UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

Via J. F. Kennedy, 6 – 43125 Parma – Italia

ANDREA MANTOVI

BITCOIN SELECTION RULE AND FOUNDATIONAL GAME THEORETIC REPRESENTATION OF MINING COMPETITION

WORKING PAPER EP02/2021

Parole chiave: Blockchain; Proof-of-Work; Rent Seeking; Nash Equilibrium; Additive Aggregation.

Bitcoin selection rule and

foundational game theoretic representation of mining competition

Andrea Mantovi

Dipartimento di Scienze Economiche e Aziendali

Parma, Italy

Abstract. *The Bitcoin selection rule posits that miners are perfect substitutes in the contest for the block reward. It is well established that the additive aggregation property of the rule characterizes Proof-of-Work as a Tullock contest, whose unique pure strategy Nash equilibrium has long been identified in terms of entry thresholds and best responses to the aggregate scale of activity. It is the aim of the present contribution to deepen such properties by embracing them into a unifying analytical picture that posits an inherent reciprocal relationship between the aggregate scale of activity and a benchmark gauge of marginal cost. In such terms we identify the precise in-and-out-of-equilibrium link between the functions employed by Szidarovszky and Okuguchi (1997) and Arnosti and Weinberg (2018) for discussing the structure of the game. The result paves the way to insightful graphical representations on the connection between descriptions of absolute and relative levels of activity. Our results may cross-fertilize more realistic models of blockchain phenomenology; potential lines of progress of our approach are briefly sketched.*

Keywords. Blockchain. Proof-of-Work. Tullock Contest. Nash Equilibrium. Aggregative Games.

JEL Classification. C72, D82, E42, O33.

This draft: January 14, 2022.

1 Introduction

The performance of Bitcoin and altcoins over the last decade represents a financial breakthrough whose foreseeable implications are increasingly debated. More generally, blockchain technologies supporting decentralized finance ("Defi") projects are attracting $bn investments in payment and lending services (see Kruppa, 2021). No wonder, increasing reasearch efforts are addressing such financial innovations, in particular the properties of the Proof-of-Work (PoW) mechanism conceived by Nakamoto (2008) as a technological substitute for trust in a central institution/intermediary. This is the theoretical arena we shall be addressing.

The PoW mechanism posits a competition for brute forcing a hash inequality based on SHA-256 (Garay et al., 2015) by repeatedly changing the input to the hash function until output is small enough (Capponi et al., 2021). The competition is 'egalitarian', in the sense that all competitors use the same brute force method; this egalitarian instance is a key element of the decentralization philosophy. The competition results in the solution of the cryptographic problem; the correctness of the solution can be easily verified, and represents the objective element around which decentralized consensus is meant to cluster – in a well known expression, *trust the math*. Well, an economic literature is addressing the soundness of such a scheme: "certain properties of decentralized systems are implied by their underlying economic structure and thus cannot be solved via cryptographic methods" (Leshno and Strack, 2020, p. 270). It is our aim to deepen such economic structure, assuming the reader familiar enough with the mechanisms of block validation, updating of the chain and reward schemes; the online Appendix to Catalini and Gans (2020) is an excellent review.

Economists aim at simplification and stylized definitions. Well, the definition of blockchain may not be taken as settled. The term has not been introduced by Nakamoto (2008), and over the years has been used for different distributed ledgers, irrespective of potentially inhabiting cryptocurrencies. In the words of Andolfatto (2018), what exactly is a blockchain depends on who you ask. The Author does even ask whether the achievement of decentralized consensus is worth the effort. One should not underestimate issues of definition, since different incentives and objectives may be at stake.

Miners have been conjectured to be users of blockchains (Halaburda et al., 2021), have been depicted as investors in state-of-the-art mining equipment (Capponi et al., 2021) and as competing on price in the sale of specialized hardware (Arnosti and Weinberg, 2021), and the conceptual separation between 'pure' miners and other types of players is essentially methodological, that is, functional to the definition of the degrees of freedom and interaction channels that may enlighten what precisely is dictated by a protocol. As is well known, it takes more than learning the rules of chess to appreciate the complexity of sophisticated play; analogously, the bare statement of the protocol does not convey straightforwardly its strategic implications.[1] For instance,

[1] The analogy with chess is clearly partial, since, among other things, the rules of chess are fixed once and for all, whereas a blockchain protocol may be updated, and technological progresses may reshape competiveness factors. Still, it may be inspiring to envision the principles of medium play (like positional play or the logic of sacrifices) as characterizations of emergent phenomena in a parallel with emergent phenomena like the evolution of mining pools.

Arnosti and Weinberg point out that the significant concentration of Bitcoin mining is an *unexpected* consequence of the protocol, and a major concern for the Bitcoin community.

Over the last years game theory (GT) has been largely employed in the discussion of the strategic implications of a protocol, and a whole taxonomy is being compiled of Nash equilibria of noncooperative games representing mining competition and various types of attacks (see Liu et al., 2019) to which a blockchain may be subject, the paradigm being the "majority" attack. Still, as is well known, there is more to GT than the characterization of Nash equilibria, and a number of conditions have been thoroughly investigated under which players – whether boundedly or perfectly rational – may happen to coordinate on a Nash equilibrium of some game. Evidently, it is beyond our goals to provide even a brief sketch of such results;[2] rather, our aim is to refine both the analytical representation and the conceptual interpretation of the stage competition among miners as foundational stylized definition of PoW (in line with Dimitri, 2017; Arnosti and Weinberg, 2018; Leshno and Strack, 2020; Halaburda et al., 2021; Capponi et al., 2021), upon which more refined models (definitions) may build. In fact, what exactly is a blockchain can be considered to depend on the level of strategic complexity that a game theoretic representation is meant to target (in the sense of Gintis, 2009, subsection 8.8). The target of the present contribution is the strategic role of the aggregate scale of activity.

As is well known, entrant miners or incumbent increasing activity rates affect negatively the expected reward of others; the term *externality* has been largely adopted for denoting such effect. We shall not follow such a convention, and rather adopt the language of *aggregative* games, in which payoffs are functions of some "aggregator" of strategy profiles (see Jensen, 2010, and references therein): the global level of mining activity is the additive aggregator in the selection rule that will pivot our discussion.

The basic mining game is a Tullock contest that has been long shown to admit a unique Nash equilibrium in pure strategies that fixes a threshold of participation. In what follows, by Nash equilibrium (NE) we shall always mean pure strategy NE. We shall embrace such results in a global (in-and-out-of-equilibrium) picture building on the functions Y and X employed respectively by Szidarovszky and Okuguchi (1997) and Arnosti and Weinberg (2018) for the characterization of the unique NE of the game. Our key result (Proposition 1) is the analytical link between X and Y, a result that cross-fertilizes interpretations of absolute and relative levels of strategic activity. The result builds on a change of variable that posits an inherent connection between aggregate scale and marginal costs in Tullock contests. In such respect, the foliation of strategic space in terms of the simplices of constant s can be appreciated as a conceptually significant map. Despite the fact that the basic game is not symmetric – players in general face different cost functions – the symmetry of the selection rule manifests itself in the additive aggregation property of best responses, and the foliation of strategic space by simplices is *adapted* to such a property.

