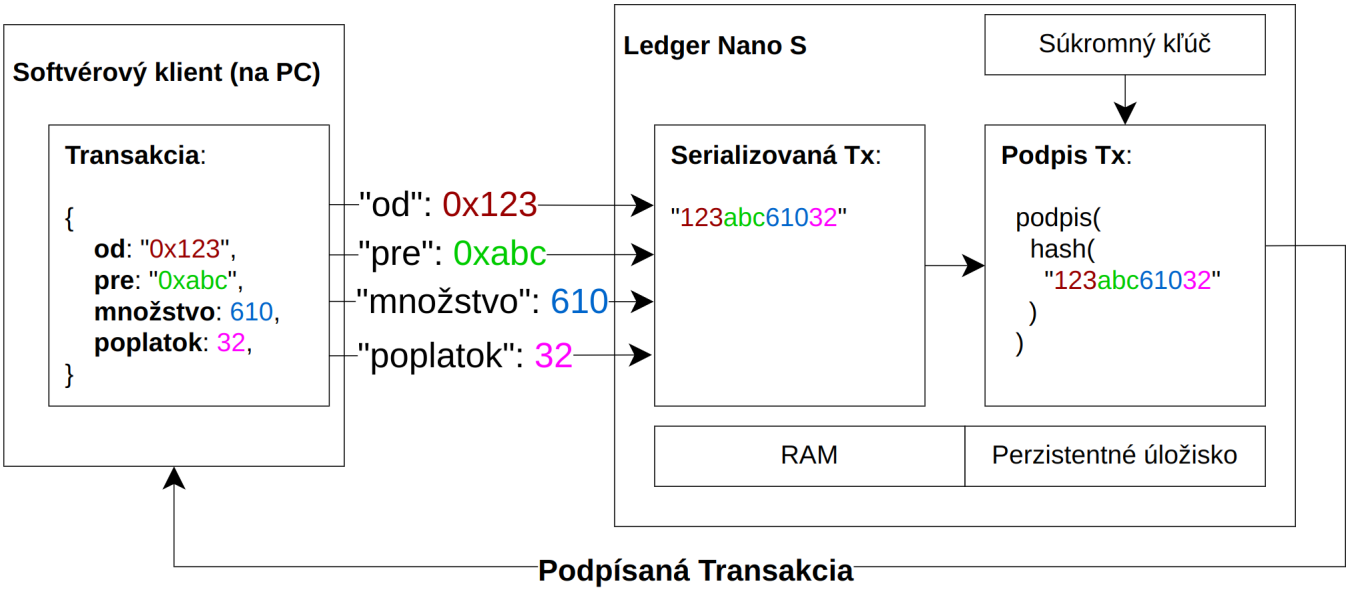
Manažovanie pracovných tokov v Ledger NanoS pomocou hashovacích stromov

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

14. júna 2024

Ledger NanoS - cieľ



Obmedzenia

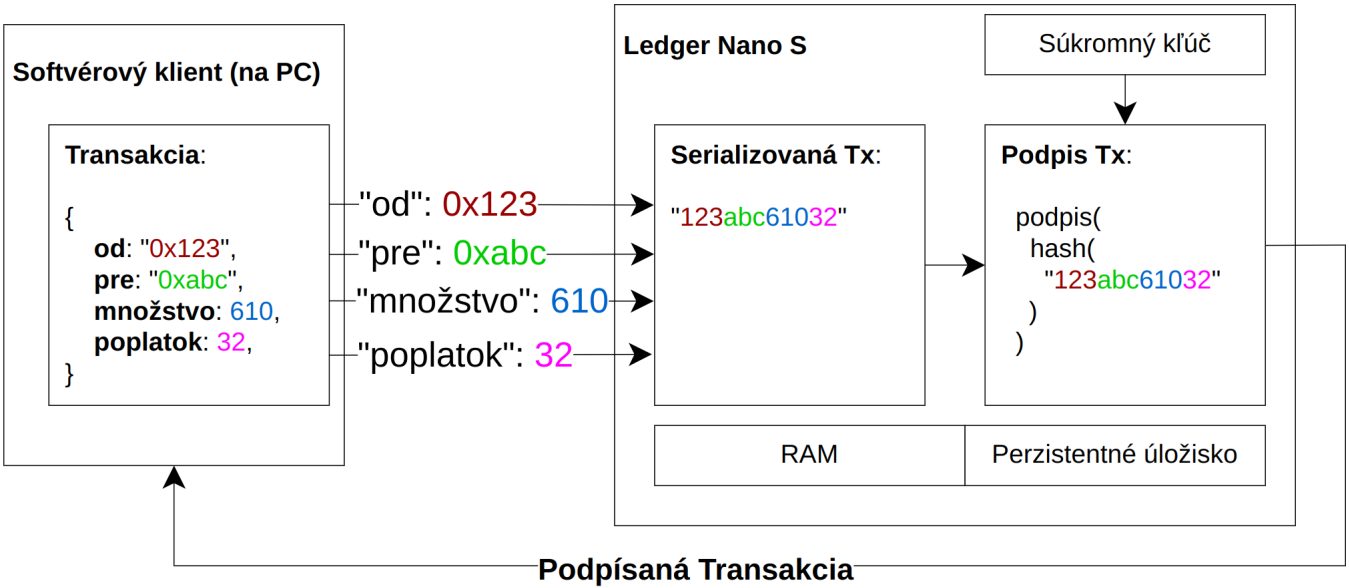
- Použiteľná RAM: $\sim 2\,\text{kB}$
- Kapacita APDU: $255\,\text{B}$
- Perzistentné úložisko: $\sim 160\,\text{kB}$
- Procesor: $\sim 60\,\text{MHz}$

