



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Implications of Dissemination Strategies on the Security of Distributed Ledgers

Luca Serena, Gabriele D'Angelo, Stefano  
Ferretti

# Dissemination Protocols



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Dissemination protocols = Algorithms to spread the information within a peer to peer system

There are several strategies that can be applied, depending on the features required. The features that one can be interested to optimize are:

- **Coverage**, that is the percentage of the nodes that receive the message.
- **Efficiency**, it is often desirable to minimize the network traffic
- **Anonymity**, in certain systems it is desirable to hide the real identity of the sender of a transaction

# Gossip Protocols



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

- Fixed Probability
- Probabilistic Broadcast
- Dandelion
- Dandelion ++

# Dandelion

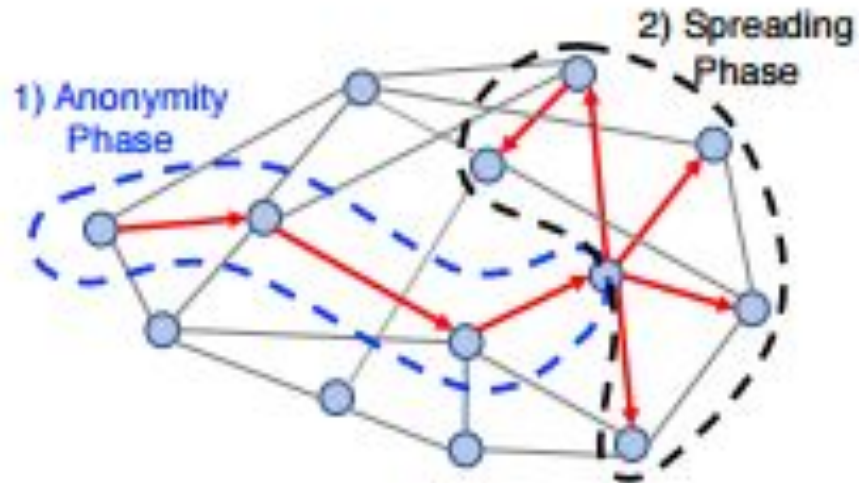


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Dandelion consists of two phases:

**Stem phase** = the message is sent to just one neighbor that is selected at random

**Fluff phase** = the message is broadcasted, all the neighbors receive it



# Dandelion ++



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Based on Dandelion but with some improvements:

- Greater guarantees against deanonymization attacks
- A fail-safe mechanism improves the security against Denial of Service attacks

Dandelion ++ is currently used by **Zcoin** and **Monero**



# LUNES-blockchain



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Lunes-blockchain is a discrete events simulator that is able to reproduce the behaviour of a Bitcoin-based blockchain and to simulate certain attacks on the system. It consists of three phases that are executed separately:

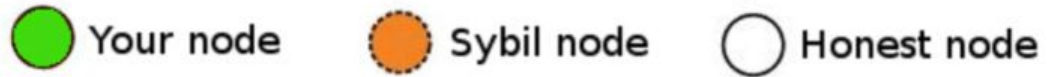
- Network Creation
- Simulation Execution
- Attacks Evaluation

