C[1]¿m1
Contractcontract {} Functionfunction {} Ifif {} Elseelse {}

Nebulas Technecial Whitepaper

Nebulas Team

August 21, 2017

Abstract

Abstract is here
Blue text is for blue.
Red text is for comment.
Here are some examples for citation, GNU pthread [21], PARSEC [4].

Contents

1 Introduction

2 NAS Coin

robin

3 Account and Address

Robin

4 Blocks and Transactions

Wenbo

5 Nebulas Rank

5.1 Nebulas Rank Overview

Currently the Blockchain technology and community have grown into a large scale ecosystem. However, people's perception of Blockchain world is still relatively flat; there is no reasonable way to evaluate the entity, such as user's address, on the blockchain yet. Therefore, we try to come up with a universal value measurement. By mining activities occurs on chain, the value of every entity (address) is able to be quantified as **Nebulas Rank**. **Nebulas Rank** is aimed at two goals:

- As a native value measurement, **Nebulas Rank** could become core algorithms for many fundamental scenarios, such as consensus (see §**??**), DIP (see §**??**) and Blockchain search engine (see §**??**), etc.
- **Nebulas Rank** could inspire various value measurements, as well as deeper insights into the blockchain ecosystem.

Based on the goals above, we define the value measurement of **Nebulas Rank** to be three-fold:

- Liquidity, the frequency and scale of transactions, is the first dimension that **Nebulas Rank** considers. Essentially, by means of capital liquidity, financial activity can promote efficient configuration of social resources and promote economy development. Blockchain established a value network. Thus more transactions and larger transaction scale produce better liquidity, and better liquidity further increases more transactions and larger transaction scale, forming a complete mechanism of positive feedback.
- Propagation, the scope and depth of liquidity, is the second dimension that **Nebulas Rank** considers. In social network, the propagation property, i.e. speed, scope and depth of information propagation, is key measurement indicating network quality and users growth. We see same pattern in the Blockchain world. Better propagation means wider and deeper assets liquidity, which improves the quality of assets in the Blockchain world, and increases the scale of assets.
- Interoperability is the third dimension that **Nebulas Rank** considers. During the early stage of Internet, there were just simple websites and isolated information. Nowadays, all kinds of Internet platforms begin to interact with each other and the small information islands begin to disappear. This tendency could be understood as a process of recognizing information from higher dimensional perspective. We believe that Blockchain world also follows the same roadmap, whose development will be faster. There will be more information of users' assets, smart contract and DApp. And also, there will be more frequent interactions among them. Thus better interoperability will become more important.

We choose transaction records on chain as source data for **Nebulas Rank**. Because comparing with real world, the "trajectory" in Blockchain world is more clear and trustworthy: the transaction data on chain loyally records every transferring among addresses and invoking of "smart contracts". But it is not trivial to design rank algorithm for Blockchain transaction data, since comparing with real world, the transactions in Blockchain world are naturally anonymous and bears larger data scale. So we depict three properties for **Nebulas Rank**:

- Truthful. An entity must pay reasonable effort to improve its rank, which assures that the algorithm can identify trusted valuable users. On one hand, in scenarios like consensus and DIP, truthful ranking encourages users to contribute truthfully in order to realize positive feedback. On the other hand, truthful result provides meaningful hierarchy representation of all users, which will be more helpful for decision makers;
- Computable. As a fundamental field, **Nebulas Rank** of every user should be accessible instantly and thus requires low computational complexity;
- Reproducible. Due to consensus and DIP, the running result of **Nebulas Rank** algorithm needs to be identical by any client.

Next we design basic framework of **Nebulas Rank**. First, transaction records are represented in the form of graph. By the definition of transaction graph (entity graph), every node is mapped to one entity, and each edge represents the transferring between two entities[47]. Transaction graph embeds the fact that money transferring among users leads to assets flowing, which helps to represent the concepts of liquidity and propagation defined before. Meanwhile, the form of graph is convenient to formulate the interoperability among contracts. With the derived transaction graph, we rank nodes by their network

centrality. In the scenario of **Nebulas Rank**, LeaderRank[13][26] is a more reasonable measurement and outperforms PageRank and NEM[31].

