



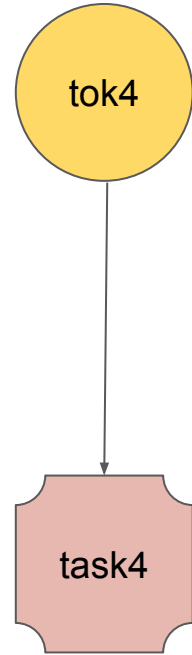
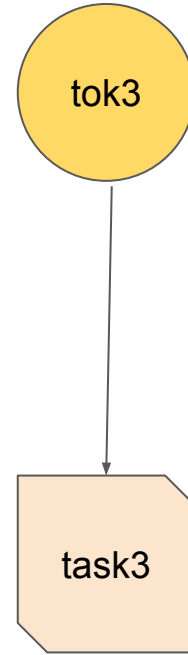
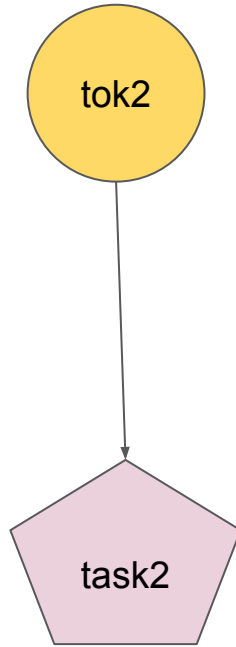
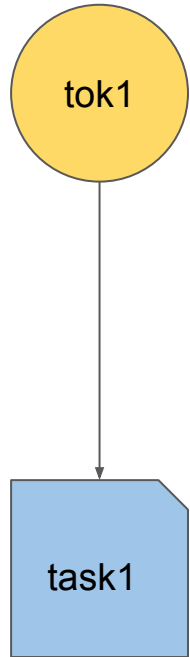
Anonymous Credit Tokens

