Formally Verify Finance like a Reactive System

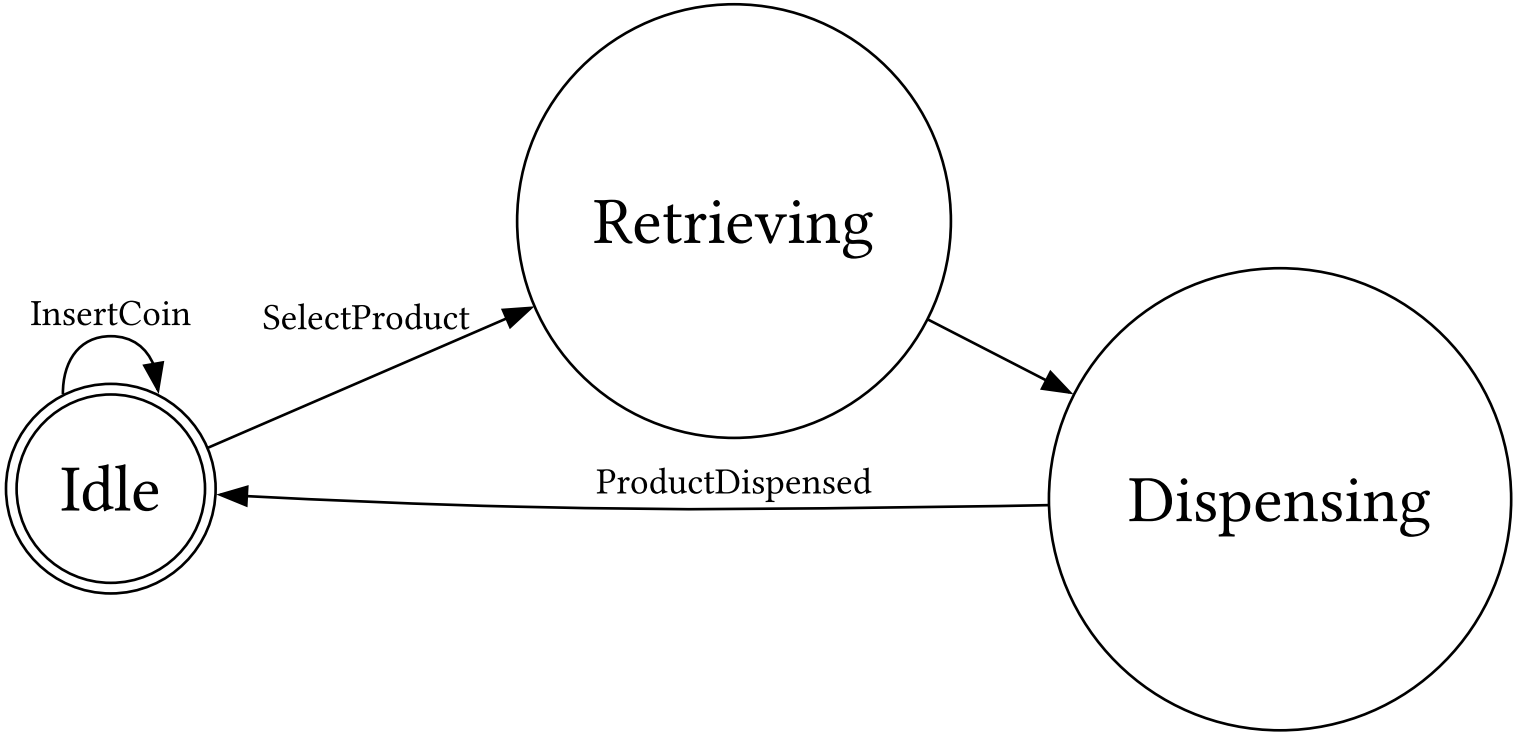
Lessons from Model Checking

Quinn Dougherty

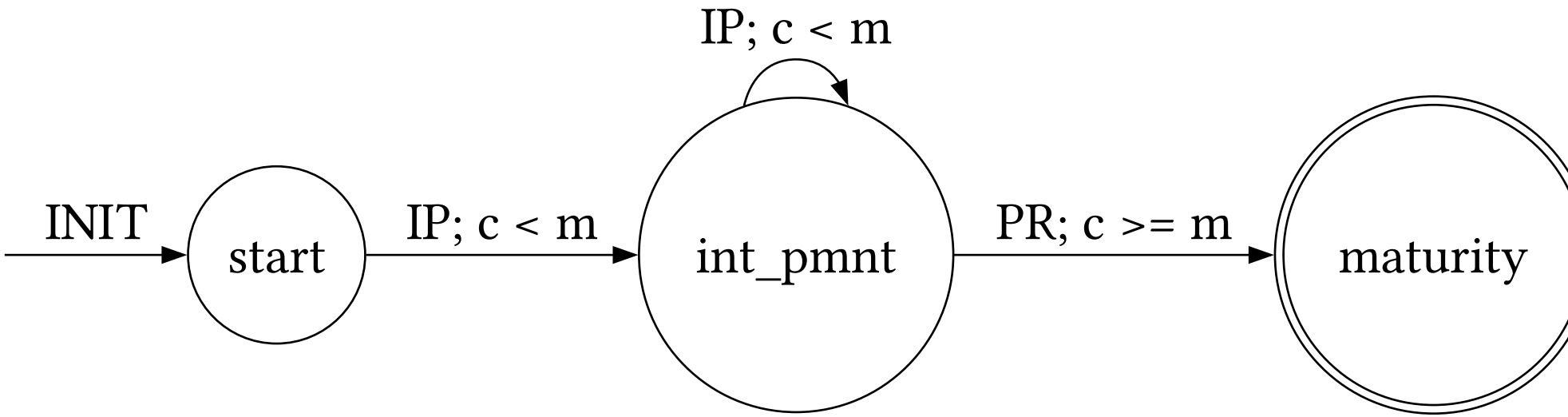
Casper Association

2024-05-14

Automata


Retrieving
InsertCoin
SelectProduct
Idle
ProductDispensed
Dispensing

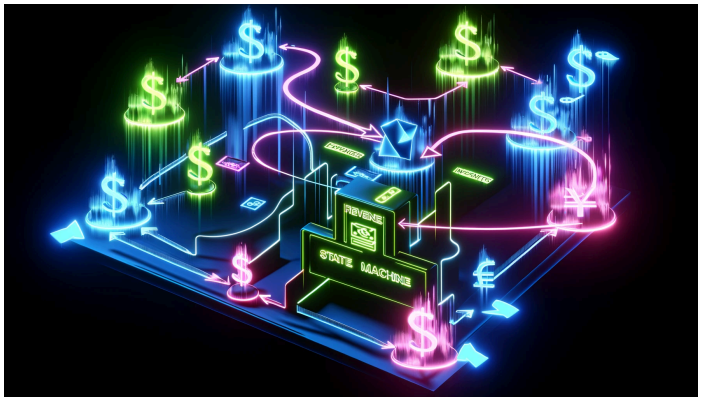
Principal at Maturity (PAM)



- c: *clock*
- m: *maturity date*
- IP: interest payment event
- PR: principal repayment event
- All events increment clock c by 1

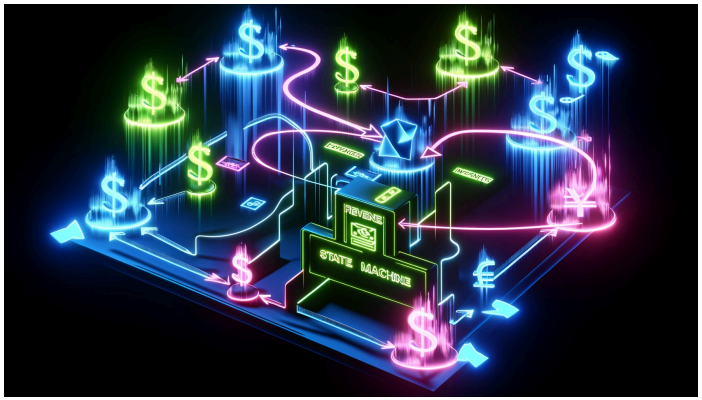
Reactive systems

- A **reactive system** is a software system embedded in an environment that responds to sensor input
  - often in continuous/infinite time horizon