5.2 Transaction Graph

This subsection introduces how to derive transaction graph from transaction history.

First, we take effective transferring among individual addresses during the past T (generally T is the number of blocks in a month) blocks, denoted by T_{xs}:

$$T_{xs} = \{(st\tau a)|\tau = \#CurrentBlock - T \ldots \#CurrentBlock \wedge a > 0\} \tag{1}$$

, where s, t and a are source address, target address and transfer amount.

Then based on T_{xs}, a directed weighted simple graph is constructed, denoted as $G = (VEW)$, where node set, edge set and edge weights are denoted by V, E and W respectively. Additionally, let $N = |V|M = |E|$. For simplicity, every node is represented by an integer between 1 and N.

ŁŁŁKŁw_e

$$w_e = \sum_{i=1}^{K} a_i s.t. a_i \in \{a|(st\tau a) \in T_{xs}\} \wedge a_1 \geq a_2 \ldots \tag{2}$$

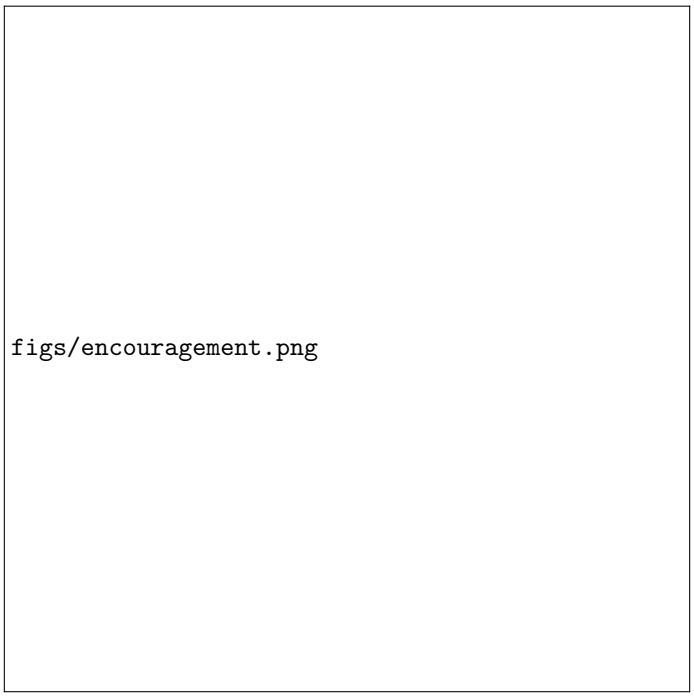

Figure 1: Ł

ŁŁTŁC_v1ŁŁŁE_v[1]Ł$C_v E_V$
ŁŁ
ŁŁ§5.1§**??**
Ethereum#3629091201751#38007752017531171, 684Ł$T = 171, 684$ $K = 22$