Samuel Schlesinger

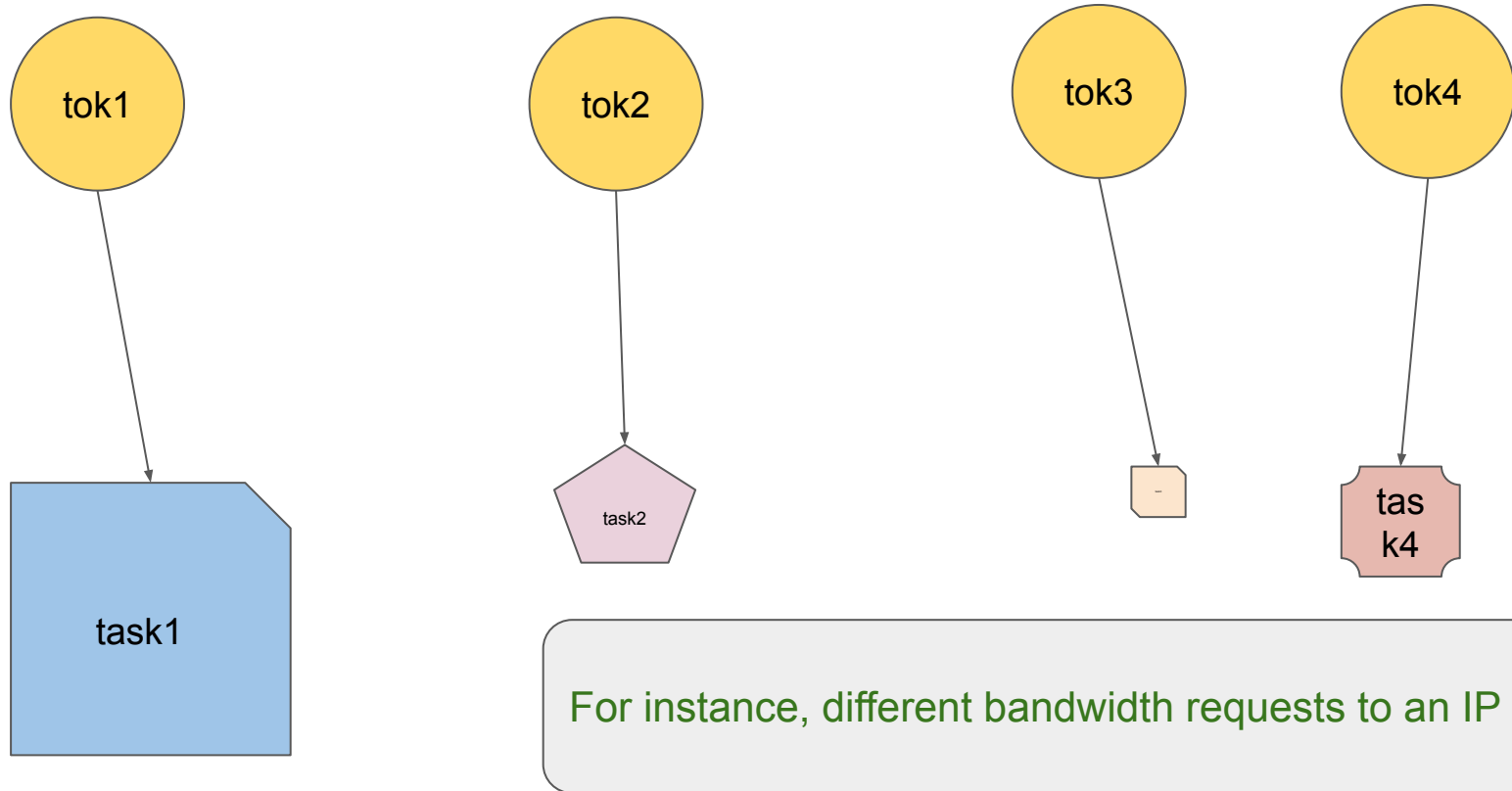
Collaborators

- Jonathan Katz

