Empirical Analysis of Crypto Currencies

Manoj Kumar Popuri and Mehmet Hadi Gunes

Abstract Analysis of the currency networks is not easy as the transactions are not centralized but rather take place over a large number of banks and commercial entities. Digital crypto currencies, however, require a public ledger to work and provide an opportunity for analysis of currency transactions. A crypto currency is a medium of exchange using cryptography to secure the transactions and to control the creation of new units. In this paper, we analyze two of the popular crypto currencies, i.e., Bitcoin and Litecoin. We construct network of transactions from public transaction ledger. We investigate the structure of currency transaction network by measuring the network characteristics.

1 Introduction

Currency is a medium of exchange, which arose out of need to address the inefficiency of barter. Digital currency is a form of currency that is electronically created and stored [14]. Crypto currencies are often decentralized digital cash systems and there is no single overseeing authority [13]. The first public crypto currency was Bitcoin, proposed in 2008 by Satoshi Nakamoto, a pseudonym [10]. Even though the system went online in January 2009, Bitcoin had very few users and didn't have real world value for a year. Since its inception, over 48 million transactions took place. The market value of Bitcoins in circulation peaked at about 14 billion USD on May 12, 2013, and as of Dec 1, 2015 is about 5.63 billion USD.

The Bitcoin system operates as an online peer-to-peer network, and anyone can join the system by installing the client application. Instead of having a bank account maintained by a central authority, each user has a unique address that consists of a pair of public and private keys. Existing coins are associated to the public key of the owner, and outgoing payments have to be signed by the owner using the

Manoj Kumar Popuri
University of Nevada, Reno, e-mail: mpopuri@unr.edu

Mehmet Hadi Gunes
University of Nevada, Reno e-mail: mgunes@unr.edu

corresponding private key. After validation of transaction with the owner's public key, the successful transactions are formed into blocks.

The transactions of all the crypto currencies are available to anyone by installing the client and connecting to peer to peer network. Such detailed information is rarely available in financial systems, making the the crypto currency networks a valuable source of empirical data involving monetary transactions. Due to the anonymity of the crypto currencies and potentially unlimited number of pseudo identities a user could generate, however, it is hard to determine which observed phenomena are specific to the system and which results can be generalized.

An earlier study by Daniel et.al. analyzes the Bitcoin transaction network to investigate the movement of money and observe the dynamics of the network [7]. In their analysis of Bitcoin data on May 7th 2013, they observe 17 million transactions among 13 million addresses where only a million of them had nonzero balance. According to their analysis there is a strong correlation between the balance and the indegree of individual nodes. They found that the Bitcoin network is gradually increasing since 2010 with some fluctuations, e.g., the boom in the exchange rate in 2011. According to their analysis both the in-degree and out-degree are highly heterogeneous with power law distributions. They also found that Bitcoin network is disassortative except for only a brief period in the initial deployment where the number of nodes were few.

The study of networks has emerged in diverse disciplines as a means of analyzing complex relational data [12]. Network analysis has been applied to physical phenomena [15], biological systems [6], transportation systems [1], social networks [11], software systems [3], linguistics [2] and academy [5].

In this paper, we compare two most popular crypto currencies as a network, by analyzing their transaction ledger. We map the transaction network of Bitcoin and Litecoin digital currencies from their public ledger and analyze the complex network of each digital currency. In our network, the nodes are the addresses of Bitcoin users and the edges are the transaction between two users.

2 Bitcoin Network

We downloaded the Bitcoin ledger and decoded the data collected from the wallet. Bitcoin network is a growing network where the number of unique addresses created increases exponentially. The major increase in the number of unique addresses occurred after the first boom in 2011 and the second one when the Bitcoin market value crossed 1000 USD. The network we are analysing is comprising of $N = 49{,}390{,}594$ nodes, total incoming transactions $E_{in} = 151{,}933{,}127$, and total outgoing transactions $E_{out} = 151{,}857{,}042$. We also divide the transaction data by year to study the evolution of the network over the years.

