BDA 7570/4060 **CLASS NOTES - 2** SHARM76

Summary of **Uncovering the Bitcoin blockchain: an analysis of the full users graph** by **Damiano Di Francesco Maesa, Andrea Marino, Laura Ricci** published on **October 2016**

Introduction: With advancement of digital technology, every person is able to connect to every other person directly for information exchange. But so is not the case for financial exchange. Various cryptocurrencies were proposed earlier that can be used for online transactions but did not succeed due to lack of complete decentralization. But later, this direct exchange became possible with the commencement of Bitcoin Blockchain. In this paper, the authors take a deep insight to find the time-evolution of Bitcoin and also validate the conjecture ”rich gets richer” with respect to Bitcoin users. They also determined the most critical users/nodes in Bitcoin network using graph analysis. The main focus of study was transaction graph built using Bitcoin data. It is mentioned in the paper that all the previous work was done on data present till 2013 which had almost 10 million transactions but a huge jump in the number of transactions was seen after that which took the total number to more than a 100 Million. The authors used this data in their experiment.

Methodology

1) All inputs in multiple input transactions are considered to belong to the same user.
2) Each address is nothing but a user’s alias.
3) p2pkh, p2pk and p2sh types of scripts were taken into consideration. Rest were ignored.
4) Graph G is the group of clusters where each cluster(contains all addresses that belong to the same user) represents a user.

Data retrieved:

1) Connectivity of nodes in the graph over time.
2) Centrality of nodes.
3) Richness of nodes over time.

Implementation

The implementation includes the following steps:

1) Publicly available Blockchain data is used to build the graph.
2) A directed transaction graph is built using the data parsed in Step 1.
3) Clustering statistics are used to find the critical nodes/users in the network.

Results

Through this paper, the authors were able to prove the following: the increase in number of nodes in the network over time, increase in out-degree of nodes which means transactions increased over time, increase in the number of nodes in strongly connected component, cluster frequency is inversely proportional to its size, most critical node Mt. Gox was identified which was handling almost 70% of transactions in 2013-2014, conjecture ”rich-gets-richer” was validated to be true in Bitcoin network.