Our approach may complement high-level dimensions of analysis like those of Catalini and Gans (2020). According to the Authors, it matters not only to identify the key costs that drive the activity of participants to

[2] See Aumann (1987) for a landmark discussion of epistemic aspects, and Gintis (2009) for equilibrium refinement notions and a discussion on the unification of behavioral sciences.

the blockchain, but as well to envision a growth perspective in which the sustainability of the ecology is at stake. Along such sophisticated lines of thought one is forced to abandon the cardinal nature of the payoffs of the basic one-shot risk-neutral setting, and switch to ordinal payoffs. We shall comment on that in section 5 under the inspiration of a metaphor in which the additive aggregation property of the selection rule compares to a 'DNA' that replicates and shapes the development of a PoW organism (similar metaphors have been suggested; for instance, the online Appendix to Catalini and Gans, 2020, envisions digital fingerprints as DNA of blocks).

Our focus on the competitive aspects of PoW represents a sharp economic perspective that does not cover directly (but may have implications for) other types of protocols, like Proof-of-Stake, and a variety of themes in computer science that lie beyond our goals. The plan of the rest of the paper is as follows. In the following subsection we cover the related literature. In section 2 we introduce the basic mining game. In section 3 we review the analytical discussion of Tullock contests in terms of aggregate best responses and absolute activity levels, that we connect in section 4 with the approach to relative levels, and discuss the conceptual reach of our key result. Analytic insights on the persistence of additive aggregation with ordinal payoffs are developed in section 5. A final section sketches potential lines of progress.

1.1 Related literature

The foundational game theoretic representation of PoW is the strand of literature to which the present article is meant to contribute in first instance. Dimitri (2017) seems to be the first to address the stage mining game as a contest. The Author assumes linear homogeneous cost functions, characterizes the unique NE with an explicit expression for the equilibrium strategy profile, and establishes that "the intrinsic structure of the Bitcoin mining game seems to prevent the emergence of a monopolistic mining activity." Out-of-equilibrium behavior is not addressed. The Author assumes that miners know each other's marginal costs, presumably with the intent of strengthening the empirical grip of the equilibrium strategy profile. Our in-and-out-of-equilibrium discussion does complement such an analysis, with no assumption about players' knowledge beyond the fact that they respond to the aggregate scale of activity.

The present contribution builds substantially on the equilibrium characterization set forth by Arnosti and Weinberg (2018). The Authors explicitly follow Tullock (1980) in their analytical discussion; explicit expressions for equilibrium variables are derived via the function X, reaffirming the well known fact that at least two players are active at the NE of the game. The Authors aim at a game theoretic foundation of the empirical tendency to concentration in Bitcoin mining, an unexpected emergent phenomenon of a PoW ecology. Well, Arnosti and Weinberg (2018) succeed in showing that even seemingly small cost imbalances lead to significant concentration of mining in our stylized model. This kind of instability is something that we shall deepen by reconsidering the properties of the function X. By means of a change of variable we shall enlighten an inherent connection between, on the one hand, aggregate best responses and absolute levels of

activity, and, on the other hand, the allocation of competitive advantages and relative levels of activity. Arnosti and Weinberg (2018) discuss an instability that manifests itself in *different games* for increasing asymmetry of costs functions; our strategic picture enables us to envision a more profound tendency to concentration, namely, one that manifests itself *within the same game*, and unfolds with the aggregate best response scale of activity as departure from the symmetry of expenditures that holds in the limit of vanishing activity levels (see the Remark in section 3). Such an in-and-out-of-equilibrium picture is the essence of the present contribution, in which graphical representations, we shall be arguing, provide intuitive but profound insights on empirical evidence (see the end of section 4).

Leshno and Strack (2020) as well depict the economics of PoW as a Tullock contest by reviewing key results in the extant literature. Specifically, the paper is meant to deepen the theoretical properties of the PoW selection rule. The Authors isolate three independent properties of the rule and discuss their implications, in particular showing that the Bitcoin selection rule is the only rule that satisfies such properties (see section 2 below). Our emphasis on the linear aggregative property does sharpen the content of such results. Jensen (2010) argues at length on the theoretical relevance of aggregative games, that, in the author's view, fix a natural perspective on the analytical problems we shall be dealing with.

An emerging literature addresses more articulated models that embed the stage mining game as a submodel. For our methodological purposes of great interest are Capponi et al. (2021), Arnosti and Weinberg (2021) and Cong et al. (2021), that shall be part of our discussion, in particular concerning the conception of more elaborated game forms and the transition from cardinal to ordinal payoffs. In the author's view, additive aggregation should preserve (to some extent, in some form) in more articulated settings if decentralized consensus is to emerge even at higher levels of model building or empirical phenomenology. This is the sharp methodological/analytical target of our approach. Wider perspectives on blockchain economics have been elaborated. A comprehensive review of the microeconomics of cryptocurrencies is provided by Halaburda et al. (2021) with a thorough discussion of both demand and supply of a token like Bitcoin. Our work concerns the supply side of the problem, and the paper by Halaburda et al. (2021) can represent a cogent frame for our considerations.

A less-economic and more-technically oriented literature covers the strategic interactions tailored by PoW beyond the competition among miners in its various aspects, and in particular the various types of attacks to which the network may be subject. In a landmark analysis, Eyal and Sirer (2014) discuss the incentive compatibility of PoW. In the words of the Authors, the mining reward structure is essential to the currency's decentralized nature; our approach is meant shed further light on such a statement, that the subsequent literature has been continuously refining. Liu et al. (2019) offer a review of such approaches, and in fact a 'taxonomy' of such models that provides a comprehensive perspective on the issues at hand, thereby enhancing the cross-fertilization of extant results that is also among the aims of this paper.

A more qualitative literature on blockchain evolution for sure represents another relevant connection with our work. For instance, profound insights developed by Catalini and Gans (2020) concern the evolution of the

environments and of the incentives that should underlie the process. Our discussion of the transition between cardinal and ordinal payoffs may provide useful elements. Budish (2018) as well provides high level insights to which our results may contribute further elements. The Author argues about the incentive compatibility of a PoW protocol w.r.t. various attacks, and parametrizes the problem in terms of stock values V_{attack} that gauge, so to say, 'thresholds' of honest behavior. Our in-and-out-of-equilibrium discussion may contribute fine grained analytical insights for such high level discussions.

Evidently, our analytic considerations apply to general Tullock contests that share the Bitcoin selection rule, and our results do contribute to the theoretical inquiry on such games. The landmark paper by Szidarovszky and Okuguchi (1997) in particular, conceived well before the advent of Bitcoin, shapes the aggregate best response perspective upon which our methodology builds, and for which our results can represent a line of progress. Noticeably, recent advances in the theoretical characterization of PoW seem to have renewed interest in Tullock contests. For instance, Ewerhart (2017) demonstrates that a lottery contest admits a best response potential, a fact that has significant dynamic implications beyond the existence and uniqueness of a static NE. Altman et al. (2019) discuss Tullock contests with common coupled constraints and establish the existence of a normalized equilibrium therein. Our graphical representations may contribute sharp insights on such lines of progress. True, the methodological core of our discussion is a change of variable in the function X that does not seem to feature in the above literature, and whose implications gauge the conceptual reach of our approach.

