We are further interested on the fairness aspects of the rewarding mechanism in Tendermint blockchains. In [3], Garay *et al.* define the notion of chain-quality as the proportion of block mined by honest miners in any given window; and the authors study the conditions where the ratio of blocks in the chain that were mined by malicious players over the total block in a given window is bounded. Kiayias *et al.* in [6] proposes Ourobouros, a Proof-of-Stake protocol, where they also analyse the chain-quality property. Pass *et al.* address in [7] one of the vulnerabilities of Bitcoin studied formally in Eyal and Sirer [2]. In [2] the authors prove that if the adversary controls a coalition of miners holding even a minority fraction of the computational power, this coalition can gain twice its share. Fruitchain proposed in [7] overcomes this problem by ensuring that no coalition controlling less than a majority of the computing power can gain more than a factor $1+3\delta$ by not respecting the protocol, where δ is a parameter of the protocol, and Fruitchain also provides a mechanism where miners are rewarded more often than in Bitcoin. In [1], Eyal analyses the consequences of attacks in system where pools of miners can infiltrate each other, and shows that in such a system, there is an equilibrium where all pools earn less than if there were no attack. In [4], Guerraoui and Wang study the effect of the delay of message propagation in Bitcoin, and show that in a system of two miners, a miner can take advantage of the delay and be reward exponentially more that its expectation. In [5], Gürcan *et al.* study the fairness from the point of view of the processes that do not participate to the mining; the authors provide the following condition needed to satisfy the fairness for users who do not participate to the mining process: $C(\phi) < 1/(1 - P(\phi))$, where $C(\phi)$ is the cost of waiting a transaction with fee ϕ to be confirmed, and $P(\phi)$ is the probability for a block with fee ϕ to be confirmed.

We study the fairness in open systems, where the number of processes in the system may be infinite, to express the fact that processes can enter and leave. To do so, we define the fairness of a protocol by the fairness of its *selection mechanism* and its *reward mechanism*, where the selection mechanism selects the process that will participate to provide a given block, and the reward mechanism is how the rewards are given to processes that participate in appending a new block. In this work, we study the reward mechanism, and in which condition that mechanism for a certain class of Blockchain protocol can be fair.

References

[1] Ittay Eyal. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, pages 89–103, 2015.

[2] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, pages 436–454, 2014.

[3] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 281–310, 2015.

[4] Rachid Guerraoui and Jingjing Wang. 2018.

[5] Önder Gürcan, Antonella Del Pozzo, and Sara Tucci Piergiovanni. On the bitcoin limitations to deliver fairness to users. In *On the Move to Meaningful Internet Systems. OTM 2017 Conferences - Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, October 23-27, 2017, Proceedings, Part I*, pages 589–606, 2017.

[6] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 357–388, 2017.

[7] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing, PODC 2017, Washington, DC, USA, July 25-27, 2017*, pages 315–324, 2017.