# Sybil Attack

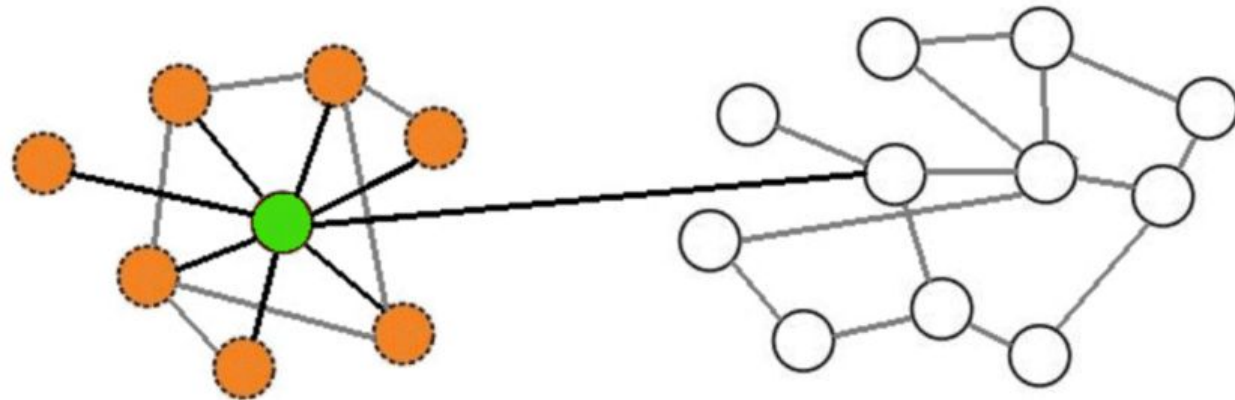


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

The Sybil Attack is a type of Denial of Service attack where an attacker creates a large number of pseudonymous identities and uses them to gain a disproportionately large influence.



In our case  
the attacker  
will not relay  
the transactions  
of a certain node.



# Setup and Methodology



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

In order to evaluate the influence of the attack, the execution is repeated 99 times, each time with an increasing percentage of malicious nodes.

The malicious nodes are chosen at random among all the nodes and the results of each run are an average of some hundred executions, in which the identity of the victim is always changed.

The graphs are populated by 10000 nodes, the coverage is given by the percentage of honest nodes who received the message by the victim.