2 Stage mining competition as a contest

The properties of the stage competition among miners fix the theoretical foundations of decentralized consensus in its PoW implementation; this is the analytical problem we shall be dealing with. True, to begin with, it may be worth noticing that recent events seem to witness the concrete empirical relevance of such conceptual constructs. In May 2021 China has outlawed the activity of Bitcoin mining, and the media have covered the rapidly spreading incentives to enter the industry in other parts of the globle (see Szalay and Stafford, 2021). This reshift of activity easily aligns with general insights about entry/exit dynamics: it is somewhat natural to expect new entries in an industry that has faced a significant exit flow. On the other hand, it is not that straightforward to refine the picture of the incentives at play in a context like the Bitcoin mining industry, if only for its recent development. It has been argued that miners "are incentivized to turn on as many machines as possible when the price of Bitcoin is high" (ivi). Among other things, our analysis is meant to sharpen the content of such type of remarks (see for instance Figure 4 and comments below). Let us recall the basic elements of the game.

A number n of potentially active players (miners) can participate to the hashing contest for solving the cryptopuzzle assigned to a single block. Each player chooses the amount of (costly) computational resources to deploy knowing that such amount gauges the probability of succeeding. Specifically, the selection rule

$$p_i(x) = \frac{x^i}{\sum_{j=1}^{n} x^j} \equiv \frac{x^i}{s(x)} \quad , \quad i = 1, \dots, n \tag{1}$$

defined on the positive *n*-orthant (the space of strategy profiles) fixes the probability p_i with which miner *i* wins the block reward, given the resources x^j (in some units) deployed by all *n* potentially active players in the contest. Only one miner wins the reward in this stylized construct. Following Leshno and Strack (2020), let us consider a unit reward $\mathbb{1}$ as numeraire; one can then define dimensionless cost functions $c_i(x^i)$ and write $\left(p_i - c_i(x^i)\right)\mathbb{1}$ for the expected profit (payoff) of the risk-neutral miner *i*. As pointed out by Dimitri (2017), such payoffs encompass the (exogenous and time varying) exchange rate between the crypto numeraire and the currency that pays costs.

The game is one-shot and simultaneous (therefore we shall speak of *levels* or *scales*, and not rates, of activity) and does fit the class of rent-seeking contests named after Tullock (1980), that after having been studied for decades, are now the subject of renewed interest (see subsection 1.1 above). In particular, an economic literature is sharpening the implications of rule (1) and of the payoff structure of the game. Rule (1) is homogeneous of degree 0, i.e. it is invariant w.r.t. rescaling of all activity levels by the same factor. This specific form of additive aggregativity is at the centre of our analytic approach, for which Leshno and Strack (2020) provide insightful preliminaries.

The Authors tailor a theoretical analysis of PoW that isolates three fundamental properties of the selection rule, namely, the symmetry (perfect substitutability) of participants, the absence of incentives to assume fake identities, and the absence of incentives to merge (i.e. share resources in the hope of acquiring economies of scale). Leshno and Strack (2020) demonstrate that such properties are independent, i.e. neither implies any other, and that the Bitcoin selection rule (1) is the only rule that satisfies such properties. As a relevant consequence, the Authors notice that their "findings show that certain properties of decentralized systems are implied by their underlying economic structure and thus cannot be solved via cryptographic methods." It is this kind of basic insights (that, unavoidably, come at the cost of drastic simplifications) that we target in our approach. Most notably, according to rule (1), players are perfect substitutes in contesting the reward, and in this sense each miner plays against the aggregate of competitors, so that the game, formally, resembles a two-player game, with significant gains in the tractability of the problem.

The extant literature has succeeded in representing a number of properties of the game in precise analytical form; it is our aim to frame such results within a global picture of strategic space (the space of strategy profiles) meant to cross-fertilize descriptions of absolute and relative activity allocations, that we may call "dual". The microeconomic theory of duality (Cornes, 1992) provides inspiring suggestions on the cross-fertilization of distinct formulations of economic optimizations: "investment of a little time and effort in becoming familiar with alternative formulations […] can tremendously simplify their formal analysis" (ivi, p. 3). Hopefully, something similar may result from our picture of the simplices that foliate strategic space (next section), that,

among other things, may pave the way to the introduction of recent geometric advances in mathematical economics (Mantovi, 2016).

3 Strategic expansion of absolute levels of activity

As already pointed out, a key ingredient of our approach is the global scale of activity *s*, that represents the additive (homogeneous of degree 1) aggregator of our game. The simplices $s = \sum_{j=1}^{n} x^j$ that foliate[3] strategic space (Figure 1) are the corresponding loci of strategic space. Being rule (1) homogeneous of degree 0, Euler's formula applied to all p_i yields zero, and all such simplices are equivalent as spaces of expected reward (but, evidently, not equivalent as spaces of expected payoff). Well, it turns out that the scale *s* is a key element in the characterization of the equilibrium of the game.

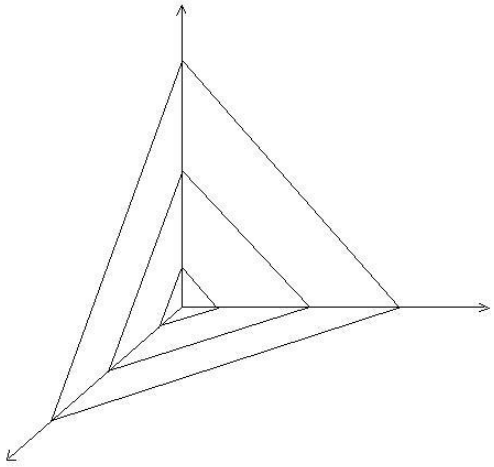

Figure 1. The foliation of 3d strategic space by the simplices $s = \sum_{j=1}^{3} x^j$.

The well known first order condition (FOC)

$$s^2 \frac{dc_i}{dx^i} = s - x^i \tag{2}$$

[3] The differential geometric notion of *foliation* of a manifold is somewhat intuitive, think of a book as a volume foliated by pages. See Spivak (1999) for a readable introduction to the relevance of the notion.

(compare Szidarovszky and Okuguchi, 1997; Arnosti and Weinberg, 2018) fixes the best responses of active players to the scale of activity *s*, in conjunction with the condition $s\frac{dc_i}{dx^i}(0) \geq 1$ of vanishing activity (ivi). In case players face the same cost function, it is straightforward to write $x = \frac{n-1}{n^2}\frac{1}{\frac{dc}{dx}(x)}$ for the identical equilibrium strategy (activity level) *x* of all players. Then, for linear homogeneous cost functions, one can write (being m_0 the common constant marginal cost)

$$xm_0 = \frac{n-1}{n^2} \tag{3}$$

The NE aggregate scale of activity *s** thus reads $(n-1)/(n\,m_0)$, and approaches $1/m_0$ for large *n*. This symmetric NE specializes the interplay between the scale invariance of the selection rule and the monotone increase of costs, with the explicit formula (3) accounting for the effects of scale transformations of m_0: definitely, the aggregate scale of activity of the symmetric NE is *inversely proportional* to m_0 . This is a well known fact that will provide inspiration for our considerations. Well known as well is the positive expected profit $1/n^2$ of each miner, so that total profit reads $1/n$: as expected, in the limit of infinite players, the 'market' approaches the perfectly competitive limit of vanishing profit.