Degree

The degree distribution captures the underlying structure of a network by summarizing the degree characteristics of the nodes. Figure 1 present the in degree and out degree distributions of the Bitcoin transactions, respectively. While *probability distribution functions* show yearly distributions, overlaid *cumulative distribution*

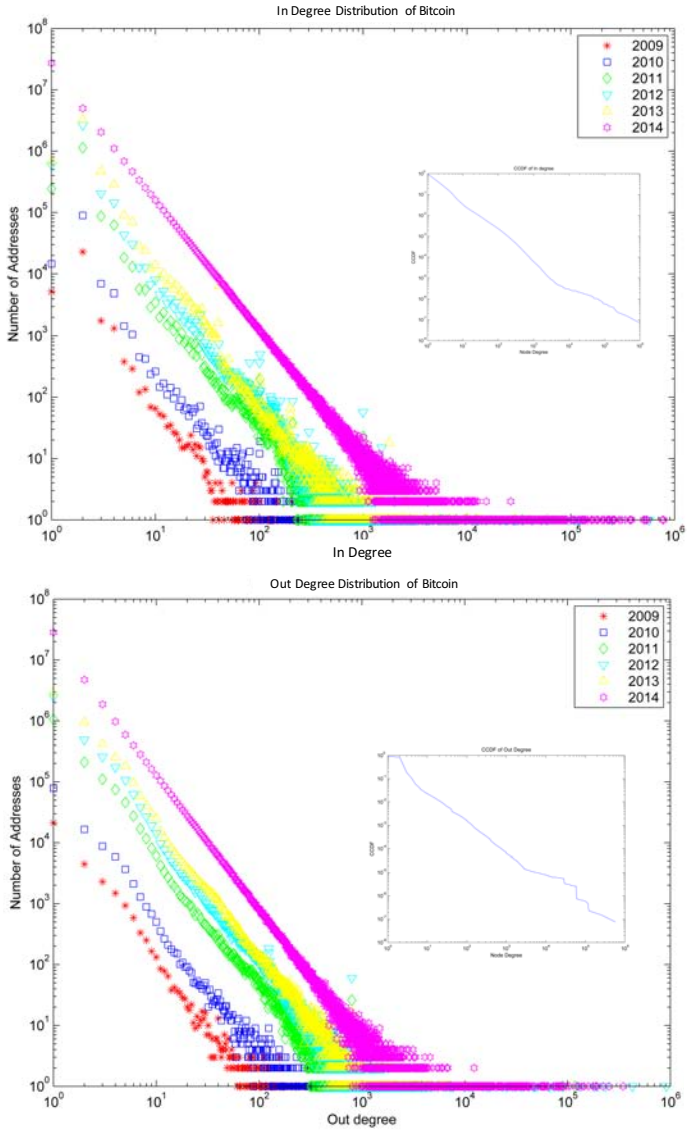

Fig. 1 Degree distribution of the Bitcoin (yearly PDF with overlaid aggregate CDF)

function shows the distribution for all transactions. We find that the degree distributions of yearly transactions as well as all transactions follow power law distribution, which makes Bitcoin network a scale free network, for both in degree and out degree. The power laws of the overall degree distributions are $\alpha_{in} \sim -2.21$ and $\alpha_{out} \sim -2.10$.

Table 1 presents the characteristics of yearly Bitcoin transactions. We observe that from 2009 to 2011 the degree distribution slope increases considerably and thereafter has been increasing but slightly.

