Improving blockchain consensus protocol

Vincent Danos* Marc Lelarge†

January 6, 2018

A blockchain consensus protocol, like bitcoin's proof of work, does two things: it ensures that the next block in a blockchain is the one and only version of the truth, and it keeps powerful adversaries from derailing the system and successfully forking the chain.

In proof of work, miners compete to add the next block (a set of transactions) in the chain by racing to solve an extremely difficult cryptographic puzzle. The first to solve the puzzle, wins the lottery. As a reward for his or her efforts, the miner receives some newly minted bitcoins and a small transaction fee.

In this project, we will propose a probabilistic model for the mining mechanism. Based on it, we will explore the impact of information propagation on possible blockchain forks as empirically observed in Ref. [1]. Then, we will see how gossip algorithms can improve communication in the network while being robust to strategic miners [2, 3].

References

[1] Christian Decker and Roger Wattenhofer. *Information propagation in the bitcoin network.* Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, 2013.

[2] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. *The economics of Bitcoin mining, or Bitcoin in the presence of adversaries.* Proceedings of WEIS. Vol. 2013. 2013.

[3] Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta. *The blockchain folk theorem.* Toulouse School of Economics, TSE-817, May 2017.

*vincent.danos@ens.fr
†marc.lelarge@ens.fr