Blockchain Games between miners

Workshop LINCS June 2019

E.A. INRIA

CONTENT

- Game theory notions
- Blockchain games and resource allocation – the splittable case
- Constraints on resources, scalability, normalized equilibrium
- Non splittable games and potential games
- Elastic demand, crowding games
- Time varying number of players, Poisson game

Non-cooperative game

- Let here be a set N of n playerss.
- Player j has an action set A(j).
- Let a be an action vector for the players
- Let U(i,a) be the utility for player i of the vector a of actions.
- Player i wishes to maximize its utility
- An action vector is an equilibrium if no player can benefit form unilaterall deviation

Blockchain game between miners

The blockchain is a distributed secure database containing validated blocks of transactions.

- A block is validated by special nodes called miners and the validation of each new block is done via the solution of a computationally difficult problem, which is called the proof-of-work puzzle.
- The miners compete against each other and the first to solve the problem announces it, the block is then verified by the majority of miners in this network, trying to reach consensus.

Blockchain game between miners

- After the propagated block reaches consensus, it is added to the distributed database.
- The miner who found the solution receives a reward either in the form of cryptocurrencies or in the form of a transaction reward.
- Because of the huge energy requirement necessary to be the first to solve the puzzle, blockchain mining is typically executed in specialized hardware.
- An Edge computing Service Provider (ESP) is introduced to support proof-of-work puzzle offloading by using its edge computing nodes

Example of advertisement for mining in cloud

Our work addresses the following two questions:

- given a single blockchain, how should rational users contribute to the mining process, possibly counting on third-party ESPs or mining pools to offload infrastructure costs?
- given multiple blockchains, e.g., in a multi-cryptocurrency ecosystem, how should rational miners distribute their monetary and/or computational budget towards mining?

Splittable approach for resource allocation game

- We assume next competition over splittable resources at a single ESP and single currency
- miner i decides how much to invest
- Its utility from investing x(i) is the payoff minus cost:

$$U(i)=x(i)/x - gx(i)$$

Where x is the total investment. This is the Tullok rent seeking game. It has a unique Nash equilibrium

Related to KELLEY MECHANISM in networking in which the goal of the network is to find a pricing g that will guarntee that the equilibrium will be globally optimal w.r.t. the payoff, and will meet some capacity constraint on the sum of x(i).

Splittable Crypto Currency (CC) game

- We next assume that a miner i has a fixed budget B(i) that it can split between various crypto currencies. Its utility from investing x(i,k) in ccurrency k is

$$U(i,k)=x(i,k)/x(k) - g(k)x(i,k) \quad \text{hence} \quad U(i)=\sum_{k=1}^{K} U(i,k)$$

Where x(k) is the total investment in currency k

This is a variation of Tullok rent seeking game. It has a unique Nash equilibrium.

Related to Kelly mechanism where there are K resources to split

Constraints

- We ask similar question as Kelley but our goal is to find prices which induce an equilibrium

- Each player may have own budget constraints.
- These are orthogonal constraints
- There may be further non orthogonal constraints on each ccurrency k of the form
- $$\sum_{i=1}^{N} x(i,k) \leq V(k)$$
- V may represent energy constraint on a currency
- Infinite number of equilibria
- How to select one

Constraints and normalized equilibrium

- $\sum_{i=1}^{N} x(i,k) \leq$ V(k)
- By KKT for each player i and policies x(-i) there exists r(i,k,x(-i)) such that the best response for player i is the solution of

$$\max U(i) + \sum_k r(i,k) \left(V(k) - \sum_{i=1}^{N} x(i,k) \right)$$

With complementarity constraints. If we set r as pricing then it guarantees that the argmax is feasible. The fix point is an equilibrium.

But this pricing is not scalable.