Table 1 Degree characteristics of yearly Bitcoin transactions

		In Degree				Out Degree			
Year	*Nodes*	*Edges*	*Max*	*Avg*	α_{in}	*Edges*	*Max*	*Avg*	α_{out}
2009	32,699	98,611	1,257	3.01	1.94	95,499	1,528	2.92	1.78
2010	122,167	374,712	1,826	3.07	2.00	478,271	5,8829	3.19	1.83
2011	1,610,899	5,198,488	118,016	3.23	2.13	5,461,888	59,297	3.39	1.88
2012	3,780,767	14,570,562	913,847	3.85	2.14	14,130,630	570,898	3.73	1.90
2013	5,082,351	16,338,332	16,969	3.21	2.19	16,442,626	69,919	3.23	1.92
2014	38,761,711	115,352,422	636,092	2.98	2.21	116,241,889	1,765,959	3.01	2.10

Assortativity

We computed the nearest neighbour degree function $K_n^{in}(K_{out})$, which measures the in degree K_{in} of the nodes with respect to out degree K_{out}. Figure 2 presents the *degree correlations* for the Bitcoin network. In the graph, we observe that there is a disassortative behaviour between the In and out Degrees of the nodes. That is, the nodes with high out degree tend to connect to the node with low in degree.

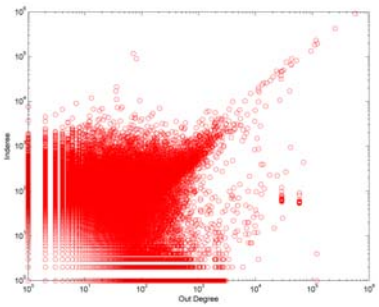

Fig. 2 Degree correlations of Bitcoin

As a summary measure *assortativity coefficient* is calculated as the Pearson correlation coefficient of degree between pairs of linked nodes. Positive values of r indicate a preference to link between nodes of similar degree, while negative values indicate preference to link between nodes of different degree. Table 2 presents the yearly assortativity coefficients of the Bitcoin transactions. We observe that the in-out degree correlation coefficient is negative, except for only a brief period in the initial phase. After mid-2010, the degree correlation coefficient stays between r $\approx$ -0.012 and r $\approx$ -0.015 suggesting that the network is disassortative. In general, for large scale-free networks, assortativity vanishes as the network size increases [9] and a similar behavior is observed in the Bitcoin network.

Clustering

We also measured the *average clustering coefficient*, which measures local density of edges. Table 2 presents clustering coefficients of the yearly Bitcoin transactions. We observed that in 2009 clustering is 0, indicating that there were no triangles among users. Then, between 2010 and 2011, clustering is high, fluctuating around 0.22. This can be due to few early adopters transferring money between their multiple accounts to test the network. As the number of users increase in the subsequent

Table 2 Network characteristics of yearly Bitcoin transactions

Year	2009	2010	2011	2012	2013	2014
Assortativity	-0.30	-0.14	-0.03	-0.025	-0.017	-0.019
Clustering	0.00	0.22	0.21	0.10	0.055	0.04

years, the clustering coefficient reduces from 0.10 in 2012 to around 0.04 in 2014, which is still much higher than a random network of similar size.

Richest Bitcoin Addresses

We traced the top 100 richest addresses in the Bitcoin and analysed for unique patterns. The total Bitcoins in circulation are 14,917,575 BTC with a market value of 377.93 USD as of Dec 1, 2015. The top 100 richest nodes in Bitcoin hold 19.88 % of wealth as shown in Figure 3. We noticed couple of interesting behaviours among the richest Bitcoin users. For instance, the richest node transfers his/her bitcoins to four new addresses and then on the same day transfers all coins back into a single new address, which becomes the new richest address.

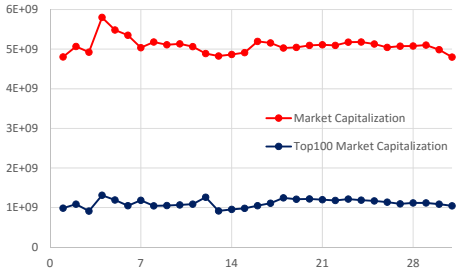

Fig. 3 Richest users during Nov 2015

Figure 4 shows the in and out degree of the top 100 users. We observe that the incoming transactions to the richest people are through mining nodes, which indicates that most of the richest nodes are miners. We also observe that approximately 73 % of the richest people have 0 out degree, which means that they just accumulate money without spending it.