Inštrukcia

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

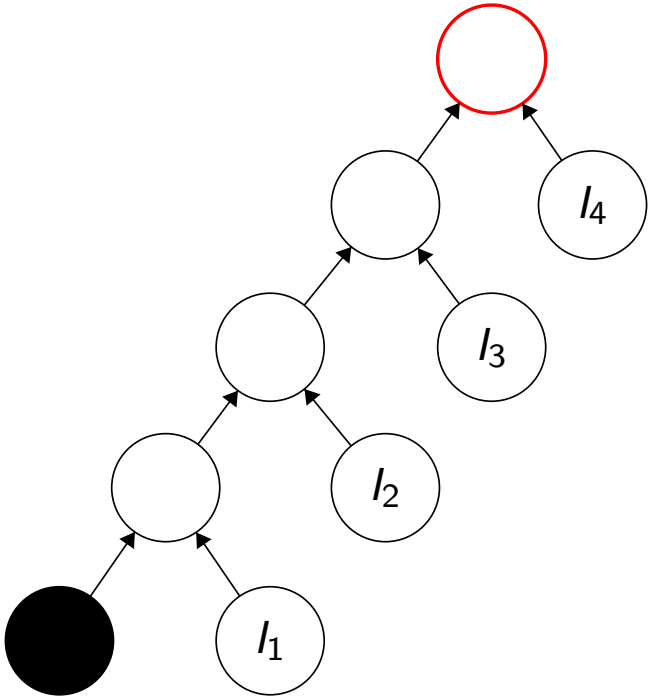
Známy prístup – Riešenie z BP

