Secure and reliable lightning networks for blockchains

Mots clés : Array
- Directeur de thèse : Maria Potop-Butucaru
- Co directeur de thèse : sara TUCCI PIÉRIOVANNI
- Co-encadrant(s) :
- Unité de recherche : Laboratoire d'informatique de Paris 6
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

Blockchain underlying overlays and the associate routing are totally unexplored from theoretical point of view. However, the performances of blockchains technologies heavily depend on the performances of the underlying routing process. Recently, Lightning technologies imposed themselves as a viable direction for improving the blockchains throughput. This technology builds on top of blockchains (e.g. Bitcoin) an overlay of secured channels opened by two parties involved in long term multi-transactions. This overlay is further used to route transactions. Designing resilient to churn self* overlays for both blockchains and Lightning technologies is more than timely.

Although blockchain technologies make strong assumptions on their underlying overlays there is no academic research that focus these overlays. The only prior research on the overlays topic has been developed in the context of dynamic networks such as P2P or wireless networks.

Another interesting point to be explored is the liveness of the overlay and more generally of the system. In blockchains the welfare of participants is a crucial factor. When participants desert the system in proof-of-work based blockchains the security of the system sinks which yields to the global sink of the system. This phenomenon is known in economy as the tragedy of commons.

The thesis targets algorithms that output overlays optimized for efficient routing in blockchains. The proposed solutions should be resilient to nodes churn, various attacks and abnormal dynamic behaviors and target to avoid the sink of the system. The challenge is to explore, the unexplored yet research direction concerning the construction of constant degree expenders tolerant to dynamic Byzantine behavior and multiple types of faults.

Another interesting challenge is to propose new formally verified routing protocols for blockchains. In order to increase the throughput in Bitcoin, the non academical research in blockchains proposed recently lightning routing networks.

Secured channels between two or more participants are opened on top of Bitcoin and transactions are routed on top of the virtual network formed by these channels.
Routing in lightning networks has some similarities with routing in P2P or mobile wireless networks or delay tolerant networks.

Flare, for example the most prominent lightning routing was inspired by the wireless ZRP routing. Interestingly, there is no academic research on this topic so far and our preliminary studies show that Flare presents severe limitations such as weak resilience to churn or deadlocks. Interestingly, none of these lightning routing protocols has been exposed to multiple types of faults, attacks or dynamic adversaries.

It should be noted that the most studied overlay for routing in classical distributed systems and networking theory is the minimum spanning tree (MST) and none of the existing algorithms is resilient to dynamic adversaries in conjunction with churn and attacks. The challenge is to design new routing algorithms optimized for the context of lightning networks subject to multiple types of faults, attacks and dynamic adversaries.