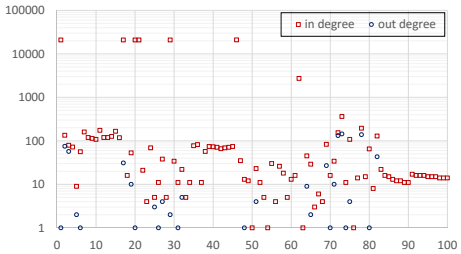

Fig. 4 Degrees of the richest 100 users

Anonymity

Even though Bitcoin data is anonymous, an active attacker can observe the IP address of a transaction request and match it to an actual user [4]. Hence, some users might be interested in hiding their IP address when communicating with the network. Anonymizer technologies allow one to hide a user's IP address and are widely used. Tor is currently the most popular anonymizer network with millions of users [8].

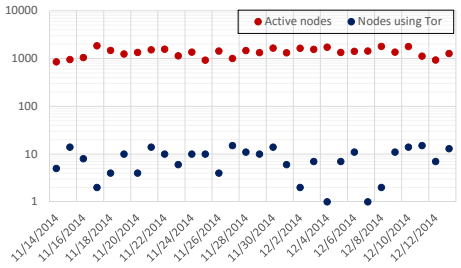

Fig. 5 Anonymity among MyWallet users

To analyze the percentage of anonymous Bitcoin users, we compared the IP addresses connected to the Bitcoin with the IP addresses of Tor exit nodes every hour. We analyzed the IP addresses for 30 days to find the ratio of users connecting to the Bitcoin anonymously as shown in Figure 5. We observed that among 800 to 2000 connects to MyWallet at a given time only up to 20 nodes are using Tor anonymizer.

3 Litecoin Network

Litecoin is refereed to as the silver form of Bitcoin where the protocol is designed so that custom hardware cannot be used for mining. Even through Litecoin market value is 1 % of Bitcoin, the Litecoin network has a total N = 6,990,919 unique addresses, total E_{in} = 56,205,576 incoming transactions, and total E_{out} = 52,456,092 outgoing transactions.

Degree

We calculated the in degree and out degree distributions of the network in Figure 7. Unlike Bitcoin network, the Litecoin network growth is continuous. The degree distributions of aggregate transactions show a power law pattern with an exponent of $\alpha_{in} \sim -2.14$ for in degree and $\alpha_{out} \sim -2.01$ for out degree.

Table 3 presents yearly Litecoin network characteristics. The in degree and out degree power law exponents are more stable than the Bitcoin network.

Assortativity

We compute the *degree correlation*, i.e., the in degree K_{in} of the nodes with out degree K_{out}, for the network in Figure 6. We find that the in-out degree correlation is dissortaative as the nodes with high degree have low in degree. The distribution is different from Figure 2 for Bitcoin where the very high degree nodes connected to other very high degree nodes.

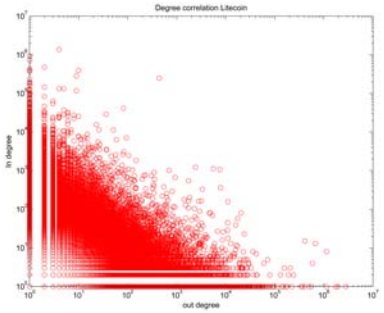

Fig. 6 Degree correlations of Litecoin

Table 4 presents *assortativity coefficient* of yearly Litecoin transactions. We find that the in-out degrees of yearly transactions is dissasortative in 2011 and 2012 but over the time become non-assortative in 2014.

Clustering

We also measured the average clustering coefficient in Table 4. We observed that, in the initial phase clustering is high. After the initial phase the clustering coefficient reduces from 0.33 in 2012 to around 0.032 in 2014.

