Proving Distributed Systems Correct using Refinement

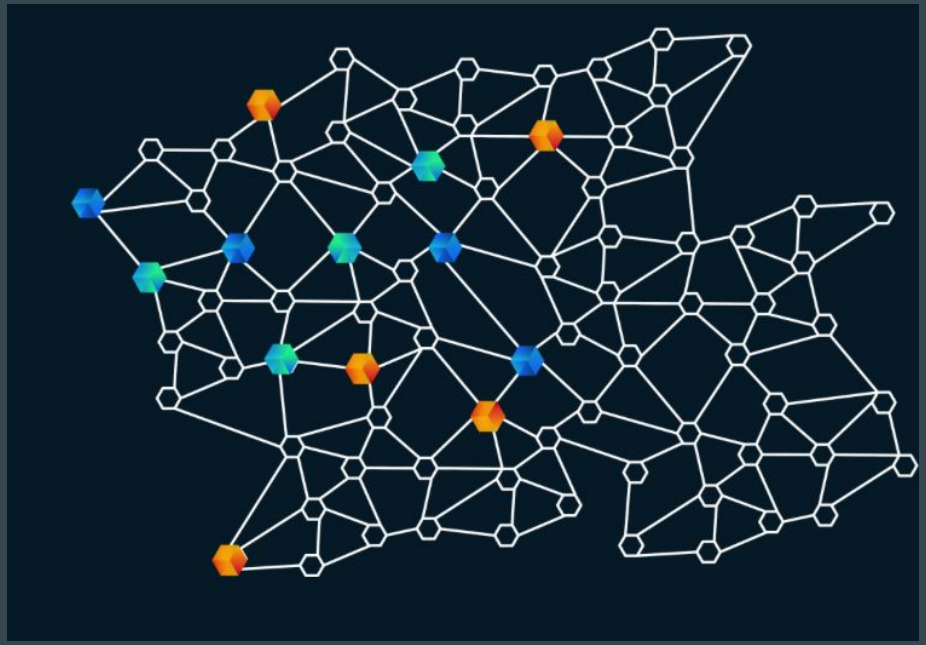
•••

Software Day 2023

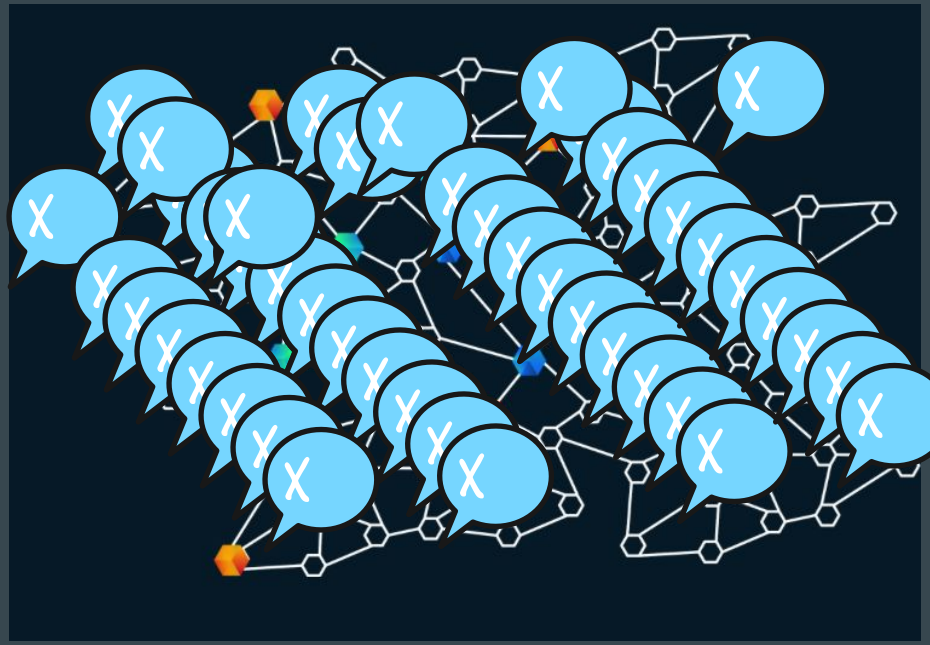
Ankit Kumar

Distributed Systems

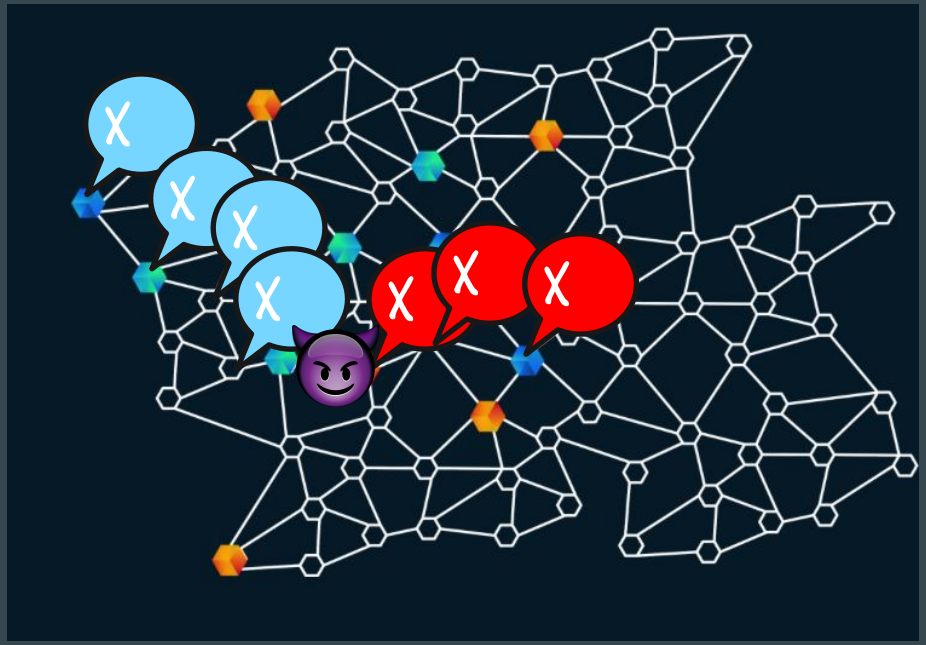
Peer-to-Peer Distributed Systems



