Graph Analysis of Blockchain P2P Overlays and Their Security Implications

Aristodemos Paphitis, Nicolas Kourtellis, Michael Sirivianos

am.paphitis@edu.cut.ac.cy

Cyprus University of Technology

Telefónica Research

Motivation

Blockchains supporting critical infrastructure

A large number of people could be affected

Network defines the level of security and resilience

Need to characterize the network

Aim

Gain resilience insights through network analysis

Diameter - Density ?

Scale – free, small – world ?

Assortativity & Clustering ?

How do they compare to the Web, Internet-AS, Online Social Networks?

Selected networks

Well known, established cryptocurrencies.
Frequently listed in top50 by CoinMarketCap

Bitcoin

BitcoinCash

DASH

Dogecoin

Ethereum

Litecoin

ZCash

Graph Metrics

Avg. Shortest Path

smaller => More robust

Network Diameter

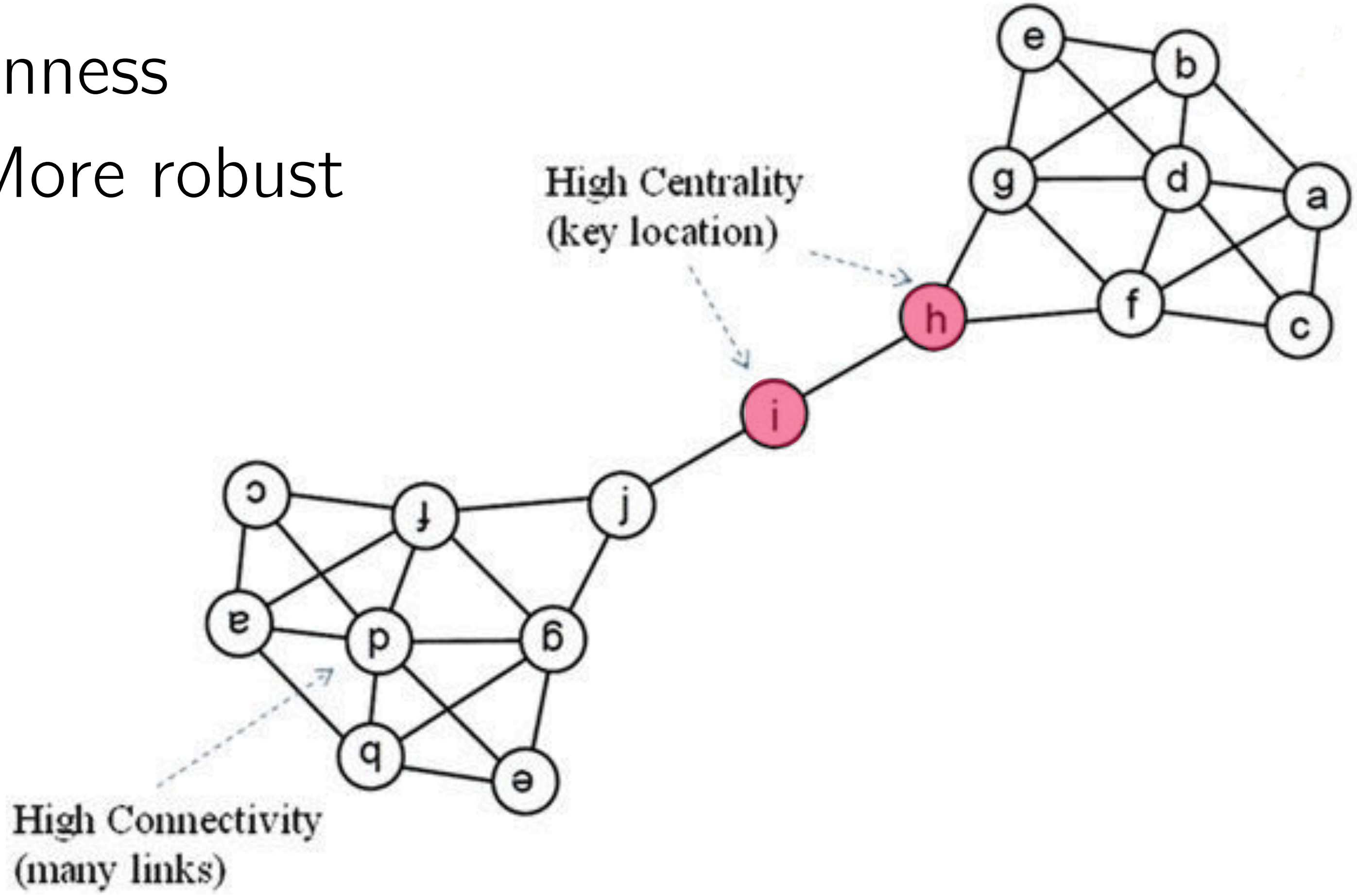
the longest shortest-path

smaller => More robust

Graph Metrics

Avg. Node Betweenness

smaller => More robust

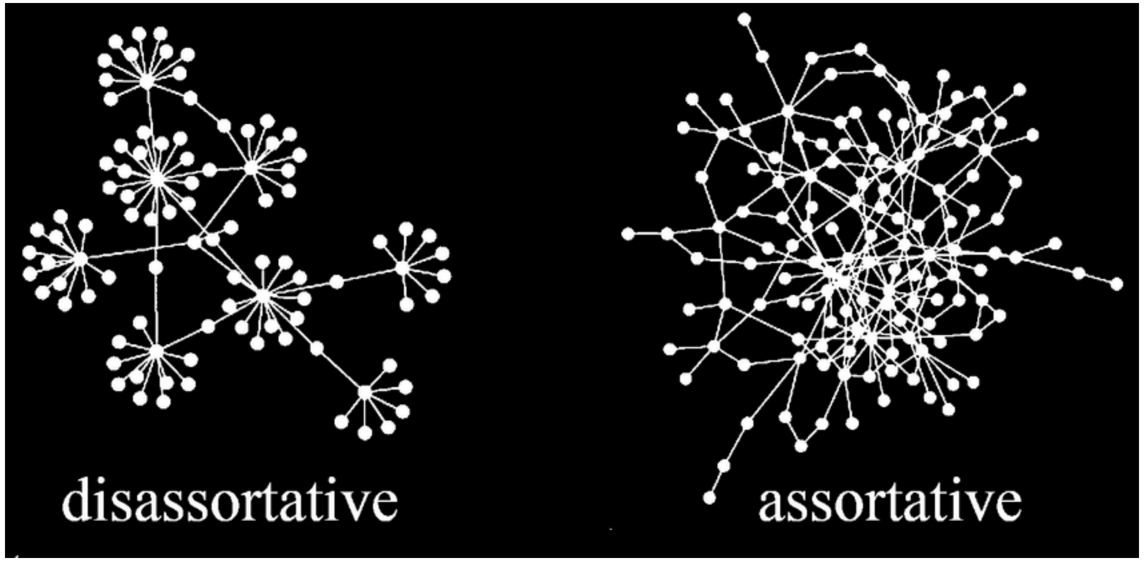


Graph Metrics

Assortativity

high-degree nodes connect to high-degree and low-degree to low-degree

disassortative networks => Less robust



Graph Metrics

Clustering

higher clustering => More robust

Graph Metrics

Diameter	Avg. Shortest Path	Avg. Node Betweenness	Assortativity	Clustering
↓	↓	↓	↑	↑

Imply higher resilience

Data collection methodology

Gather all known addresses for each reachable peer in the network

Construct **connectivity graphs** that contain ALL POSSIBLE links

Same as "*Paphitis, A., Kourtellis, N., Sirivianos, M. (2023). Resilience of Blockchain Overlay Networks. In: Network and System Security. NSS 2023. Lecture Notes in Computer Science, vol 13983. Springer, Cham.*"

