Towards private Active Choreographies on public blockchain

Henry Bergstroem[1] and Jan Mensch[1,2]

[1] Hasso-Plattner-Institut, Prof.-Dr.-Helmert-Straße 2-3, 14482 Potsdam, Germany
bergstroem@uni-potsdam.de
[2] University of Potsdam, Am Neuen Palais 10, 14469 Potsdam, Germany
jan.mensch@uni-potsdam.de

Abstract. Make it clear that we are talking about an implementation of ACs, not the BPMN standard!
We are working towards implementing a realization of ACs, that implements some visibility constraints that you would usually see in real-world applications, like confidential data and transactions.

1 Introduction

privacy in inter-organizational process execution.

The goal of this paper is to explore the notions of privacy and visibility with regards to untrusted execution of choreographies on the blockchain.

2 Background and Motivation

2.1 Blockchain-Based choreographies

basically a more specific Introduction
what did Ingo do?
what did Jan do?

2.2 Privacy Considerations

However, while discussing privacy issues, Weber et al. and Ladleif did not take any measures to actually implement them...
talk about layers. Why are they important?
Motivation!

2.3 Privacy Enhancing Technologies

talk about technologies that are currently out there
try to be a bit more high-level, not too focused on possible solutions

3 Approach

3.1 Assumptions and Scenario

do I need this? Am I referring to any of the specific points later on?

Before introducing our schema, we would like to mention the assumptions on which our proposal is based on. Each premise is marked for potential later reference.

Assumptions about the participating parties: *a* There are several parties which want to collaborate. These parties have *b* neither trust in each other nor *c* trust in any third party. They furthermore *d* want to keep their business process secret, *e* hide with whom they are collaborating and *f* hide what messages are exchanged during the collaboration. Since the parties distrust each other they also *g* only want to share messages with the entities that have to see them and keep them secret from the others. Each party *f* is "honest but curious" [**ref**]. They follow the protocol, but will try to collect as much information as possible.

Mention $x \rightarrow$ to layers from Section 2.1

Further assumptions: All data that is *g* processed on the blockchain is considered public. It is *h* possible to convert a business process into a program or state-machine in order for parties to determine that validity of a state change.

3.2 Proposed Schema

our schema

4 Evaluation

implementation

5 Discussion

- shortcomings
- How could mentioned in Section 2.3 improve Section 4?
- How did it work out in the end?
- private blockchain
- Parity
- future work

6 Conclusion

final words

References