Önder Gürcan <onder.gurcan@gmail.com>

TRUST2018 notification for paper 5

TRUST2018 <trust2018@easychair.org> 22 Mayıs 2018 08:50
Alıcı: GÜRCAN Onder <Onder.GURCAN@cea.fr>

Dear Önder,

Thank you for your submission to the TRUST 2018 workshop. We regret to inform you that your paper, Sustaining the Trust in Bitcoin by Incentivizing Solo Mining, has not been accepted for presentation at the workshop. We attach the reviews below for information.

Kind Regards,

Murat Sensoy, Robin Cohen and Timothy Norman

----------------------- REVIEW 1 ---------------------
PAPER: 5
TITLE: Sustaining the Trust in Bitcoin by Incentivizing Solo Mining
AUTHORS: Önder Gürcan and Mustafa Safa Ozdayi

Overall evaluation: -1 (weak reject)

----------- Overall evaluation -----------
This paper studies the impact of rewarding mechanisms on incentivizing solo miners. The paper takes existing Bitcoin and Fruitchain protocols for their analysis and defined two metrics (fairness and return rate) to evaluate those protocols.

Overall the paper is well written. However, I do not find enough contributions other than defining "return rate" as a metric to evaluate the two protocols. I am not convinced with the rationale behind the definition of this new metric. The authors managed to implement both protocols in a agent-based simulation framework to compare the Bitcoin and Fruitchain protocols. But, the authors of Fruitchain protocols already proved the significance of their protocol over Bitcoin. Therefore, I do not see the significance of this work and I doubt that the paper will generate enough interest in this workshop.

Authors should pay attention to the Bibliography as many of their references do not provide details of the papers, e.g. conference name missing. They might think of putting more effort into assessing the levels of trust of the miners rather than just claiming "more suitable for sustaining the trust".

----------------------- REVIEW 2 ---------------------
PAPER: 5
TITLE: Sustaining the Trust in Bitcoin by Incentivizing Solo Mining
AUTHORS: Önder Gürcan and Mustafa Safa Ozdayi

Overall evaluation: 0 (borderline paper)

----------- Overall evaluation -----------
The authors present an study of the differences between the two existing rewarding mechanisms proposed in two cryptocurrencies, namely Bitcoin and Fruitchain. To this end, they defined two properties for miners: fairness and return rate, and carry out simulations looking at the results of each cryptocurrency with regards to these properties.

I think the paper discusses the important aspect of the rewarding mechanisms of different cryptocurrencies, but I don't see a clear link to trust.

Some questions that may help the authors in the future:

- Why Bitcoin and Fruitchain? Are there other cryptocurrencies? The choice of Bitcoin seems obvious, but not Fruitchain.

- To what extent the metrics help predict the behaviour of real miners / users?

----------------------- REVIEW 3 ---------------------
PAPER: 5
TITLE: Sustaining the Trust in Bitcoin by Incentivizing Solo Mining
AUTHORS: Önder Gürcan and Mustafa Safa Ozdayi

Overall evaluation: -1 (weak reject)

----------- Overall evaluation -----------
The paper compares two blockchain proposals: Bitcoin and Fruitchain using two metrics: fairness and return rate. The main contribution is the simulation part, and the results show that Bitcoin and Fruitchain have the same fairness result, but the return rate of Fruitchain is better than Bitcoin. The paper claims then that trust will be sustained in Fruitchain because it has a better incentivizing mechanism.

The topic addressed in this paper is highly interesting and relevant for the workshop. However, the paper has some limits. The main one is the significance of the results. The interesting and somehow new part is supposed to be the simulation. However, no real data has been used to back the conclusions. Only two minors are being considered, which makes the results statistically insignificant and cannot be generalized. based on the definitions of Bitcoin and Fruitchain, the results are not surprising. It is expected that Fruitchain provides better opportunities for small minors.

The paper also needs proofreading. It has many typos and some sentences are not complete, which makes the paper hard to follow.

Minor issues

Section 1.3 and 1.4 should be merged.

The fruitchain concept is not well explained. For instance, the notion of difficulty is not well explained. The variable D is not introduced.

In the equation of the block minor, I think it should be R_i.c_1 instead of (1-c_1).

Using equality in Def. 1 makes the fairness constraint very hard. maybe an approximation would be better.
Also, the fairness in this way is binary, fair or unfair. We cannot quantify fairness and measure it degree as defined in Def. 1.

"... and ignore the fixed reward as Fruitchain only takes fees into account". This sentence is not clear; both approaches consider fixed (static) reward.

There is lack of consistency. In Section 4.1, it was indicated that p_f < 1, but in Section 4.2, p_f = 1.

If the cost is fixed (10% of the gain), there is no need to show it the figures. Only the gain is important.

I don't understand Fig. 5 a. The cost is said to be 10% of the gain, but in this figure, it's not the case. The cost is higher than the gain.

Examples of typos:

Such participation --> Such a participation

... on in Bitcoin, and may result decreased participation of users [5].

... to the underlying blockchain, and may result, decreased user participation

Section focus on the metrics to analyze incentives --> Section 3 focuses ...

In the organization paragraph (Section 1.5) is poorly written. Sections numbers are not given in many places and some sentences are not complete.

Section 2.1. (Minor node) \Theta_m --> \Theta_n

The cryptographic puzzle is tried be solved by ...

---------------------- REVIEW 4 ---------------------
PAPER: 5
TITLE: Sustaining the Trust in Bitcoin by Incentivizing Solo Mining
AUTHORS: Önder Gürcan and Mustafa Safa Ozdayi

Overall evaluation: -2 (reject)

----------- Overall evaluation -----------
As a first comment, although there are many widely-used, mainstream terminologies, this manuscript uses a totally different set of terms.

Secondly, the manuscript is heavily built on another unpublished work, i.e., reference [1]. I cannot find an available version of [1] online, which means there is no way to check the credibility of some of the claims. In particular, the two formula in subsection 2.4.

Most importantly, the manuscript is not directly related to trust at all.
Trust in blockchain protocols is a general term. It is generally used in decentralized systems, but not formally defined as a metric in the Bitcoin system, as far as I know.

-- in subsection 2.1, the use of memory pool Theta_n and so on is unnecessary. They are rarely used in the rest of the paper. In addition, the mainstream terminologies for them are unspent transactions and unspent transaction output (UTXO), rather than unconfirmed transactions and memory pool, respectively. A definition of Join and Leave is also unnecessary.

-- in the Miner Node paragraph, "the Coinbase transaction is special transaction that collects and spends any transaction fees paid by transactions included in a block" is inaccurate. The Coinbase transaction is a special transaction without input and the output is the block miner's public address. It is a chance for the block miner to collect the reward on successfully mining a block. The transaction fees could be direct to the same public address, but the Coinbase transaction itself does not spend any transaction fees.

-- the last word in subsection 2.2, it should be "blockchain height" not the "blockchain head."

-- subsection 2.4 is inadequately written. No matter the authors are referring to the model in an unpublished manuscript [1] or the published version [9], the current submission should be self-contained. However, subsection 2.4 is not sufficient for readers to understand their Fruitchain protocol.

-- section 3.1, the definition of fairness is nothing but that a miner's expected reward is proportional to its computational power, against the computational power of the entire economy. This is the mild understanding of the Bitcoin protocol as well.

-- section 3.2, I do not think there is a need for such a ratio. It is quite standard to use the variance of mining rewards as a metric to measure the need for mining pools. This is also mentioned in the original Fruitchain paper [9].