Limitations

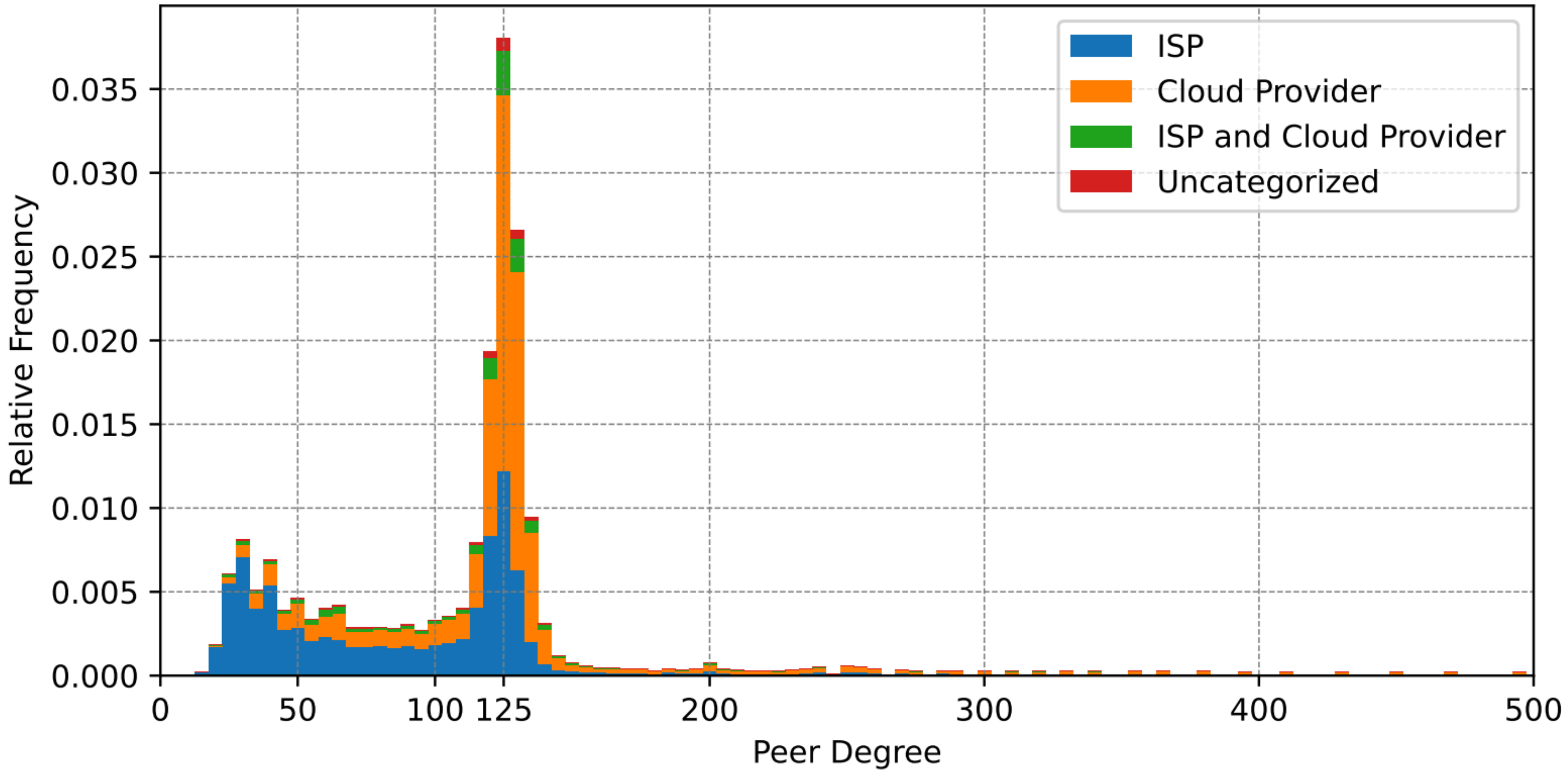
Connectivity Graphs => High number of false edges

[9] Booker, L.B.: The effects of observation errors on the attack vulnerability of complex networks

[60] Wang, D.J., Shi, X., McFarland, D.A., Leskovec, J.: Measurement error in network data: a re-classification.

