Garay et al [GKL15] (in synchronous networks) and Pass et al [PSS16] (also in networks with adversarial bounded delays) show that Nakamoto's protocol achieves chain quality close to

$$1 - \frac{\rho}{1 - \rho}$$

when the mining hardness parameter is appropiately set, and thus the above-mentioned block withholding attack is optimal.