For general cost functions, well before the emergence of Bitcoin, Szidarovszky and Okuguchi (1997) set forth a fundamental discussion of the rent-seeking game we are interested in. The Authors consider players facing possibly different (twice differentiable, increasing and convex) cost functions that vanish for vanishing activity, and target the profile of best responses via the function *Y*(*s*) (ivi, formula 6) that amounts to the sum of the best responses of agents to the scale *s* minus *s* itself. On account of (2) one can write *Y* as[4]

$$Y(s) = (n-1)s - s^2\sum_{k=1}^{K}\frac{dc}{dx^k} = s\left(-1 + \sum_{k=1}^{K} 1 - s\frac{dc}{dx^k}\right) \tag{4}$$

where the sum extends over the *K* active miners at *s*. The Authors establish the existence and uniqueness of the NE of the game via the analysis of the function *Y*, that decreases for increasing *s* in a neighborhood of the unique NE (at which, by definition, *Y* vanishes). In our geometric language, the map $s \to Y + s$ expands simplices below the NE and shrinks simplices above the NE. In this sense, aggregate best responses depict sort of 'phase transition' of strategy profiles from, so to say, 'complements to scale' (below the NE scale) to 'substitutes to scale' (above). In addition, truly relevant are the limits of best responses for small and large *s*, that we fix in the following

[4] The expression does not feature in the paper by Szidarovszky and Okuguchi (1997).

Remark. According to rule (1), players are perfect substitutes in contesting the reward. Much like in a Cournot oligopoly, each player responds to the aggregate of the competitors' output. Equivalently, players can be considered to respond to the overall scale of activity s as additive aggregator (a well defined GT notion). Provided cost functions vanish in the limit $s \to 0$, best responses are symmetric in such limit, with asymmetric cost advantages unfolding for increasing s. One can scan strategic space for increasing s and envision sort of progressive symmetry breaking (departure from symmetry), with each player characterized by a definite exit threshold. In such a scan, the connection between the homogeneity of degree 0 (scale invariance) of the selection rule (1) and the monotone increase of cost functions rationalizes the existence of a unique NE, at which the lower the cost incurred by a player, the larger his level of activity and expected payoff. In the limit of large s, in which costs exceed expected reward, no player is worth mining. It follows from the factorization of s in (4) that $Y \to 0$ in the limit of vanishing s, and its first order Taylor approximation is $(n-1)s$. It follows from (4), and in fact from simple intuition, that Y has negative infinite limit for $s \to \infty$, and in fact coincides with $-s$ for sufficiently large s, since the best responses of all players, evidently, vanish beyond a finite level of activity. Being continuous, increasing for small s and decreasing for large s, Y must have at least one maximum (we shall provide an example of such an occurrence in section 4).

The Remark does sharpen the relevance of the symmetry of the problem in the limit $s \to 0$, and the fact that strategic advantages unfold with increasing s, and result in the sequential exit of the unfit. The sign of Y marks the 'expansionary' (positive sign) and 'contractionary' (negative sign) regions of strategic space; in a perspective of best response dynamics (something that should be modelled appropriately, a task that far exceeds our goals), one may make sense of a 'strategic attraction' towards the unique NE. True, as already pointed out, our methodological target is the aggregative property of the game; in such respect, the factorization of the aggregator s in formula (4) is crucial.

Y embodies best responses, and as such represents *absolute* levels of activity; well, the aforementioned factorization enables us to consider the companion factor as embodying the *relative* levels of best responses. This is the analytical fact that we shall elaborate in the following section. For the time being, notice that the factorization of s in formulas (1) and (2) enables us to write FOCs as

$$s\frac{dc}{dx^k} = 1 - p^k \,, \tag{5}$$

an expression that already conveys some insight on the connection between absolute and relative levels of activity, and in particular between the aggregate scale of activity s and the distribution of marginal costs. Let us follow Arnosti and Weinberg (2018) in such a direction.

4 Cost competitiveness and relative levels of activity

Assume players face linear homogeneous cost functions $c_k(x^k) = m_k x^k$ (an assumption, recall, that is empirically significant), and order the n players in terms of decreasing competitiveness, i.e. from lower to higher marginal cost. Following Tullock (1980), Arnosti and Weinberg (2018) define the function

$$X(m) \equiv \sum_{k=1}^{n} \max\left(1 - \frac{m_k}{m}, 0\right) \tag{6}$$

for $m \in (0, \infty)$. Each value of the positive real number m gauges a benchmark of competitiveness that partitions players into those with marginal cost lower than m and the rest, that we may call the 'unfit' w.r.t. m. In fact, X is the sum over players of what we may call a "cost competitiveness index" $1–m_k/m$ defined on $[m_k , \infty)$, that vanishes for $m = m_k$ and then monotonically increases for increasing m, approaching the limit 1 for $m \to \infty$. The parallel is evident with the maximal symmetric competitiveness of players in the limit of vanishing activity stated in the above Remark, a competitiveness that progressively diminishes for increasing costs. The function $X(m)$ can then be interpreted as an aggregate competitiveness index that depends on a benchmark gauge m of marginal cost.

Well, taken at face value, X is not a function on strategic space, and does not seem to admit analytical comparison with the function Y of the previous section. Furthermore, Y has the dimension of activity, whereas X is dimensionless. Still, the following remarks seem to point at a relationship of some kind between the two functions.

The function (6) is continuous, vanishes in the interval $(0, m_1]$, has positive piecewise countinuous derivative for $m \geq m_1$, and approaches the value n in the limit of large m. The sum in (6) receives positive contributions only from players with $m_k < m$, and therefore selects the players 'fit at m'; as we have seen, an analogous selection is gauged by Y. Followig Tullock (1980), Arnosti and Weinberg (2018) identify the NE of the rent-seeking game as corresponding to the value 1 of the function X. Then, the monotonicity of X makes it possible to identify a unique value m^* of the variable m corresponding to the unique NE of the game, in some analogy with the NE value of the aggregator s. Definitely, at m^*, X is the sum of the probabilities of winning the mining game according to the FOCs (2). Generalizing the symmetric case, in equilibrium, active players (at least two) make positive profit. Along the line of argument, the Authors find that apparently mild deviations from cost symmetry do result in a significant increase in market share for the players facing lower costs: in the words of the Authors, Bitcoin is "a natural oligopoly." This is a major insight that our analytic detour is meant to substantiate further in terms of the following analytical steps.

Let us recall the previous Remark (section 3 above) in our strategic interpretation of the function X, in particular concerning the fact that, being larger marginal cost a strategic disadvantage, *not only* at the NE one expects that the lower m_k the larger the activity and expected payoff of player k. The function X provides

explicit global analytical shape of such an occurrence, opening the way to transparent graphical representations. Consider the following

*Example***.** Consider 4 players with marginal costs 0.25, 0.5, 0.75, 1. Check that the condition $X = 1$ identifies activity levels that yield $p^1 = 2/3$, $p^2 = 1/3$, $p^3 = p^4 = 0$; only two miners are active at the NE of the game. Plot the function X in different portions of the domain so as to display both global and local properties.

