LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

Bitcoin Mining as a Contest: Open Review

Author: Nicola Dimitri*†

Reviewers: Reviewer A, Reviewer B, Reviewer C

Abstract. The final version of the paper "Bitcoin Mining as a Contest" can be found in Ledger Vol. 2 (2017) 31-37, DOI 10.5915/LEDGER.2017.96. There were three reviewers who responded, none of whom have requested to waive their anonymity at present, and are thus listed as A, B, and C. After initial review (1A), the author submitted a revised submission and responses (1B). The revised submission was reviewed once again by Reviewer A, who determined that the author had adequately and substantively addressed the stated concerns, thus completing the peer-review process. Author's responses in are in bullet form.

1A. Review

Reviewer A:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

The incentive structure naturally prevents the formation of a monopoly

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Important references are missing

Please assess the article's level of academic rigor:

Excellent (terms are well defined, proofs/derivations are included for theoretical work, statistical tests are included for empirical studies, etc.)

† N. Dimitri (dimitri@unisi.it) is Professor of Economics at The University of Siena, Italy, and Corvers Chair in Innovation Procurement at the Maastricht School of Management, NL
*1N9ukmAq6EhhVigrAHiMMzSHdEwDAcLskP

Please assess the article's quality of presentation:

Good (not excellent but a long way from poor)

How does the quality of this paper compare to other papers in this field?

Top 10%

Please provide your free-form review for the author in this section.:

Nicola Dimitri examines Bitcoin mining from a game-theorectic perspective in this paper. Unlike other works on mining game theory that considered how big a block a miner should produce (e.g., "The Bitcoin Mining Game" by Nicolas Houy), this paper examines the question of how much hash power a miner should deploy, given his operating costs and other factors relevant to the decision. I believe this is the first scholarly paper to examine this question from such an angle.

Dimitri makes the novel observations that (1) bitcoin mining is more profitable if fewer independent entities are actively mining, and (2) that the incentive structure naturally prevents the formation of a monopoly, as it always remains profitable for the miner with the second lowest operating costs to mine. I found both of these results intriguing and the theory supporting them sound.

The paper is well written and clear and the topic is an important one. I suggest that Ledger accept this paper without hesitation. That said, I think there are three main ways the paper could be improved:

1. The model used is very simple. I appreciate that such a model makes possible the interesting analytic observations the author makes. Further, I intuitively believe that these observations will hold if applied to more accurate (complex) models; however, I think the author should speak to this in either the conclusion or in a new section after Section 3.

For example, presently the efficiency of bitcoin mining hardware is increasing at such a rapid pace, that the most efficient mining hardware today may not be profitable a year from now. The model assumes however that it is very easy for a miner to deploy additional hashpower at the same marginal cost, which I don't think is true today because hash power doesn't go "off line" -- it goes to the garbage dump because it will never be profitable again. However, as mining hardware becomes further "commoditized," large pools of off-line hashpower likely will exist (and in general it will be faster to quickly ramp-up one's hash power), and so I suspect the author's model is actually better targetted for how the industry may look a decade from now than it does today.

2. The importance (and elegance) of the equations derived by the author weren't obvious to me until I derived them myself (see attached document). It was in this derivation that I really understood why a mining landscape with a large number of miners will have lower profit

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

levels than a mining landscape with fewer miners. (I am actually still uncertain about the derivation of Eq. (4)). I suggest that the author include an appendix that derives Eqs. (2), (3) and (4) to aid the reader who may not be as ambitious as I was. Hopefully, my attached derivations are of use to the author in creating this appendix.

3. I think the author could discuss WHY these results are important in more detail. For example, a major concern (especially in light of Bitcoin "block size limit debate") is that larger blocks would lead to a monopoloy situation. As far as I know the work in this paper is the first to show why their is also a nature mechanism to prevent a monopoly, which counteracts this concern to some degree.

Also, there is a strong desire in certain segments of the Bitcoin community to have a "highly decentralized" mining landscape with thousands or hundreds of thousands of independent miners. This work shows that that too may be unreasonable, as it would require most miners making no profit.

The way I see it, the author has demonstrated that the mining market will always exist in a sort of "gray area" between perfect competition and a monopoly situation.

Below are some notes I made as I read through the paper:

Abstract:

"with complete information" --> "assuming complete information"?