Table 3 Degree characteristics of yearly Litecoin transactions

		In Degree				Out Degree			
Year	*Nodes*	*Edges*	*Max*	*Avg*	α_{in}	*Edges*	*Max*	*Avg*	α_{out}
2011	22,400	754,734	170,892	33.69	1.81	63,163	4037	2.81	2.21
2012	545,576	10,391,318	1,124,344	19.04	1.90	2,484,673	395,841	4.55	2.13
2013	2,546,672	25,208,855	2,765,143	9.89	2.02	17,876,786	734,660	7.01	2.00
2014	6,735,643	19,850,699	360,129	2.94	2.21	32,031,470	1,373,967	4.75	2.12

Table 4 Network characteristics of yearly Litecoin transaction networks

Year	2011	2012	2013	2014
Assortativity	-0.036	-0.027	-0.015	-0.000
Clustering	0.33	0.18	0.062	0.038

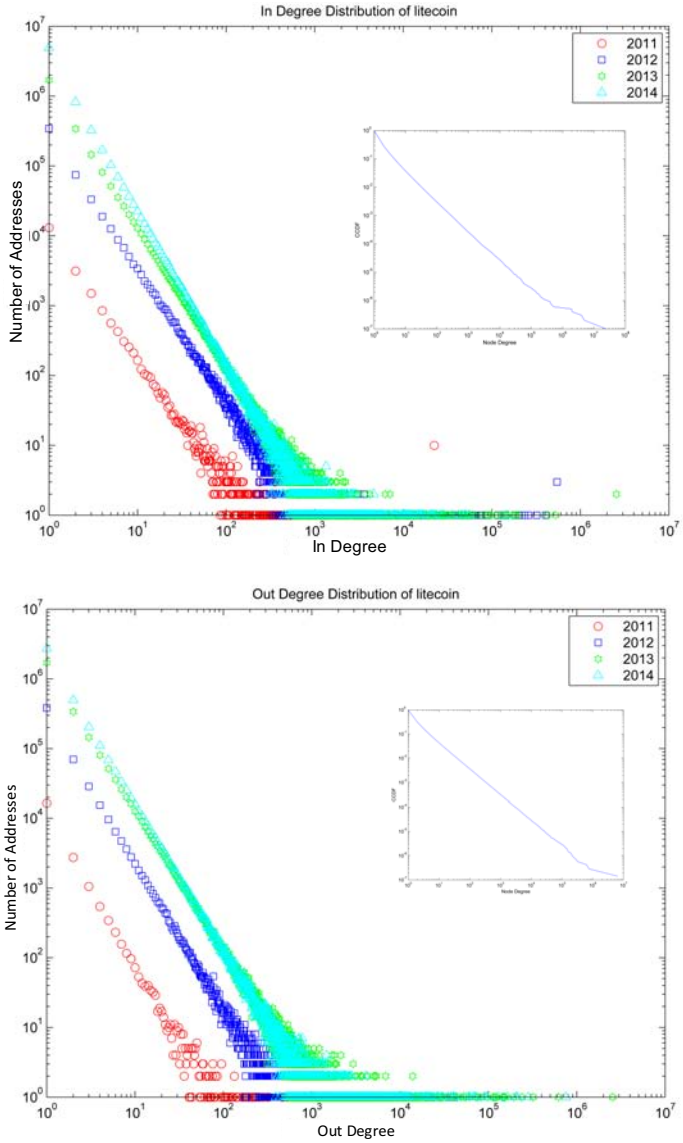

Fig. 7 Degree distribution of the Litecoin (yearly PDF with overlaid aggregate CDF)

Richest Litecoin Addresses

The total Litecoin in circulation are 43,455,110 LTC with a market value of 0.00959 USD as of Dec 1, 2015. The 48.89 % of the total market capitalization of the Litecoin is hold by the richest 100 people. We observed that the behaviour of the top 100 addresses in the Litecoin network are