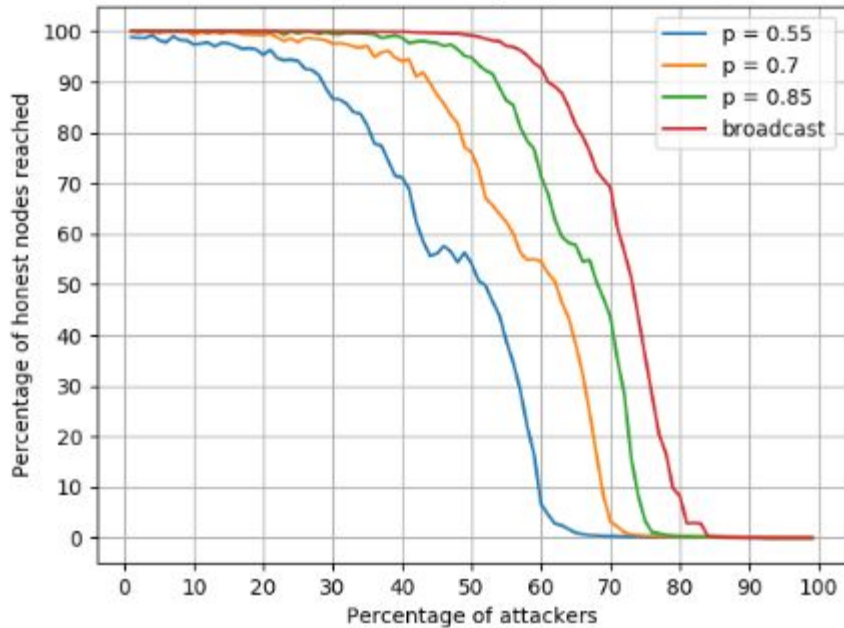


# Tests on Probabilistic Broadcast

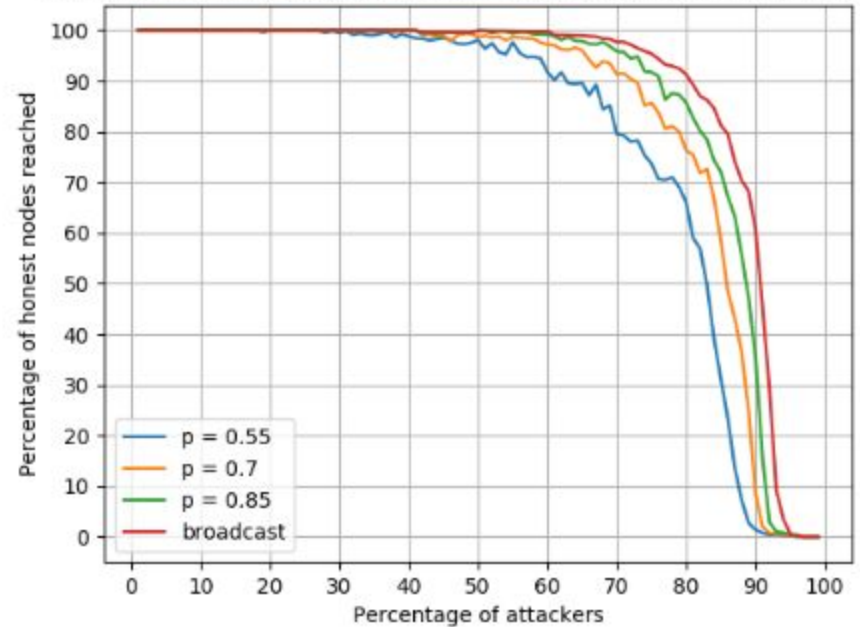


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Probabilistic Broadcast, Random Graph (10000 nodes, 40000 edges)



Probabilistic Broadcast, Random Graph (10000 nodes, 80000 edges)