Intro:

First paragraph is too generic. Your readers know this stuff. I suggest removing it completely, and then slightly adapting paragraph 2: for example:

"One of Bitcoin's most distinguishing features is that registration of transactions is done through the so called mining activity undertaken by some subjects."

In the first paragraph when describing the miners' incentive to include fee-paying transactions, it might be helpful to cite:

+ Nicolas Houy. "The Bitcoin Mining Game." Ledger, Vol 1, pp 53 - 68, 2016. http://ledgerjournal.org/ojs/index.php/ledger/article/view/13/59

+ Peter R Rizun. "A Transaction Fee Market Exists Without a Block Size Limit." Scaling Bitcoin Montreal, 2015. https://www.bitcoinunlimited.info/resources/feemarket.pdf

Paragraph 3: "Due to the assumption of exponential waiting time...." confusing...it's a memoryless process...the probability density function for the arrival time of the next block is a

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

decaying exponential. Is there some way to make it more clear what you mean by "exponential waiting time"?

Paragraph 4: "receiving as prize a given..." --> "receiving as the prize a given..." or "receiving the given amount of Bitcoin as the prize..."

Second-to-last paragraph: "Lowering one's marginal costs could also induce negative expcted profits by some of the miner" --> "expected" [spelling]

2. Model

X_i -> confusing for a time parameter. Can you use T or t or tau?

X = min Xi -> confusing. Explain that X is the actual block time (i.e., the miner who solves the next block first [has the minimum value of X]).

h(n) = Sum(h[i], {i, 1, n}) : can we just call this H?

For the Bitcoin protocol it is

[Reviewer A comments were accidentally truncated at this point]

Reviewer B:

Dear Ledger editors,

Thank you for having let me the opportunity to read and comment the article "The Bitcoin Mining Game" by N. Dimitri. As I will try to show in the remainder of this report, my opinion is that this article does not meet the quality standards that Ledger and the research in cryptocurrency deserve. As it is, I recommend that it be rejected.

1) One of the major problems with this article is that it looks like an application that is standard in some other field (economics in this case) and that it has been applied to Bitcoin without checking for the cryptocurrency specificity. Hence, the model is not clear to me. One the following two cases are possible and I cannot say which one the author is dealing with:

a) Short term: Miners have already invested in mining chips and mining farm buildings that are sunk costs now. For each block, they wonder if the cost of electricity (plus a few other insignificant costs in the short term) is worth mining and they can turn off a part of their chips (or turn on without an upper bound from previous investments). In this case, the model seems *about* acceptable but this is a very small part of the mining activity that is studied and conclusions like "the intrinsic structure of the mining activity seems to prevent the formation of a monopoly" are way overstated since we are only in short term and in the long term, the game would look very different (see b). Also, in reality, it should be noted that miners certainly have different quality chips (hence non constant marginal costs), they represent

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

pools, the way they mine has an impact on security issues, have choices to make regarding fees to collect and hence R is endogenous, etc... Sensitivity of the results to these simplifications should be studied or at least noticed (see remark 2).

b) Medium-Long term: in this case, the problem is much more interesting but then: miners should choose their marginal costs (they can choose their location and the chips they buy (possibly continuously, possibly with different investments prices that decrease over time)), free entry should be guaranteed (n infinite), the game should be dynamic (repeated at least) with farsighted players. Also, in this case, a feature that is fundamental with Bitcoin and that is never mentionned by the author should be considered: the mining market structure should have an impact on Bitcoin value and hence on the reward value. For security reasons, if the mining activity is to oligopolistic, Bitcoin looses value. (Maybe the author is considering such a game without defining it in the beginning of Section 3?)

In my opinion, if the author is studying a), then he should clearly say so, be much less definitive about his statements and, in my opinion, just consider his study as a preliminary step for studying b). If the author is studying b), the model is clearly not close enough to reality to be considered valid. I understand that a model cannot describe reality perfectly. Yet, in order to be published and have scientific value, a model should be precise enough to explain some data (where others don't) or should be as close to reality as one can be in order to be a first building block. In this case, none of these requirements are met and the results given in the paper may just be misleading and may just give false intuitions about reality (the way it is often done in Economics). Because Ledger is not only a journal for game theorists or economists, it is important that intuitions be published only when we, experts, have reasons to believe that the simplifications inherent to modelization are not important enough to make the results pure speculation. It is not my opinion for this article.

