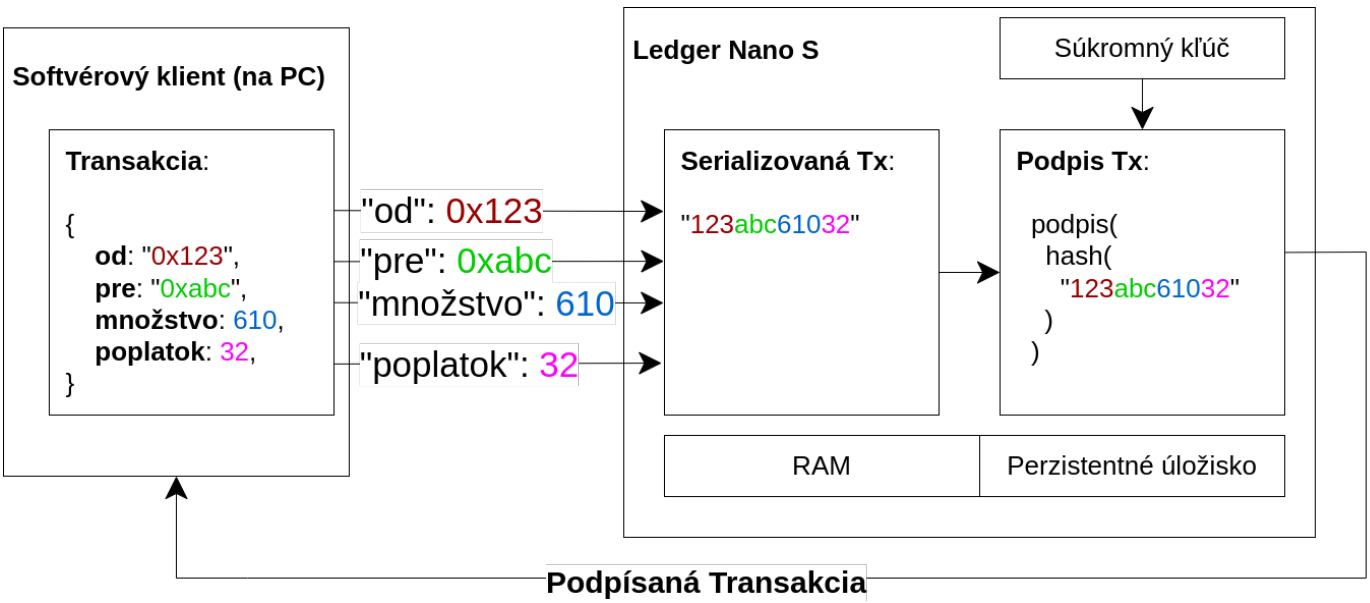
Manažovanie pracovných tokov v Ledger NanoS pomocou hashovacích stromov

Bc. Daniel Oravec
Školiteľ: doc. RNDr. Robert Lukoťka, PhD.

14. februára 2024

Outline

Ledger NanoS - cieľ



Obmedzenia

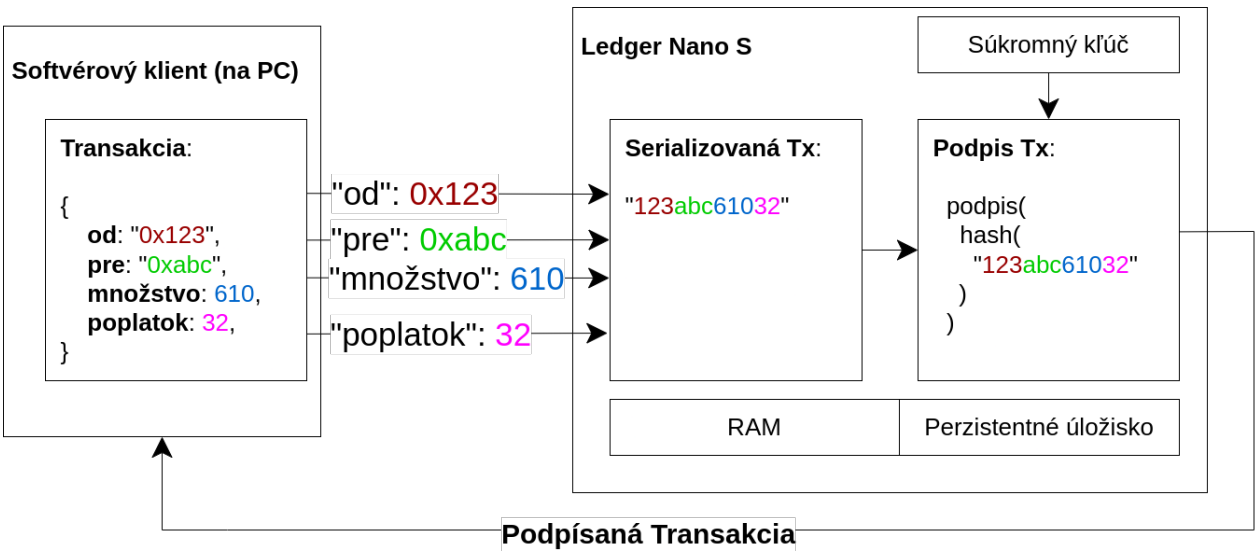
- Použiteľná RAM: $\sim 2\,\mathrm{kB}$
- Kapacita APDU: $255\,\mathrm{B}$
- Perzistentné úložisko: $\sim 160\,\mathrm{kB}$

Inštrukcia

(**konštantná hlavička**, variabilné dáta)
(**množstvo**, 1234)

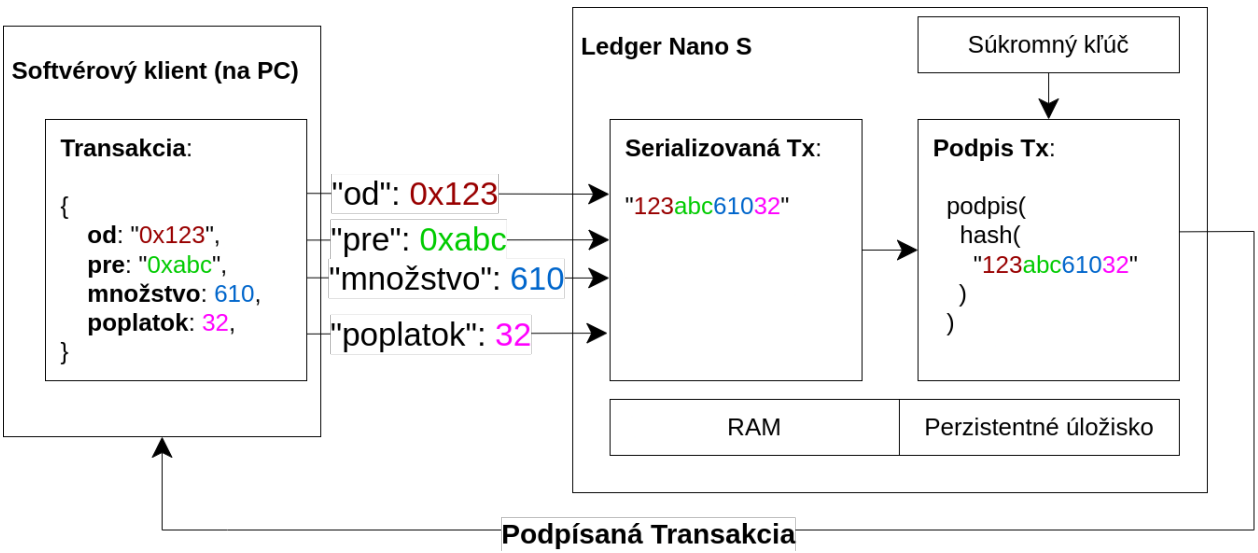
Známe prístupy (1)