[1]ŁŁŁ

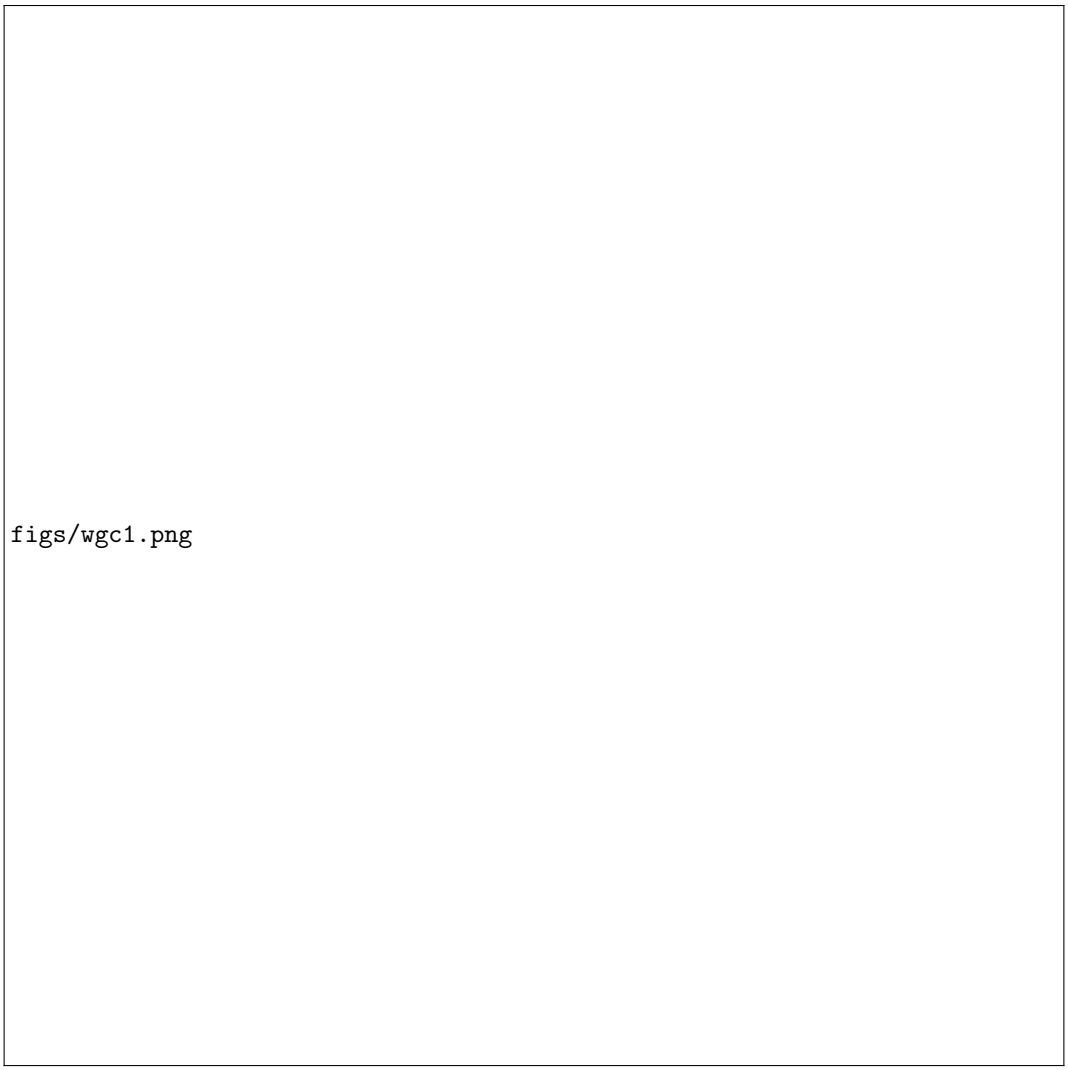

Figure 2: Ł
ŁŁ

5.3 Ranking Algorithm

ŁŁ
LeaderRank[13][26]ŁGroundŁ$\mathcal{G}N+1$GroundŁŁŁ

$$\forall v \in V, w_{(v,\mathcal{G})} = \alpha A_v \tag{3}$$

$$\forall v \in V, w_{(\mathcal{G}v)} = \beta B_v \tag{4}$$

$$\forall v \in V, A_v = \{ \sum_{(u,v)\in E} w_{(u,v)} - \sum_{(v,u)\in E} w_{(v,u)}0\} + \lambda C \tag{5}$$

$$\forall v \in V, B_v = \sum_{(u,v)\in E} w_{(u,v)} + \mu C \tag{6}$$

$$C = median\{w_e | e \in E\} \tag{7}$$

$\alpha, \beta, \mu, \lambda$ŁŁłGroundŁŁGroundŁ
LeaderRankPageRankŁŁGroundŁPageRankdamping factor[10][38](9)H(8)(10))GroundŁ

