ELASTIC Project
Secure Systems Group, Aalto University

Xuan-Huy Ngo, Lachlan J. Gunn
Contact: *huy.ngo@aalto.fi, lachlan@gunn.ee*

WebAssembly Migration with Fair Exchange

Background

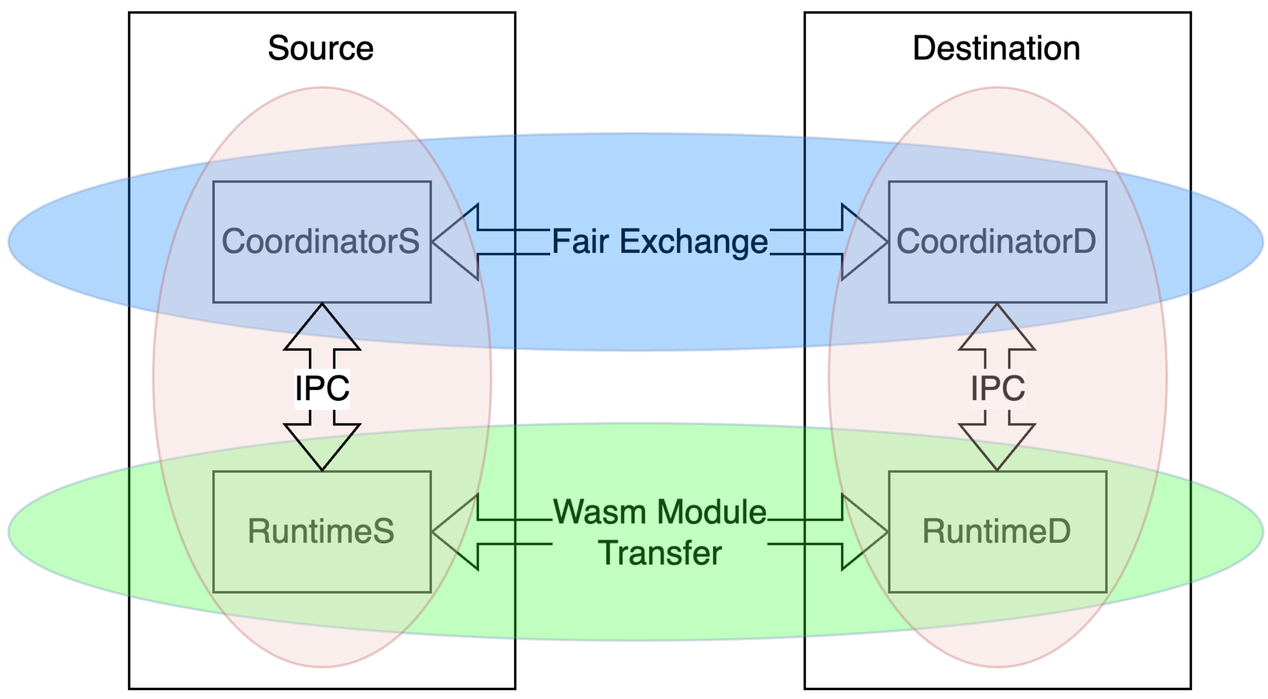
- WebAssembly (Wasm): portable binary instruction format offers sandboxed execution environment
- Fair Exchange: ensures fairness among parties where none of the parties can take any advantage over the others

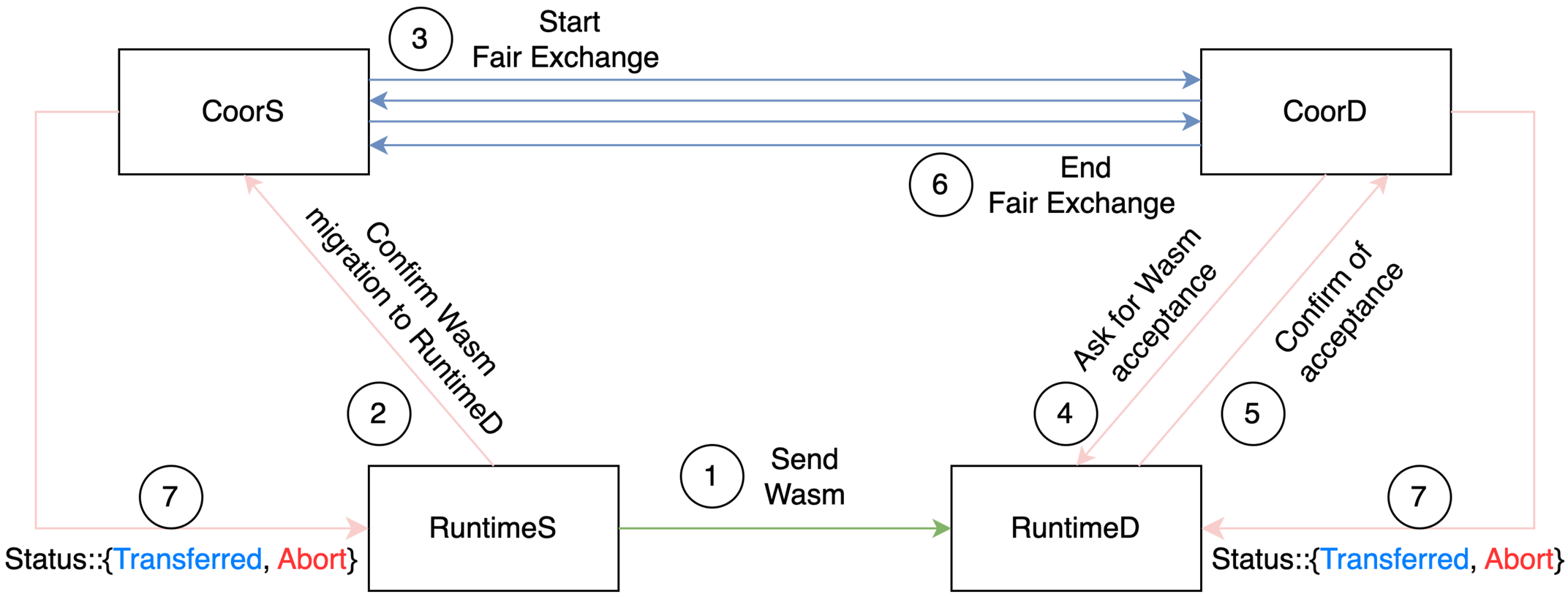
Objectives

- Practical protocol of migrating module to different place while persisting their states
- Guarantee atomicity property of a module
- Non-repudiation of module migration with CONFIRM message
- Module always ends up in exactly one place

Optimistic Fair Exchange

- If both parties behave correctly and the fair exchange completes, no involvement of a third party is required
- If there is disruption, Trusted Third Party (TTP) is required to resolve conflict and enforce fairness





[1] Asokan, Nadarajah, Victor Shoup, and Michael Waidner. "Optimistic fair exchange of digital signatures." *International Conference on the Theory and Applications of Cryptographic Techniques*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998.
[2] Geisler, Wojciech. "Reliable migration of WebAssembly trusted applications." (2022).

Aalto University
Co-funded by the European Union
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.