- Kód aplikácie predstavuje DKA



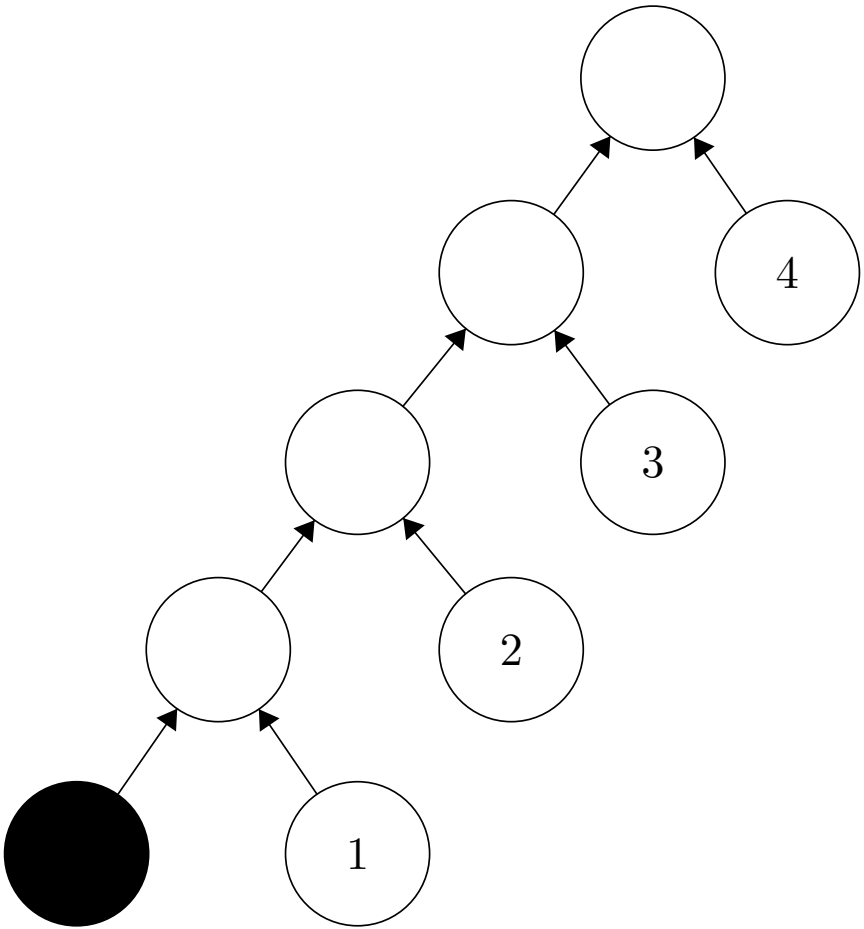
Známe prístupy (2) - Riešenie z BP

- DKA u klienta + overovanie integrity



Známe prístupy (2) - Riešenie z BP

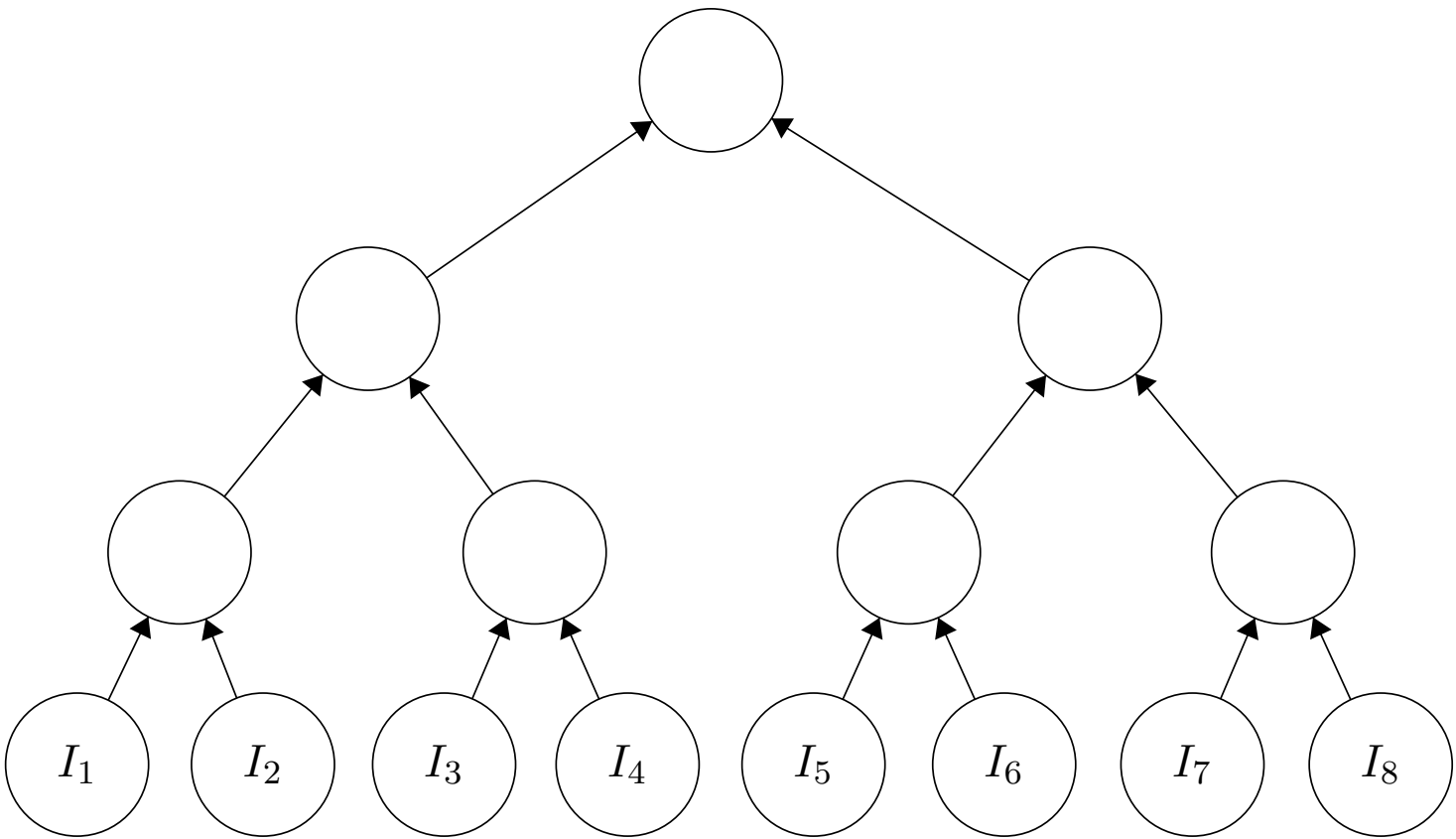
- Overenie až na konci



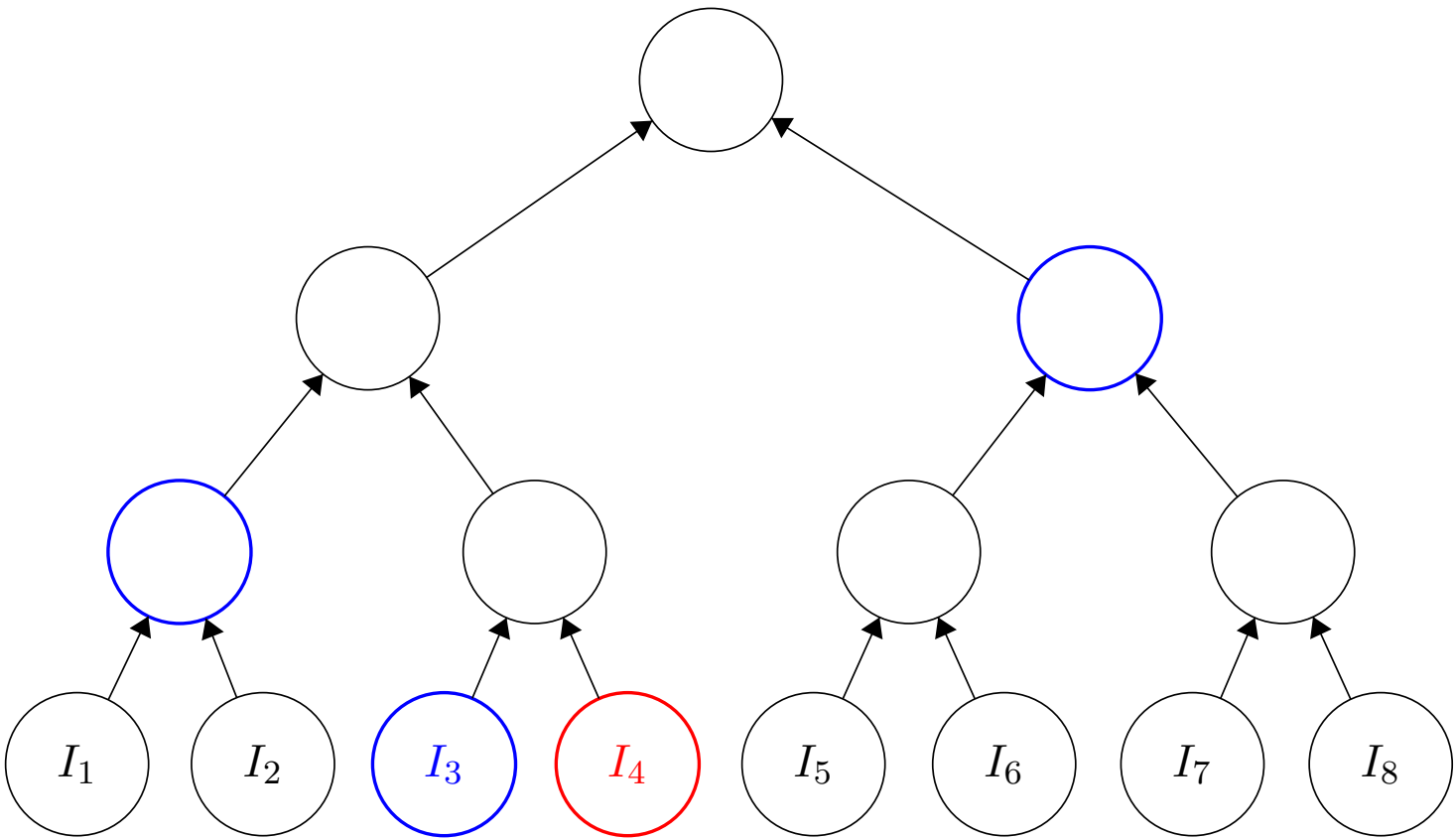
Hlavný cieľ našej práce