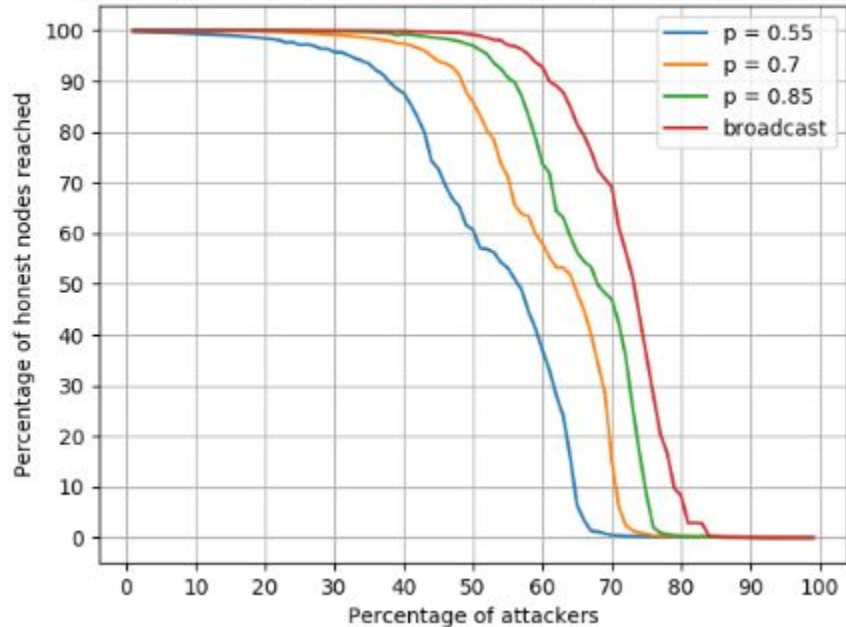


# Tests on Fixed Probability

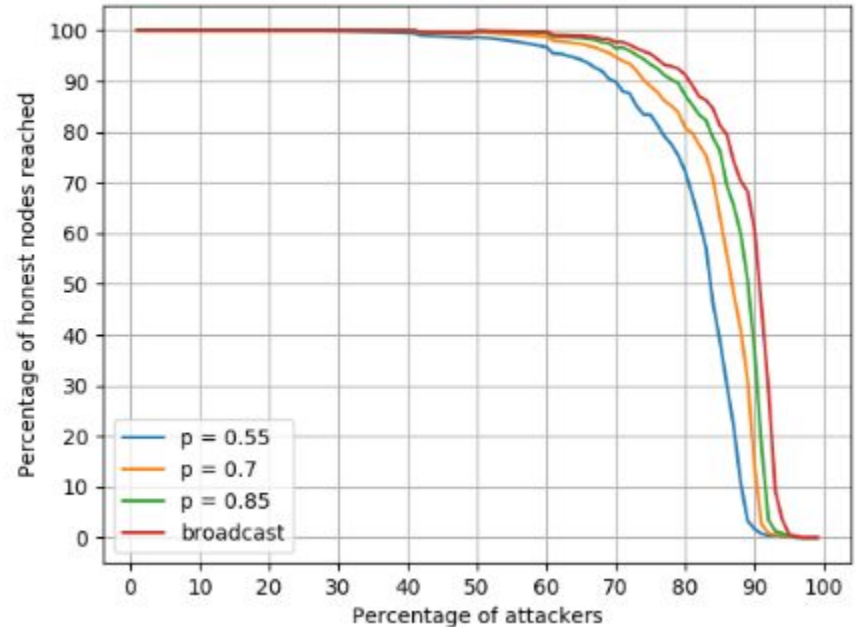


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Fixed Probability, Random Graph (10000 nodes, 40000 edges)



Fixed Probability, Random Graph (10000 nodes, 80000 edges)