Compare Connectivity Graph with real network

[32] Estimating the Peer Degree of Reachable Peers in the Bitcoin P2P Network

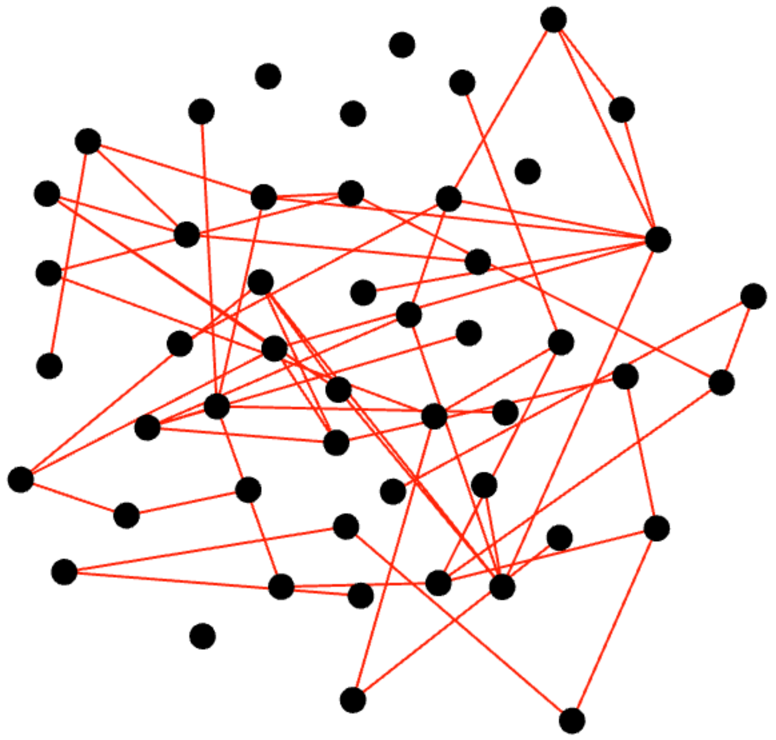


32. Grundmann, M., Baumstark, M., Hartenstein, H.: On the peer degree distribution of the bitcoin p2p network. 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) pp. 1–5 (2022)