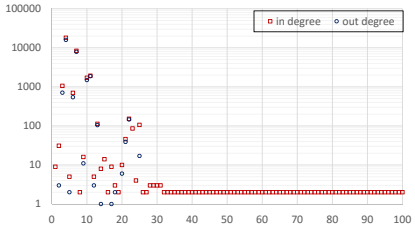

Fig. 8 Degrees of the richest 100 users

similar to the Bitcoin's richest users. We find that among the 100 richest nodes 82 % of the nodes have 0 out degree as shown in Figure 8. We observe an interesting pattern among the richest Litecoin users where more than two thirds of the 100 richest nodes simply transfer their Litecoins into a new account while paying a small transaction fee. This can be an indication that those accounts belong to a single user.

4 Conclusions

We have performed a detailed analysis of the two popular digital currencies, i.e., Bitcoin and Litecoin. After becoming popular after 2011, Bitcoin is characterized by a dissasortative degree correlation and power law in- and out-degree distributions. Litecoin network has disassortative degree correlation and power law in- and out-degree distributions since inception in 2011. The characteristics of richest nodes in Bitcoin and Litecoin are similar. We also found that majority of the richest nodes are interested in just accumulating money.

Acknowledgements This material is based upon work supported by the National Science Foundation under grant number EPS- IIA-1301726.

References

1. Dorothy P. Cheung and Mehmet H. Gunes. A complex network analysis of the United States air transportation. In *IEEE/ACM ASONAM*, page 699–701, Washington, DC, USA, 2012.
2. Grace Crosley and M.H. Gunes. *Using complex network representation to identify important structural components of Chinese characters*, *Complex Networks*, page 319–328, 2014.
3. Andrew Dittrich, Mehmet H. Gunes, and Sergiu Dascalu. *Network analysis of software repositories: Identifying subject matter experts*, *Complex Networks*, pages 187–198, 2013.
4. Esra Erdin, Chris Zachor, and M.H. Gunes. How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys Tutorials*, 17(4):2296–2316, 2015.
5. Hakan Kardes, Abdullah Sevincer, Mehmet H. Gunes, and Murat Yuksel. Six degrees of separation among US researchers. In *IEEE/ACM SONAM*, pages 654–659, 2012.
6. Kakajan Komurov, M.H. Gunes, and Michael A. White. Fine-scale dissection of functional protein network organization by statistical network analysis. *PLoS ONE*, 4(6):e6017, 2009.
7. Dniel Kondor, Mrton Psfai, Istvn Csabai, and Gbor Vattay. Do the rich get richer? An empirical analysis of the bitcoin transaction network. *PLoS ONE*, 9(2):e86197, 02 2014.
8. Bingdong Li, Esra Erdin, Mehmet H. Gunes, George Bebis, and Todd Shipley. An overview of anonymity technology usage. *Computer Communications*, 36(12):1269 – 1283, 2013.
9. Jörg Menche, Angelo Valleriani, and Reinhard Lipowsky. Asymptotic properties of degree-correlated scale-free networks. *Physical review E*, 81(4):046103, 2010.
10. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *White Paper*, 1(2):1–9, 2008.
11. Jeffrey Naruchitparames, Mehmet H. Gunes, and Sushil J. Louis. Friend recommendations in social networks using genetic algorithms and network topology. In *IEEE CEC*, pages 2207–2214, 2011.
12. Mark Newman. *Networks: An introduction*. Oxford University Press, Inc., New York, NY, USA, 2010.
13. Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. Structure and anonymity of the bitcoin transaction graph. *Future Internet*, 5(2):237–250, 2013.
14. M. Shoaib, M. Ilyas, and M. Sikandar Hayat Khiyal. Official digital currency. In *ICDIM*, pages 346–352, 2013.
15. Guoxun Tian and Mehmet H. Gunes. *Complex network analysis of ozone transport*, *Complex Networks*, page 87–96, 2014.