Stanford MS&E 339

Ashish Goel

Strategic formation of Credit Networks
Lecture Sketch
10/6/22

The Evolving Topology of the Lightning Network

Tension: All nodes establishing a relationship with a central hub is good for efficiency, but bad for robustness, decentralization, and anonymity

“The largest connected components for each of these snapshots account for almost the entire network, with only a few disconnected components mainly composed by single pairs. The number of nodes simultaneously on-line in our time snapshots grows from 518 (in February 2018) to 3613 (in January 2019), while the corresponding number of channels increases from 1910 to 23853. This determines a decreasing pattern in the density of the links present in the network, which is only 1.45% in February 2018 and reaches even lower values in January 2019 (about 0.37%). The LN has been evolving, therefore, from a fairy sparse initial configuration to even higher levels of sparsity along its short life. Interestingly, the degree distribution shows the tendency of the network to establish a few channels per node. The median degree, for instance, increases from a value of only 2 (in February 2018) to 3 (in January 2019) edges per node, while the corresponding average values move from about 7 to 12.5. This is an interesting aspect of the LN given its need to route transactions, but also given the vocation of the Bitcoin framework to be an uncentralized system”

From: Martinazzi and Flori (2020): https://doi.org/10.1371/journal.pone.0225966

Informal aside: Explanders and Erdos-Renyi graphs (also known as Bernoulli Random Graphs)

— G(N, p): N node network, where every pair of nodes has an edge with probability p (iid)

— If $p > (c_1 \log n)/n$ then the network is connected whp, if $p < (c_2 \log n)/n$, then the network is not connected whp, for suitable c_1 and c_2

— When the network is connected, the expected shortest path between two nodes is small, and the number of edges that go out of any large subset of nodes is proportional to the size of the subset (i.e. the network is an expander)

— Expanders have high liquidity (i.e. success probability) when edge capacities are the same or similar

— So the problem with the lightning network is not the number of edges, but the skew in the capacity so that there are a small number of large hubs

Nash Equilibria

Consider N participants (agents), each of which can decide how much to trust each of the other participants

Assume that agent a_j has a strategy space S_j which is the space of all feasible trust vectors for this agent. Each trust vector or "strategy" comes with some cost for the agent

Given a network topology G with initial credit values, there is some benefit $U_j(G)$ that this agent receives

Nash Equilibrium: A strategy for each agent such that no agent has an incentive to deviate

There is also some system welfare W(G) that gets generated, which may just be the sum of the individual utilities

Desiderata: The Nash Equilibrium should lead to high system welfare.

Hands On Exercise for modeling strategic behavior in lightning or credit networks — 15 minutes to discuss, 2 minutes to report for each group

Divide into groups of 4-6

Come up with the model of cost and benefit for each participant

Come up with the model of welfare

See if you can analyze this for a small network (say 4 identically minded agents)

One Example Model

(The assumptions are only to understand strategic network formation — once the network is formed, the actual behavior may differ)

Assume that a_j has a trust budget B_j and let $c_{j,k}$ denote the initial trust capacity from a_j to a_k established by a_j

Assume further a_j is only allowed to transact directly (i.e. no multi-hop transactions allowed), and only with a small number of nodes (given by the set T_j)

Assume that the transaction rate from a_j to a_k is given to us, denoted $R_{j,k}$

Assume $R_{j,k} = R_{k,j}$

Assume that the utility of an agent is given by the probability of successful transactions, i.e. $U_j = \sum_k R_{j,k}(1- 1/(c_{j,k} + c_{k,j} + 1))$

Analyzing the Simple Model

A (complete) Potential Game

The Potential happens to be the same as the sum of the utilities !

Hence, nash Equilibrium is easy to calculate, and the “Price of anarchy” is 1

All Nash Equilibria are cycle reachable

Great network structure, despite the model being flawed

—

A More Realistic Model

Agent a_j carries a risk r_j of default, known to everyone

Nash equilibria tend to result in hubs: everyone should just trust the least risky node, which is not a great network topology

Mechanism Design: Design the rules of the game (e.g. The lightning protocol) such that rational self-interested users act in a way that leads to a healthy network

First Project Problem (also needs a definition of what a “healthy” network is)

Stable coins

A digital currency whose value is pegged to a Fiat currency

Four potential types:

— Trust us (not really used)

— Partial or Complete Reserve in a fiat currency; acquire more reserve to guarantee backing as more currency is issued; the provider of the stablecoin does direct redemptions and sales (e.g. Tether)

— Risks: inadequate collateral can cause runs, but also result in inflated value

— Partial or Complete Reserve in baskets of other cryoto-assets

— Value maintained by automatic burning or issuing of the underlying basket of crypto-assets, sometimes a single cryptocurrency issued by the same entity