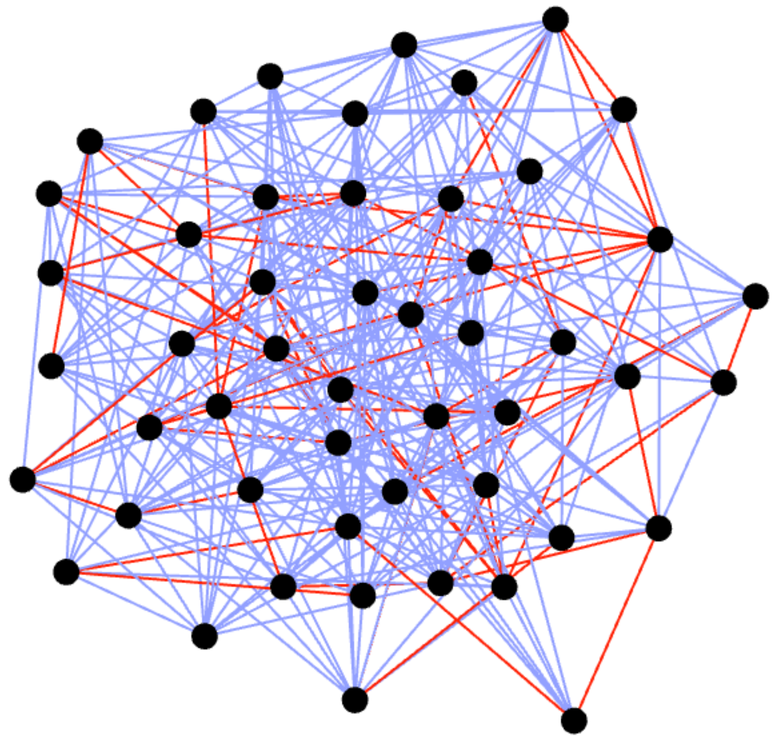
G_{real} => the real graph

G_{obs} => connectivity graph, reconstructed from our data collection

$\mathrm{G}_{\mathrm{real}}$



$\mathrm{G}_{\mathrm{obs}}$

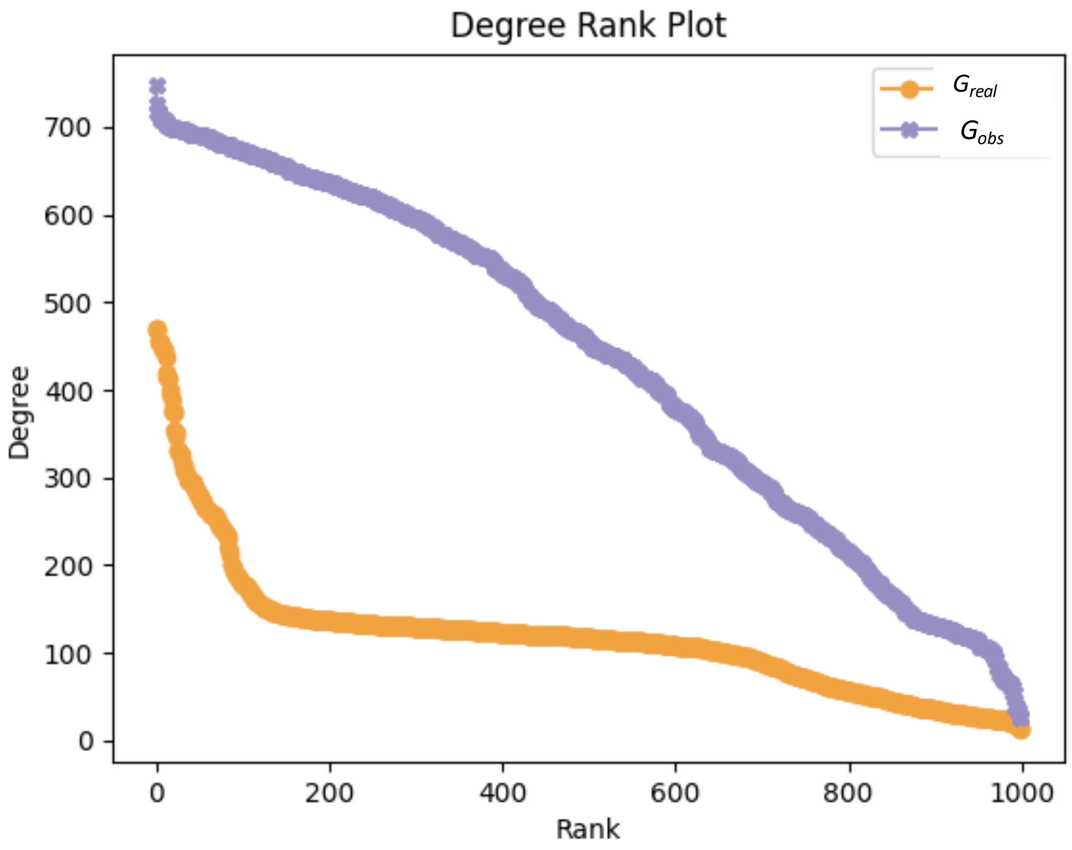


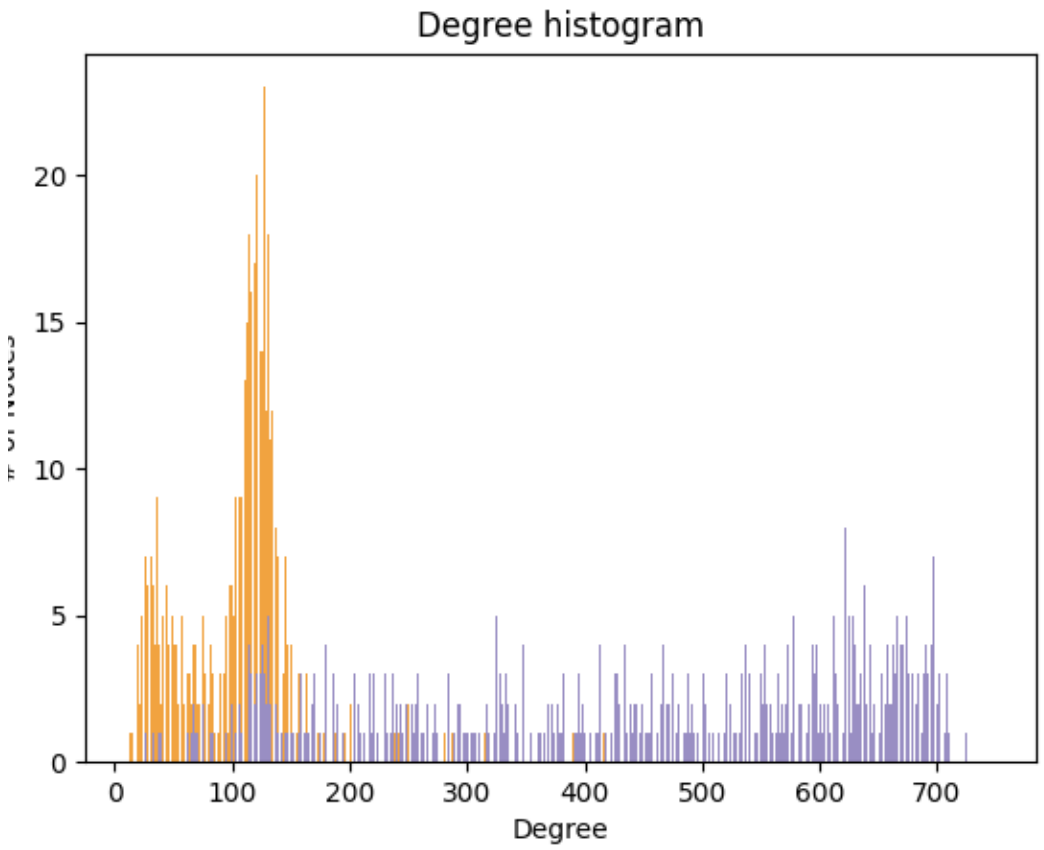
N = 1000

Sample random graphs for example purposes.
NOT Real graphs

G_{real} => the real graph

G_{obs} => connectivity graph, reconstructed from our data collection





Comparing Connectivity Graph with real network

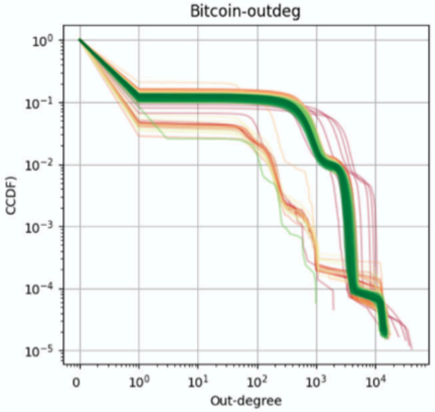
	Avg. Shortest Path	Avg. Degree	Clustering	Assortativity	Avg. Betweenness
G_{real}	1.89	115	0.21	-0.02	**448**
G_{obs}	1.56	**438**	**0.63**	0.07	280

