Abstracts

On Reward Sharing in Blockchain Mining Pools

Burak Can[1], Jens Leth Hougaard[2], and Mohsen Pourpouneh[2](✉)

[1] Department of Data Analytics and Digitalisation, Maastricht University, Maastricht, the Netherlands
b.can@maastrichtuniversity.nl

[2] Department of Food and Resource Economics (IFRO), University of Copenhagen, Copenhagen, Denmark
{jlh,mohsen}@ifro.ku.dk

Abstract. This paper provides, for the first time, a rich mathematical framework for *reward sharing schemes* in mining pools through an economic design perspective. We analyze and design schemes by proposing a comprehensive axiomatic approach. We depart from existing literature in various ways. First, our axiomatic framework is not on the consensus protocols but on the mining pools in any of these protocols. Second, our model is not restricted to a static single block, since various schemes in practice pay the miners repetitively over time in various blocks. Third, we propose reward sharing schemes and allocations not on the miners in a pool but instead on the shares submitted by these miners.

We demonstrate the flexibility of this space by formulating several desirable axioms for reward sharing schemes. The first condition ensures a *fixed total reward* that the fee charged by the pool manager is the same for any two rounds in a history. The second condition, *ordinality*, requires that time-shifts should not affect the reward distribution, so long as the order of shares is preserved. The third condition, *budget limit*, requires the pool manager to charge a nonnegative fee. The fourth condition, *round based rewards*, requires that the distribution of the rewards in a round only depends on that round. Finally, we introduce two axioms concerning fairness, *absolute redistribution* and *relative redistribution*, which demonstrates how the rewards should be redistributed when the round is extended by an additional share. We show that, together with other axioms, each of these fairness axioms, characterize two distinct classes of reward sharing schemes. Thereafter, we characterize the generalized class of proportional reward schemes, i.e., k-pseudo proportional schemes, which satisfy both of these axioms simultaneously. We introduce a final condition, *strict positivity*, which guarantees positive rewards for all shares, for any history. Imposing this additional condition single outs the well-known proportional reward scheme. The full article is available at: https://arxiv.org/abs/2107.05302.

Keywords: Blockchain · Fairness · Mining pools · Mechanism design

Can Gratefully Acknowledges Financial Support by the Netherlands Organisation for Scientific Research (NWO) Under the Grant with Project No. 451-13-017 (VENI, 2014) and Fonds National de la Recherche Luxembourg. Hougaard and Pourpouneh Gratefully acknowledge the Support by the Center for Blockchains and Electronic Markets Funded by the Carlsberg Foundation Under Grant No. CF18-1112

I. Caragiannis and K. A. Hansen (Eds.): SAGT 2021, LNCS 12885, p. 409, 2021.
https://doi.org/10.1007/978-3-030-85947-3

On Submodular Prophet Inequalities and Correlation Gap (Abstract)

Chandra Chekuri and Vasilis Livanos(✉)

University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

Abstract. We present a general framework for submodular prophet inequalities in the model introduced by Rubinstein and Singla [1], in which the objective function is a submodular function on the set of potential values instead of a linear one, via greedy Online Contention Resolution Schemes and correlation gaps. The framework builds upon the existing work of [1], yielding substantially improved constant factor competitive ratios for both monotone and general submodular functions, for various constraints beyond a single matroid constraint. As an additional improvement, it can be implemented in polynomial time for several classes of interesting constraints.

Along the way, we strengthen the notion of correlation gap for non-negative submodular functions introduced in [1], and provide a fine-grained variant of the standard correlation gap. For both cases, our bounds are cleaner and tighter. Furthermore, we present a refined analysis of the Measured Continuous Greedy algorithm for polytopes with small coordinates and general non-negative submodular functions, showing that, for these cases, it yields a bound that matches the bound of Continuous Greedy for the monotone case.

A full version of this paper is available at https://arxiv.org/abs/2107.03662.

Keywords: Combinatorial prophet inequality · Submodularity · OCRS

Reference

1. Rubinstein, A., Singla, S.: Combinatorial prophet inequalities. In: Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM (2017), pp. 1671–1687. longer ArXiv version is at http://arxiv.org/abs/1611.00665

I. Caragiannis and K. A. Hansen (Eds.): SAGT 2021, LNCS 12885, p. 410, 2021.
https://doi.org/10.1007/978-3-030-85947-3

Vote Delegation and Misbehavior

Hans Gersbach, Akaki Mamageishvili, and Manvir Schneider(✉)

CER-ETH, ETH Zürich, Zürichbergstr. 18, 8092 Zürich, Switzerland
{hgersbach,amamageishvili,manvirschneider}@ethz.ch

In this paper we study vote delegation and compare it with conventional voting. Typical examples for vote delegation are validation or governance tasks on blockchains and liquid democracy. Specifically, we study vote delegation with well-behaving and misbehaving agents under three assumptions. First, voting is costly for well-behaving agents. That means, if a well-behaving individual abstains or delegates his/her vote, s/he is better off than with voting as long as his/her action does not affect the voting outcome. Second, the minority—composed of misbehaving voters—always votes. The rationale is that this minority is composed of determined agents who have either a strong desire to disrupt the functioning of the system, or to derive utility from expressing their minority view. Third, the preferences of agents are assumed to be private information. We evaluate vote delegation and conventional voting regarding the chance that well-behaving agents win.