- Overovanie po každom kroku

Hashovacie stromy

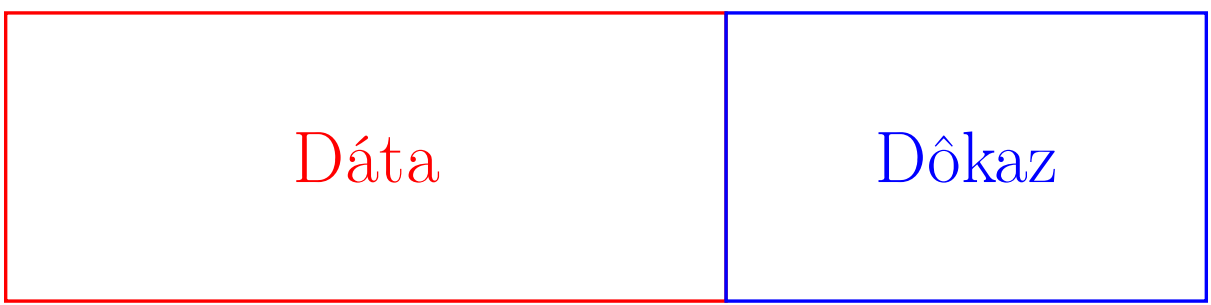


Hashovacie stromy



Správa s dôkazom

- APDU – 255 B



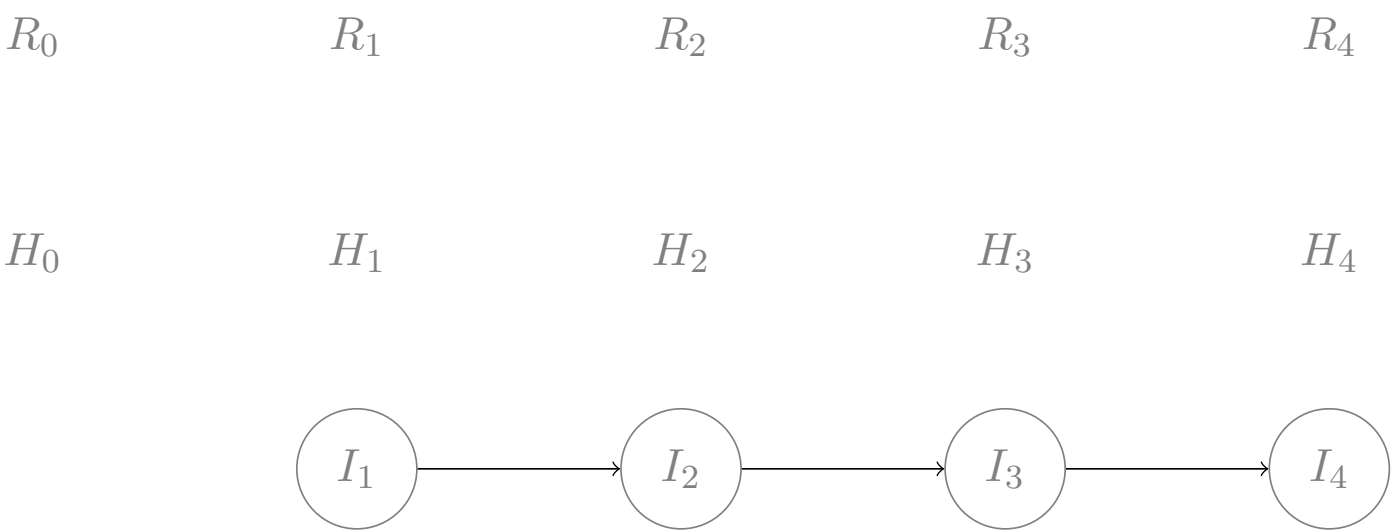
Iné vektor-komitment schémy

- KZG (pairing), Catalano-Fiore (RSA)
  - Prijateľné veľkosťou dôkazov
  - Neprijateľné výpočtovou náročnosťou

