Work Stages for Holistic Specs

1: Focal II

define (small step version from Swapsies)

🔶

5: Chainmail II

define (as in current POPL-aimed paper)

🔶

30: Better names for terms

31: Write explanations

2: Focal II execution properties
formulate lemmas
connectivity-begets etc... 🤔🤔

🔶

6: Form. Policies

express OCAP and some contracts' policies in Chainmail II 🤔

🔶

12: Study competition

11: Show 1-2-6 to competition

our position wrt IRIS and deVries 🔶

3: prove execution properties
by hand 🤔🤔

🔺

7: Prove Policies

that code adheres to policies
by hand 🤔🤔

🔺

13: Logic for Policies

develop a logic for proofs of adherence to policies 🤔🤔🤔🤔

💜

20: Tool for Policies

a tool to support proofs adherence to policies

4: prove execution properties
by tool

💜

8: Prove policies
by tool 💜💜

9: Prove Mixed Code

prove by hand
that our code adversary code has behaviour 🤔

🔺

14: Hoare Logic for Mixed Code

some of it in Swapsies 🤔🤔

💜

21: Tool for Mixed Code

a tool to support proofs adherence to policies

10: prove mixed code
by tool 💜

🔶 100% must have been done

🔺 50% could be enough

💜 would help to have;

🤔 thinking needed