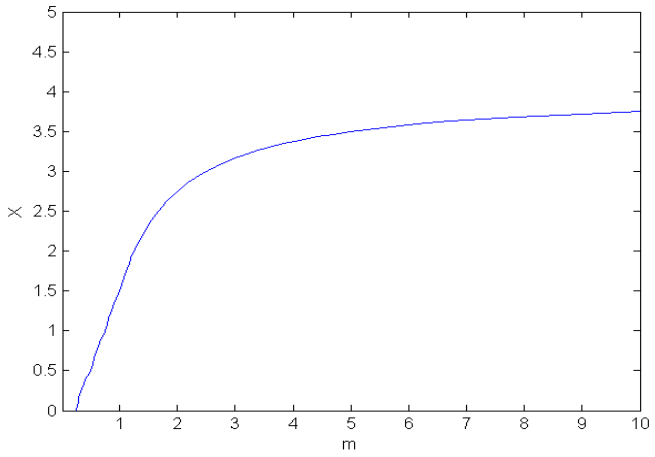

Figure 2. Plot of the function X in the example, i.e. $m_k = k/4$, $k = 1, 2, 3, 4$. Monotonicity and the large m limit 4 are clearly displayed.

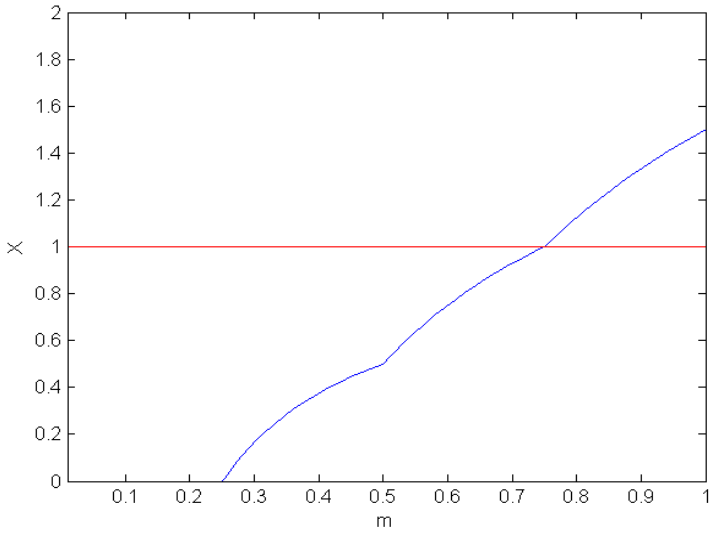

Figure 3. The same function in the domain $(0, m_4)$. Being $m^* = 0.75 = m_3$, only players 1, 2 mine actively in equilibrium. Notice the discontinuities in the slope at the points of entry of miners.

Fig. 2 displays the limits for small and large m, the monotone increase of X for $m \geq m_1$, and the unique m^* for which $X(m^*) = 1$. Fig. 3 displays the discontinuities of the slope at the points of entry. The two plots represent clearly the evolution of cost competitiveness, beyond the fact that players with marginal cost larger than m^* do not mine. One may argue about the level of generality that should be ascribed to such plots (the author is not aware of any such plot in the literature), but for the moment our purpose is to build intuition on a potential connection with Y (the author is not aware of any plot of Y in the literature).

The variable m is not a function on strategic space. Still, recall from the previous section that the unique NE of the symmetric game features an inverse proportionality between the common marginal cost and the aggregate scale of activity s. An educated guess, then, invites us to interpret the argument m of X as the reciprocal of s, and then define the function $X(s)$ on strategic space as

$$X(s) \equiv \sum_{k=1}^{n} \max\left(1 - s\frac{\partial c_k}{\partial x^k}, 0\right) \tag{7}$$

In the symmetric case in which all players face the same marginal cost m_1 one can write $X(s) = n(1–m_1 s)$ for $s \in (0, 1/m_1]$, and $X = 0$ for larger s. It is easy to check that the NE condition $X = 1$ identifies the well known equilibrium condition $s^* m_1 = (n – 1)/n$. Consider then the previous example.

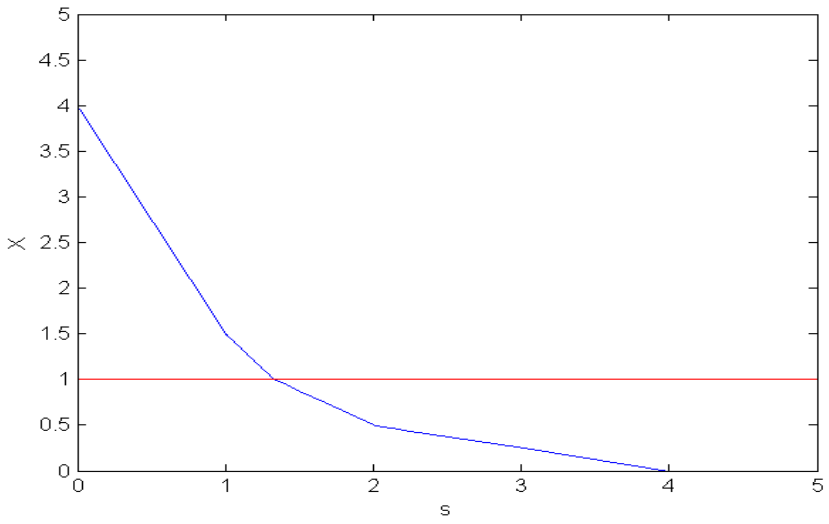

Figure 4. The function (7) for the example. Notice the discontinuities in the slope of the piecewise linear function at the points of exit, and the Nash equilibrium at the reciprocal 4/3 of $m^* = 0.75$. The function vanishes identically beyond the exit threshold $s = 4$.

Figure 4 is a plot of function (7) for our example. One can read the figure as a tale of decreasing competitivenss in which the initial limit 4 coincides with the number of players and with the upper bound of the range of (7). As stated in the above Remark, players have symmetric and maximal competitiveness in the limit $s \to 0$ in which costs vanish. Then, with increasing s, and therefore costs, the differences in cost competitivenss manifest themselves as the montone decrease of the value of X. Equivalently, one can read Figure 4 as a tale in which the limit of small m corresponds to the limit of large s on the right, at which no player is worth mining (beyond $s = 4$). Then, moving to the left towards smaller s (larger m), one reaches a threshold s_1 at which player 1 (the fittest) makes positive expected profit. Further contraction spans the other thresholds at which players, one after another, switch to positive expected profits until they gain maximal competitiveness in the limit of vanishing activity.

The transparency of this tale enriches our approach to a 'map' of strategic space, a scan of competitivenss along the foliation of simplices depicted in Figure 1. In the author's view, such plots provide valuable inspiration for appreciating the true content of analytical manipulations. Notice, the value $X = 1$ of the unique NE of the game does not seem to play any special role in the above plot; it may be useful, then, to sharpen the connection between the above map and the arguments in the previous section.

One may argue that our interpretation of m as reciprocal of the scale s is implicit in part of the arguments developed by Arnosti and Weinberg (2018). The Authors in fact notice that m^* (c^* in their notation) is the reciprocal of the NE scale of activity s^*, and write an expression for the NE levels (ivi, Corollary 3) that in our notation can be written as

$$x^i = s^* \max\,(1 - s^* m_k, 0)\ , \qquad i\ = 1, \dots , n\ , \tag{8}$$

with the factorization of the equilibrium scale displaying clearly the link between absolute and relative levels of activity. Well, in the author's view, the conceptual relevance of such an occurrence deserves *explicit* in-and-out-of-equilibrium discussion, beyond the sharp focus on NE. The functions X and Y represent distinct analytical tools that have been successfully employed in the identification of the unique NE of the game. One can then compute the NE scale of the game to the desired approximation, possibly exactly, and then fix the relative levels of activity according to FOCs. With that said, we are interested in a *global* strategic question: can one fix a definite analytical link between the functions X and Y?