Does there exist an equilibrium x for which the vector r DOES NOT DEPEND on i nor on x? If yes this is called normalized equilibrium

Main results

- THM1. The blockchain game has a unique normalized equilibrium
- Prf: x is an equilibrium if and only if

X in argmax (U(i) + $\sum_k$ r(k) (V(k) − $\sum_{i=1}^{N} x(i,k)$)) equivalently

X in argmax (U(i) - $\sum_k$ r(k) x(i,k))

Which are the KKT conditions for x to be an equilibrium in the non constrained problem where r are the cost g(k)

THM2. There is a primal dual learning scheme that guarantees that the constraints are met during the whole learning process

Discrete setting: Congestion games

- A directed graph (G,E,V) with a set of links E and vertices V.
- Each of a finite set of players has to ship a single packets from its source to the destination.
- The cost of a path is the sum of the costs of the links over the path.
- A link cost is an incrneasing function of the number of users that use the link.
- Rosenthal showed that this is a potential game

Potential game

- A game has a potential P if for every player i, and any action vectors a and b that differ only in the action of player i,

$$P(a)-P(b)=U(i,a)-U(i,b)$$

A game with an ordinal potential

the equality is replaced by an inequality

$$P(a)-P(b) \geq U(i,a)-U(i,b)$$

If the potential has a maximum then the game has an equilibrium.

Limits of best (or of better) responses are equilibria of the game

[Shapely and Monderer]

Discrete CC game between Miners

- There are K crypto-currencies and a single ESP
- There are N miners
- A puzzle related to crypto currency k requires from a miner a random time with expectation $s=1/\mu(k)$; we assume that a new puzzle is available at crypto currency k every $T>>s$ secs
- Denote by L(k) the number of miners that compete over the k-th currency. The probability that a miner is the fastest is 1/L(k)

Constant number of miners

- L is vued as a strategy.
- The utility for a miner to solve puzle k is

$$U(k,L(k)) = \mu(k)/L(k) - g(k)$$

- where g(k) is the cost for using the ESP for solving a puzzle related to the k-th crypto currency
- L is an eqilibrium if for all k for which L(k)>0 and all k'

$$U(k,L(k)) \geq U(k',L(k')+1)$$

- In other words no player can gain by deviating from k to k'

ESP association game with Elastic demand

- We assume a single currrency and R user classes
- A miner of class r pays g(r) for using the ESP per attempted puzzle
- We assume that a miner participates only if the utility is non-negative
- Let L be an R dimensional vector of loads.
- The utility for a class r user to join the miners is

$$U(r,L)=1/|L| - g(r)$$

- If L(r)>0 and 0 otherwize
- A player consists of one arrival
- This is a crowding game and has a unique equilibrium

A deadline T

- IF there is a deadline (typically 10mins) then the first part of the utility is multiplied by the μrobability that the fastest miner terminates before T i.e. by

$$(1-\exp(-|L|\mu T)$$

Stochastic ESP Association Game

- We now investigate a situation in which the number of miners varies in time.
- Consider a Poisson disributed arrival process of miners.
- Upon arrival, say at time t, a miner observes the number N(t) of competing miners present.
- The time to compute a puzzle by a miner is exponentially distributed with mean $1/\mu$ if it is the only one attached to the ESP. When there are n miners attached then the service rate is n times slower. We model the service rate of a given miner at time t as a processor sharing with rate $\mu/N(t)$.
- Should the miner participate or not in the puzzle
- The utility for participaing in the mining depends on futur arrivals and their decision

Equilibrium structure [EA and Shimkin]

- We model this as a game.
- Threshold (l,q)
- An arrival at time t joins the mining if N(t)>l.
- It doe not join if N(t)<l and it joins with probabiity q if N(t)=l
- (l,q) is an equilibrium if it is the optimal threshold give n that every one else uses that same threshold.

- Learning based on stochastic approximation

Extension: Equilibrium structure [Kushner]

- We model this as a game.
- For each r there is anoher threshold (l,q)_r
- A type r arrival at time t joins the mining if N(t)>l(r). It doe not join if N(t)<l(r) and it joins with probabiity q(r) id N(t)=l
- (l,q) is an equilibrium if it is the optimal threshold given that every one else uses that same threshold.

- Learning based on stochastic approximation

Reference

- *E. Altman and N. Shimkin* , Individually Optimal Dynamic Routing in a Processor Sharing System: Stochastic Game Analysis , *EE Pub No. 849* , August 1992. A later version can be found in *Operations Research* , pp. 776--784, 1998.

- Extension by Kushner to R classes

- Mandar: extention for M/M/infinity queue or M/M/K/K. This models unlimited resources at the ESP.

Current work

- Adversarial modeling – worse case attack
- Coalition game and incentives in presence of adversarial nodes