Typy hashov

- H_i – hash konštantných hlavičiek prvých i inštrukcií
  - $H_0 = hash(0)$
  - $H_i = hash(H_{i-1}, \text{hlavička}_i)$
- R_i – reverzný hash $H_i, H_{i+1}, ..., H_n$
  - $R_n = hash(1)$
  - $R_i = hash(R_{i+1}, H_{i+1})$

Pridanie nového typu transakcie



Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

Pridanie nového typu transakcie

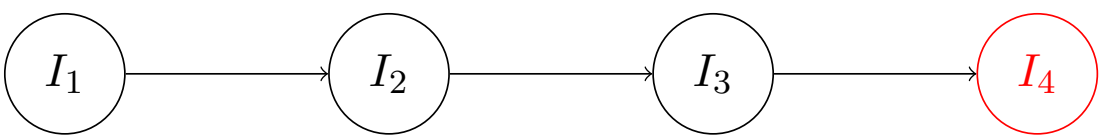
R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4



Pridanie nového typu transakcie

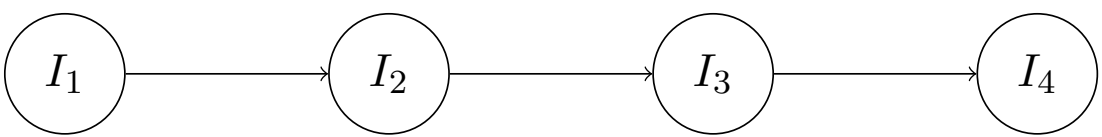
R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

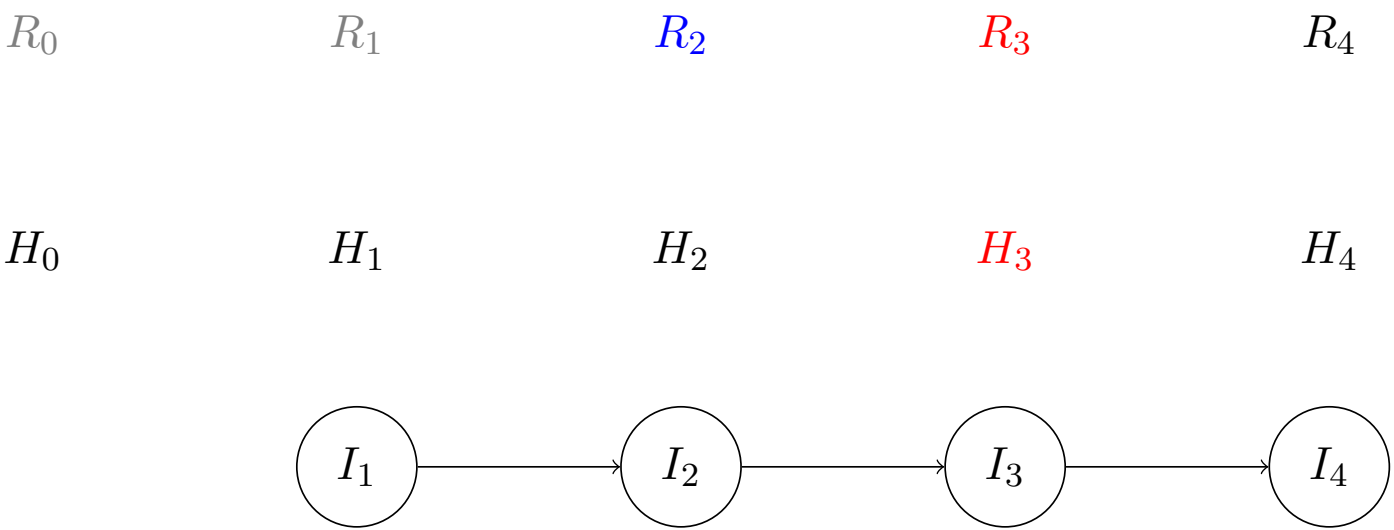
Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4



Pridanie nového typu transakcie



Pridanie nového typu transakcie

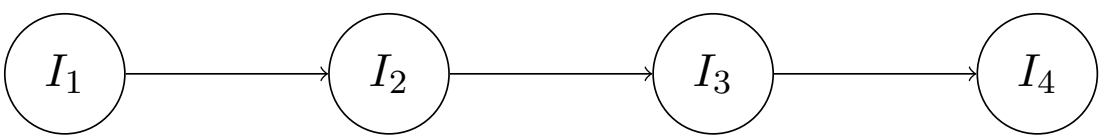
R_0 R_1 R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

