Cryptocurrencies in Systems with Decentralized Trust

Recently, the idea of trust assumptions was explored in completely new way. All this started as cryptocurrency systems [7, 8] proposed to encompass users who do not necessarily hold the same assumptions of who to trust.

Indeed, conventional data-replication services are based on *quorums* [6, 9], subsets of system participants matching two important conditions: in every run of the system, *every* two quorums should have at least one benign participant in common and *some* quorum should only contain benign participant. It is assumed that the participants share the global knowledge about the quorum system. Under this assumption, a rich variety of important distributed abstractions can be implemented.

Recently proposals [7,8] reconsidered this global assumption with a more realistic gist: based on its local knowledge, a participant might have its own idea about which subsets of other participants are trustworthy and which are not. However, the proposed systems lacked formal specifications and it was unclear what kind of service guarantees there were able to provide.

A few recent articles [2,3,10] proposed alternative (and sometimes contradicting each other) formalizations of *federated* or *decentralized* quorum systems and explored their power in implementing Byzantine reliable broadcast [1] and solving consensus.

The goal of this project is to explore the potential of building asynchronous asset transfer sysems [4, 5], also known as *cryptocurrencies* in federated quorum systems.

Location

Located in the Paris area, Télécom Paris (formerly known as ENST or École nationale supérieure des télécommunications) is one of the top French public institutions of higher education and research (Grandes Écoles), a founding member of Institut Polytechnique Paris. In collaboration with httph://epfl.ch, it has established Institut Eurécom at Sophia-Antipolis.

Contact

Prof. Petr Kuznetsov
`https://perso.telecom-paris.fr/kuznetso/`
`petr.kuznetsov@telecom-paris.fr`
INFRES, Télécom Paris, Institut Polytechnique Paris

References

[1] G. Bracha and S. Toueg. Asynchronous Consensus and Broadcast Protocols. *JACM*, 32(4), 1985.

[2] C. Cachin and B. Tackmann. Asymmetric distributed trust. In *OPODIS*, 2019.

[3] Á. García-Pérez and A. Gotsman. Federated byzantine quorum systems. In *22nd International Conference on Principles of Distributed Systems, OPODIS 2018, December 17-19, 2018, Hong Kong, China*, pages 17:1–17:16, 2018.

[4] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. AT2: asynchronous trustworthy transfers. *CoRR*, abs/1812.10844, 2018.

[5] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D.-A. Seredinschi. The consensus number of a cryptocurrency. In *PODC*, 2019. `https://arxiv.org/abs/1906.05574`.

[6] D. Malkhi and M. Reiter. Byzantine quorum systems. *Distributed Computing*, 11?(?):203–213, 1998.

[7] D. Mazieres. The stellar consensus protocol: A federated model for internet-level consensus, 2016.

[8] D. Schwartz, N. Youngs, and A. Britto. The ripple protocol consensus algorithm, 2018.

[9] M. Vukolic. The origin of quorum systems. *Bulletin of the EATCS*, 101:125–147, 2010.

[10] Álvaro García-Pérez and M. A. Schett. Deconstructing stellar consensus. In *OPODIS*, 2019.