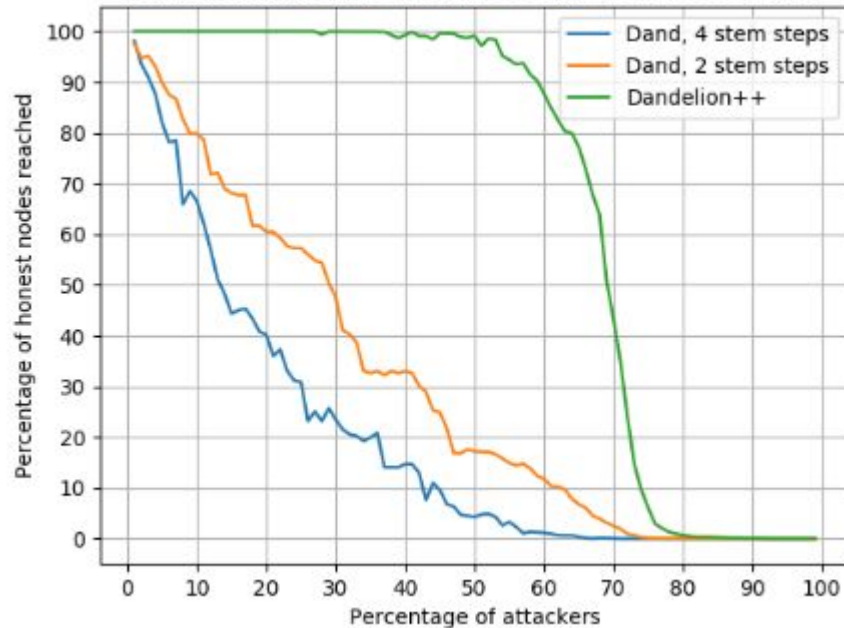


# Tests on Dandelion

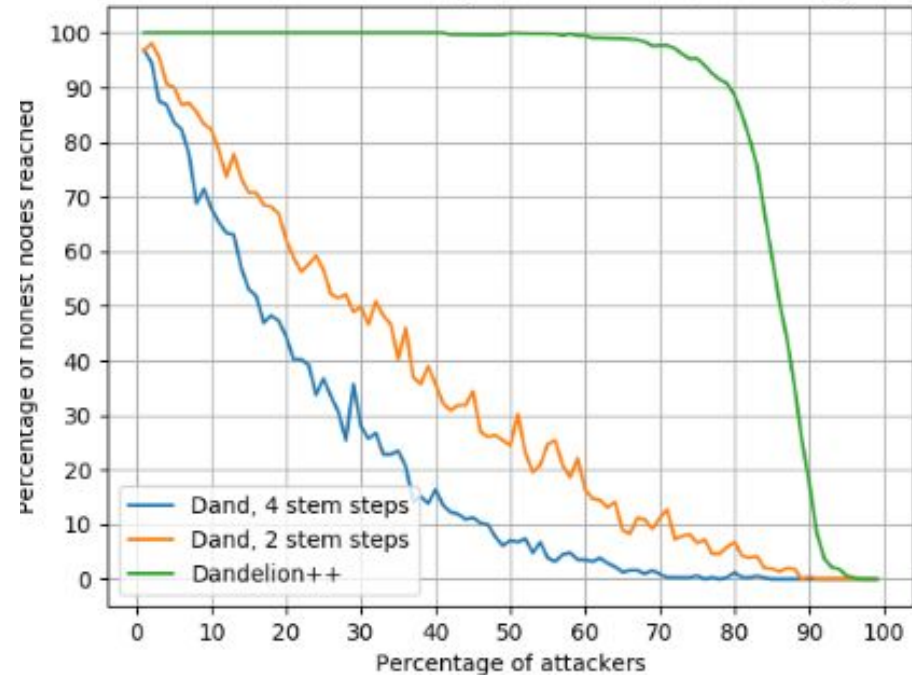


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Dandelion, Random Graph (10000 nodes, 40000 edges)



Dandelion, Random Graph (10000 nodes, 80000 edges)

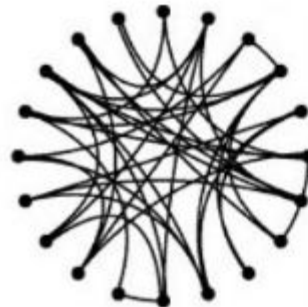


# Tests on Small World topology

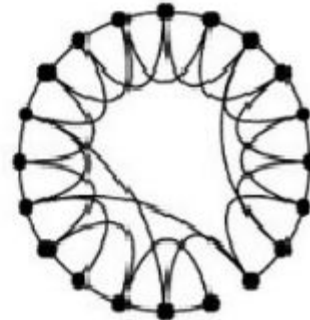


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

The previous tests were made on random graphs. The tests were then repeated on a small world graph, to check if the topology of the network could influence the results, but it turned out that no significant change could be noticed.



Random graph



Small-world graph

# Conclusions



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

- The average degree of the nodes plays an important role for resisting to Sybil attacks
- Dandelion is easily vulnerable to Sybil attacks, but Dandelion++ gives the same level of resilience as pure broadcast
- In all the tested network configurations, with Probabilistic Broadcast and Fixed Probability having 40% or lower of malicious nodes does not compromise the system



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# DiLeNA: Distributed Ledger Network Analyzer

Luca Serena, Gabriele D'Angelo, Stefano  
Ferretti

# Graphs



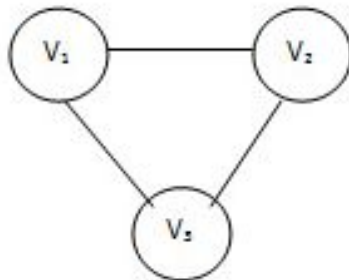
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

A graph consists of a set of nodes and edges (links between two nodes).

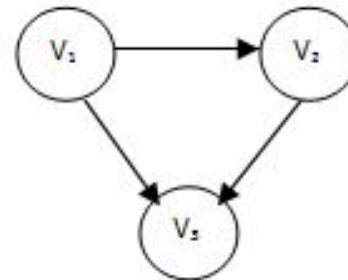
A graph can have multiple meanings, for example nodes can be entities and the edges can represent interactions between two entities.

Graphs can either be directed or undirected.

**Undirected Graph**



**Directed Graph**



# Metrics on the graphs



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

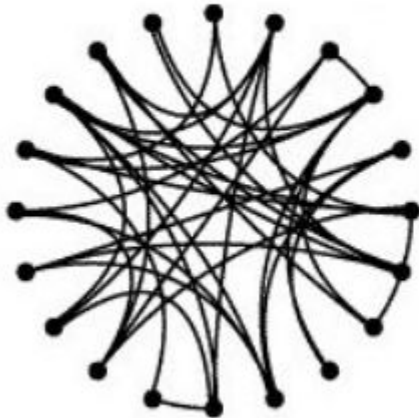
- **Degree Distribution**, it indicates which is the percentage of nodes having a certain number of connections. In directed graphs one can refer to in-degree, out-degree or total degree.
- **Average shortest path length**, it indicates the average shortest path between any two couples of nodes. Shortest paths can be computed with Dykstra algorithm
- **Average clustering coefficient**, that is the average of the clustering coefficients of all the nodes. The clustering coefficient of a node is the fraction that indicates how many edges between his neighbors exist among all the possible ones.



