Blockchains as Mean Field Games

Co-Directeurs de thèse :
Idris Kharroubi (LPSM, Sorbonne Université) idris.kharroubi@upmc.fr
Maria Potop-Butucaru (LIP6, Sorbonne Université) maria.potop-butucaru@lip6.fr

Blockchain phenomena is similar to the last century gold rush. Blockchain technologies are publicized as being the technical solution for fully decentralizing activities that were for centuries centralized such as health, administration or banking. Therefore, prominent socio-economical actors all over the world are attracted and ready to invest in these technologies. Despite their large publicity blockchains are far from being a technology ready to be used in critical economical applications and scientists multiply their effort in warning about the risks of using this technology before understanding and fully mastering it. Interestingly, many recent attempts to alarm on vulnerabilities of popular blockchains like Bitcoin are target of defenders brigading.

The impact of blockchain crosses different disciplines. The first application of this technology is the Bitcoin protocol which the homonym cryptocurrency is based upon [1]. The main drawback of Bitcoin and other similar blockchains is their limited scalability.

Recently, Lightning Networks [2] have been developed in order to solve this issue through private micro-payments. 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. As of today, Lightning Networks are used by more than 5.000 nodes, with more than 25.000 channels created.

The current literature on lightning networks proposes no mathematical model to explain and forecast various phenomena that happens in these networks. In a preliminary study [3] we used a wide range of models from non cooperative game theory in order to prove the safety of the protocol proposed in [2]. Our goal is to introduce more advanced models to understand the behaviors of agents in lightning network.

The main challenge is to explore the recent field of mean field games [4,5] which have been recently introduced in order to model non-cooperative games with large number of symmetric agents.

The first step is to identify the utilities of the agents such that they best represent their objective. The current literature considers centrality properties or other topological features, but there is no model for utilities as a function of the actual costs, i.e. fees, of the agents. Although they have the same set of strategies, their utilities can vary. Hence it is necessary to take into account this possible asymmetry in the framework of mean field games. A possible solution to this problem maybe bayesian games or a more general definition of the game for large number of agents has to be given. Once a solution is computed, it is possible to translate it into a forecast of the expected topology of the network, to test this result and compare it with the existing lightning networks topologies.

Furthermore, we will focus on how various changes may impact the network. That is, given the network it is possible to understand how small changes, such as adding shortcuts, can affect its topology.

Another issue to be investigated is the analysis of attacks, such as for instance blocking a third-party node with a large amount of transactions, with possible ad hoc solutions, such as loopback links. Indeed, Byzantine behaviours can be modeled as a zero-sum game.

A further inquiry is understanding whether current protocols with constant fees are proper or not for lightning network. Introducing variable fees means adding a new degree of freedom to the model. Current theory of mean field games does not provide solutions if too general assumptions are given. Hence we would like to focus our research on expanding this area of game theory in order to identify the boundaries of all the possible protocols that can be implemented on lightning networks. Therefore it would be possible to create a protocol that induces a specific topology.

Finally, it should be noted that Lightning networks are an application of smart contracts(an important tool derived from blockchain). Our ultimate goal is to generalise the game theoretical framework derived from the mean field game model to study the impact of any smart contract on a large network.

Bibliography

[1] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
[2] Joseph Poon and Thaddeus Dryja. (2016). The Bitcoin lightning network: Scalable off-chain instant payments.
[3] Paolo Zappala and Maria Potop-Butucaru (2019). Game theoretical model for lightning networks (work in progress).
[4] Guéant O., Lasry JM., Lions PL. (2011). Mean Field Games and Applications. In: Paris-Princeton Lectures on Mathematical Finance 2010. Lecture Notes in Mathematics, vol 2003. Springer, Berlin, Heidelberg
[5] Cardaliaguet, Pierre. (2012). Notes on Mean Field Games.