As already pointed out, Y embodies levels of activity, and therefore has the dimension of s, whereas X is a dimensionless (pure) number, so that one expects to (possibly) compare Y with sX. Well, the change of variable $s = 1/m$ enables an explicit comparison of the contents of X and Y: s is the additive aggregator that can be factored out (see formula 4 above), thereby separating the description of relative (dimensionless) activity levels. One can then effectively compare the limits discussed in the previous sections. For $s \to 0$, X has limit n (the number of potentially active players), whereas Y has vanishing limit and first order Taylor approximation

(n –1)s. For large s, X has vanishing limit (and in fact vanishes identically above a definite threshold), whereas Y has limit $-\infty$ (and in fact coincides with $-s$ beyond a definite threshold). Such premises are correctly represented in the following

Proposition 1. The functions $X(s)$ and $Y(s)$ satisfy the identity

$$Y = s\,(X - 1) \tag{9}$$

It is not difficult to check (9) by comparing (4) and (6). Notice the factorization of the scale s that reflects the same occurrence in formula (4). The analytical simplicity of the proof of the identity should not lead one to underestimate the conceptual link uncovered by the proposition, for which the above Remark, again, provides a useful synthesis. Not only does the change of variable $s = 1/m$ enable one to scan strategic space with respect to both variables s and m, but the equivalence of X and Y enables us to project the best response significance of Y onto the sequential cost competitiveness pattern represented by X. Definitely, X coincides with $(Y+s)/s$. In words, X coincides with the aggregate absolute best response to s diveded by s, i.e. X coincides with the aggregate *relative* best response to s. Then, by definition, X equals 1 at a NE. Insightful implications of our result concern graphical representations.

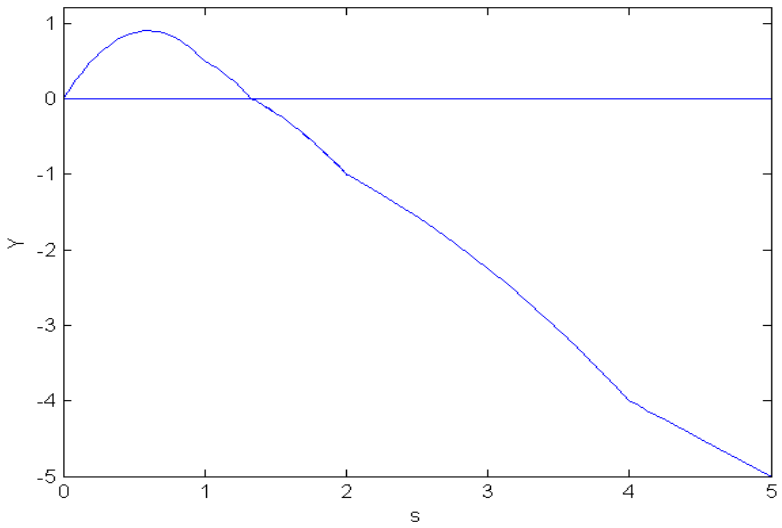

Figure 5. The function Y for the example. Notice the initial slope $Y' = 3$ = number of players minus 1, the Nash equilibrium at $s = 4/3$ and the discontinuities in the slope at points of exit (compare Fig. 4). Y coincides with $-s$ for $s \geq 4$.

Figure 5 plots the function Y for our example. Figg. 4 and 5 tell the same story in different forms: the former in terms of the dimensionless function X that aggregates relative contributions of activity, the latter in terms of the absolute contributions embodied by Y. In the authors' view, such plots convey valuable insights on the content of identity (9): the plot in Fig. 4 is piecewise linear, due to the occurrence of linear homogeneous cost functions; as a consequence, the plot in Fig. 5 is piecewise quadratic as long as miners are active; above the last exit threshold, $Y = -s$ is linear.

The exact equivalence of the content of Figg. 4 and 5 may help intuition. The piecewise linearity of the aggregate cost competitiveness X depicted in Fig. 4 has (due to formula 9) the same content of the aggregate best response picture depicted in Fig. 5. Both plots scan the foliation of strategic space via the simplices of constant aggregate activity (Fig. 1). The unique NE of the game is characterized *by definition* by the condition $Y = 0$; then, identity (9) sheds new light on the corresponding condition $X = 1$. Noticeably, Fig. 5 displays a maximum of Y that does not seem to have been commented in depth in the literature. Recall, the existence of at least one such maximum follows from the continuity of Y and the different slopes for small s (positive slope) and large s (negative slope). Beyond their theoretical relevance, our results may prove useful in the interpretation of empirical data.

Consider first the recent exit of chinese Bitcoin miners and the subsequent entry of miners from other parts of the globe. It is widely held that miners "are incentivized to turn on as many machines as possible when the price of Bitcoin is high" (Szalay and Stafford, 2021). Well, Figg. 4 and 5 above provide intuitive analytical elements for sharpening the in-and-out-of-equilibrium content of one such statement. How much is "high" and how strong are the incentives is something that our formula (9) connects with the entry sequence depicted by the function X (media have commented at length on the lowering of competitiveness barriers to entry) and with the pattern of best responses represented by Y. After the exit flow, the system is expected to adjusts to a new 'equilibrium' (something, arguably, close to a NE), and best responses are the rational driver of such adjustment. With that said, one must not forget that our basic game is not the complete story of PoW and cryptocurrencies, and that for sure other incentives are at play in the Bitcoin industry (see for instance Budish, 2018; Halaburda et al., 2021).

Consider then the carbon footprint of Bitcoin. The figure is continuously monitored via estimates of electricity consumption that, unavoidably, build on definite assumptions on aggregate 'equilibrium' properties. Well, Arnosti and Weinberg (2021) challenge the assumption of competitive equilibrium (vanishing profit) upon which some estimates build, since active miners make positive profits in our NE. Our considerations do align with such a remark, and our global strategic pictures may provide inspiration for conceiving estimates of out-of-equilibrium activity, perhaps following shocks in the exogenous parameters of the game (see Hale and Kinder, 2021, for the sharp fall in Bitcoin price in May).

To sum up, we seem to have succeeded in fixing an insightful in-and-out-of-equilibrium connection between the analytical results of Szidarovszky and Okuguchi (1997) and Arnosti and Weinberg (2018), thereby refining the global picture of the game beyond the well known characterization of the unique NE. The aggregate best

response pattern depicted by *Y* in absolute terms is perfectly equivalent to the sequential picture of cost competitiveness dictated by *X* in relative terms, once our change of variable is duly acknowledged. These conceptual and analytical advances may provide sharp building blocks for discussing emerging phenomena in the evolution of a blockchain environment.