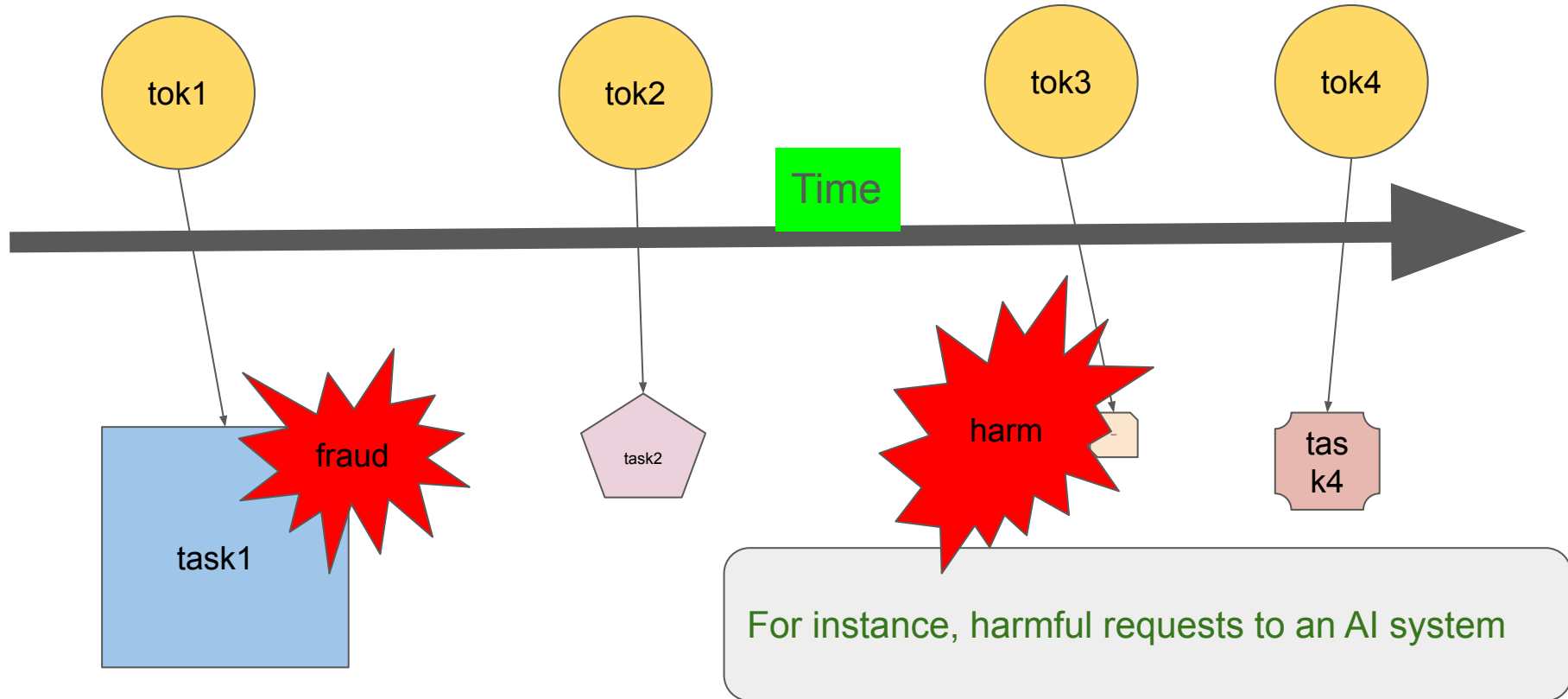
Privacy Pass



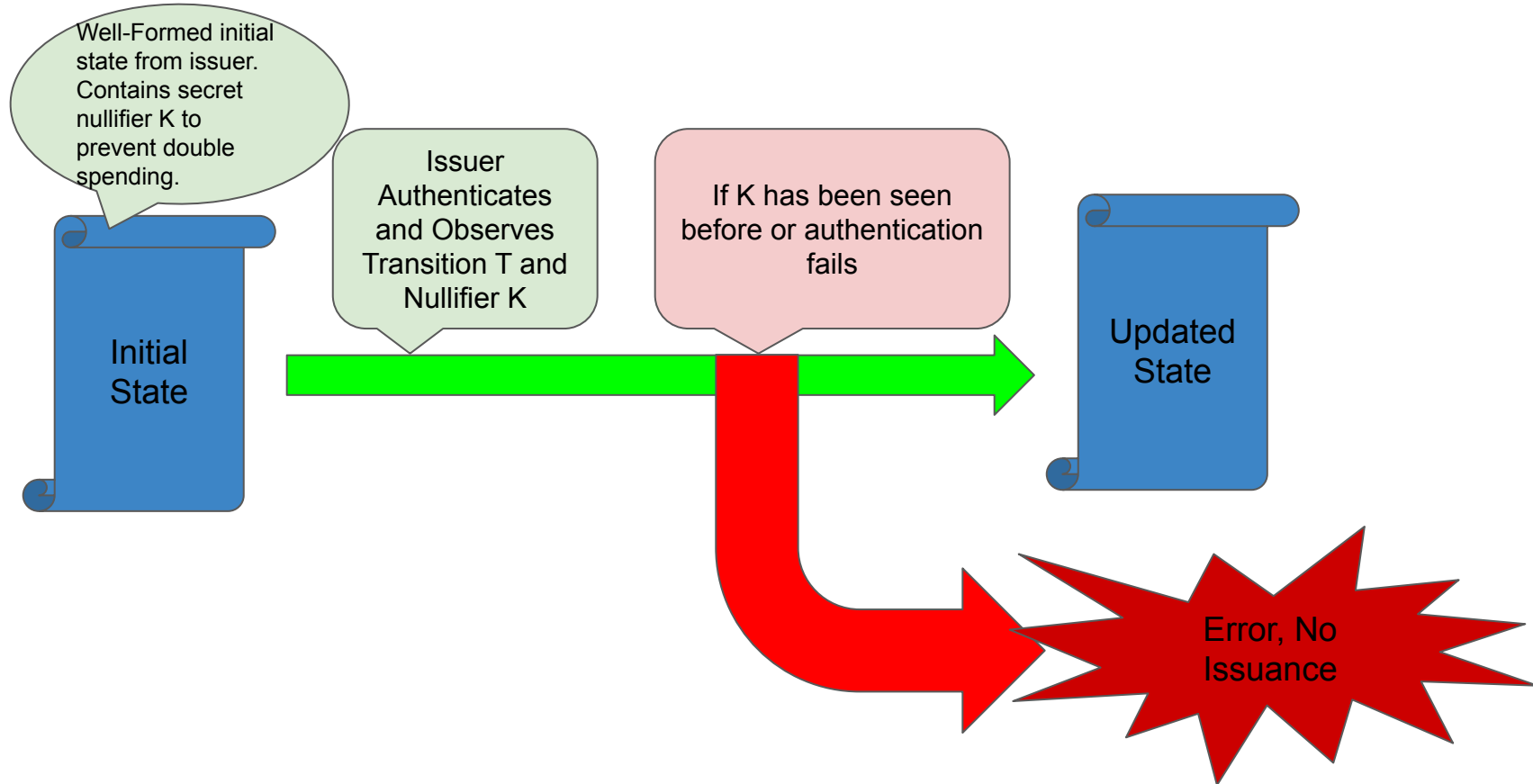
Privacy Pass Downside: Cost Differences



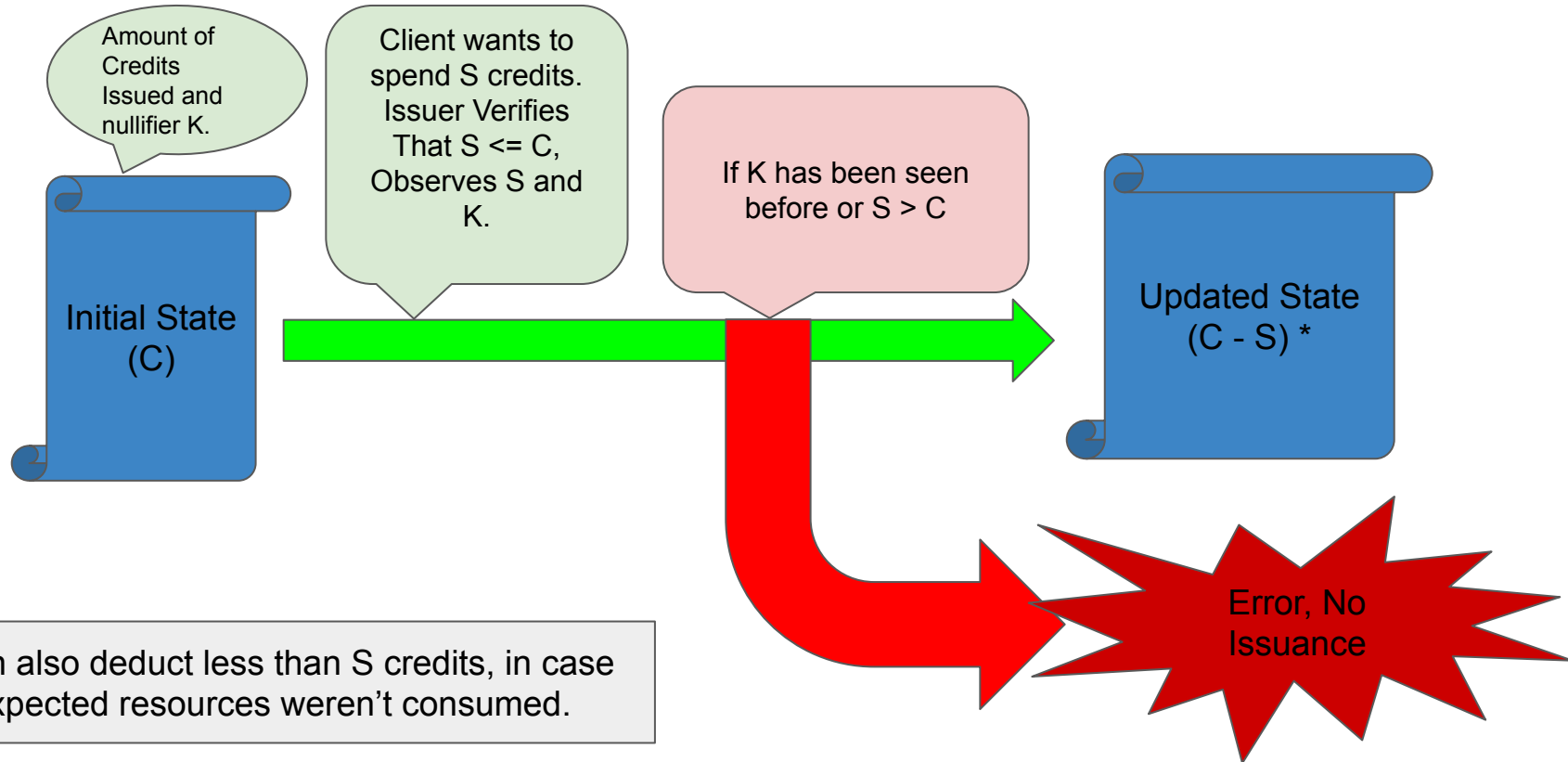
Privacy Pass Downside: Can't React to Abuse