$$P^{t+1} = H \times R^t P^1 = [\frac{1}{N} \frac{1}{N} \cdots \frac{1}{N} 0]^T \tag{8}$$

$$h_{ij} = \frac{w_{(ji)}}{\sum_k w_{(jk)}} \tag{9}$$

$$\forall v \in V P_v^* \leftarrow P_v^* + \frac{P_{\mathcal{G}}^*}{N} \tag{10}$$

LeaderRank§5.1

- LeaderRankŁŁŁ**Nebulas Rank**Ł
- (4)(6)Ł§**??**
- LeaderRank§5.2

labelsubsec:robust
ŁŁŁNebulas Rank

-
-
-
- łłŁ

Nebulas Rankł

- TłŁł
- łŁ§5.291%łK2ŁŁ
- ł
- Ł1łŁłŁł
- łł§5.2453, 285łŁ970, 5771, 169ł449, 746łŁŁ99.2%133łŁŁ0.03%ł
- PageRankNCDawareRank[35],(4)(6)ŁŁłGroundŁŁł**Nebulas Rank**

20175Ethereum§5.2
Nebulas Rank1[2] Ł

[2]: Etherscan[**etherscan**]

Table 1: **Nebulas Rank**10Ł

		Nebulas Rank		(Ether)	(Ether)
1	0x267be1c1d684f78cb4f6a176c4911b741e4ffdc0	0.449275	Kraken_4	3214232.06	350008.00
2	0xd4c5867cec094721aabc3c4d0fd2f2ac7878c79a	0.093798		58000.00	100947.00
3	0x027beefcbad782faf69fad12dee97ed894c68549	0.049277	QuadrigaCX	207440.11	65606.40
4	0x0ee4e2d09aec35bdf08083b649033ac0a41aa75e	0.046831		56465.00	60087.96
5	0xc257274276a4e539741ca11b590b9447b26a8051	0.037628		1071105.93	1434106.72
6	0xa53e0ca7d246a764993f010d1fde4ad01189f4e6	0.033488		7764.68	3201.00
7	0xf259e51f791e9ed26e89b6cae4a7c6296bfbd0b8	0.033481		3307.00	7731.30
8	0xf195cac8452bcbc836a4d32cfb22235af4ac1e9c	0.026343		10863.87	2315.69
9	0x94435d12c51e19d5b5c8656763f9069d37791a1a	0.024970		12938.58	15858.90
10	0x7580ba923c01783115d79975d6a41b3d38eff8d5	0.021670		263000.00	364793.49
16	0xcafb10ee663f465f9d10588ac44ed20ed608c11e	0.004995	Bitfinex_1	360000.00	1435858.40
51	0xd94c9ff168dc6aebf9b6cc86deff54f3fb0afc33	0.000868	yunbi_1	1179224.74	1202539.53
64	0x70faa28a6b8d6829a4b1e649d26ec9a2a39ba413	0.000590	Shapeshift	52501.81	651933.49

Nebulas Rank Borgatti [6]ŁłłŁŁ**Nebulas Rank**3ŁŁ**Nebulas Rank**

Figure 3: Nebulas Rank v.s.

łRank

ŁXŁYEther$Ł$ŁYEther4

Figure 4:

Shapeshift (0x70faa28a6b8d6829a4b1e649d26ec9a2a39ba4135ŁŁŁŁ§5.2**Nebulas Rank**ŁŁ

