Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

21 maggio 2026

La rete P2P di Bitcoin è sconosciuta *by design*: i nodi *raggiungibili*[1] della rete sono noti, ma se fra due nodi u e v esiste o meno un arco è noto solo ai nodi u e v. Cercare di capire se sia possibile progettare delle tecniche che rivelino la topologia della rete P2P di Bitcoin è un'area di ricerca attualmente attiva (si vedano per esempio, [3, 1, 2]).

Al contrario della rete P2P di Bitcoin, la rete dei canali Lightning è nota. Ogni nodo è identificato da una chiave pubblica; i canali (gli archi) devono essere noti affinché un nodo u, che debba effettuare un pagamento a un nodo v, possa cercare un cammino da u a v lungo il quale instradare il pagamento. Si osservi che la rete dei canali Lightning è in realtà un multigrafo, perché fra due nodi u e v potrebbe esserci più di un arco.

Il file `https://francescopasquale.it/pcd2526/pcd_lightning_snapshot_260521.zip` contiene uno *snapshot* della rete Lightning, così come era nota al nostro nodo Lightning il 21/05/2026. L'archivio compresso consiste in un fle json con la descrizione dei nodi e degli archi della rete, oltre a tutta una serie di informazioni.

Esercizio 1. Scrivere un programma che legga il file e calcoli il numero totale di nodi, il numero totale di archi e il numero di coppie di nodi fra le quali c'è più di un arco.

Esercizio 2. Scrivere un programma che legga il file, calcoli il numero di componenti connesse del (multi)grafo e il diametro della componente maggiore (quella con il maggior numero di nodi).

Riferimenti bibliografici

[1] Sergi Delgado-Segura, Surya Bakshi, Cristina Pérez-Solà, James Litton, Andrew Pachulski, Andrew Miller, and Bobby Bhattacharjee. Txprobe: Discovering bitcoin's network topology using orphan transactions. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, volume 11598 of *Lecture Notes in Computer Science*, pages 550–566, Frigate Bay, 2019. Springer. `http://fc19.ifca.ai/preproceedings/58-preproceedings.pdf`.

[2] Shaoyu Li, Shanghao Shi, Yang Xiao, Chaoyu Zhang, Y Thomas Hou, and Wenjing Lou. Bijack: Breaking bitcoin network with tcp vulnerabilities. In *European Symposium on Research in Computer Security*, pages 306–326. Springer, 2023. `https://shaoyu-li.github.io/files/bijack.pdf`.

[3] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*

[1] Indirizzi ip che rispondono al comando version

(UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, July 18-21, 2016, pages 358–367, Toulouse, 2016. IEEE Computer Society. https://philipp-andelfinger.net/pdfs/neudecker2016timing.pdf.