Pridanie nového typu transakcie

R_0 R_1 R_2 R_3 R_4

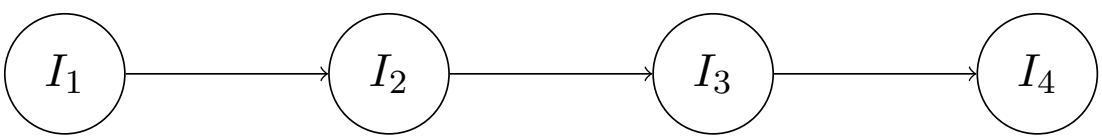
H_0 H_1 H_2 H_3 H_4



Interakcia so softvérovým klientom

$\boldsymbol{R_0}$ R_1 R_2 R_3 R_4

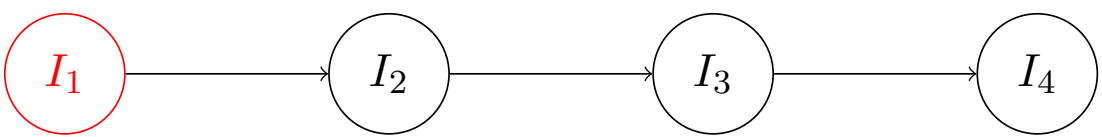
H_0 H_1 H_2 H_3 H_4



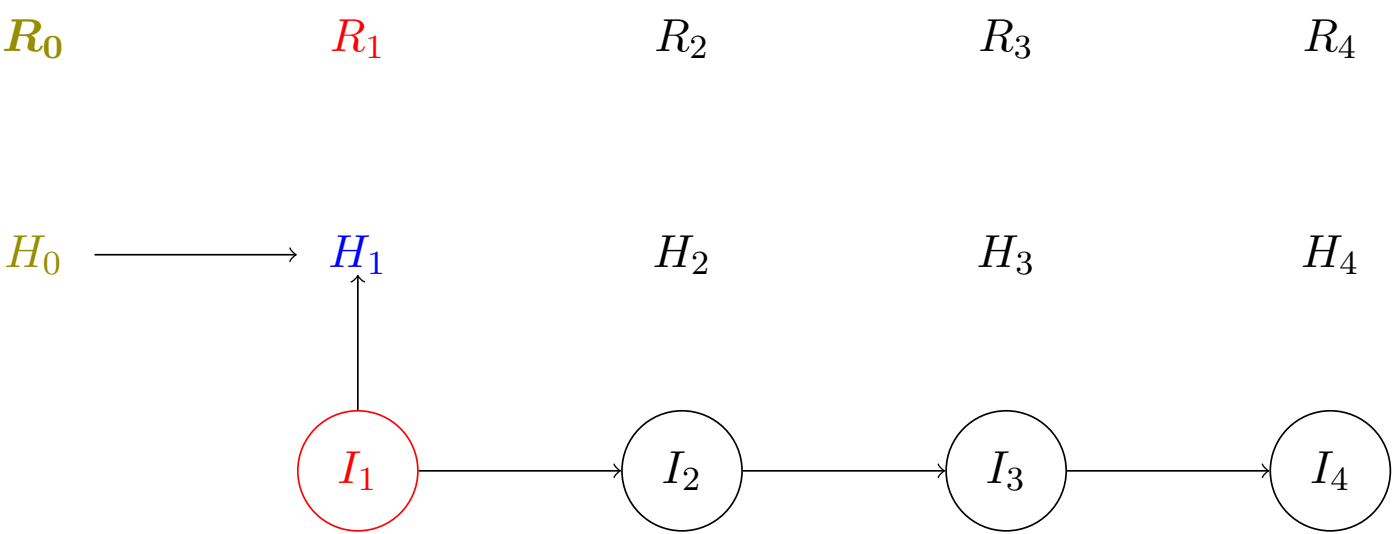
Interakcia so softvérovým klientom

$\boldsymbol{R_0}$ R_1 R_2 R_3 R_4

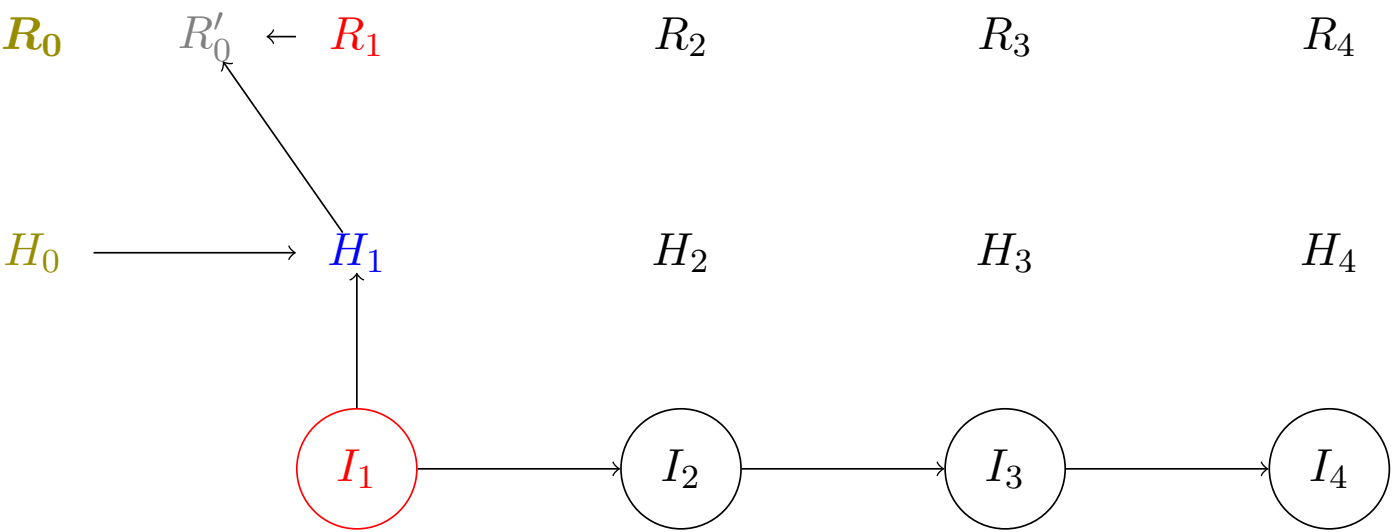
H_0 H_1 H_2 H_3 H_4



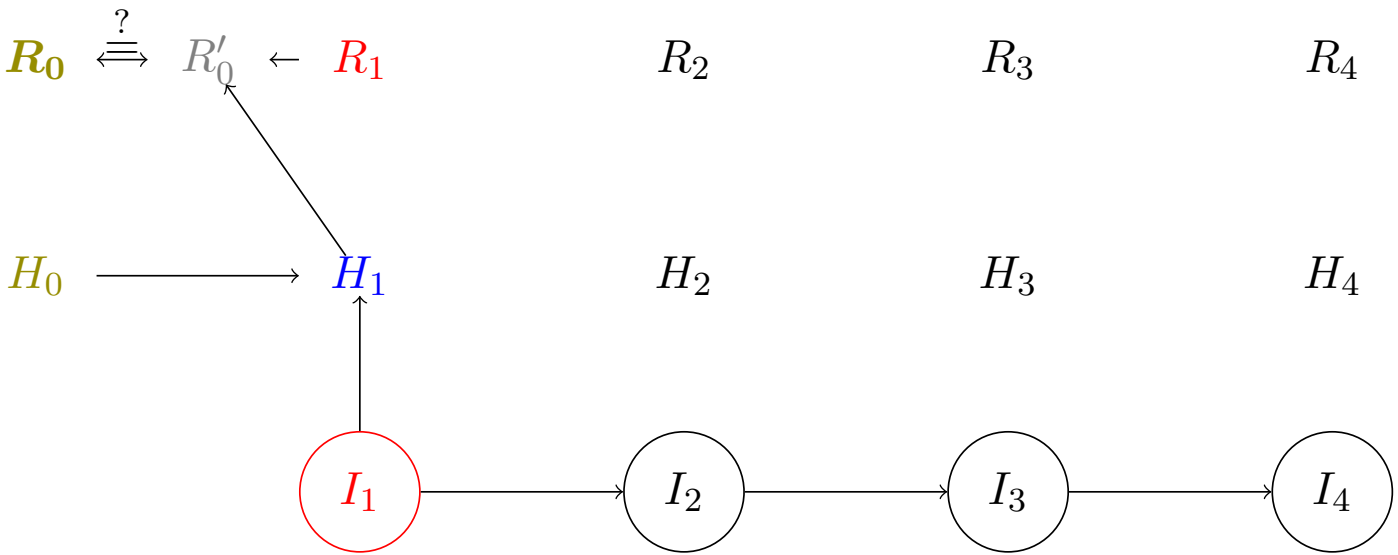
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Interakcia so softvérovým klientom