One chance is that the results obtained by the author are very simple to get (not considering remark 3), hence, there may be some room to go further in the direction given by this study.

2) The litterature about Bitcoin is now important in quantity and quality and Ledger is an important factor for this richness. And part of this literature is related to the mining aspect of the Bitcoin protocol (mining pools and fee market studies being certainly the most numerous). The author should really show how his article is related to the litterature and give more context. Just as a remark, the author should also be aware that an article published in Ledger this year has the same title as his! Again, this lack of context and background gives the feeling that the author is just applying a theory designed for some other framework and without making the effort to enter in the Bitcoin literature.

3) There is a problem with the Proposition: Equation 2 is false as it is since it is only true for the active miners. For the others, they meet the $h_i\geq0$ condition (that need to be clearly stated) and hence 2 is "only" an inequality in this case of non active miners. Then, n in 4 means "active" miners and is endogenous. Hence, the Proposition is true once one value for n has been assumed. Hence, the existence and uniqueness of such n that allows 4 to be satisfied for all active miners should be proved.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

Reviewer C:

I uploaded my notes on the paper, most of which were minor edits. I thought equation (3) was very elegant. The conclusions match what I saw in real life. The only unintuitive result is the anti-monopoly tendency, but the math makes sense.

I am not convinced that marginal costs are transparent, I said as much in my notes. For example, as someone who recently opened up a large-scale mining operation, I found it very hard to price the cost of rent, electricity and support. Certainly this was true if you asked me what my competitors were paying for such things. If these costs aren't transparent, does that hamper your ability to find a Nash Equilibrium? I imagine it might.

I can also tell you that the most important comparison in our mining business model was the ratio of our mining efficiency to the efficiency of the network. That is to say, we would be most successful if we could be at least as cost efficient (per hash) as the network's cost efficiency (per hash). And true to the model, this has nothing to do with R.

In practice, we knew that we would not be able to keep up with the efficiency of better miners, so we modeled this into our business. And because we didn't know any other miner's cost efficiency per hash, to measure our cost efficiency relative to the rest of the industry, we would simply use our day-to-day profitability as a gauge.

Thanks for the opportunity to review this. Please do have a look at my notes. I tried a new pdf annotator, so I'm not sure the format will work for you.

[Substantive comments from accompanying .pdf are reproduced here]

p.1 “While the optimal amount of computational power selected depends also on the reward for solving the puzzle the decision to be an active miner is only affected by the mining costs.”

In this paper, mining activity *does* depend on R insofar as R must be > 0. If R = 0, then no miner can be profitable. It is wrong to exclude this caveat (Granted, it’s such a boring caveat you might wish to save introducing the caveat later). Rizun paper’s conclusion has this same dependency.

p.2 “Since mining costs are increasing, the chosen level of power is becoming a critical issue for the Bitcoin community, which is what motivates out analysis.”

1) Show that mining costs are increasing or remove this.
2) The chosen level of power might be critical to each miner facing the decision, but it’s not clear why it’s “critical” to the Bitcoin network.

p.2 “Indeed, mining activity can be seen as a contest where participants are trying to come first in the competition for the solution of the puzzle, receiving as prize a given amount of Bitcoins as well as some fees from the other participants.”

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

Fees aren't coming from other participants, usually, but from non-participating fee payers.

p.3 "Given their limited numerosity, it is not unrealistic to think that miners could make some reasonable guesses on the computational power of the opponents."

Of course miners will have reasonable guesses as to the computational power of their opponents! organofcorti or coin.dance, for example, are sources that can tell you how much hashpower is under any one miner's control. You've switched the paragraph's focus in this sentence from knowing each others' marginal costs ci to knowing their computational power hi. If this was intentional, it needs introduction (eg "We also assume complete information on hi, that is miners know each others' computational power.") If it was not intended, then it needs to be fixed. In general, I think marginal costs are not at all transparent, which hurts the assumption of this paragraph.

p.4 "Moreover, they are decreasing in n, obtaining as highest values $E\Pi i(h) = R/4$ and $Eri(h) = 1$ at $n = 2$," but at n=1, E = R and ERoR = undefined. the point remains the same, i'm just curious as to why you'd stop at n = 2

p.5 "That is, the intrinsinc structure of the bitcoin mining game seems to prevent the emergence of a monopolistic mining activity although if the rate of return, for one of the players, would become lower than the market interest rate then a miner may find it convenient to stop mining and invest resources in alternative activities."