- DKA u klienta + overovanie integrity



Známy prístup – Riešenie z BP

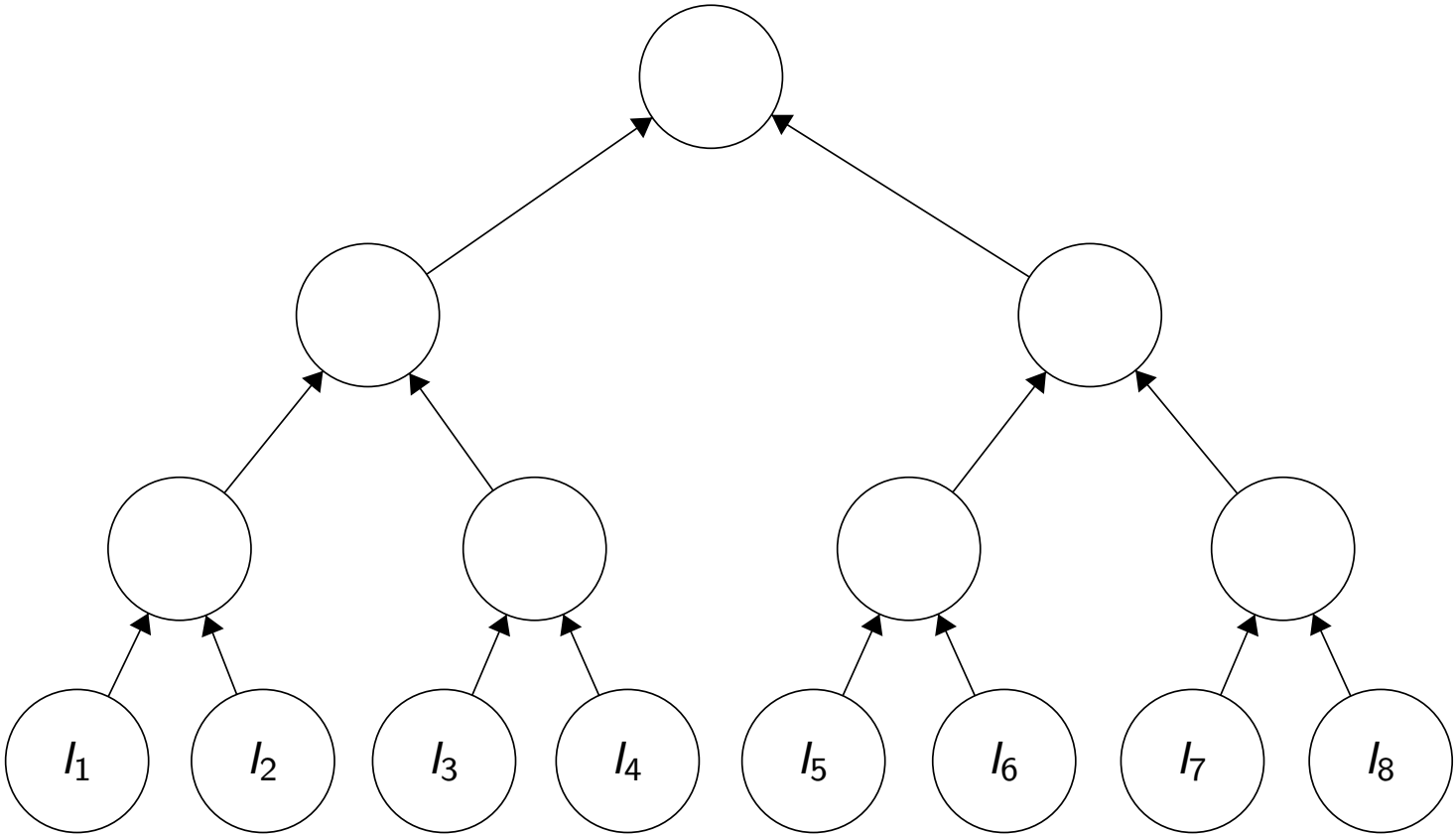
- Overenie až na konci



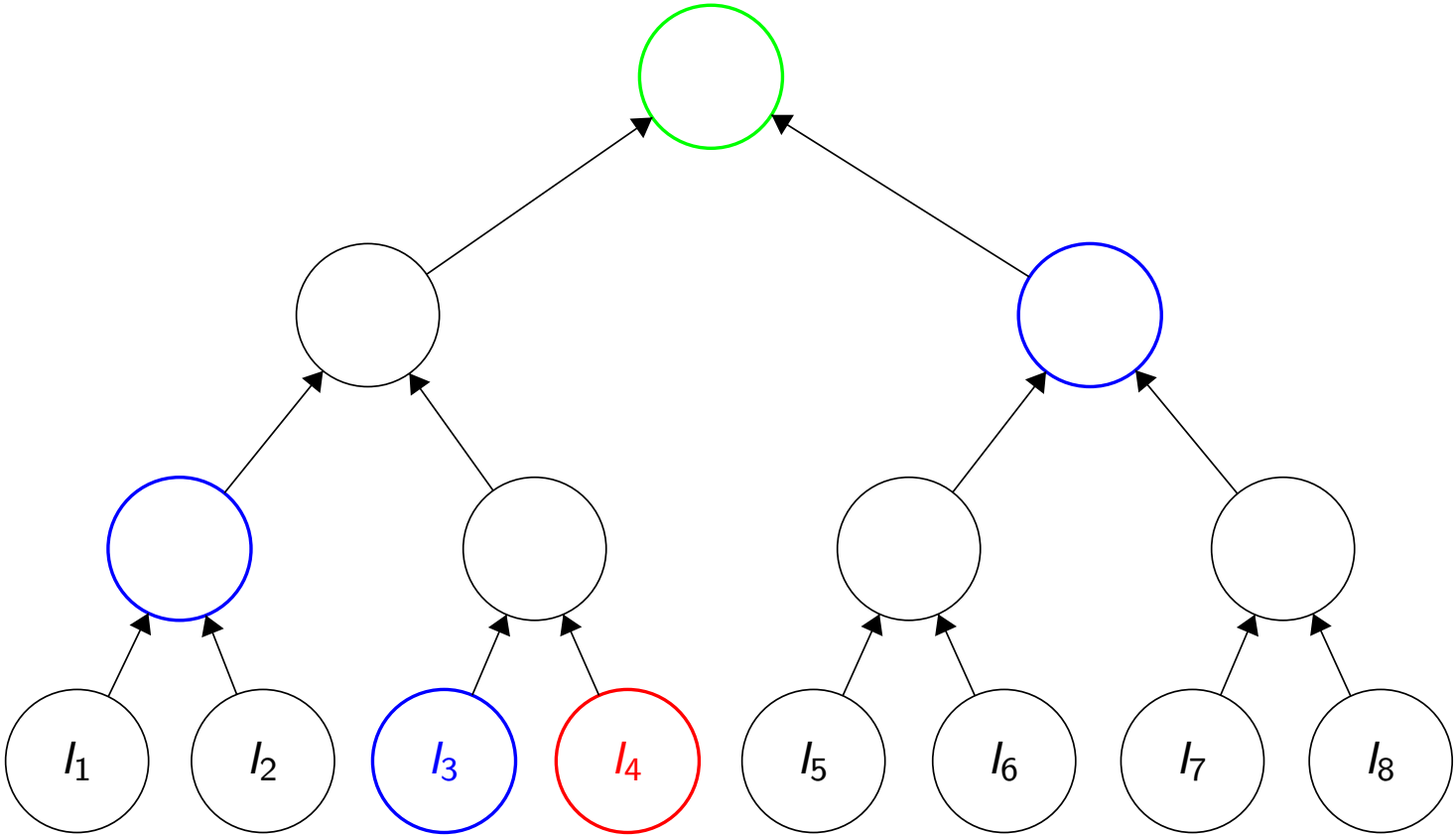