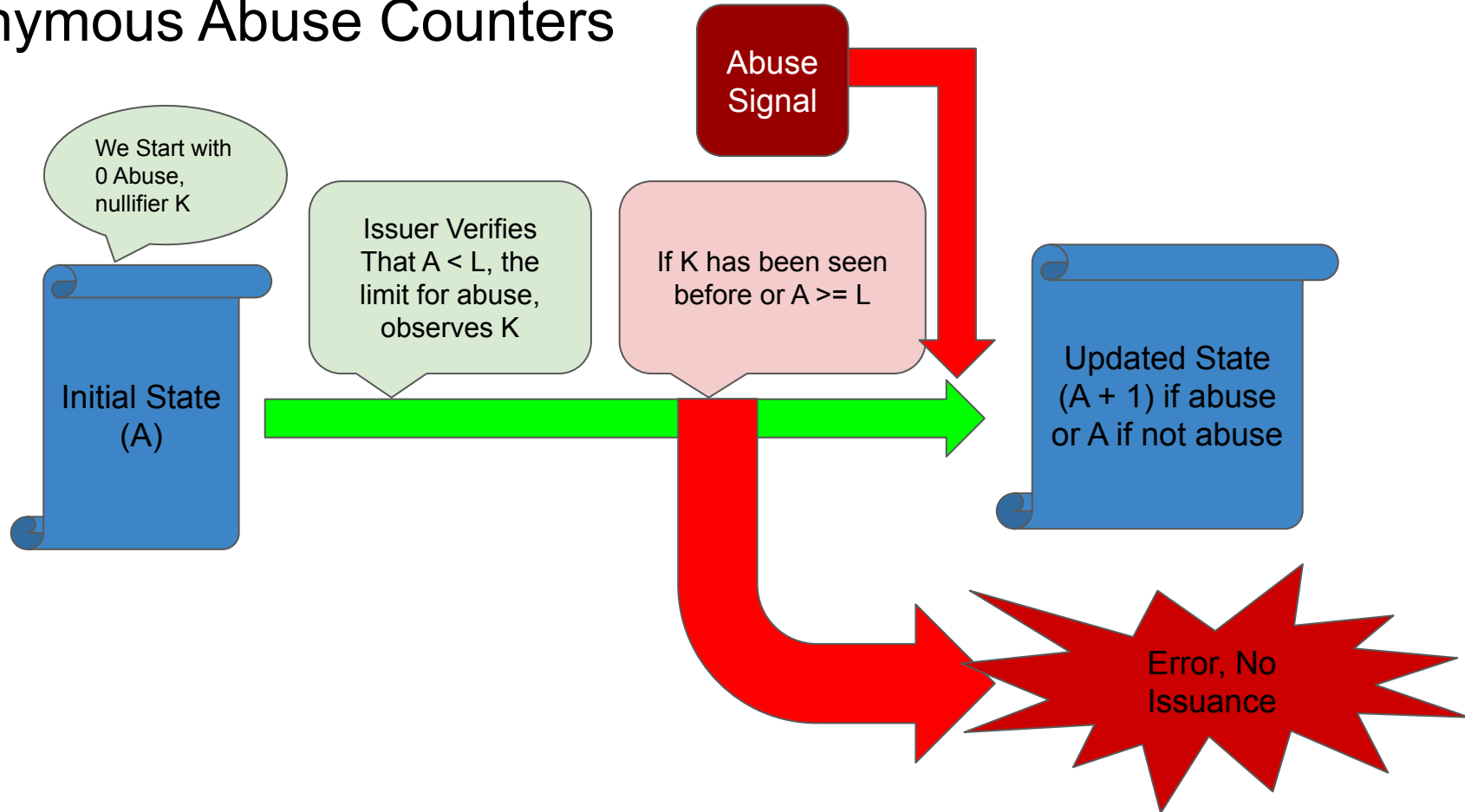
Anonymous State Machines



Anonymous Credit Tokens



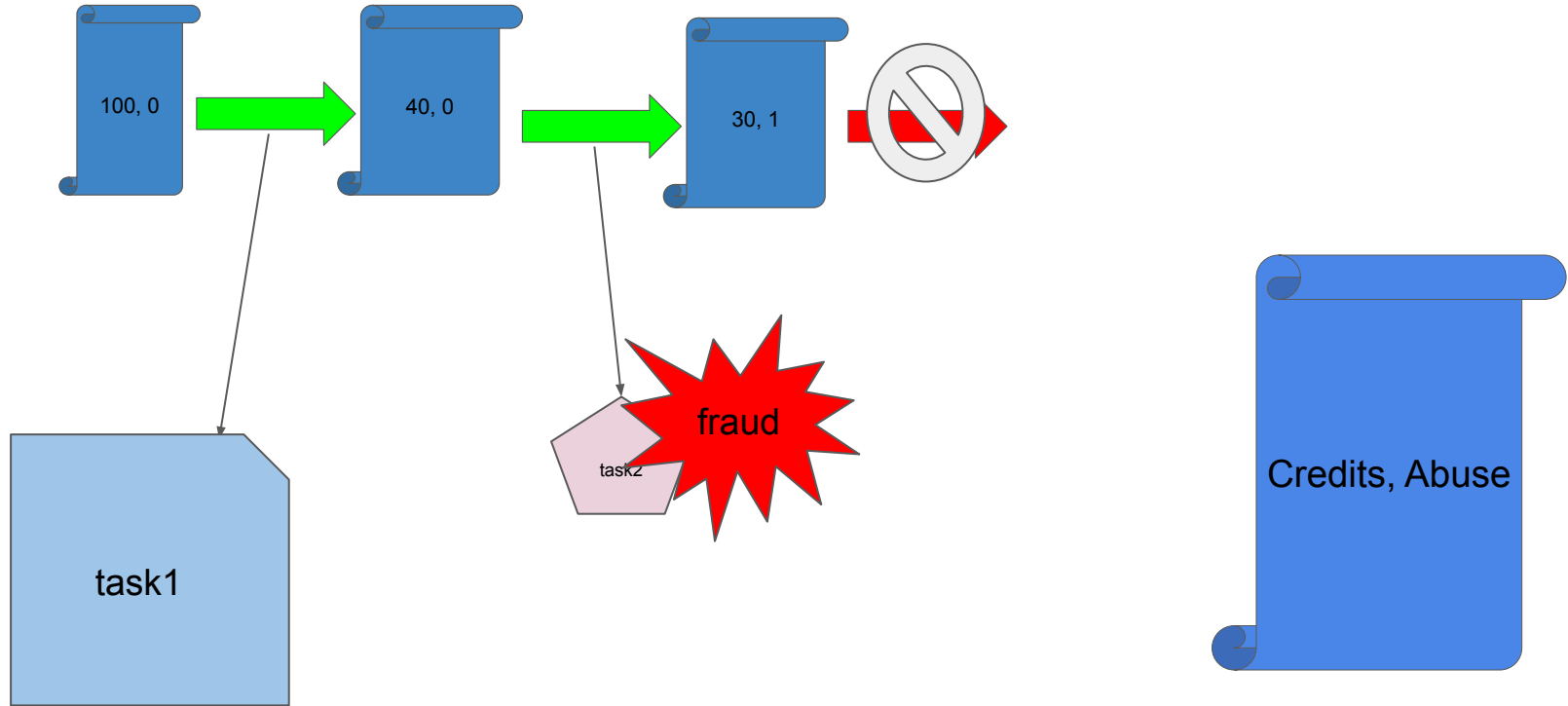
Anonymous Abuse Counters



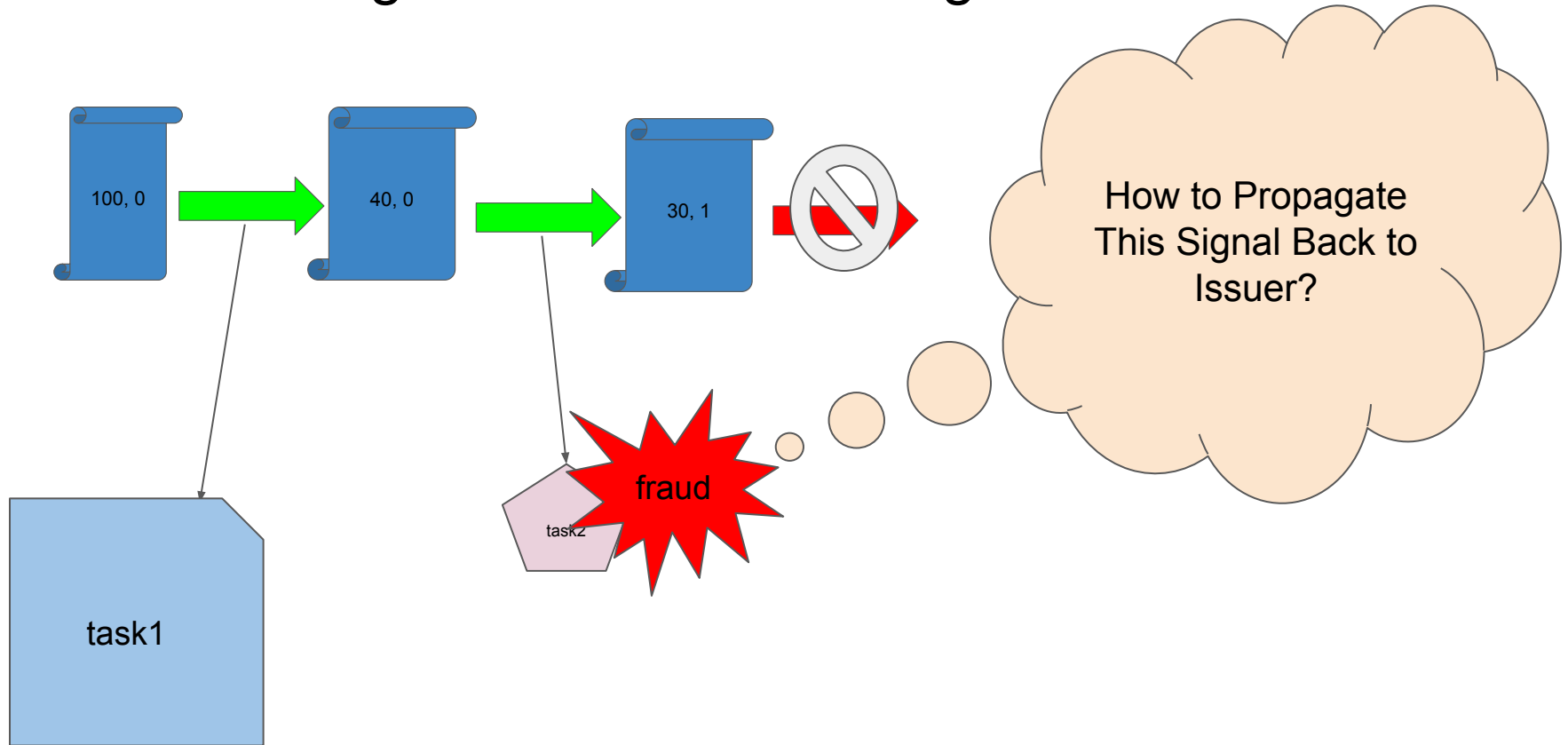