Average of 20x runs.
Consistent results – insignificant variance between runs

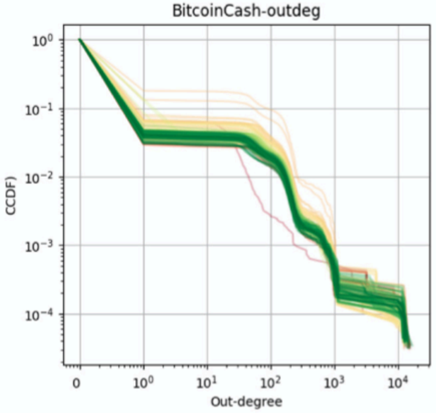
Graph Metrics

	Diameter	Avg. Shortest Path	Avg. Node Betweenness	Assortativity	Clustering
	↓	↓	↓	↑	↑
Bitcoin	↓	↓	↑	→	
Bit.Cash	↓	↓	↑	↓	
Dash	↓	↓	↓		
Dogecoin	↓	↓	↓		↑
Ethereum	↓	↑	↓		↓
Litecoin	↓	↓	↓		
ZCash	↓	↓	↓	→	↑

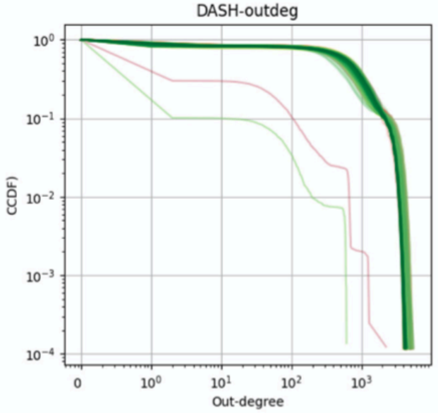
Degree Distribution



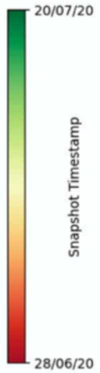
(a) Bitcoin



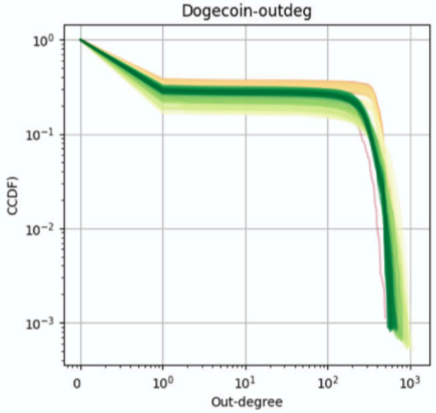
(b) Bitcoin Cash



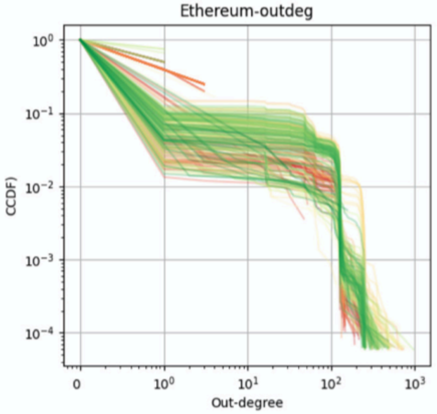
(c) Dash



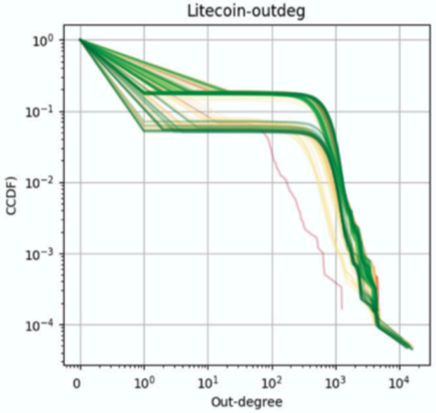
(d) Colorbar



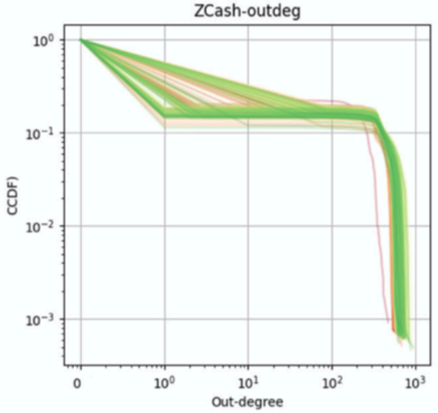
(e) Dogecoin



(f) Ethereum

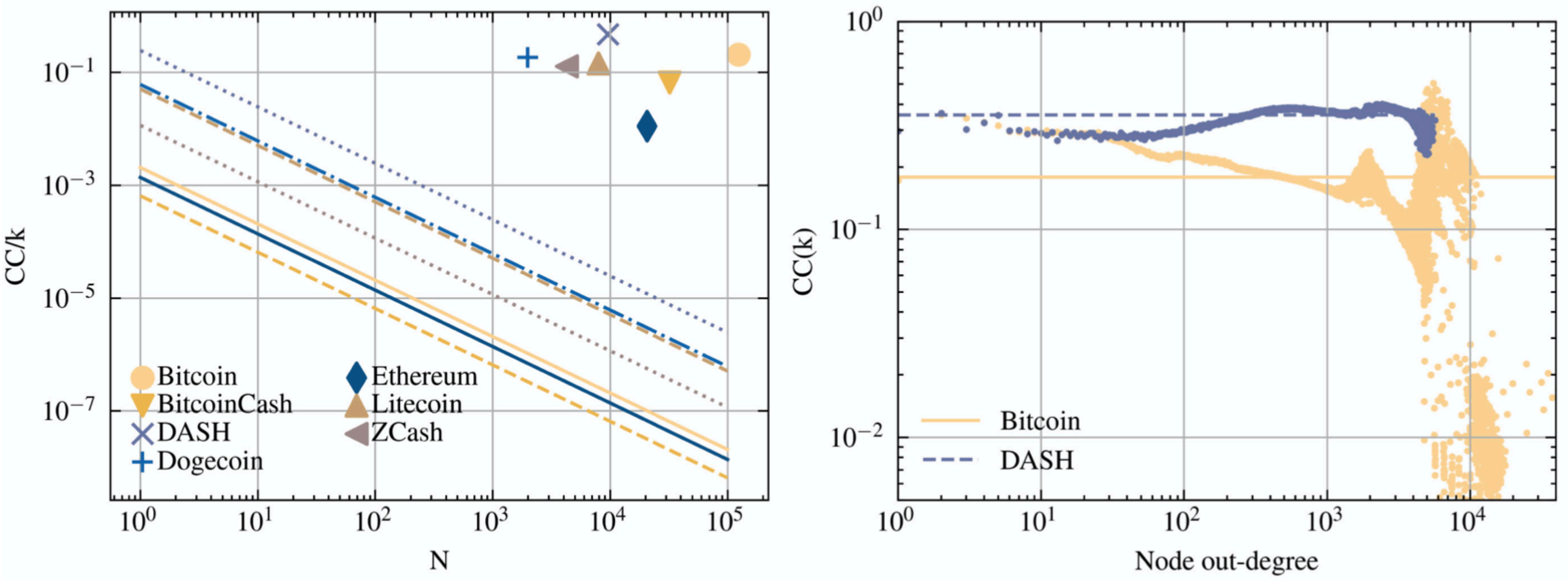


(g) Litecoin



(h) ZCash

Clustering



CC/k
N
Bitcoin
BitcoinCash
DASH
Dogecoin
Ethereum
Litecoin
ZCash
CC(k)
Node out-degree
Bitcoin
DASH

Presence of Unreachable Peers

Table 4. Presence and median in-degree of unreachable peers in each overlay.

Network	% of unreachable nodes	Median in-degree
Ethereum	98%	4
BitcoinCash	96%	3
Bitcoin	88%	3
Litecoin	86%	**75**
ZCash	84%	4
Dogecoin	73%	**68**
DASH	18%	**984**

Results

Blockchain P2P networks are:

- Highly dynamic
- Not scale-free but deg. distr. are exponential
- Not small-world
- Most have neutral assortativity
- Not random characteristics
- BTC & BCH very high betweenness -> less resilient

Conclusions

Characteristics of *less resilient* structures

Increased vulnerability to targeted attacks

Blockchain nets. are dissimilar (Despite sharing same protocols)

Very dynamic

Different from random networks

Dissimilar to known nets. => New models are required