the general phenomenon. If we evaluate the chain impact measure cumulative distribution as before we obtain a similar but smoother plot, shown in Figure 2(c2). For the almost pseudo-spam case we can also consider a new parameter that is the common outputs amount value of transactions and chains. The common output amount value cumulative distribution for almost PS-transactions found is depicted in Figure 3(a). We can immediately observe how the common output amount value used in our case study (0.00001 BTC) in Section 3 is the most frequent value for almost PS-transactions, covering 43.8% of all such transactions. We also note that all of the highest frequency common values are all "clean" values (for example 1, 600, 1000, 1250, 2750, 3000, 3500). This is compatible with human designed transactions rather than random purchase transactions, since prices are usually expressed in traditional fiat currencies such as USD or EUR, and their change in BTC is rarely a "clean" number. In Figure 3(b), we show the common output amount values cumulative distribution of the almost PS-chains found. In this graph the highest frequency values are clean numbers (1000, 7800, 10000, 100000, 200000, 500000, 1000000) as in the previous graph but the value 0.00001 has a smaller importance. This happens because a lot of the transactions with this common output value were joined in single long transactions.



(a) (b)

Fig. 3: Common output amount (expressed in 10^{-8} BTC) cumulative ditributions for almost PS-transactions (a) and almost PS-chains (b)

5 Verifying Conjecture 3.1

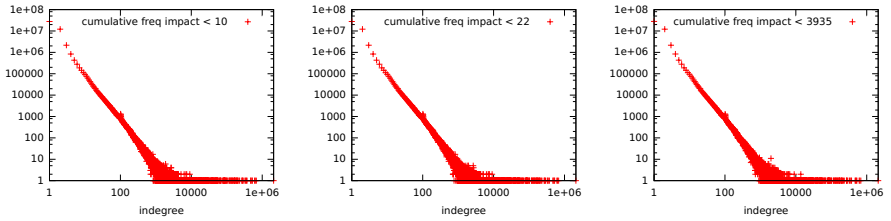
In the following, we aim to prove Conjecture 3.1 by proving that the four outliers observed at the beginning of Section 3 are caused by few PS-chains targeting a small set of addresses artificially increasing their corresponding cluster's indegree. It is worth observing that not all of the output addresses of PS-chains are among those four outliers. Those other addresses do not stand out because they are part of already popular clusters, and so their indegree is marginally affected by those transactions while the pseudo-spam effect is more visible in other unpopular addresses. We also observe that we shall not expect all of the clusters with an indegree value of 708, 709, 771 or 772 to be artificially inflated. In fact, it is natural to expect the existence of a number of clusters, e.g. about 10, with these indegrees.

We start by checking if the clusters marked as outliers have at least one address that appears as output in a PS-chain. We find out that 1 630 over 1 647 clusters satisfy this. It means that only 17 clusters are not affected by the PS-chains. These findings are consistent with what we expected. More precisely, if we restrict just to cluster not involved in PS-chains we obtain an *outlier-free* indegree distribution. This alone is of course not enough to prove our supposition yet. We have only observed that all the outliers take part in a PS-chain but we still have to prove that the PS-chains are the sole cause of those outliers. To do so we firstly introduce the PS-set notion.

Definition 5.1. Given an almost PS-chains set C and a threshold $r \in \mathbb{R}$ we define as *pseudo-spam set* (PS-set) the set of transactions t_i such that there exists j with $t_i \in c_j$, $c_j \in C$, $|c_j| > 1$, and $impact(c_j) \geq r$, where $impact(c_j)$ is defined as the sum of the number of common outputs of each transaction $t_u \in c_j$.

In other words, given a threshold, a PS-set derived from an almost PS-chains set is the set of all the almost PS-transactions belonging to a chain in the candidate set that is not a singleton and has a chain impact measure greater than the threshold.

Now that we have a general definition for the artificial behavior we are trying to isolate we can finally verify whether Conjecture 3.1 is true or not. To check if a



(a) (b) (c)

Fig. 4: Comparing the indegree distribution of the users graph pruned of the transactions belonging to the PS-set for threshold values of 10 (a), 22 (b) and 3935 (c).

pseudo-spam set alone is causing the indegree distribution outliers we re-compute the indegree distribution of the blockchain, ignoring the transactions belonging to the PS-set derived from the almost PS-chains candidate set obtained in Section 4, for increasing values of the threshold.

