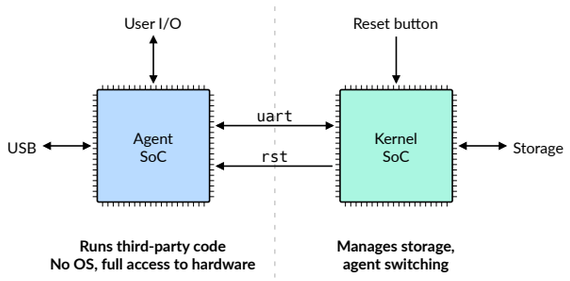
Notary: A Device for Secure Transaction Approval

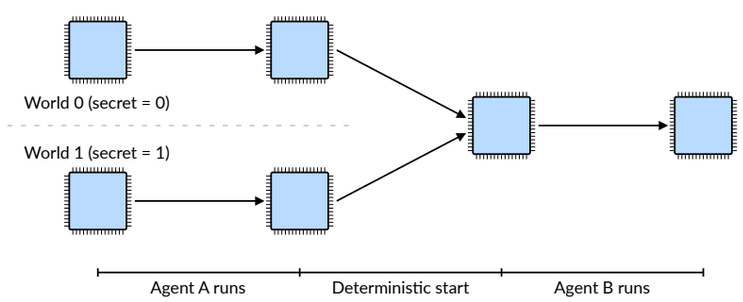
Anish Athalye, Adam Belay, Frans Kaashoek, Robert Morris, Nickolai Zeldovich
MIT CSAIL

Existing hardware wallets support many apps,
but have weak isolation between agents.

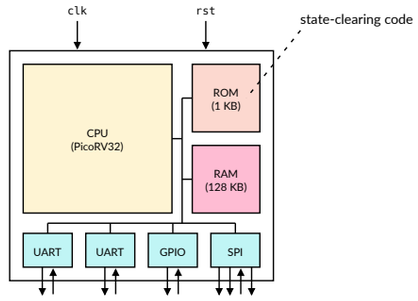
Notary's separation architecture provides isolation with **reset-based switching** to run agents one-at-a-time on a dedicated SoC.



Notary provides **non-interference** between agents with software that clears all internal SoC state between switches.



Notary **formally verifies the deterministic start property** by analyzing the SoC at the RTL level.



Deterministic start: all internal state is cleared after running for n cycles after reset.

$$\exists s_f \,.\, \forall s \,.\, \mathrm{run}(\mathrm{rst}(s), n) = s_f$$

We built Notary, a hardware wallet that provides strong isolation for transaction approval applications.

anish.io/notary