R_0 $\boldsymbol{R_1}$ R_2 R_3 R_4

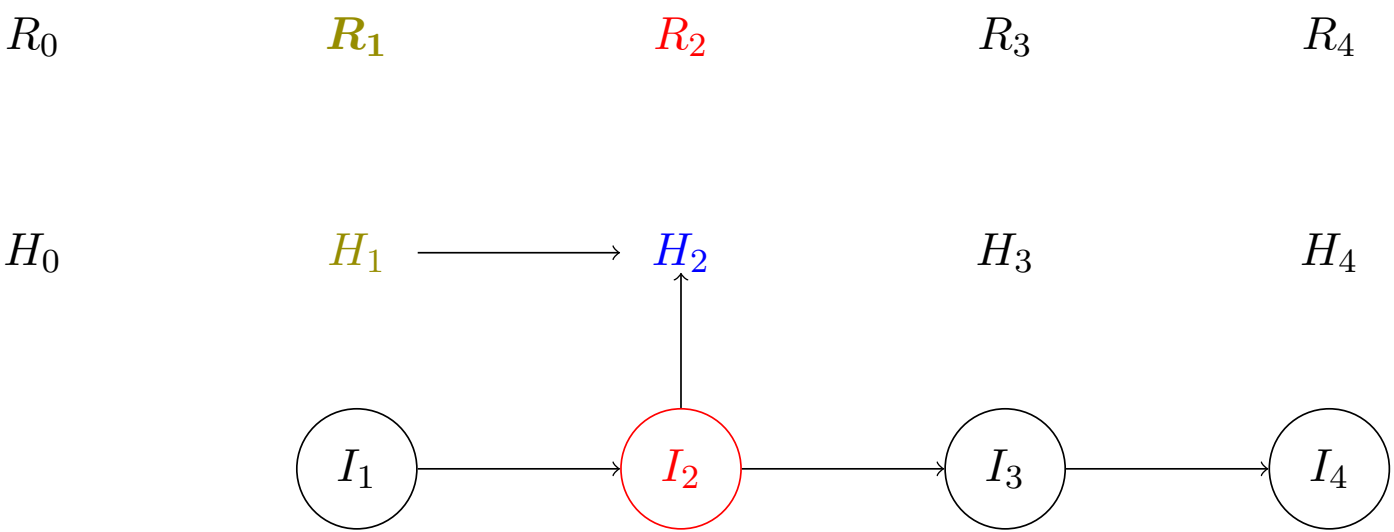
H_0 H_1 H_2 H_3 H_4

Interakcia so softvérovým klientom

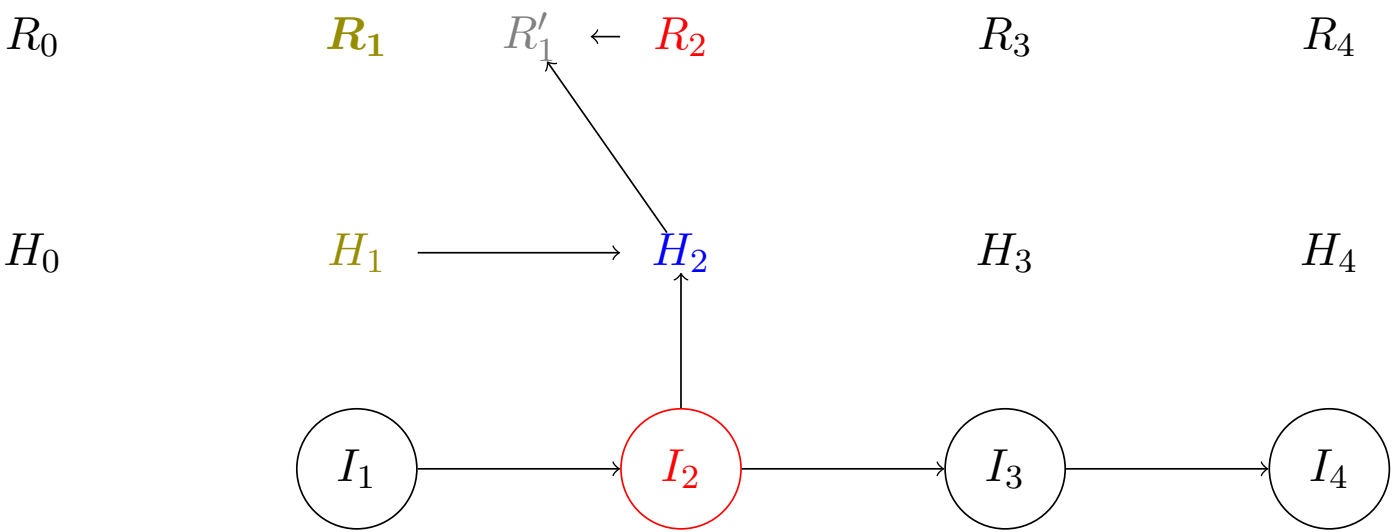
R_0 $\boldsymbol{R_1}$ R_2 R_3 R_4

H_0 H_1 H_2 H_3 H_4

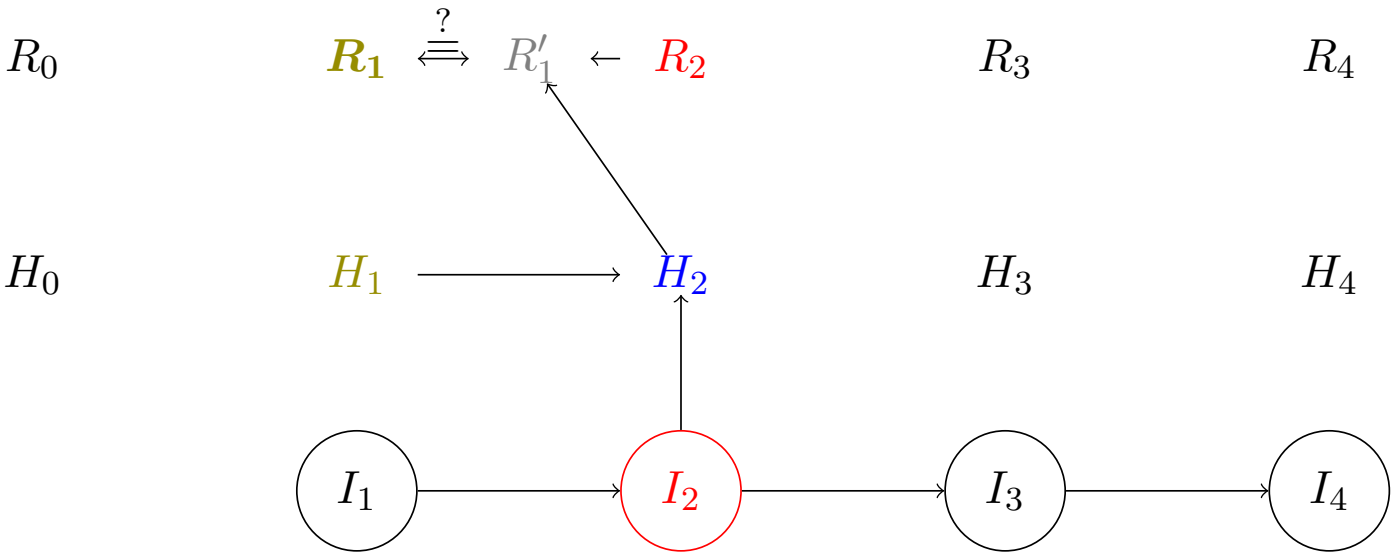
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



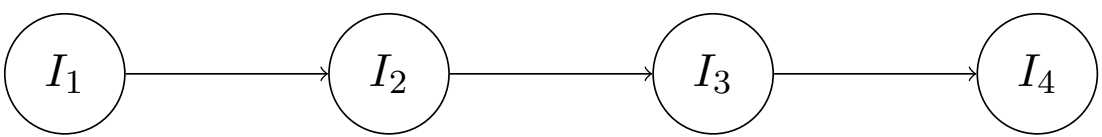
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom