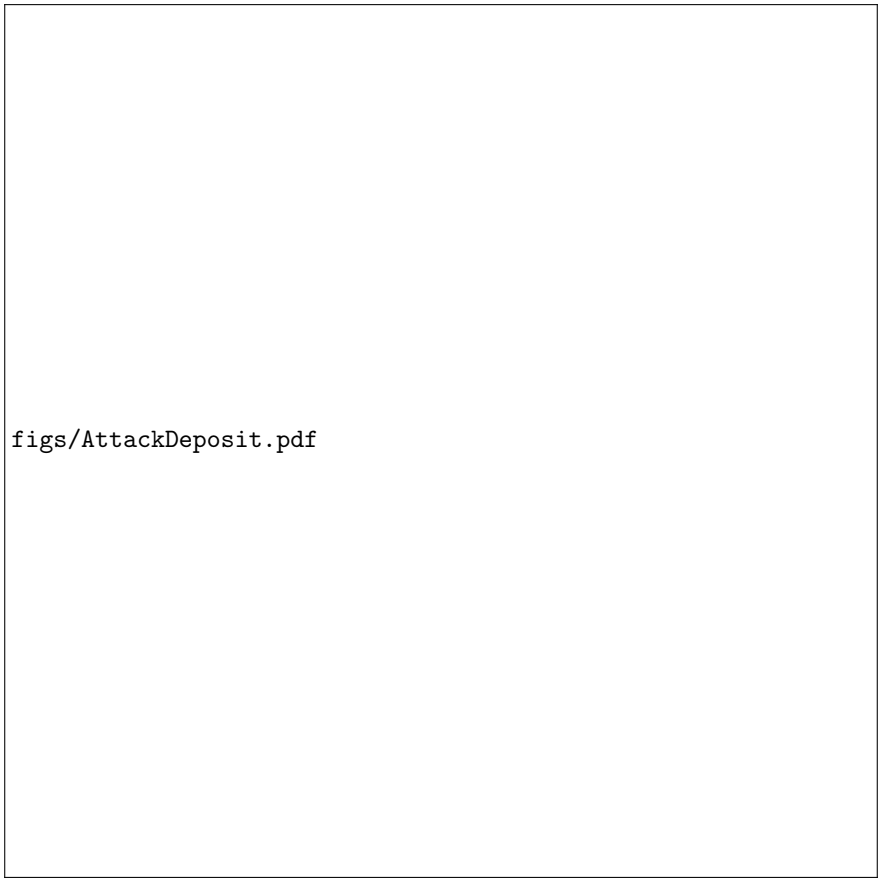

Figure 5: Ł

5000, Ł
ŁŁ
NR§5.2§5.3
PR*§5.2PageRank
NCD*§5.2NCDawareRank
NCD$^\#$[31]NCDawareRank
PR$^\#$[31]PageRank
PageRankdamping factor0.15NCDawareRankpscan[11]$\eta = 0.75$, $\mu = 0.1$

5.4 Related Works

Łł[32][17] [5] Katz[23] [42] [18][19][20][36][33] PageRank[10] HITS[24] SALSA[43] [6][7][27]**Nebulas Rank**Borgatti [6][20] ()[33]Ł**Nebulas Rank**

ł[30]2009ŁŁ[41][22][34][2] [28][37][39][16][15] Ł[12][1] **Nebulas Rank**Tschorsch and Scheuermann [47]ŁŁŁŁ[40][9][44][3][14][29][8][25][45] Ł

Nebulas Rank NEM[31]Proof-of-Importance NCDawareRank[35] NCDawareRank[35]Proof-of-ImportanceSCAN[48][46][11]ŁŁ
Kester, and Pillai [16]PageRankŁŁPageRankŁ**Nebulas Rank**LeaderRank[13][26] PageRankPageRankŁŁLead-
erRankŁGroundŁŁŁ**Nebulas Rank**ŁLi *et al.* [26]ŁLeaderRankGroundŁ