  - often with actuator output effecting the environment



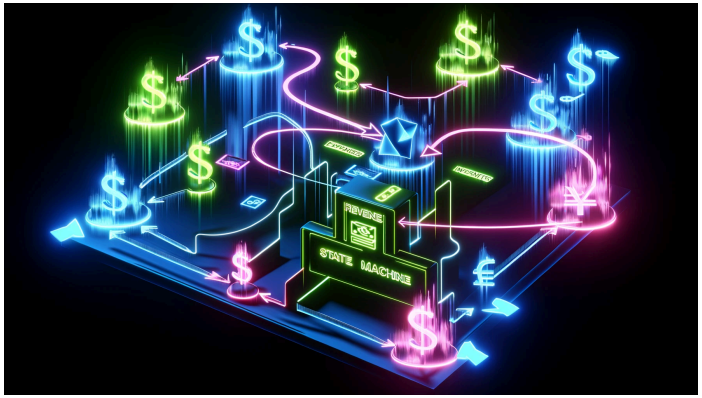
Reactive systems

- A **reactive system** is a software system embedded in an environment that responds to sensor input
  - often in continuous/infinite time horizon
  - often with actuator output effecting the environment
- Examples: traffic lights, airplane autopilot, fitness tracker on smartwatch, cruise control on a car



Temporal Logic

- Logic aware of time step
- We can **specify** correctness of a financial contract as well as safety and liveness properties



$$\text{PAM} : \Diamond\ \text{Mat} \wedge \neg\ \text{Mat}\ U\ \text{IP} \wedge \Box(\text{IP} \rightarrow (\bigcirc\ (\text{IP} \vee \text{PR}))U\ \text{Mat})$$