Combining Anonymous State Machines

- Take the AND of two state machines
- $\text{State} = (\text{State1}, \text{State2})$
- $\text{Transition}(\text{State}, t, \text{State}') = \text{Transition}(\text{State1}, t, \text{State1}') \ \&\& \ \text{Transition}(\text{State2}, t, \text{State2}')$

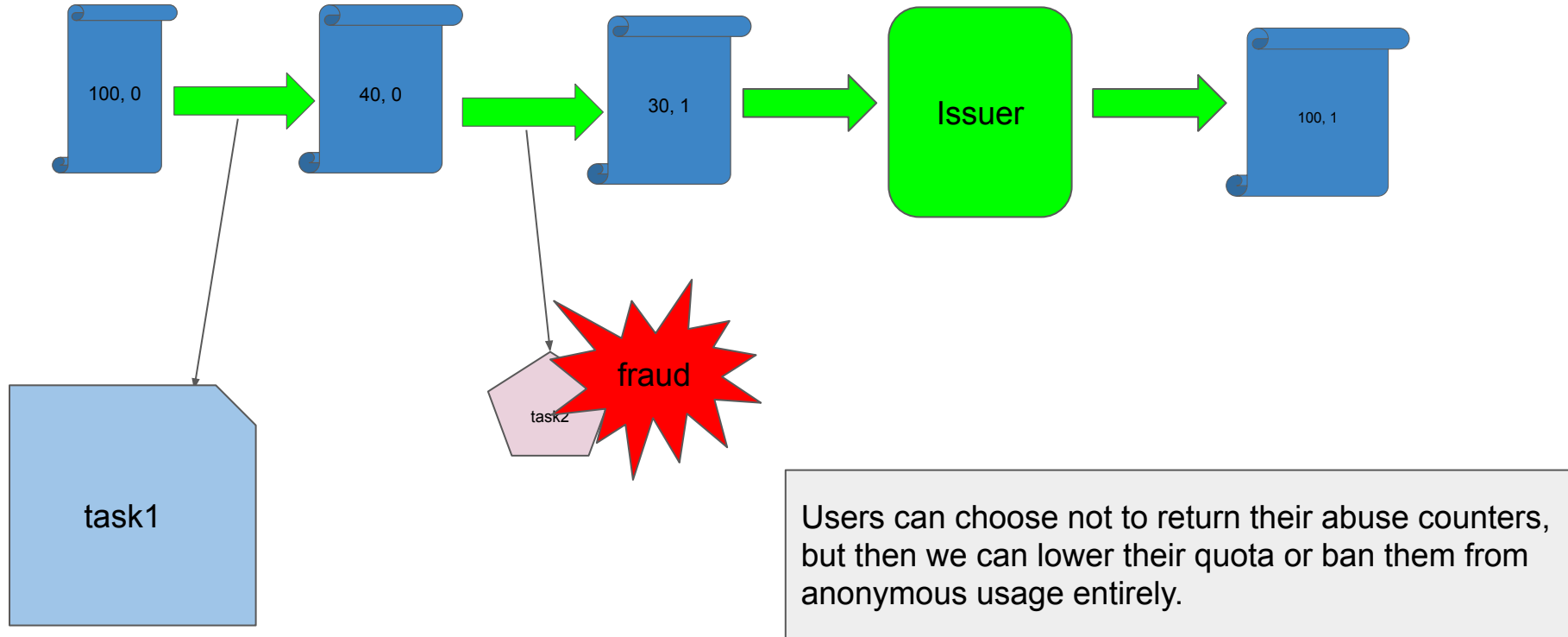
Anonymous Credit Tokens with Abuse Counters (L = 1)