…which makes the whole corollary a bit weaker.

1B. Author's Response

- Before starting with my reply I would like to warmly thank the editor and the three anonymous referees for detailed and constructive comments

Reviewer A:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

- Thanks

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

The incentive structure naturally prevents the formation of a monopoly

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

- Yes

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Important references are missing

- The suggested references have now been inserted as well as some more on my side

Please assess the article's level of academic rigor:

Excellent (terms are well defined, proofs/derivations are included for theoretical work, statistical tests are included for empirical studies, etc.)

- Thanks

Please assess the article's quality of presentation:

Good (not excellent but a long way from poor)

- Thanks

How does the quality of this paper compare to other papers in this field?

Top 10%

- Thanks

Please provide your free-form review for the author in this section:

Nicola Dimitri examines Bitcoin mining from a game-theorectic perspective in this paper. Unlike other works on mining game theory that considered how big a block a miner should produce (e.g., "The Bitcoin Mining Game" by Nicolas Houy), this paper examines the question of how much hash power a miner should deploy, given his operating costs and other factors relevant to the decision. I believe this is the first scholarly paper to examine this question from such an angle.

Dimitri makes the novel observations that (1) bitcoin mining is more profitable if fewer independent entities are actively mining, and (2) that the incentive structure naturally prevents the formation of a monopoly, as it always remains profitable for the miner with the second-lowest operating costs to mine. I found both of these results intriguing and the theory supporting them sound.

- Thanks

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

The paper is well written and clear and the topic is an important one. I suggest that Ledger accept this paper without hesitation. That said, I think there are three main ways the paper could be improved:

- Thanks for this

1. The model used is very simple. I appreciate that such a model makes possible the interesting analytic observations the author makes. Further, I intuitively believe that these observations will hold if applied to more accurate (complex) models; however, I think the author should speak to this in either the conclusion or in a new section after Section 3.

For example, presently the efficiency of bitcoin mining hardware is increasing at such a rapid pace, that the most efficient mining hardware today may not be profitable a year from now. The model assumes however that it is very easy for a miner to deploy additional hashpower at the same marginal cost, which I don't think is true today because hash power doesn't go "off line" -- it goes to the garbage dump because it will never be profitable again. However, as mining hardware becomes further "commoditized," large pools of off-line hashpower likely will exist (and in general it will be faster to quickly ramp-up one's hash power), and so I suspect the author's model is actually better targetted for how the industry may look a decade from now than it does today.

- I fully agree that the model is very simple and does not have the ambition to study the dynamics. Indeed, i also fully agree that the environment is moving rapidly and what is valid today may not be valid next year. Therefore, i decided to confine myself to a short term approach for two main reasons: (1) it is hard to have realible prediction on how the ecosystem and related technology would evolve (2) in any case, whatever the state of the technology and protocol, in the short run i believe the model could capture the main drivers behind the miners' reasoning. In the paper, the longer term considerations are then discussed as the outcome of possible sequences of the short run set-up, with no explicit introduction of time in the model.

2. The importance (and elegance) of the equations derived by the author weren't obvious to me until I derived them myself (see attached document). It was in this derivation that I really understood why a mining landscape with a large number of miners will have lower profit levels than a mining landscape with fewer miners. (I am actually still uncertain about the derivation of Eq. (4)). I suggest that the author include an appendix that derives Eqs. (2), (3) and (4) to aid the reader who may not be as ambitious as I was. Hopefully, my attached derivations are of use to the author in creating this appendix.

- Thanks for kind words, i now introduced an appendix with the equations derivation

3. I think the author could discuss WHY these results are important in more detail. For example, a major concern (especially in light of Bitcoin "block size limit debate") is that larger blocks would lead to a monopoloy situation. As far as I know the work in this paper is the first to show why their is also a nature mechanism to prevent a monopoly, which counteracts this concern to some degree.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

- As for block size i now introduced few considerations in the conclusions

Also, there is a strong desire in certain segments of the Bitcoin community to have a "highly decentralized" mining landscape with thousands or hundreds of thousands of independent miners. This work shows that that too may be unreasonable, as it would require most miners making no profit.

- The word “may” is crucial. The analysis suggests that it all depends on the costs structure. If miners’ marginal costs are relatively similar then they would deploy similar computational power and there could be a larger number of active miners. If marginal costs are sufficiently different then a lower number of miners is likely.