# Graphs Topologies



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA



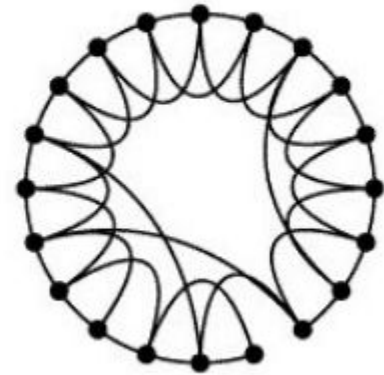
Random graph



Scale-free graph



K-regular graph



Small world graph

# Erdos - Renyi Model



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Erdos Renyi Model is the most used technique to generate a random graph of a given size.

There are two variants of the algorithm:

1. The user inserts the number of nodes and edges to be created.
2. The user inserts the number of nodes and the probability that there is a connection between two nodes.

# Small World Graph



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Small world graphs are a graph topology where most of the nodes are not connected to each other, but most of the vertices can be reached by other nodes through a short number of hops.

To investigate if a graph has small world properties, it is necessary to make a comparison with a random graph of the same size.

The analyzed graph must have:

- A similar or minor average shortest path length compared to the random graph
- A significantly higher average clustering coefficient

# DILENA



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

DILENA is a software tool for the analysis of the graphs based on networks' transactions. It is structured in two parts:

- Graph Generator: the transactions of a certain blockchain referring to a specified period of time are downloaded and the corresponding directed graph is created.
- Graph Analyzer: some metrics are calculated on the graph, in order to determine whether it has small world properties or it doesn't.

# Setup and Methodologies



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Blockchains analyzed: **Bitcoin** and **Ethereum**



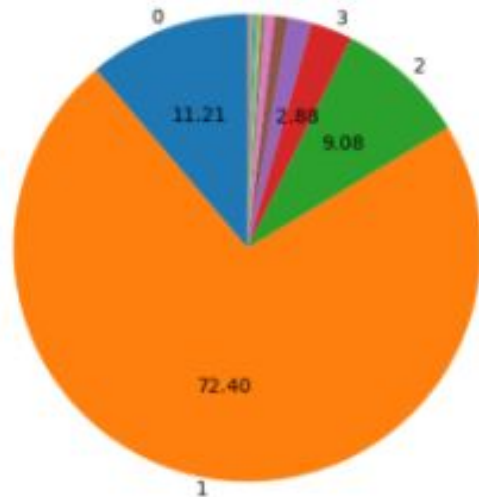
**bitcoin** ethereum

Period of time considered: december 2010 for Bitcoin, December 2016 for Ethereum. The aim was to analyze a full month in the second year of life of the cryptocurrencies.

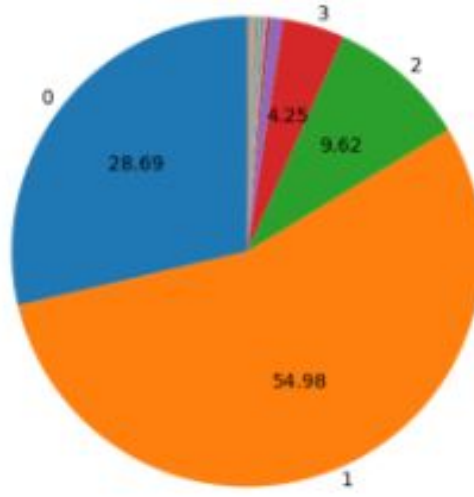
# Ethereum Degree Distribution



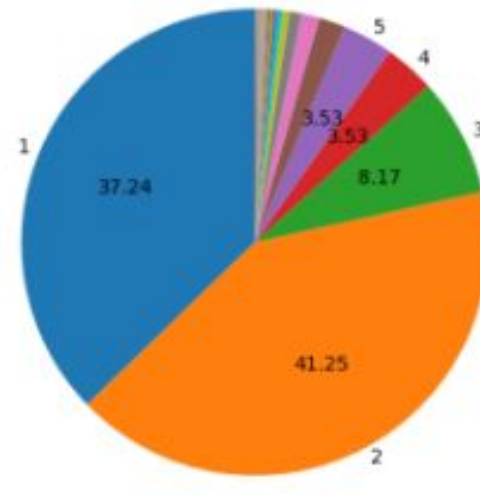
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA



(a) Ethereum in degree distribution



(b) Ethereum out degree distribution



(c) Ethereum total degree distribution



The node with the highest degree showed an amount of connections with almost the 10% of the node set.