R_0 R_1 $\boldsymbol{R_2}$ R_3 R_4

H_0 H_1 H_2 H_3 H_4

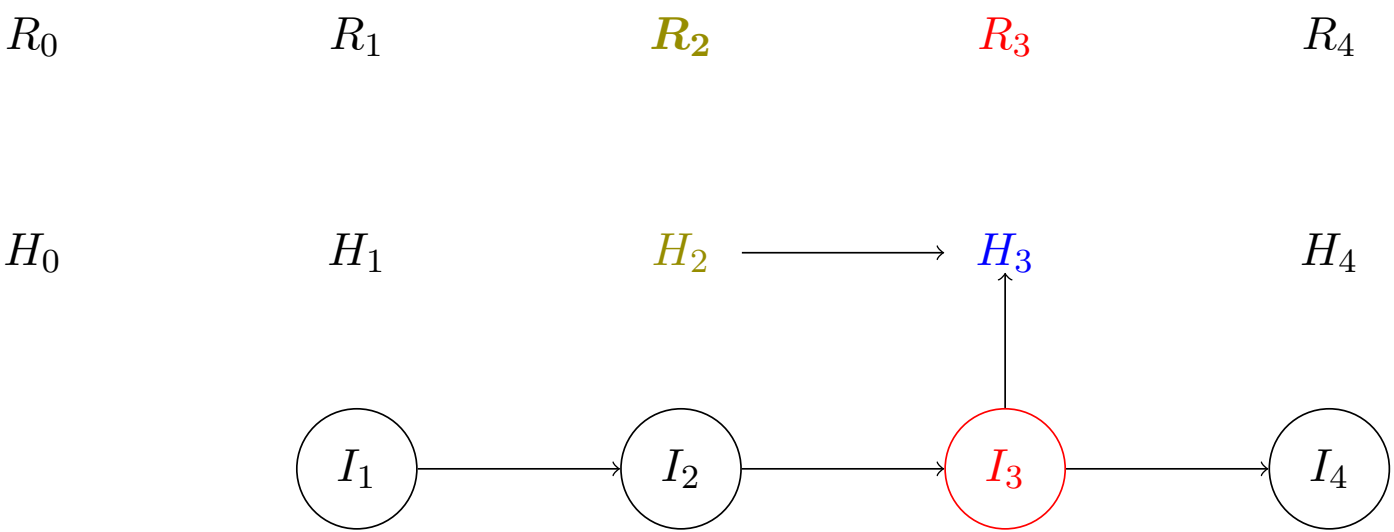


Interakcia so softvérovým klientom

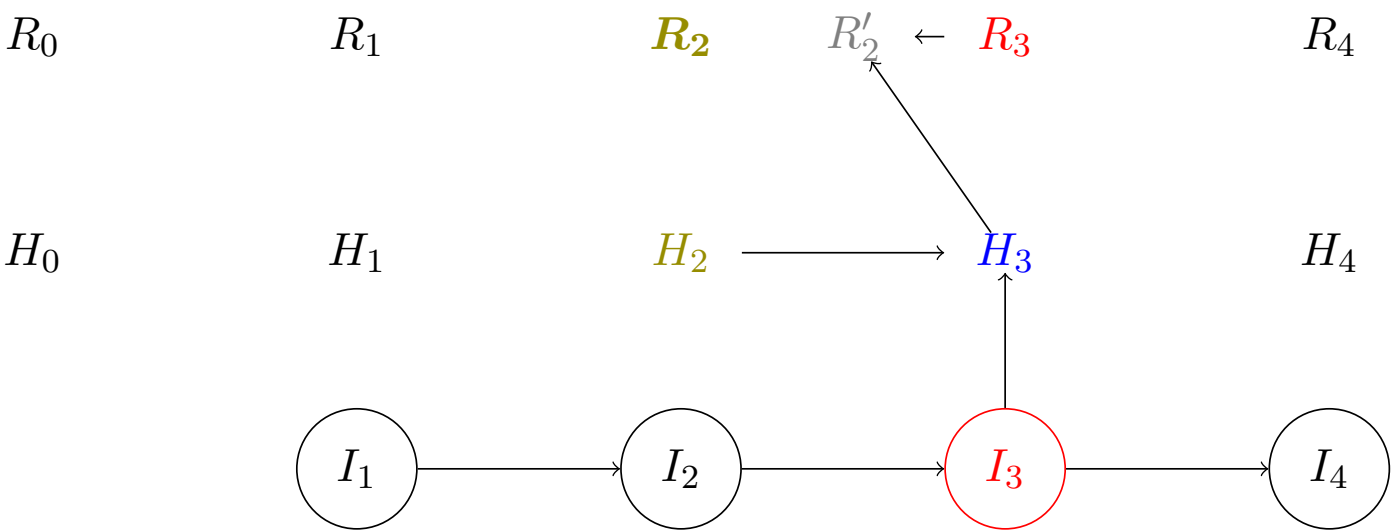
R_0 R_1 $\boldsymbol{R_2}$ R_3 R_4

H_0 H_1 H_2 H_3 H_4

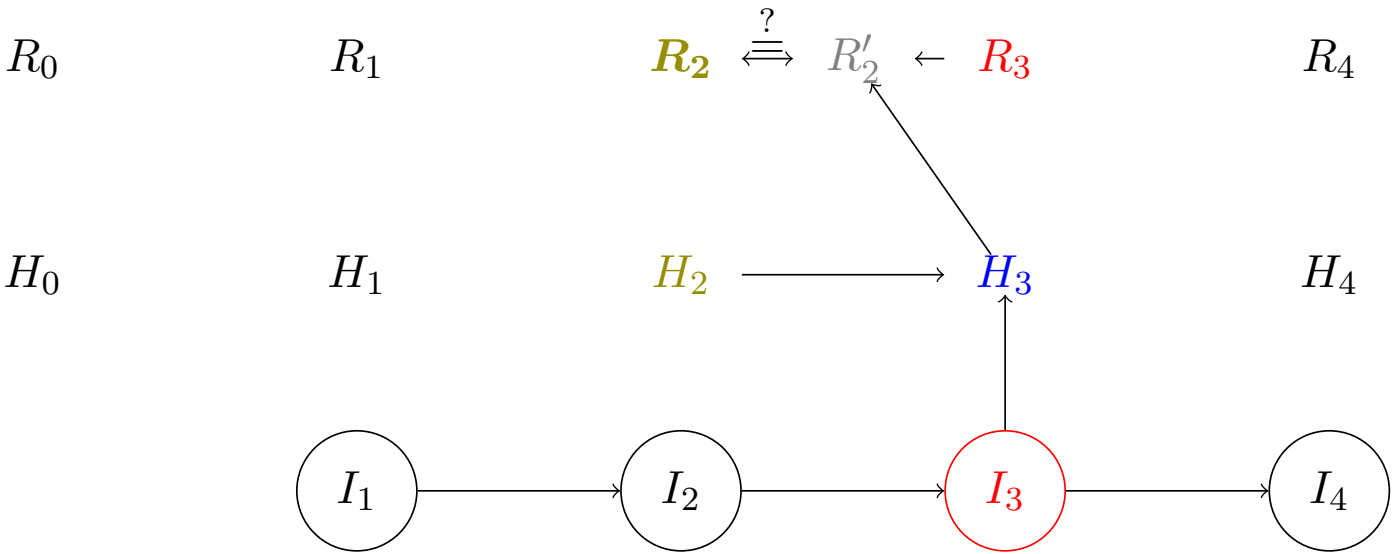
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Interakcia so softvérovým klientom

