Gmail Pranav Unni <pranavcosmos4@gmail.com>

# CBT'2023 notification for paper 3991

**CBT'2023** <cbt2023@easychair.org> Mon, Jul 31, 2023 at 8:20 PM
To: Pranav Unni <pranavcosmos4@gmail.com>

Dear Pranav,

It is our pleasure to inform you that your paper

Designing a Private Asynchronous On-Chip Blockchain & Consensus Algorithm towards Secured Data Management

has been ACCEPTED for presentation at CBT 2023, and ACCEPTED for publication in the corresponding post-proceedings of the event (LNCS volume that will appear after the conference).

Below are the (anonymous) referees' comments about your paper.

Please confirm receipt of this email including the (possibly updated) title and the complete list and affiliations of the authors, together with a proof of regular registration at the event (workshops), already available at:

https://esorics2023.org/attend/registration/

As soon as we get back your confirmation, we will distribute the list of accepted papers in the website.

Please also confirm us the name of the author that will attend the workshop and present your work. Otherwise, the paper will be withdrawn from the program.

Kindly send your confirmation, camera-ready PDF and details to:

cbt2023@easychair.org

You will then receive a second message, with the precise instructions and guidance on how we plan to prepare the workshop programme, collection of sources and copyright form for the LNCS volume, (all this information will be collected using Springer's EquinOCS system, later on).

The page limit will be 17 pages (including bibliography) and is strict. Please follow strictly the author instructions of Springer when preparing the final version:

https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines

Appendices shall be removed from the final camera-ready version of your paper.

Looking forward to receiving your confirmation.

Kind Regards,

CBT 2023 Chairs

SUBMISSION: 3991
TITLE: Designing a Private Asynchronous On-Chip Blockchain & Consensus Algorithm towards Secured Data Management

---------- REVIEW 1 ----------
SUBMISSION: 3991
TITLE: Designing a Private Asynchronous On-Chip Blockchain & Consensus Algorithm towards Secured Data Management
AUTHORS: Dr.Soumya Banerjee, Dr. Samia Bouzefrane and Pranav Unni

---------- Overall evaluation ----------
This paper outlines a new reputation based consensus algorithm (rrPoA) in which a dynamic reputation score is calculated for all nodes in a IoT network. The consensus algorithm is designed primarily for low-powered IoT devices that cannot run heavyweight protocols such as PoW or PoS. The authors provide a number of equations which show in detail as to how the reputation is calculated and how the algorithm adapts in the face of malicious nodes in the network. The authors also run a number of experiments that measure the performance of the consensus algorithm with 100% trusted nodes, 50% trusted nodes and 20%

malicious nodes in the network. The results seem to match the expectations of the algorithm performance as assumed by the authors.

One of the aspects of the protocol that I could not fully grasp was in relation to the use of PUFs in the consensus algorithm. It was also not clear as to what the security keys which are stored on the blockchain are used for. I think this aspect should be clarified in a bit more detail.

---------- REVIEW 2 ----------
SUBMISSION: 3991
TITLE: Designing a Private Asynchronous On-Chip Blockchain & Consensus Algorithm towards Secured Data Management
AUTHORS: Dr.Soumya Banerjee, Dr. Samia Bouzefrane and Pranav Unni

---------- Overall evaluation ----------
This paper considers blockchain protocols for IoT devices. It proposes to use a special type of consensus based on Proof of Authority in order to deal with malicious parties in the network. The proof of authority defines authorized nodes in the network that will be used as leaders to establish consensus. These are nodes that have a positive above average reputation. In each round of the protocol, a new leader is chosen in a round robin fashion among authorized nodes. The authors evaluate their protocol based on 50 IoT devices and show that the reputation score behaves correctly.

The paper is well written and motivates the new type of consensus well based on the application. The idea to use the round robin proof of authority for IoT devices is interesting and seems to be working well in practice. I believe that one weakness of this paper are the evaluation results, which only show the correctness of the algorithm, but do not compare it to other consensus protocols. The authors mention for example the proof of authentication, which is normally used in such devices. It would have been nice to see a comparison in energy usage of both protocols to better understand the trade-off between fault-tolerance and energy consumption in such devices. Overall, I believe that the paper could be interesting for the CBT community and propose a weak accept.