Around 10 nodes with a degree higher than 2000



# Metrics on Ethereum

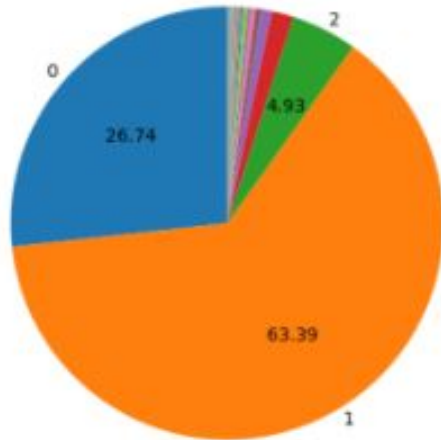
<b>Graph</b>	<b>Graph ACC</b>	<b>Main Component ASPL</b>	<b>Main Component ACC</b>
<i>Ethereum</i>	0.02099	1.4256	0.02134
<i>Random</i>	0.000014	10.3584	0.000015

- The ratio of the average clustering coefficient between the Ethereum and the random generated graph is 1469 
- The ratio of the average shortest path length between the Ethereum and the random generated graph is 0.14 

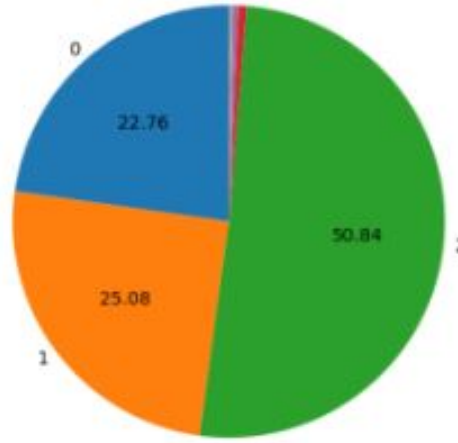
# Bitcoin Degree Distribution



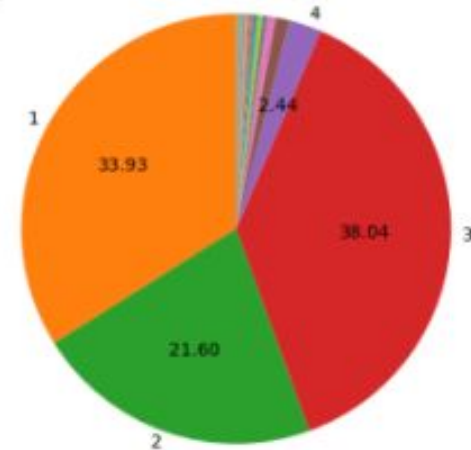
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA



(a) Bitcoin in degree distribution



(b) Bitcoin out degree distribution



(c) Bitcoin total degree distribution

Almost 1/2 of the nodes has either 0 in-degree or 0 out-degree



Few nodes with a very high degree, acting as hubs of the network



# Metrics on Bitcoin



Graph	Graph ACC	Main Component ASPL	Main Component ACC
<i>Bitcoin</i>	0.0235	190.4879	0.024
<i>Random</i>	0.000026	6.461	0.000029

- The ratio of the average clustering coefficient between Bitcoin and the random generated graph is 828 
- The ratio of the average shortest path length between Bitcoin and the random generated graph is 29.5 

# Possible Extensions to DILENA



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

- Analyze other distributed ledgers



- Increase the level of parallelization

# Conclusions



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

Ethereum transactions graph has small world properties, while the Bitcoin's one has not.

## WHY?

- Presence of smart contract in Ethereum (many interactions among groups of users are performed through smart contracts, that thus become common network neighbors to all these users).
- Consistent presence of anonymous accounts.