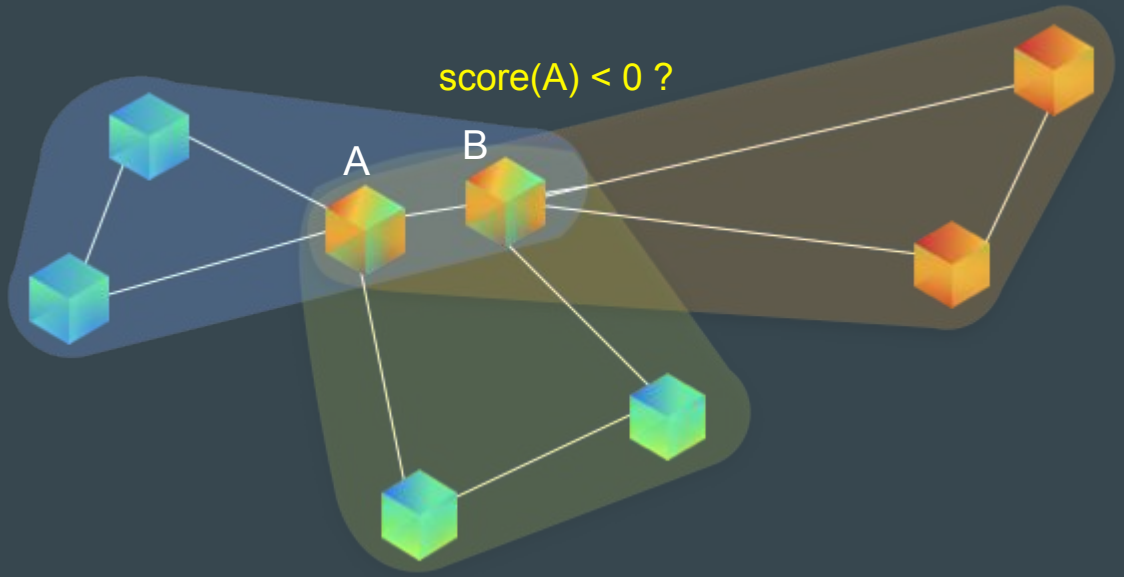
P2P Systems - Flooding



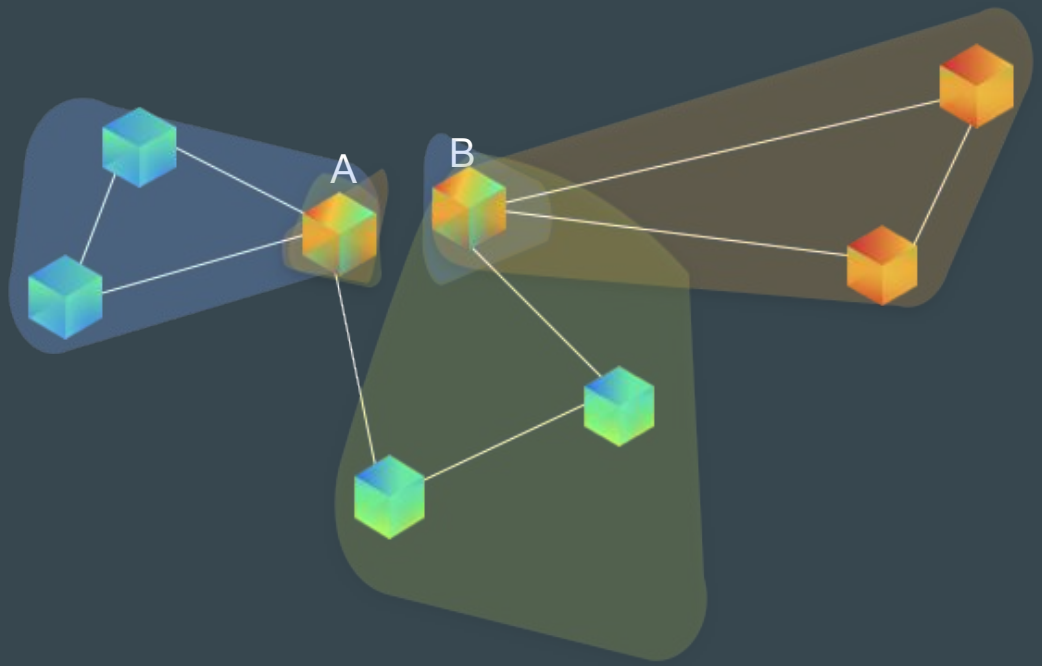
P2P - Gossip Protocols



GossipSub



GossipSub



Previous work (to appear at ACL2 workshop ‘23 and S&P ‘24)

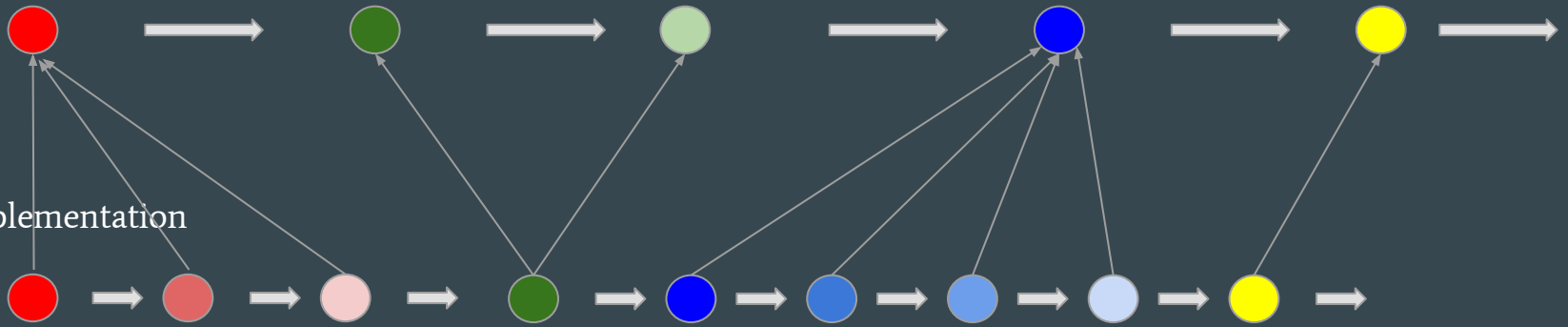
- A fully executable spec formalized in ACL2S
- Fine grained control over weights, parameters, events and messages
- Properties about the scoring function
- Verified properties for FileCoin and Eth2.0
- FileCoin satisfied all, while Eth2.0 satisfied only 2
- Generated an attack based on exposed vulnerabilities