The way I see it, the author has demonstrated that the mining market will always exist in a sort of "gray area" between perfect competition and a monopoly situation.

- I agree on the interpretation. It looks like that

Below are some notes I made as I read through the paper:

Abstract:

"with complete information" --> "assuming complete information"?

- Done

Intro:

First paragraph is too generic. Your readers know this stuff. I suggest removing it completely, and then slightly adapting paragraph 2: for example:

"One of Bitcoin's most distinguishing features is that registration of transactions is done through the so called mining activity undertaken by some subjects."

- I actually left this generic part, since i thought a broad introduction was needed anyway, though very short. If you really think it should be eliminated do let me know.

In the first paragraph when describing the miners' incentive to include fee-paying transactions, it might be helpful to cite:

+ Nicolas Houy. "The Bitcoin Mining Game." Ledger, Vol 1, pp 53 - 68, 2016. http://ledgerjournal.org/ojs/index.php/ledger/article/view/13/59

+ Peter R Rizun. "A Transaction Fee Market Exists Without a Block Size Limit." Scaling Bitcoin Montreal, 2015. https://www.bitcoinunlimited.info/resources/feemarket.pdf

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

- Inserted

Paragraph 3: "Due to the assumption of exponential waiting time...." confusing...it's a memoryless process...the probability density function for the arrival time of the next block is a decaying exponential. Is there some way to make it more clear what you mean by "exponential waiting time"?

- I now rephrased the sentence and think should be clearer

Paragraph 4: "receiving as prize a given..." --> "receiving as the prize a given..." or "receiving the given amount of Bitcoin as the prize..."

- Done

Second-to-last paragraph: "Lowering one's marginal costs could also induce negative expcted profits by some of the miner" --> "expected" [spelling]

- Done, thanks

2. Model

X_i -> confusing for a time parameter. Can you use T or t or tau?

- As I define it in the text, the subscript i is not for time but for a generic miner. Indeed X_i stands for the random variable expressing the waiting time to obtain the puzzle solution by miner i.

X = min Xi -> confusing. Explain that X is the actual block time (i.e., the miner who solves the next block first [has the minimum value of X]).

- See the above clarification on X_i

h(n) = Sum(h[i], {i, 1, n}) : can we just call this H?

- Good point but decided to leave X_i because I need a notation for the total computational power deployed as a function of the number of active miners.

For the Bitcoin protocol it is

[Reviewer A comments were accidentally truncated at this point]

Reviewer B:

Dear Ledger editors,

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

Thank you for having let me the opportunity to read and comment the article "The Bitcoin Mining Game" by N. Dimitri. As I will try to show in the remainder of this report, my opinion is that this article does not meet the quality standards that Ledger and the research in cryptocurrency deserve. As it is, I recommend that it be rejected.

- Sorry that was not found of interest

1) One of the major problems with this article is that it looks like an application that is standard in some other field (economics in this case) and that it has been applied to Bitcoin without checking for the cryptocurrency specificity.

- Interesting point which deserves a clarification. Contest theory is wide spread in social sciences as contests are wide spread in real life. To me bitcoin mining is exactly a contest, because victory is probabilistic and everyone has to spend to participate. This is the only reason why I proposed to model mining as a contest. I'm not sure I agree that it does not capture the criptocurrency specificity. In no other economic context that I know money supply is ruled through a competition and emitted in the form of a reward to the competitors.

Hence, the model is not clear to me. One the following two cases are possible and I cannot say which one the author is dealing with:

a) Short term: Miners have already invested in mining chips and mining farm buildings that are sunk costs now. For each block, they wonder if the cost of electricity (plus a few other insignificant costs in the short term) is worth mining and they can turn off a part of their chips (or turn on without an upper bound from previous investments). In this case, the model seems *about* acceptable but this is a very small part of the mining activity that is studied and conclusions like "the intrinsic structure of the mining activity seems to prevent the formation of a monopoly" are way overstated since we are only in short term and in the long term, the game would look very different (see b). Also, in reality, it should be noted that miners certainly have different quality chips (hence non constant marginal costs), they represent pools, the way they mine has an impact on security issues, have choices to make regarding fees to collect and hence R is endogenous, etc... Sensitivity of the results to these simplifications should be studied or at least noticed (see remark 2).