5 Additive aggregation and ordinal payoffs

The previous analytic results pertain to the essential stage of mining competition in which payoffs are *cardinal* and reflect the precise profit opportunities in place. Evidently, models meant to stylize more sophisticated interactions and outcomes may find it hard to account for exact expected profit prospects; for instance, just the introduction of risk-aversion forces one to abandon the cardinal nature of payoffs. In a sense, the basic mining game may can represent a 'microfoundation' of a 'macroeconomics' of a blockchain accounting for various exogenous and endogenous effects. Evidently, expected reward and costs may vary for a variety of reasons (just think of the volatility of Bitcoin price), and it is far from guaranteed that the unique NE that we have been discussing may represent a cogent 'attractor' (a stability point, in some sense) of empirical dynamics. The NE we have been discussing rules out players inferior to a well specified competitiveness threshold, but it may be difficult to collect significant evidence of this effect in the early days of Bitcoin. Furthermore, entry-exit decisions entail frictions and real options characterized by intrinsically undetectable idiosyncratic elements. At some level of analytical description, one is forced to switch to qualitative analytical models in which the creativity of the scholar does participate in the conception of *ordinal* payoff functions. Well, should one expect the linear aggregation property to maintain, in some form, in the transition from cardinal to ordinal? In the author's view, this is a right question, and in this section we consider a game with significant generality in which the additive aggregation property maintains.

According to Catalini and Gans (2020), the nature of a public good should be ascribed to a blockchain ecology, for which one may distingush different phases of growth. "If in the first phase of growth of a blockchain-based network, incentives are predominantly targeted at accelerating adoption, in the second phase the key challenges from a market design perspective are ensuring that the incentives continue to support contributions of key resources to the ecosystem and avoiding a tragedy of the commons" (ivi, p. 87). The transparency of these qualitative insights – that, noticeably, are not specific to blockchains, and rather apply to a variety of real and digital platforms – witness the relevance of the problem of the commons. Let us follow Binmore (2007) in a sketch of the tragedy as a problem of linear aggregation (scale).

Suppose ten families share a common ground for grazing identical goats (the game is symmetric), and the payoff (buckets of milk) from grazing a goat on a fraction a of the common ground is proportional to $\exp\left(1-\frac{1}{10a}\right)$. Such a simple functional form represents transparently the fact that the larger the fraction a of

land grazed, the larger the payoff, and that in the limit of vanishing *a* the payoff approaches 0. Evidently, one ascribes qualitative nature to such a smart payoff function, whose usefulness displays readily.

Assume families cannnot agree to graze different parts of the ground, and each grazes the common ground at will ($a = 1$). Write n for the number of goats that a family chooses to graze, and N for the total chosen by opponents. The payoff for the identical families can be written

$$n \ \exp\left(1 - \frac{n}{10} - \frac{N}{10}\right) = \ n \exp\left(1 - \frac{n+N}{10}\right) \tag{10}$$

explicitly manifesting the problem as one of response to the *aggregator* scale $n + N$. In fact, we are faced with the strategically simplest case of response to scale, in which every player has its own dominant strategy, namely, always graze 10 goats, irrespective of what others may do; such an equilibrium is highly inefficient – a tragedy – and is a prototype problem of mechanism design. Notice, the factorization of the exponential in (10) is key for such an occurrence, and witnesses the relevance of a smart choice of payoff functions; our methodological point is the persistence of the aggregator element in a conception of the effects that may lead from the basic rent-seeking game to the high-level stylization of the tragedy.

The tragedy differentiates from Tullock contents being symmetric at every scale of activity, no strategic advantages or disadvantages manifest with the aggregator scale. The aggregation property maintains as the symmetry of the game. Insights like this shape a methodological connection between the payoffs in the two games, that are both one-shot static games. An analytical representation of the insights by Catalini and Gans should represent the emergence of incentives that may lead to the tragedy, and the payoffs of the game as functions of such incentives. Our methodological approach may prove useful in opening the door to recent analytical results on aggregation and best response dynamics (Jensen, 2010). In the authors' view, this line of thought may unfold the methodological reach of our results, that we address in the concluding section.

6 Conclusions

It was the aim of the previous sections to deepen the properties of PoW in terms of a global (in-and-out-of-equilibrium) picture of the basic mining game. We have connected descriptions of absolute and relative aggregate activity by establishing the precise functional dependence between the two functions that have been employed in the literature for the characterization of the unique Nash equilibrium of the Tullock contest. In the author's view, the change of variable at the root of such result establishes a far reaching conceptual connection between the aggregate scale of operation and the distribution of cost competitiveness. As pointed out in the Introduction, the present contribution was meant to focus sharp methodological problems, and does

not cover many important themes; for a comprehensive review of the economics of blockchain see Halaburda et al. (2021).

The previous results may spark advances in the methodological elaboration of Tullock problems in their various interpretations; still, our focus is the relevance of the stage mining game in the debate on blockchain and cryptocurrencies. In the words of Capponi et al. (2021), cryptocurrencies are only as secure as their networks: our approach aims at providing both conceptual and analytical elements for refining the 'chart' of the incentives by means of which to frame the problem. Consider for instance the way the basic mining model is employed by Altman et al. (2020) for introducing bounds on resources and shadow prices in a symmetric setting; our in-and-out-of-equilibrium picture on the asymmetry of strategic advantages may provide further elements to the picture.

A more mathematically oriented line of progress may be considered as well. According to a recent literature (see Mantovi, 2016), the differential operator $\mathbf{Z} \equiv \sum_{i=1}^{n} x^i \frac{\partial}{\partial x^i}$ at play in Euler's equation can be interpreted as a vector field whose flow maps simplices onto simplices; such geometric refinements may be employed to shed further light on the properties of the functions we have been investigating, in particular in the methodological philosophy of aggregative games (Jensen, 2010). Still, it is on conceptual grounds that this concluding section is meant to tread.

It goes without saying that different foundational models for a theory of PoW can be advocated. For instance, Garay et al. (2015) envision the technological steps for adding validated blocks (input validation, input contribution, chain reading) to the well-ordered chain as a natural basis for the analysis of the Bitcoin protocol. According to the Authors, this is the "backbone" of the protocol, and a preferred perspective on problems of synchronization. Well, it is neither our aim to counter one such approach, nor to advocate a preferred foundational picture. The point is that a methodological foundation is functional to the direction of theoretical development one is interested in; our focus on the stage mining game can be considered to complement the economic arguments of Budish (2018) on the relevance of differentiating stocks from flows in the analysis of the incentives that gauge the robustness of a protocol. More generally, our choice is in line with a literature (see subsection 1.1 above) that already displays substantial comparability and cross-fertilization; it is our aim to contribute further elements of comparability and cross-fertilization to the enterprise. After all, economic models are complementary building blocks of analysis whose conceptual transparency and analytical comparability[5] make the difference. In such respect, the following stand out.

Arnosti and Weinberg (2021) depict a sequential game in which the basic rent-seeking competition represents the second stage of a game whose first stage features players competing on price for selling specialized hardware. This is a neat example of the way the stage game may represent the basic building block of strategic analysis: the Authors employ backward induction to identify the global equilibrium starting from the partial equilibrium of the (last stage) basic game. The Authors find that in the two-stage game the production of

[5] In the current macroeconomic jargon one speaks of *small* and *modular* models (see Vines and Wills, 2018, and references therein).

mining equipment will be dominated by the miner with the most efficient hardware. The generality (and limits) of backward induction represent a well developed line of inquiry (see Binmore, 2007; Gintis, 2009) by means of which to argue about the methodological reach of such type of results. Our in-and-out-of-equilibrium strategic picture may provide a cogent perspective on such lines of aergument.

