Term Project Summary

Introduction

Bitcoin was proposed by Satoshi Nakamoto in 2009 originally as the first decentralised, peer-to-peer digital currency. All transactions ever occurred over Bitcoin network are stored publicly in the blockchain. Users' identities are protected as encrypted digital wallets are used to store bitcoins and send payments. With the blockchain technology and cryptography, Bitcoin provides unprecedented privacy, security, and transparency.

Each transaction takes place between two bitcoin wallet addresses, one the sender, and the other the receiver. The bitcoin transaction network can be analysed in the simplest way where a digital wallet address is a node, and a transaction is a directed link between the sender and receiver nodes. In this analysis, we were interested in the most common properties of complex networks, such as degree distribution and average clustering coefficient. Besides, the timestamp of transactions are also recorded in blockchain, enabling study of the time evolution of and dynamical processes within the bitcoin network.

Methods

We extracted bitcoin addresses and transactions from the blockchain. The dataset was collected and pre-processed by a group at University of Illinois at Chicago. Then using relevant tools provided and the Python package NetworkX, the transaction data are reconstructed as a network and its properties analysed. Each bitcoin address becomes a node, and each transaction a directed link in the network. We adopted the standard definition of degree and clustering coefficient, and calculated these quantities in Python.

Results

The degree distribution was plotted separated for in degrees and out degrees. Both distributions were found to follow the power law. The best-fit exponents were -0.218 for in degrees, and -0.206 for out degrees.

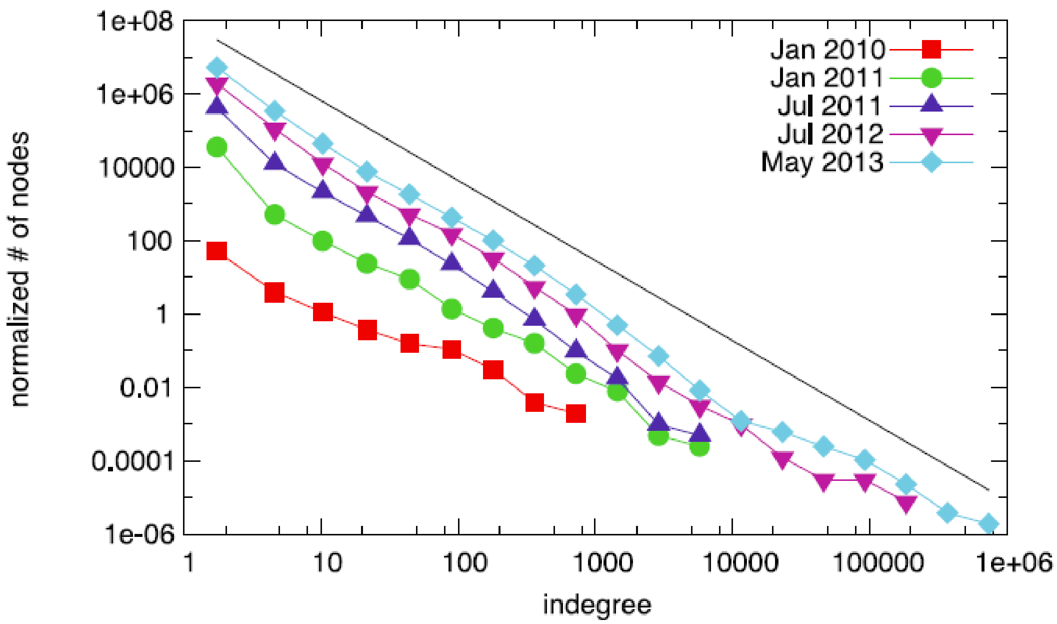


Fig 1: Time evolution of in-degree distribution. The curve quickly takes shape and didn't change much after 2011. The first year was impacted by the small user population and network size in both wallet addresses and transactions.