6 PoD

jingchan

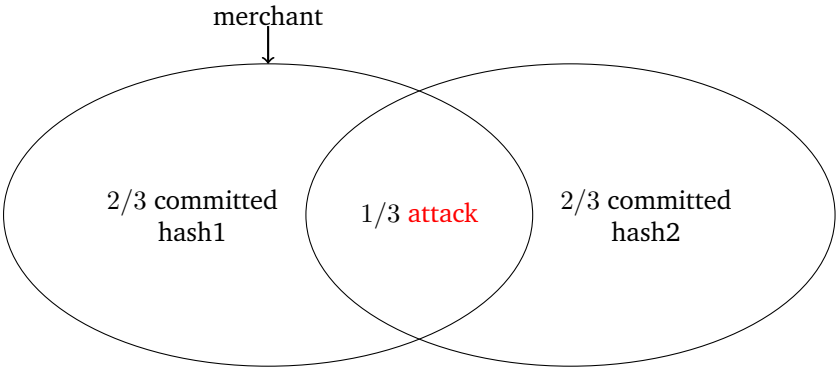

Figure 6: Attack

7 DIP

Shangshu

8 Nebulas Force

wenbo

9 Smart Contract

Wenbo

10 Infrastructure and Developing Tools

References

[1] Luke Anderson *et al.* "New kids on the block: an analysis of modern blockchains." In: (2016). arXiv: 1606.06530. URL: http://arxiv.org/abs/1606.06530.

[2] Annika Baumann, Benjamin Fabian, and Matthias Lischke. "Exploring the Bitcoin network." In: *WEBIST 2014 - Proceedings of the 10th International Conference on Web Information Systems and Technologies* 1 (2014), pp. 369–374. ISSN: 9789897580239 (ISBN). DOI: 10.5220/0004937303690374. URL: https://www.engineeringvillage.com/blog/document.url?mid=cpx%7B%5C_%7D9ce5505146fd48dcbdM557010178163125%7B%5C&%7Ddatabase=cpx.

[3] Morten L Bech and Enghin Atalay. "The topology of the Federal Funds markets." In: *Economic Policy Review* 14.2 (2008).

[4] C. Bienia and K. Li. "Parsec 2.0: A new benchmark suite for chipmultiprocessors." In: *Proceedings of the 5th Annual Workshop on Modeling Benchmarking and Simulation*. 2009.

[5] Phillip Bonacich. "Factoring and weighting approaches to status scores and clique identification." In: *Journal of Mathematical Sociology* 2.1 (1972), pp. 113–120.

[6] Stephen P. Borgatti. "Centrality and network flow." In: *Social Networks* 27.1 (2005), pp. 55–71. ISSN: 03788733. DOI: 10.1016/j.socnet.2004.11.008.

[7] Stephen P. Borgatti and Martin G. Everett. "A Graph-theoretic perspective on centrality." In: *Social Networks* 28.4 (2006), pp. 466–484. ISSN: 03788733. DOI: 10.1016/j.socnet.2005.11.005.

[8] Michael Boss, Martin Summer, and Stefan Thurner. "Contagion Flow Through Banking Networks." In: *Lecture Notes in Computer Science 3038* (2004), pp. 1070–1077. ISSN: 03029743. DOI: 10.1016/j.jfi.2008.06.003. arXiv: 0403167v1 [arXiv:cond-mat].

[9] Michael Boss *et al.* "The Network Topology of the Interbank Market." In: *Quantitative Finance* 4.6 (2004), pp. 677–684. ISSN: 1469-7688. DOI: 10.1080/14697680400020325. arXiv: 0309582 [cond-mat]. URL: http://arxiv.org/abs/cond-mat/0309582.

[10] Sergey Brin and Lawrence Page. "Reprint of: The anatomy of a large-scale hypertextual web search engine." In: *Computer Networks* 56.18 (2012), pp. 3825–3833. ISSN: 13891286. DOI: 10.1016/j.comnet.2012.10.007. arXiv: 1111.6189v1.

[11] Lijun Chang *et al.* "pSCAN: Fast and Exact Structural Graph Clustering." In: *IEEE Transactions on Knowledge and Data Engineering* 29.2 (2017), pp. 387–401.