Results: We provide three insights. First, if the number of misbehaving voters is high, both voting methods fail to deliver a positive outcome. Second, if the number of misbehaving voters is moderate, conventional voting delivers a positive outcome, while vote delegation fails with probability one. Third, with numerical simulations, we show that if the number of misbehaving voters is low, delegation delivers a positive outcome with a higher probability than conventional voting. Formally, we find that for any cost of voting c, there are thresholds $f^*(c)$ and $n^*(f)$ such that for any number of misbehaving voters f above f^* and an expected number of well-behaving agents above n^*, misbehaving voters will have the majority of votes and will win.

Our results have immediate implications for blockchains, i.e. they infer that vote delegation should only be allowed if it is guaranteed that the absolute number of misbehaving agents is below a certain threshold. Otherwise, vote delegation increases the risk for negative outcomes. Our results can also help assess the performance of vote delegation in democracy, a form of democracy known as "liquid democracy". Indeed, for a liquid democracy, our result is the worst-case result when delegating agents cannot trust those to whom they delegate. In the context of liquid democracy, we can view misbehaving voters as a determined minority who will vote no matter the costs. Well-behaving agents are a majority and balance costs of voting and impact on the outcome. Our result implies that if the size of the determined minority is not too small, vote delegation can lower the likelihood that the majority wins.

A Full Version of the Paper Can Be Found at https://arxiv.org/abs/2102.08823.
Partly Supported by the Zurich Information Security and Privacy Center (ZISC)

I. Caragiannis and K. A. Hansen (Eds.): SAGT 2021, LNCS 12885, p. 411, 2021.
https://doi.org/10.1007/978-3-030-85947-3

Efficiency of Equilibria in Games with Random Payoffs

Matteo Quattropani(✉) and Marco Scarsini

Luiss, Viale Romania 32, 00197 Rome, Italy
{mquattropani,marco.scarsini}@luiss.it

We consider normal-form games with n players and two strategies for each player, where the payoffs are i.i.d. random variables with some distribution F. For each strategy profile, we consider the (random) average payoff of the players, called average social utility (ASU). Most of the literature on games with random payoffs deals with the number of pure (or mixed) equilibria and its dependence on the payoffs distribution. Here we consider a different issue, i.e., efficiency of equilibria.

We first show that the optimal ASU converges in probability to a deterministic value that can be characterized in terms of the large deviation rate of F. Then we move to examine the asymptotic ASU of the pure Nash equilibrium (PNE). We start by considering the case in which F has no atoms. In this case, it is well known that asymptotically the number of PNE has a Poisson distribution with mean 1. This implies that we typically do not have many equilibria. We show that, when equilibria exist, in the limit they all share the same ASU. We then consider the case in which F has some atoms. Amiet et al. [1] show that the presence of atoms in the distribution F dramatically changes the existence issue: in this case, with probability converging to 1 as the number of players grows to infinity, there will be exponentially many PNE. We show that in this case the ASU of the best and the worst pure equilibrium converge in probability to two values, which we call x_{beq} and x_{weq}. Studying the best and worst PNE is standard in algorithmic game theory, which is often preoccupied with worst-case scenarios. The unusual phenomenon in our asymptotic framework is the high number of PNE, so that it is also important to study the efficiency of "most" equilibria. In this respect, we show that asymptotically all but a vanishingly small fraction of equilibria share the same ASU, x_{typ}, which lies between the two extrema x_{beq} and x_{weq}. In other words, most PNE have the same asymptotic ASU, but there exist also PNE having a quite different efficiency.[1]

Reference

1. Amiet, B., Collevecchio, A., Scarsini, M., Zhong, Z.: Pure Nash equilibria and best-response dynamics in random games. Math. Oper. Res., forthcoming (2021b)

[1] The full version of this paper is available at: https://arxiv.org/abs/2007.08518.

I. Caragiannis and K. A. Hansen (Eds.): SAGT 2021, LNCS 12885, p.412, 2021.
https://doi.org/10.1007/978-3-030-85947-3

Author Index