“Collective Coin Flipping” is a CSPRNG (cryptographically secure pseudo-random number generator) model, first described in an eponymous paper back in 1985. The goal of the paper was to come up with a method to perform collective coin flipping which is only slightly biased despite the presence of adversaries.

The authors first noted that this problem was considered before, mostly in the field of the Byzantine Generals Problem research, and that all past solutions were based on the assumption that information

may be communicated so that only some of the parties can read it (usually achieved by using cryptography). However, the authors’ idea was to completely avoid such assumptions, i.e. to deal only with games of complete information. They analyzed several Boolean functions on which every variable has only a small influence, as a way to achieve the goal in such an open environment.

Original paper: http://www.cs.huji.ac.il/~nati/PAPERS/coll_coin_fl.pdf

I’ve stumbled upon this work a few times already, and AFAIK Polkadot is considering using it, too. I wonder if anyone has looked into it? @JustinDrake or @vbuterin, maybe?

I’ve skimmed through several papers that iterate upon this work and these two might be worth mentioning:

1. “Random Selection with an Adversarial Majority” (link); describes the first protocols that solve the random selection problem in the presence of a dishonest majority in the full-information model (the model introduced by the original paper).

2. “Lower Bounds for Leader Election and Collective Coin-Flipping in the Perfect Information Model”

(link); defines lower bounds (in terms of number of rounds and number of bits per round) for any n-player coin-flipping protocol that is resilient against corrupt coalitions of linear size.