- Many thanks for this good point. It is correct that the model is based on sunk investments being already made, and that's why a concentrate only on variable costs. I also agree that *R* will be endogenously determined by the fees, and I further agree on the other observations. But I still believe that in the short run the model captures the main forces driving decisions. As said, the medium-long run considerations in the paper are made with reference to a sequence of short run set-ups, rather than by a formal introduction of the time subscript

b) Medium-Long term: in this case, the problem is much more interesting but then: miners should choose their marginal costs (they can choose their location and the chips they buy

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

(possibly continuously, possibly with different investments prices that decrease over time)), free entry should be guaranteed (n infinite), the game should be dynamic (repeated at least) with farsighted players.

- Very good point. This i intend to pursue in future research in fact.

Also, in this case, a feature that is fundamental with Bitcoin and that is never mentionned by the author should be considered: the mining market structure should have an impact on Bitcoin value and hence on the reward value. For security reasons, if the mining activity is to oligopolistic, Bitcoin looses value. (Maybe the author is considering such a game without defining it in the beginning of Section 3?)

- Good point too, but my goal was simply limited to enquiring the economic profitability of the mining activity, as electricity bills for mining seem to be increasing.

In my opinion, if the author is studying a), then he should clearly say so, be much less definitive about his statements and, in my opinion, just consider his study as a preliminary step for studying b).

- I now say this more explicitly in the introduction and conclusions

If the author is studying b), the model is clearly not close enough to reality to be considered valid. I understand that a model cannot describe reality perfectly. Yet, in order to be published and have scientific value, a model should be precise enough to explain some data (where others don't) or should be as close to reality as one can be in order to be a first building block. In this case, none of these requirements are met and the results given in the paper may just be misleading and may just give false intuitions about reality (the way it is often done in Economics).

- I see the point but if readers agree on the essential variables considered in the model then perhaps the work can give some broad, initial, insights on the major forces at stake for economic profitability of mining. Then the model could be further enriched and elaborated to test how robust are the main conclusions when additonal elements are also considered.

Because Ledger is not only a journal for game theorists or economists, it is important that intuitions be published only when we, experts, have reasons to believe that the simplifications inherent to modelization are not important enough to make the results pure speculation. It is not my opinion for this article.

- Fully agree and I was happy to read that the other two reviewers found the model and its conclusions consistent with what they think and reason as experts. For what I could tell this was also the case when I recently presented the paper to a specialised conference.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

One chance is that the results obtained by the author are very simple to get (not considering remark 3), hence, there may be some room to go further in the direction given by this study.

- Yes and I plan to do that in future work

2) The litterature about Bitcoin is now important in quantity and quality and Ledger is an important factor for this richness. And part of this literature is related to the mining aspect of the Bitcoin protocol (mining pools and fee market studies being certainly the most numerous). The author should really show how his article is related to the litterature and give more context. Just as a remark, the author should also be aware that an article published in Ledger this year has the same title as his! Again, this lack of context and background gives the feeling that the author is just applying a theory designed for some other framework and without making the effort to enter in the Bitcoin literature.

- I agree. I noticed the article with the same title only after I submitted the paper, which now has a different title. As for mining pools I am certainly aware of them, and some related literature, stemming from the celebrated Eyal and Emin paper on the forking attack. However, whether or not the miner in my model is an individual or a pool the short term reward will still be *R*, regardless of the interpretation. Obviously, a pool will have more computational power and, plausibly, a lower marginal cost. Notice that unless there would be liquidity constraints for the miners, in the model all actve miners are self-financing since, in case, they would be able to borrow and return the money over time to the lender because on average they enjoy positive profits.

3) There is a problem with the Proposition: Equation 2 is false as it is since it is only true for the active miners. For the others, they meet the $h_i\geq0$ condition (that need to be clearly stated) and hence 2 is "only" an inequality in this case of non active miners.

- Indeed i only consider active miners. Therefore, equation 2 is a necessary condition for a profit maximising miner to be active

Then, n in 4 means "active" miners and is endogenous. Hence, the Proposition is true once one value for n has been assumed. Hence, the existence and uniqueness of such n that allows 4 to be satisfied for all active miners should be proved.

- Good point but I believe what I'm doing is correct. Indeed, in the paper I assume that there are n active profit maximisers miners and look at the conditions which characterise their behaviour at a Nash Equilibrium

Reviewer C:

I uploaded my notes on the paper, most of which were minor edits. I thought equation (3) was very elegant. The conclusions match what I saw in real life.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

- Thanks. I am very pleased to read so. I sent back your annoted version with my answers

The only unintuitive result is the anti-monopoly tendency, but the math makes sense.

