Review: Towards Private Active Choreographies on Public Blockchain

Authors: Henry Bergstroem and Jan Mensch

Reviewer: Maximilian Völker

Content Summary

The approach presented in this paper aims for more privacy in choreographies. The protection includes the model level (a), as well as the type and origin of exchanged messages (b) and their content (c). The paper starts with a short introduction motivating the need for more privacy, followed by foundations needed to understand the solution. Additionally, some concepts are mentioned that the authors considered at the beginning.

Based on assumptions, the approach addressing the three mentioned issues is explained: In order to hide the messages' contents (c), the concept of "Circles" is introduced. By this, each collaborator can only read messages which are sent by members of the same circle because a symmetric key (belonging to the circle) is used for encrypting the message. In order to protect the model (a), each participant is in possession of a "custom" model, containing only as much information as needed for execution. Details of this representation are defined to be out of scope. To advance the state of the instance, a consensus mechanism is provided. Subsequently, the overall process of sending messages is described, where also (b) is addressed. A new message is symmetrically encrypted with the circle's key and then each participant of the choreography must sign the hash of this message with a private key in order to consent to the state-change. A smart contract on the blockchain validates all signatures and confirms the message and therefore the state-change of the model.

Then, a prototypic implementation is described, followed by a discussion about drawbacks of the approach and how to address them. The paper is closed by alternative approaches and a short summary.

Major Remarks

The introduction and background chapters motivate your approach very well and provide sufficient information to the reader in order to understand your explanations later on. In chapter 2.3 – Privacy Enhancing Technologies, you present the techniques you considered in clear and short way, but I wondered what the drawbacks of *SMPC*, *SNARKS* and *Parity* are and why you did not build on one of these approaches (you mentioned reasons for the other approaches though). In chapter 5.2 you take up these approaches and evaluate them further, but when reading chapter 2 it left me a bit confused, as they seemed to be interesting starting points to consider.

The approach chapter is well written and very comprehensive. I found myself sometimes a bit overwhelmed by the thirteen assumptions you made and referenced. Maybe it is possible to reference to them as groups (e.g. a+b+c as trust, d+e+f as secrecy). The subsubsection titles could be improved by using a more consistent logic, "Protecting the Model Layer" is very clear and understandable but follows another naming convention than "Circles" and "Consensus Mechanism". In the explanatory text to figure 3 you describe the schema of the consensus mechanism and even though you stated in the beginning that the communication is done counterclockwise, I missed the information that *P*, after signing the hash, passes on the message to *C* to sign and so on (but your figure illustrates this well).

Your discussion is very good to read, too. It answers many questions and shows that you pondered about many aspects of your approach. Only in the subsection about “Knowledge of progress […]” I wondered how nodes can have different levels of importance for giving their consent. I thought each node has to give its consent to each message in an equal way? As already mentioned, for the “alternative approaches” I would have liked a hint in chapter 2.3, that you will elaborate on these techniques later.

Minor Remarks

- Some more formal or wording-related issued are highlighted directly in the paper.
- Additionally, the part where you describe the structure of the paper starts with more or less complete sentences but in the end, they somehow miss verbs, which stands out a bit.
- Consider replacing figure 1 by an image with a higher resolution, as it looks a bit blurry when printed out.
- You use citations in the abstract, which is, at least after my knowledge, quite uncommon. I think, citing and referencing in the introduction should be sufficient as long as you do use direct quotes.
- The first sentence in “Introduction” matches the first sentence of the abstract exactly.

Summary

All in all, I really enjoyed reading your paper. It is very well readable and understandable. Even though it is a quite theoretic topic, it was easy to follow, and you did not elaborate too much on finer details giving a good overview of your approach. I also liked that you took the disadvantages into account and proposed possible counter measurements.