[12] Tao Hung Chang and Davor Svetinovic. "Data Analysis of Digital Currency Networks: Namecoin Case Study." In: *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS* (2017), pp. 122–125. DOI: 10.1109/ICECCS.2016.023.

[13] Duan Bing Chen *et al.* "Identifying influential nodes in large-scale directed networks: The role of clustering." In: *PLoS ONE* 8.10 (2013), pp. 1–10. ISSN: 19326203. DOI: 10.1371/journal.pone.0077455.

[14] Giorgio Fagiolo. "The International-Trade Network: Gravity Equations and Topological Properties." In: (2009). arXiv: 0908.2086. URL: http://arxiv.org/abs/0908.2086.

[15] Danno Ferrin. "A Preliminary Field Guide for Bitcoin Transaction Patterns." In: *Texas Bitcoin Conference* (2015). URL: http://texasbitcoinconference.com.

[16] Michael Fleder, Michael S. Kester, and Sudeep Pillai. “Bitcoin Transaction Graph Analysis.” In: *. . . -Transaction-Graph-Analysis. Pdfffdfffdfffd . . .* (2015), pp. 1–8. arXiv: 1502.01657. URL: http://arxiv.org/abs/1502.0165%7B%5C%%7D5Cnhttp://people.csail.mit.edu/spillai/data/papers/bitcoin-project-paper.pdf%7B%5C%%7D5Cnhttp://arxiv.org/abs/1502.00165%7B%5C%%7D5Cnhttp://arxiv.org/abs/1502.01657.

[17] L Freeman. “A set of measures of centrality: I. Conceptual clarification.” In: *Soc. Networks* 1 (1979), pp. 215–239.

[18] Linton C Freeman. “A set of measures of centrality based on betweenness.” In: *Sociometry* (1977), pp. 35–41.

[19] Linton C Freeman. “Centrality in social networks conceptual clarification.” In: *Social networks* 1.3 (1978), pp. 215–239.

[20] Linton C Freeman, Stephen P Borgatti, and Douglas R White. “Centrality in valued graphs: A measure of betweenness based on network flow.” In: *Social networks* 13.2 (1991), pp. 141–154.

[21] *GNU Portable Threads*. http://www.gnu.org/software/pth/.

[22] Bernhard Haslhofer, Roman Karl, and Erwin Filtz. “O Bitcoin Where Art Thou? Insight into Large-Scale Transaction Graphs.” In: ().

[23] Leo Katz. “A new status index derived from sociometric analysis.” In: *Psychometrika* 18.1 (1953), pp. 39–43.

[24] Jon M Kleinberg. “Authoritative sources in a hyperlinked environment.” In: *Journal of the ACM (JACM)* 46.5 (1999), pp. 604–632.

[25] Lothar Krempel. “Exploring the Dynamics of International Trade by Combining the.” In: December (2002), pp. 1–22.

[26] Qian Li *et al.* “Identifying influential spreaders by weighted LeaderRank.” In: *Physica A: Statistical Mechanics and its Applications* 404 (2014), pp. 47–55. ISSN: 03784371. DOI: 10.1016/j.physa.2014.02.041. arXiv: arXiv:1306.5042v1.

[27] Linyuan Lü *et al.* “Vital nodes identification in complex networks.” In: *Physics Reports* 650 (2016), pp. 1–63. ISSN: 03701573. DOI: 10.1016/j.physrep.2016.06.007. arXiv: 1607.01134.

[28] Sarah Meiklejohn *et al.* “A fistful of Bitcoins: Characterizing payments among men with no names.” In: *Proceedings of the Internet Measurement Conference - IMC ’13* 6 (2013), pp. 127–140. ISSN: 15577317. DOI: 10.1145/2504730.2504747. URL: http://dl.acm.org/citation.cfm?id=2504730.2504747.

[29] L Morten, J Robert, and E Walter. “The topology of interbank payment flows.” In: (2006).