R_0 R_1 R_2 $\boldsymbol{R_3}$ R_4

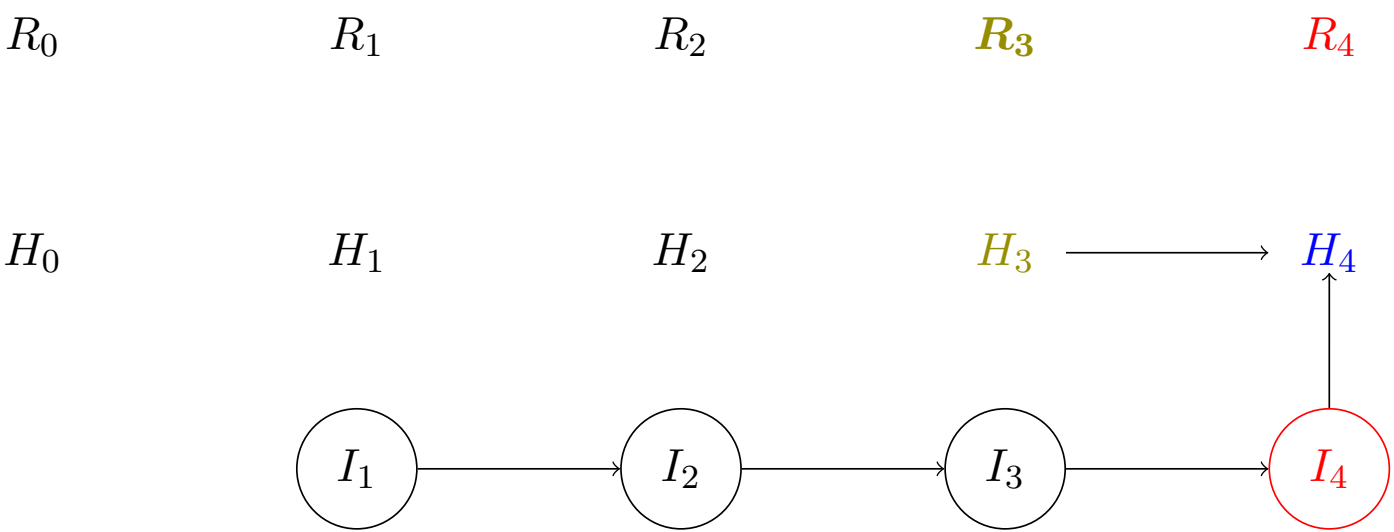
H_0 H_1 H_2 H_3 H_4

Interakcia so softvérovým klientom

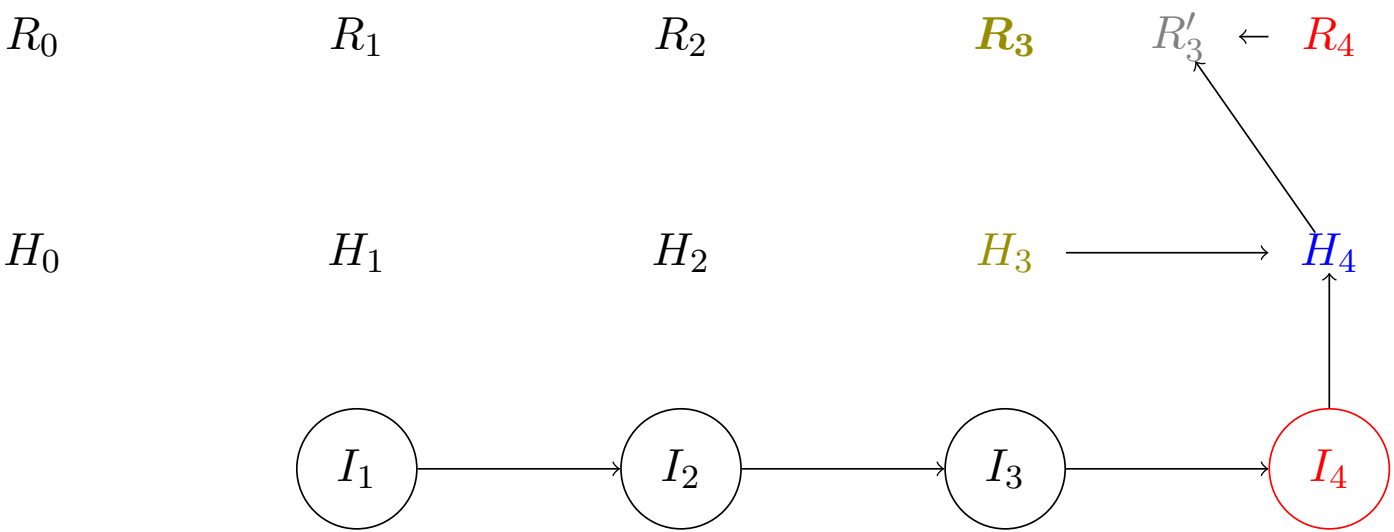
R_0 R_1 R_2 $\boldsymbol{R_3}$ R_4

H_0 H_1 H_2 H_3 H_4

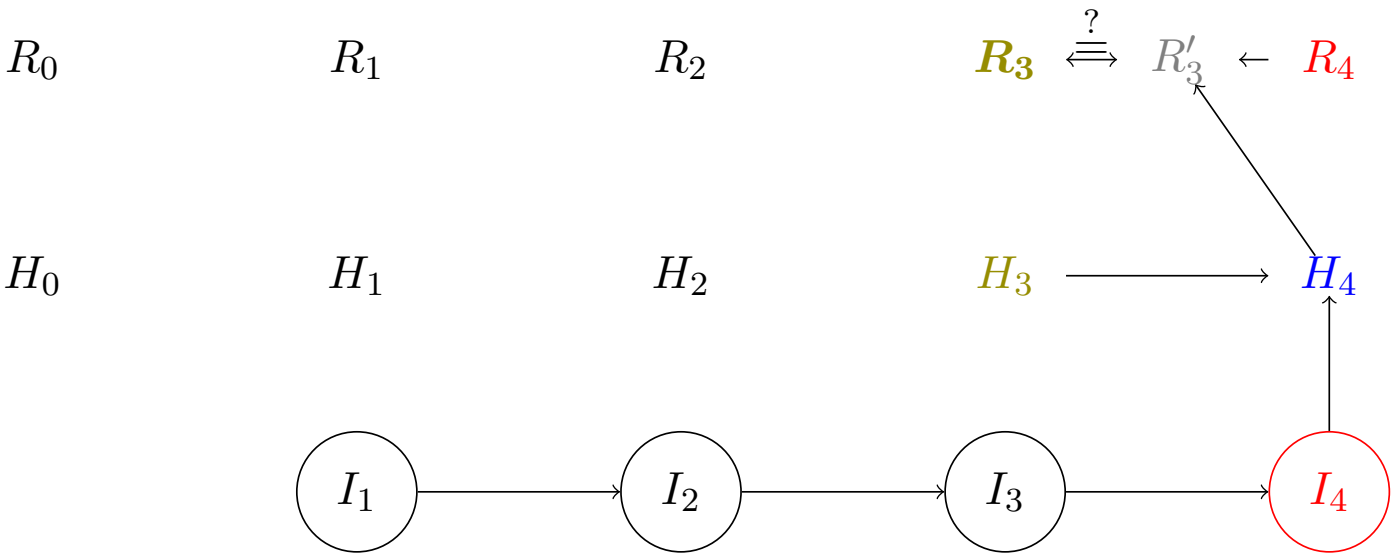
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Interakcia so softvérovým klientom



Záver

Ďalšie časti práce:

- Krok späť / krok dopredu
- Pohľad na zložitejšie transakcie cez hashovacie stromy
- Pohľad na postupnosti inštrukcií ako na regulárny jazyk

Možnosti rozpracovania:

- Hľadanie ďalších aplikácií prezentovaného prístupu
- Implementácia

Zložitejšie transakcie

Transakcia obsahujúca pole variabilnej dĺžky