Review: Towards Private Active Choreographies on Public Blockchain

The paper “Towards Private Active Choreographies on Public Blockchain” proposed by Henry Bergstroem and Jan Mensch addresses the lack of privacy regarding untrusted process executions on blockchain technologies. Their goal is to create a communication pattern on the blockchain, that can enforce the flow of active choreographies, an extension to the BPMN 2.0 choreography standard, as well as restrict the visibility of information to the corresponding participants.
To achieve this they introduced a scheme that keeps untrusted process executions private on the Model, Communication and Content Level. The scheme works with visibility circles that define visibility constraints for all participants. Only members within a circle can read each other messages. In order to protect the Model Layer, the process logic has to be executed off-chain. However, the scheme can still enforce the flow of the process using a consensus algorithm that is based on digital signatures of each participant to confirm or reject a certain state of the process.
To evaluate the approach they implemented a simplified version of their approach using a local instance of the Ethereum blockchain. This approach contributes a private way to execute untrusted active choreographies on public blockchains.

The paper presents the contribution in a well structured form. The chapters build on each other in a logical way including well placed cross references and provide the reader with the necessary information to understand the approach. The language is comfortable to read while still explaining the approach in a scientific way. The use case example in section 3 provides a great illustration of the approach through the whole section. In addition to it, the idea is also founded by many references to related topics.
However, there are still some points that can be improved. On one hand the paper does not provide a description of the term blockchain although it is a significant component of the approach. The term should be introduced briefly either in section 2 explaining the background or in the introduction section 1. In terms of terminology, the term asymmetric has been mistaken by the term asynchronous when talking about the key-pairs in section 3.2.
On the other hand the labels of the assumptions explained in section 3.1 are difficult to resolve when encountering them later in other sections. An additional table could improve the look up process for the corresponding assumption.
Because section 4 seems to be the evaluation part of the paper, there should be a statement that evaluates the approach relating to implementation or time overhead for example. If the section is the evaluation of this paper, it should have the title “Evaluation” and it should be a major part of the justification or falsification of the feasibility of the approach.
Finally section 6 being the conclusion of the paper should be extended with a brief summary of the whole approach in combination with ideas how the approach could be improved in the future.

Some minor remarks concerning the readability are missing introductions in the main section 3 and section 5. Furthermore the understandability of relation of the labels sym1 and sym2 in section 3.2 referring to the symmetric keys and therewith to the visibility circles could be improved by using the labels of the corresponding participants within the circle instead of 1 and 2.