[30] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System.” In: *Www.Bitcoin.Org* (2008), p. 9. ISSN: 09254560. DOI: 10.1007/s10838-008-9062-0. arXiv: 43543534534v343453. URL: https://bitcoin.org/bitcoin.pdf.

[31] *NEM Technical Reference*. http://nem.io/NEM_techRef.pdf. Accessed: 2017-08-01.

[32] Mark Newman. *Networks: an introduction*. Oxford university press, 2010.

[33] Mark EJ Newman. “A measure of betweenness centrality based on random walks.” In: *Social networks* 27.1 (2005), pp. 39–54.

[34] Dá Niel Kondor *et al.* “Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network.” In: *PLoS ONE* 9.2 (2014). DOI: 10.1371/journal.pone.0086197.

[35] Athanasios N. Nikolakopoulos and John D. Garofalakis. “NCDawareRank.” In: *Proceedings of the sixth ACM international conference on Web search and data mining - WSDM ’13* February 2013 (2013), p. 143. DOI: 10.1145/2433396.2433415. URL: http://dl.acm.org/citation.cfm?doid=2433396.2433415.

[36] Jae Dong Noh and Heiko Rieger. “Random walks on complex networks.” In: *Physical review letters* 92.11 (2004), p. 118701.

[37] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. “Structure and Anonymity of the Bitcoin Transaction Graph.” In: *Future Internet* 5.2 (2013), pp. 237–250. ISSN: 1999-5903. DOI: 10.3390/fi5020237. URL: http://www.mdpi.com/1999-5903/5/2/237/.

[38] Lawrence Page *et al. The PageRank citation ranking: Bringing order to the web.* Tech. rep. Stanford InfoLab, 1999.

[39] Thai Pham and Steven Lee. “Anomaly detection in bitcoin network using unsupervised learning methods.” In: *arXiv preprint arXiv:1611.03941* (2016).

[40] Marc Pröpper, Iman van Lelyveld, and Ronald Heijmans. “Towards a network description of interbank payment flows.” In: (2008).

[41] Dorit Ron and Adi Shamir. “Quantitative Analysis of the Full Bitcoin Transaction Graph.” In: ().

[42] Gert Sabidussi. “The centrality index of a graph.” In: *Psychometrika* 31.4 (1966), pp. 581–603.

[43] Computer Science and The Technion. “The Stochastic Approach for Link-Structure Analysis (SALSA) and the TKC E ect.” In: (2001).

[44] M. Ángeles Serrano, Marián Boguñá, and Alessandro Vespignani. “Patterns of dominant flows in the world trade web.” In: *Journal of Economic Interaction and Coordination* 2.2 (2007), pp. 111–124. ISSN: 1860711X. DOI: 10.1007/s11403-007-0026-y. arXiv: 0704.1225.

[45] Ma Angeles Serrano and Marián Boguñá. “Topology of the world trade web.” In: *Physical review. E, Statistical, nonlinear, and soft matter physics* 68.1 Pt 2 (2003), p. 015101. ISSN: 1063-651X. DOI: 10.1103/PhysRevE.68.015101. arXiv: 0301015 [cond-mat].

[46] Hiroaki Shiokawa, Yasuhiro Fujiwara, and Makoto Onizuka. “SCAN++: efficient algorithm for finding clusters, hubs and outliers on large-scale graphs.” In: *Proceedings of the VLDB Endowment* 8.11 (2015), pp. 1178–1189.

[47] Florian Tschorsch and Björn Scheuermann. “Bitcoin and Beyond : A Technical Survey on Decentralized Digital Currencies.” In: *IEEE COMMUNICATIONS SURVEYS & TUTORIALS* PP.99 (2015), pp. 1–1. ISSN: 1553-877X. DOI: doi:10.1109/COMST.2016.2535718.

[48] Xiaowei Xu *et al.* “Scan: a structural clustering algorithm for networks.” In: *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2007, pp. 824–833.