Algorithmic Game Theory and Blockchains

Elias Koutsoupias
University of Oxford, UK

Abstract

Algorithmic game theory has developed into a mature field over the past three decades. However, the emergence of blockchains has raised new fundamental questions at the intersection of computer science, economics, and game theory.

2012 ACM Subject Classification Theory of computation → Algorithmic game theory

Keywords and phrases Blockchains, Mining games, Reward sharing schemes, Distributed game theory

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2022.1

Category Invited Talk

1 Algorithmic game theory

Incentives play an increasingly important role in computer science. It is now hard to imagine a time when game-theoretic issues were not part of computer science, but it was a mere three decades ago that incentives entered the computer science narrative.

To be clear, algorithmic issues of game theory questions have been considered since the inception of game theory in the 1940s. Similarly, game theorists have traditionally contributed significantly to the algorithmic theory. For example, the development of prediction algorithms in the 1950s was part of the game theory agenda, and algorithms for equilibria in the 1960s were great examples of successful algorithms.

About three decades ago there was a significant shift when it became clear that the traditional analysis of algorithms was insufficient. The reason was the widespread adoption of the internet and the web, whose protocols run at the participating nodes. It was realized that the users may have an incentive not to follow the prescribed use. One can argue that algorithmic game theory was born out of such considerations.

Research in the new field have been mainly concentrating around three research branches:

- Computational issues of game theory and economics. This research area focuses on the algorithmic aspects of game theory and economics. A significant breakthrough in this area was the proof that the computation of a Nash equilibrium of a game is PPAD-complete, which strongly suggests that the problem is intractable.
- Price of anarchy. This research area investigates the quality of equilibria. A major success in this area has been the discovery that congestion games have relatively small price of anarchy, meaning that even when players act selfishly, the outcome is close to the socially optimal one.
- Algorithmic mechanism design. This research branch studies how to design mechanisms that incentivize participants to behave in a desired way, even when they have conflicting interests. Some notable achievements in this field include the development of efficient algorithms for computing almost optimal mechanisms, and the resolution of the Nisan-Ronen conjecture, which had been an open problem for many years.

2 Incentives and blockchains

Many research directions are still active in traditional algorithmic game theory, but the advent of blockchains has changed the game. Blockchains have brought new fundamental questions at the intersection of computer science, games, and economics. Here are a few examples.

2.1 Mining games

An ideal blockchain is a sequence of blocks and the process of adding blocks to it is known as "mining." In proof of work blockchains, users can add a block only by solving a crypto-puzzle, while proof of stake systems randomly select users with probability proportional to their stake. However, the distributed nature of the system means that changes are not immediately communicated to all users, which can result in multiple users extending the blockchain from the same point, creating a tree structure instead of a path. To address this, the protocol advises miners to create blocks at the end of the longest known branch and immediately propagate them to the network. If all miners follow this advice, the reward structure guarantees revenue proportional to computational power or stake. Nevertheless, selfish miners may deviate from the advice if it serves their interests, raising the question of which "mining game" they play and what equilibria exist in these games. Unlike games in classical game theory where players' strategies and utilities are given explicitly or implicitly, mining games are indirectly defined by the blockchain protocol.

2.2 Reward sharing schemes

Blockchains require an adequate number of active participants to maintain the system. Blockchain consensus protocols incentivize every user to be an active participant by paying them for mining a new block. However, this has led to undesirable effects, such as excessive energy consumption and a concentration of power among a small number of mining pools. Reward sharing schemes attempt to address these issues by incentivizing the formation of pools of users in a transparent manner. To form a pool, users delegate their stake to one of its members, the pool leader, who runs the protocol on their behalf.

These schemes are based on payments that attempt to encourage a good selection of pool leaders. The quality of a reward scheme is determined by criteria such as liveness, efficiency, decentralization, and Sybil resiliency.

2.3 Distributed computing with incentives

In traditional mechanism design, a mediator collects inputs from participants and runs payment and allocation algorithms. However, in blockchains, this takes the form of smart contracts. Smart contracts are algorithms that have a state, which updates when appropriate transactions are issued by members. While there is a lot of hype surrounding the potential of smart contracts, there are also significant risks associated with them due to the complex game-theoretic analysis required even for simple contracts. Despite these challenges, the number of deployed smart contracts on actual blockchains is growing at a rapid pace, making it crucial to develop a robust theory to understand their power and limitations.

Smart contracts are fundamentally distributed algorithms with incentives. The theory of distributed computation has been studied extensively, but without incentives. A notable success in this area was the characterization of what can be computed by distributed protocols, which involved discovering a surprising connection to algebraic topology. The question now is whether a similar characterization exists for distributed tasks when participants act selfishly.