- As said, the model suggests that cutting down one's marginal costs can exclude other miners but not all of them. Yet monopoly can take place if the outside (to bitcoin) investment options are more rewarding.

I am not convinced that marginal costs are transparent, I said as much in my notes. For example, as someone who recently opened up a large-scale mining operation, I found it very hard to price the cost of rent, electricity and support. Certainly this was true if you asked me what my competitors were paying for such things. If these costs aren't transparent, does that hamper your ability to find a Nash Equilibrium? I imagine it might.

- Good point. In case information on the other miners' costs are not available or in any case uncertain, the effort deployed at the nash equilibrium of the complete information model can be interpreted as follows. Whatever the investment made by the active miners leading to positive profits, on average it can not be too different from the one in the model

I can also tell you that the most important comparison in our mining business model was the ratio of our mining efficiency to the efficiency of the network. That is to say, we would be most successful if we could be at least as cost efficient (per hash) as the network's cost efficiency (per hash). And true to the model, this has nothing to do with R.

- I'm very pleased to read so

In practice, we knew that we would not be able to keep up with the efficiency of better miners, so we modeled this into our business. And because we didn't know any other miner's cost efficiency per hash, to measure our cost efficiency relative to the rest of the industry, we would simply use our day-to-day profitability as a gauge.

- Very good

Thanks for the opportunity to review this. Please do have a look at my notes. I tried a new pdf annotator, so I'm not sure the format will work for you.

- Thanks again. Please do look at my answers to your comments in the annoted pdf version

[Substantive comments from accompanying .pdf are reproduced here]

p.1 "While the optimal amount of computational power selected depends also on the reward for solving the puzzle the decision to be an active miner is only affected by the mining costs."

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

In this paper, mining activity *does* depend on R insofar as R must be > 0. If R = 0, then no miner can be profitable. It is wrong to exclude this caveat (Granted, it's such a boring caveat you might wish to save introducing the caveat later). Rizun paper's conclusion has this same dependency.

- Done.

p.2 "Since mining costs are increasing, the chosen level of power is becoming a critical issue for the Bitcoin community, which is what motivates out analysis."

1) Show that mining costs are increasing or remove this.
2) The chosen level of power might be critical to each miner facing the decision, but it's not clear why it's "critical" to the Bitcoin network.

- Done.

p.2 "Indeed, mining activity can be seen as a contest where participants are trying to come first in the competition for the solution of the puzzle, receiving as prize a given amount of Bitcoins as well as some fees from the other participants."

Fees aren't coming from other participants, usually, but from non-participating fee payers.

- Done.

p.3 "Given their limited numerosity, it is not unrealistic to think that miners could make some reasonable guesses on the computational power of the opponents."

Of course miners will have reasonable guesses as to the computational power of their opponents! organofcorti or coin.dance, for example, are sources that can tell you how much hashpower is under any one miner's control. You've switched the paragraph's focus in this sentence from knowing each others' marginal costs ci to knowing their computational power hi. If this was intentional, it needs introduction (eg "We also assume complete information on hi, that is miners know each others' computational power.") If it was not intended, then it needs to be fixed. In general, I think marginal costs are not at all transparent, which hurts the assumption of this paragraph.

- complete information on the marginal costs at the Nash Equilibrium implies also on computational power, since hi depends on marginal costs, as well as on the number of miners and the reward

p.4 "Moreover, they are decreasing in n, obtaining as highest values $E\Pi i(h) = R/4$ and $Eri(h) = 1$ at $n = 2$," but at n=1, E = R and ERoR = undefined. the point remains the same, i'm just curious as to why you'd stop at n = 2

- Good point. Indeed, I now specify that the analysis holds for at least two active miners, and addedd a new paragraph to discuss one miner.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96

p.5 “That is, the intrinsinc structure of the bitcoin mining game seems to prevent the emergence of a monopolistic mining activity although if the rate of return, for one of the players, would become lower than the market interest rate then a miner may find it convenient to stop mining and invest resources in alternative activities.”

…which makes the whole corollary a bit weaker.

- to some extent. yet remains true that reducing one's marginal cost could never induce all other miners to have negative profits

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2017.96