- Verification of GossipSub in ACL2s (Won the best student paper award at ACL2 Workshop ‘23)
- Formal Model-Driven Analysis of Resilience of GossipSub to Attacks from Misbehaving Peers (S&P ‘24)

Ankit Kumar, Max von Hippel, Panagiotis Manolios Cristina Nita-Rotaru

Refinement

Specification



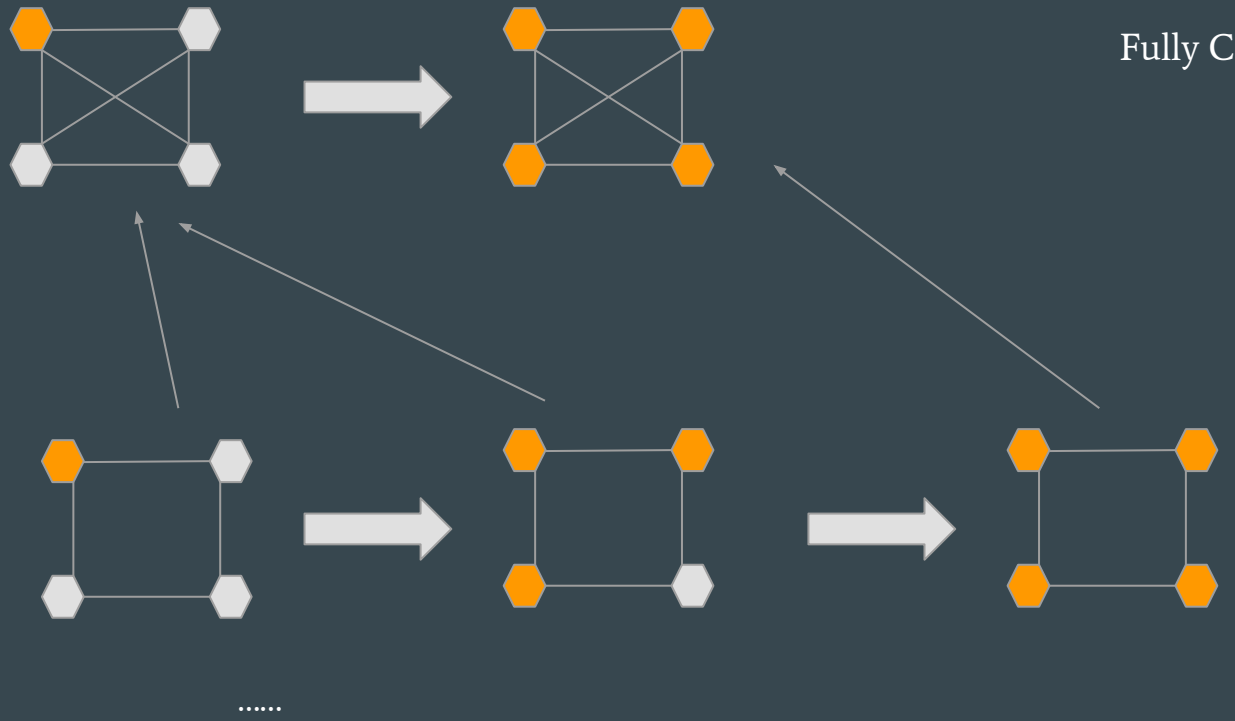
Implementation

Refinement

- Local reasoning using Well Founded Equivalence Bisimulation to show related infinite computations
- Composable
  - A refines B, and B refines C, then A refines C
- Mechanizable proofs

- Mechanical Verification of Reactive Systems - Panagiotis Manolios (2001)
- Refinement Maps for Efficient Verification of Processor Models
- Automatic verification of safety and liveness for pipelined machines using WEB refinement
  - Panagiotis Manolios, Sudarshan K. Srinivasan

Refinement applied to Distributed P2P Systems



Fully Connected Broadcast

Mesh PubSub
(Not fully Connected)

.....

Ideal GossipSub

Thank You