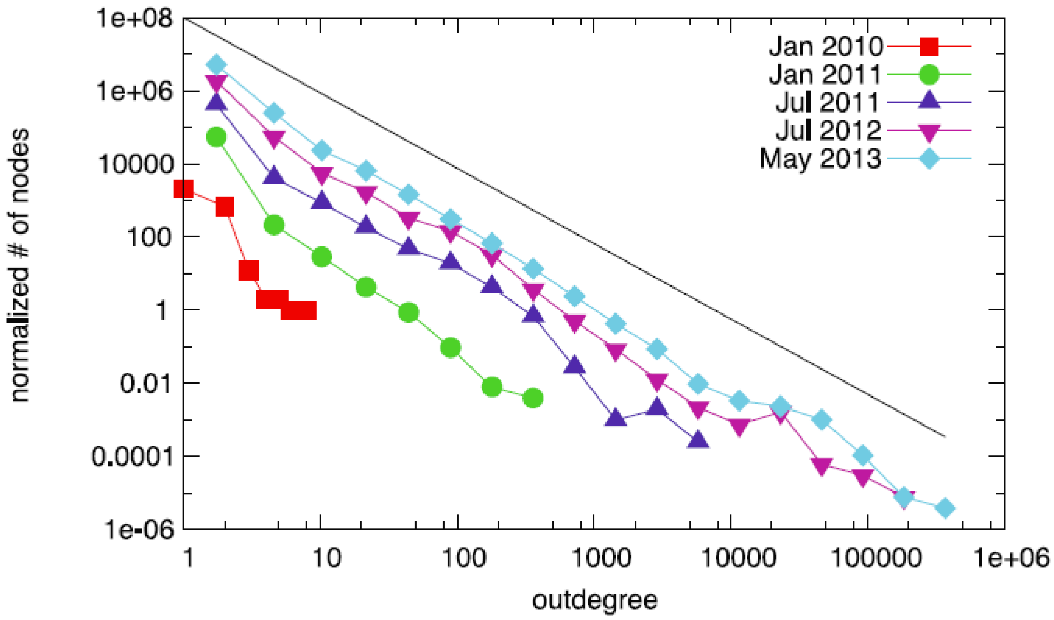
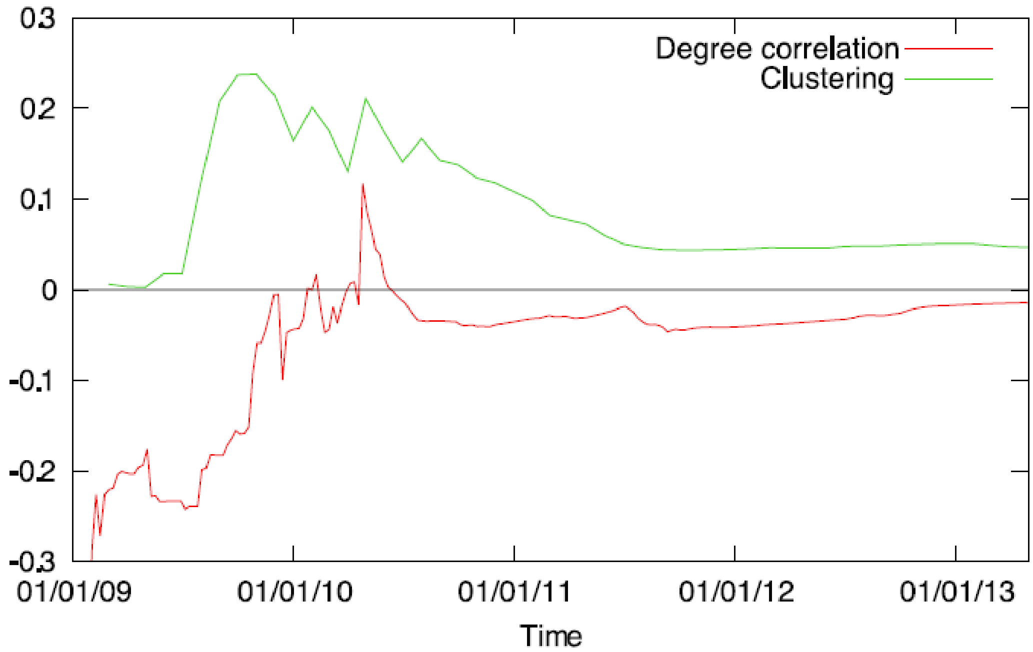


Fig 2: Time evolution of out-degree distribution. Same observations can be made as for the previous in-degree distribution.

We also analysed the degree correlation and clustering coefficient of this network, as plotted in Figure 3. Degree correlation is a measure of how nodes of similar degree are correlated, i.e. assortativity. The degree correlation mostly remained negative, indicating the network was disassortative. The average clustering coefficient peaked at 0.23 after one year and then approached a stationary value around 0.05, which was very close to that of a random network.



Conclusion

We clearly observed power law behaviour in the in and out degree distributions of bitcoin transaction network. The network is disassortative, i.e. there is no correlation between nodes of similar degree. The average clustering coefficient approaches a stable value around 0.05 over several years after launch. We also found that the giant connected component contains more than 99% of all nodes. The diameter of the network was about 14 and decreased with time as the network grew. In all aspects, the bitcoin transaction network can be effectively modelled by a random network model.

References

[1] NakamotoS (2008) Bitcoin: A peer-to-peer electronic cash system. Available: http://bitcoin.org/bitcoin.pdf.

[2] KondorD, PósfaiM, CsabaiI, VattayG (2014) Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. PLoSONE 9(2): e86197. doi:10.1371/journal.pone.0086197.

[3] B Holtz, J Fortuna, J Neff, Evolutionary Structural Analysis of the Bitcoin Network, 2013.

[4] A. Baumann, B. Fabian, M. Lischke, Exploring the Bitcoin Network, 10th International Conference on Web Information Systems and Technologies (WEBIST), 2014, doi:10.5220/0004937303690374.

[5] Dataset can be found at http://compbio.cs.uic.edu/data/bitcoin/