State of the PRoject

read the post-oopsla submission - version -

https://github.com/sophiaIC/HolisticSpecs.git OOPSLA19 - as rejected afterOOPSLA19 - slightly improved

that includes:

section 4 - chainmail **section 5** - chainmail assertions Chainmail also needs a form of hoare tripples

section 6.2 DOM example J's version in afterOOPSLA10/DOM.md - two different versions conflated - with & without callbacks callbacks need a fukll membrane = reverse wrapper; but the underlying characteristic invariant should not change

section 6.2 ERC20 example (also appendix D)

- **A1** underlying model
- **A2** operational semantics of L_oo.
  (we will have to fight about syntax; to first approximation, something that you've got, dynamically typed)
- **A3** definendess
- **A4** liniking
- **A5** module pairs / "visible states" (really "external steps"

Examples:

- **B** - Bank account - also in section 2
  - (actually three versions of the bank account:)
  - internal abstract map
  - list of nodes
  - balance in account objects
- **C** - Classical entailment
- **D** - ERC20 (should really be E)
- **E** - DAO (should be D :-)

other examples:

- menagerie of ticket dispensers - afterOOPSLA19/ticketDispenser.md
- the "honest deputy" afterOOPSLA19/HonestDeputy.md

sophia's hand-written stuff

TODO:

take a WIDTH approach FOCUS ON PROOFS of examples (or build a tool...) rather than infratrsucture / lemmas

- syntax for Loo -- actually do whatever is easiest / fastest / best to work with for Coq -
- operational semantics for Loo
    - appendix A -- "language lemmas" (From afterOOPSLA19/Notes*July*2019.pdf) -- express the language lemmas in Coq - then go on to proofs friom dispenser upwards (i.e. assert them) rather than prove the lemmas up front
- DON'T DO syntax for Chainmail -james thought actually do whatever is easiest / fastest / best to work with for Coq -
    - Sophia says: don't translate from Chainmial syntax - unfold into Coq???
        - go straight to Coq proofs
- semantics for Chainmail?
    - single state assertions
    - temporal assertions
- do the Hoare proofs for ticket dispensers
- then the Bank Account
- then the DOM

OTHER STUFF - RELATED WORK

- access congtrol logics
- temporal logical tracing etc (Havelund)
- Ilya Sergi - "Skilla" Skiller? Scylla?