Payment Routing in Lightning Networks.

Contact: Binh-Minh Bui-Xuan <buixuan@lip6.fr>
Maria Potop-Butucaru <maria.potop-butucaru@lip6.fr>

Venue: NPA and APR research teams (Networks and Performance Analysis – Algorithms, Programs and Resolution), LIP6 SU UPMC, Paris, France.

Keywords: algorithm, graph mining, temporal data.

1. Context:
Blockchain overlaying is the study of graph structures stemming from secured, online, transactions between pairs. The latter operations can be modelled by weighted and timed edges as follows. A (temporal and temporary) $\omega$-weighted edge is declared between two vertices $u$ and $v$ whenever they both trust each other and plan to perform several future transactions, to a maximum amount of $\omega$ currency units. Then, every transaction of $\delta \leq \omega$ currency units between $u$ and $v$ will decrement the edge’s weight by $\delta$, until it reaches zero. When an edge’s weight reaches zero, the edge is deleted. Besides, isolated vertices can be deleted, whereas new vertices can be dynamically introduced. The global graph arising from this model is called a lightning network. A lightning network is a particular case of a temporal graph, which consists in a vibrant research topic currently in full extension [1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13].

2. Internship research proposal:
In classical graph theory, ShortestPath asks for the computation of a path joining two given vertices with the least number of edges in a (static) graph. It can be solved by popular polynomial time algorithms such as Dijkstra, Bellman-Ford, Floyd-Warshall, and so on, see e.g. [5]. We refer to PaymentRouting the problem of routing transactions between distant vertices (from source $s$ to target $t$) through intermediary vertices in a lightning network, formally defined as follows.

A temporal weighted graph is a collection of triples of the form $(\mu, \omega, uv)$, where $\mu \in \mathbb{N}$ represents a time moment, $\omega \in \mathbb{N}$ is a weight, and $u \neq v$ are distinct vertices. Given a transaction amount $\delta$, along with two timestamped source-target vertices "$s$ at moment $\mu_s$" and "$t$ at moment $\mu_t$", PaymentRouting asks for the computation of a list

$$P = [(\mu_1, v_1v_2), (\mu_2, v_2v_3), \ldots, (\mu_{p-1}, v_{p-1}v_p)]$$

with $v_1 = s$, $\mu_1 = \mu_s$, $v_p = t$, and $\mu_{p-1} = \mu_t$, such that the route is realizable. The most common realizability criteria is timely monotone: $\mu_1 \leq \mu_2 \leq \ldots \leq \mu_{p-1}$, and $(\mu_i, \omega_i, v_iv_{i+1})$ belongs to the lightning network with $\delta \leq \omega_i$ for every $1 \leq i < p$. It is proved that topological sorting helps in extending popular ShortestPath algorithms to solve PaymentRouting when under timely monotone constraint in polynomial time on temporal graphs [2], hence, on lightning networks too. During the internship, we are interested in giving the answer to the following questions.

Main questions: Are there linear solutions to PaymentRouting on lightning networks? If precomputed information can be stored in the lightning network vertices (called hub-labelling), are there sublinear solutions to PaymentRouting?

The work will encompass both theoretical research and the confrontation of algorithms to real world graph data.
References