A two-stage model is also developed by Capponi et al. (2021), with a first stage in which miners invest in state-of-the-art computational resources, and a second mining stage with capacity constraints. Interestingly, despite some formal analogy of the models, Capponi et al. (2021) identify elements of decentralization that deviate from the conclusions of Arnosti and Weinberg (2021), thereby witnessing the richness of the conceptual panorama that can be embraced in game building. Among other things, the equilibria identified by Capponi et al. (2021) feature large enough miners (a scale effect) reducing their hash rate as other miners become less efficient. Our results on the connection between the functions X and Y may shed light on the generality of such results.

As is well known, the sequential pattern of backward induction reasoning can be interpreted in terms of strategic advantages (market power) as in a Stackelberg duopoly. This is the logic of the two stage game depicted by Cong et al. (2021) for the discussion of the forces that equilibrate the interaction of pools and infinitesimal miners. The model shapes an interpretation of the mean-reverting forces that seem to stabilize the pool size in terms of subgame perfect equilibria, in which the equilibrium of the mining subgame is a variation of our discussion, as another clue to the relevance of our focus. We do not proceed in a review of the published models that may enlighten the relevance of our approach; we seem to have made the point satisfactorily.

Definitely, as a key economic problem, the incentive compatibility of a protocol has been thoroughly investigated, and a number of Authors have been designing games meant to shape the incentives to start "attacks" at the expense of honest miners. The landmark contribution by Eyal and Sirer (2014) argues that the Bitcoin protocol is not incentive compatible, since an attack exists that can attract selfish miners until the colluding group becomes a majority. A taxonomy of Nash equilibria representing similar problems is under elaboration (Liu et al., 2019), and modifications of the protocol have been advocated, so as to foster honest behavior, in a mechanism design approach in which one expects Nash equilibria to solve such problems. Still, as already pointed out, it is far from guaranteed that players may find ways to coordinate on one such equilibrium (see footnote 2). In such respects, our basic level of analysis may represent a platform upon which higher levels, in the sense of Gintis (2009, subsection 8.8), may be built. An explicit quote is worth.

"We learn from modern complexity theory that there are many levels of physical existence on earth, from elementary particles to human beings, each level solidly grounded in the interaction of entities at a lower level, yet having emergent properties that […] are incapable of being explained on a lower level" (ivi, p. 162). The *more is different* paradigm of Anderson is at stake once we envision different layers of complexity of social systems;[6] in the words of Cong et al. (2021), blockchain offers researches a unique social science laboratory

[6] Compare the ecologic rationality of self-organizing systems discussed by Vernon Smith.

for testing economic theories. One can then envision a foundational noncooperative mining game supporting an architecture of higher level models targeting more complex phenomena like the network effects discussed by Catalini and Gans (2020), according to whom "the protocol can be used to incentivize behavior that builds network effects (both in terms of users and applications), ensures the network has sufficient resources available to meet demand, guarantees its security, encourages savings or spending behavior" (ivi, p. 86). Possibly, at some point of the architecture, a noncooperative foundation of cooperative notions – perhaps comparing with Rubinstein bargaining – may uncover subtle level effects parametrized by additive aggregates. The emerging literature may pave the way for such methodological advances.

References

Altman, E., Datar, M., Burnside, G., Touati, C. (2019). Normalized equilibrium in Tullock rent seeking games. Game Theory for Networks. Springer.

Altman, E., Menasché, D., Reiffers-Masson, A., Datar, M., Dhamal, S., Touati, C., El-Azouzi, R. (2020). Blockchain competition between miners: a game theoretic perspective. Frontiers in Blockchain 2, Article 26.

Andolfatto, D. (2018). Blockchain: what it is, what it does, and why you probably don't need one. Federal Reserve Bank of St. Louis Review 100 (2), 87-95.

Arnosti, N., Weinberg, M. (2018). Bitcoin: a natural oligopoly. 10th Innovations in Theoretical Computer Science Conference (ITCS 2019), Blum. A. ed., Dagstuhl, Germany. https://arxiv.org/abs/1811.08572

Arnosti, N., Weinberg, M. (2021). Bitcoin: a natural oligopoly. https://nickarnosti.com/ResearchPapers/Arnosti-Weinberg_BitcoinNaturalOligopoly.pdf

Aumann, R. J. (1987). Correlated equilibrium as an expression of Bayesian rationality. Econometrica 55 (1), 1-18.

Binmore, K. (2007). Playing for Real. Oxford University Press.

Budish, E. (2018). The economic limits of Bitcoin and the blockchain. NBER Working paper 24717.

Capponi, A., Alsabah, H., Ólafsson, S. (2021). Proof-of-Work cryptocurrencies: does mining technology undermine decentralization? Columbia University Working Paper.

Catalini, C., Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM 63 (7), 80-90.

Cong, L. W., He, Z., Li, J. (2021). Decentralized mining in centralized pools. Review of Financial Studies 34 (3), 1191-1235.

Cornes, R. (1992). Duality and modern economics. Cambridge University Press.

Dimitri, N. (2017). Bitcoin mining as a contest. Ledger 2, 31-37.

Ewerhart, C. (2017). The lottery contest is a best-response potential game. Economics Letters 155, 168-171.

Eyal, I., Sirer, E. G. (2014). Majority is not enough. Bitcoin mining is vulnerable.
Financial Cryptography and Data Security, p. 436-454. Springer.

Garay, J., Kiayias, A., Leonardos, N. (2015). The Bitcoin backbone protocol: analysis and applications.
Annual International Conference on the Theory and Applications of Cryptographic Techniques, 281-310. Springer.

Gintis, H. (2009). The Bounds of Reason. Princeton University Press.

Halaburda, H., Guillame, H., Gans, J., Gandal, N. (2021). The microeconomics of cryptocurrencies. Cesifo Working Paper 8841.

Hale, M., Kinder, T. (2021). Bitcoin falls sharply after China signals crypto crack down. Financial Times, May 19.

Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y. (2016). Blockchain mining games.
Proceedings of the 2016 ACM Conference on Economics and Computation, 365-382.

Kruppa, M. (2021). Silicon Valley bets on crypto projects to disrupt finance. Financial Times, June 3.

Jensen, M. K. (2010). Aggregative games and best-reply potentials. Economic Theory 43, 45-66.

Leshno, J. D., Strack, P. (2020). Bitcoin: an axiomatic approach and an impossibility theorem.
American Economic Review: Insights 2 (3), 269-286.

Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang Y. C., Kim, A. D. I. (2019).
A survey on blockchain: a game theoretical perspective. IEEE Access 7, 47615-47643.

Mantovi, A. (2016). Smooth preferences, symmetries and expansion vector fields. Journal of Economics 119, 147-169.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system.

Spivak, M. (1999). A Comprehensive Introduction to Differential Geometry. Vol. 1. Third Edition. Publish or Perish.

Szalay, E., Stafford, P. (2021). Bitcoin mining nears record pace as industry shrugs off China clumpdown. Financial Times, December.

Szidarovszky, F., Okuguchi, K. (1997). On the existence and uniqueness of pure Nash equilibrium in rent-seeking games.
Games and Economic Behavior 18, 135-140.

Tullock, G. (1980). Efficient rent seeking. Toward a Theory of Rent Seeking Society.
Buchanan J. S. et al. Eds. College Station: Texas A&M University Press.

Vines, D., Wills, S. (2018). The rebuilding macroeconomic theory project: an analytical assessment.
Oxford Review of Economic Policy 34 (1-2), 1-42.