Problem: Long Term Abuse Tracking



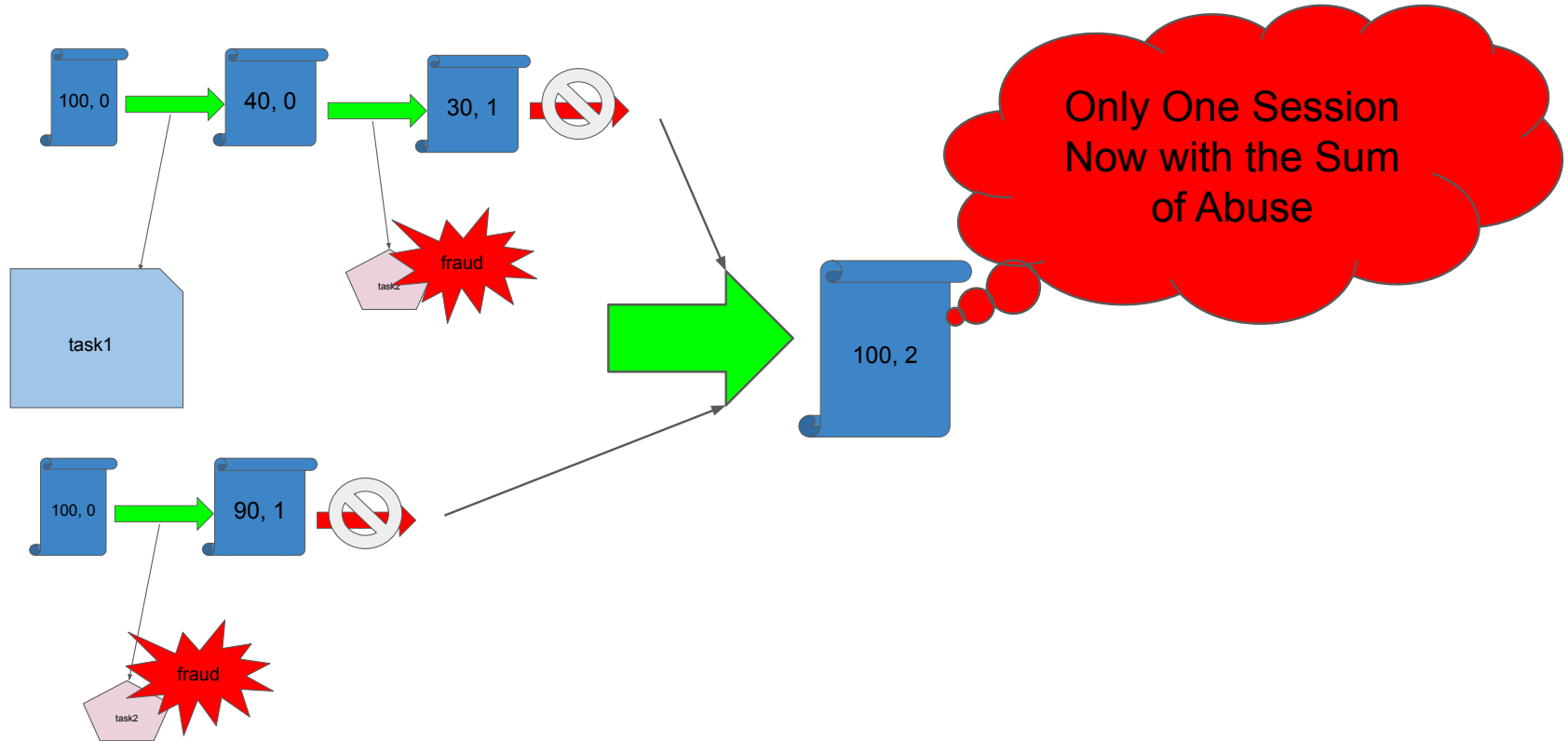
Solution: Returning Our Abuse Counters After Use



Concurrency Control

- For Single-Use Tokens:
 - $\text{Resources Allocated} = \text{Number of Tokens Issued} = \text{Number of Concurrent Sessions}$
- For Anonymous Credit Tokens
 - $\text{Concurrent Sessions} = \text{Number of Credit Tokens}$
 - $\text{Resources Allocated} = \text{Number of Credits Issued}$ *Inside* the Tokens

Concurrency in Action: Deducting Sessions, Aggregating Abuse



Specifications and Source Code

- [IETF Draft for Cryptography \(Not yet on datatracker, no abuse counters\)](#)
- [Rust Implementation](#)

Questions for You

- Does this work belong in Privacy Pass?