To choose the threshold values we look at the plot of the chain impact, shown in Figure 2(c2), and we observe that more than 50% of the chains have an impact value smaller than 10, more than 75% have an impact value smaller than 22 and more than 99% have an impact value smaller than 3935. So we choose those three values (10, 22 and 3935) to obtain a PS-set, this results in the indegree distributions depicted in Figure 4. As we can see the outliers disappear for all the values of the threshold considered without macroscopically affecting otherwise the overall distribution (see Figure 1(a) for a comparison). Not only this proves Conjecture 3.1 but it also means that the outlier generating chains of our case study are among the chains with largest impact, and so among the longest and with most outputs chains. This explains why those chains are the one that so macroscopically affect the indegree distribution of the entire network, enough to cause outliers in said distribution. Note that even if only the highest impact chains macroscopically affect the indegree distribution all the PS-transactions in the PS-set influence it. So also including lower impact chains helps cleaning the indegree distribution from artificial skewed values. Of course the lower the impact value used as threshold the more probable is the presence of false positives in the set, so a trade-of between the two has to be found.

6 Conclusions

This paper investigates the possible reasons of the presence of outliers in the indegree distribution of the bitcoin users graph. We have conducted an extensive set of analyses which have shown that the outliers are generated by artificial chains of transactions. We plan to extend our work to analyse other characteristics of the users graph. For instance, we are investigating whether the high diameter of this graph is due to other kinds of artificial transactions and we also plan to give insights into the nature of these transactions. More precisely we plan to further study the possible semantic of

PS-chains and to expand the analysis to include new types of artificial transaction patterns and their effect on the bitcoin users graph.

References

[1] Bitcoin wiki, retrieved 18 sept 2016. URL https://en.bitcoin.it/wiki/July_2015_flood_attack
[2] bitcointalk, retrieved 18 sept 2016. URL https://bitcointalk.org/index.php?topic=458934
[3] reddit, retrieved 18 sept 2016. URL https://www.reddit.com/r/Bitcoin/comments/1xenyd/just_received_weird_tiny_payments_1sochi_1enjoy/
[4] Androulaki, E., Karame, G., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Financial Cryptography and Data Security - 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers, pp. 34–51 (2013)
[5] Boldi, P., Rosa, M., Vigna, S.: Hyperanf: Approximating the neighbourhood function of very large graphs on a budget. In: Proceedings of the 20th international conference on World wide web, pp. 625–634. ACM (2011)
[6] Borassi, M., Crescenzi, P., Habib, M., Kosters, W.A., Marino, A., Takes, F.W.: On the solvability of the six degrees of kevin bacon game - A faster graph diameter and radius computation method. In: Fun with Algorithms - 7th International Conference, FUN 2014, Lipari Island, Sicily, Italy, July 1-3, 2014. Proceedings, pp. 52–63 (2014)
[7] Di Francesco Maesa, D., Marino, A., Ricci, L.: Uncovering the bitcoin blockchain: an analysis of the full users graph. In: IEEE DSAA 2016 Proceeding of 3rd IEEE International Conference on Data Science and Advanced Analytics, Montreal, Canada, October 17-19 (2016) (2016)
[8] Fergal, R., Harrigan, M.: An analysis of anonymity in the bitcoin system. In: Proceeding of 2011 PASSAT/SocialCom 2011, pp. 1318–1326. IEEE (2011)
[9] Kondor, D., Pósfai, M., Csabai, I., Vattay, G.: Do the rich get richer? an empirical analysis of the bitcoin transaction network. PloS one **9**(2), e86,197 (2014)
[10] Lischke, M., Fabian, B.: Analyzing the bitcoin network: The first four years. Future Internet **8**(1) (2016)
[11] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Internet Measurement Conference, IMC 2013, Barcelona, Spain, October 23-25, 2013, pp. 127–140 (2013)
[12] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
[13] Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: Financial Cryptography and Data Security - 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers, pp. 6–24 (2013)