Hlavný cieľ našej práce

- Overovanie po každom kroku

Hashovacie stromy

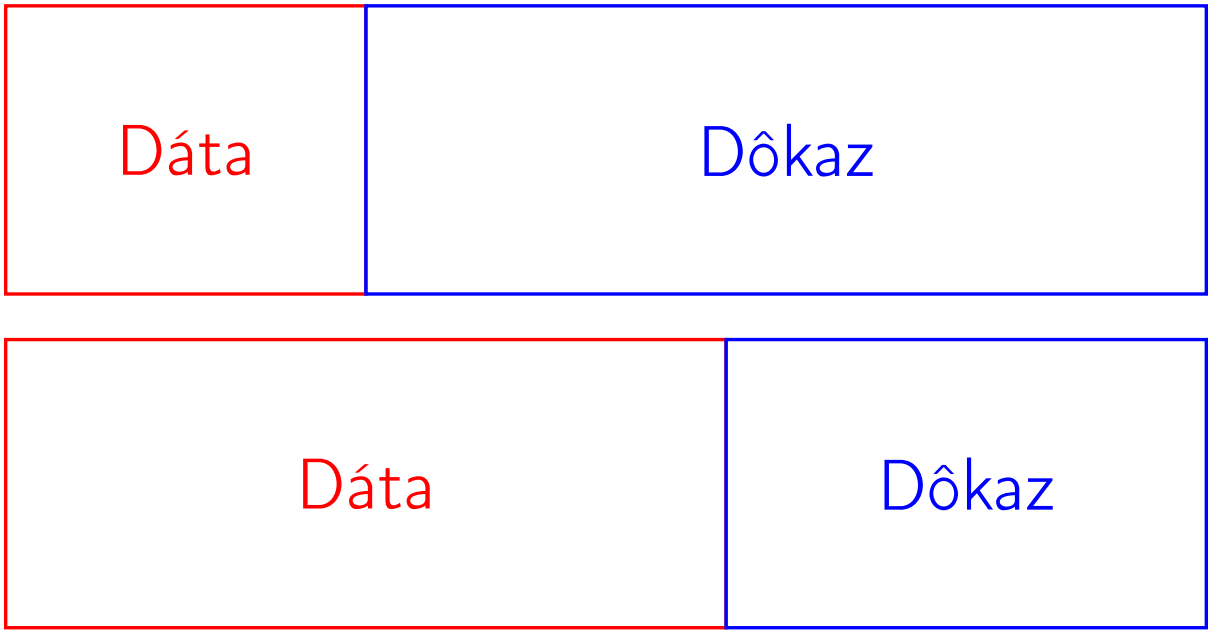


Hashovacie stromy



Správa s dôkazom

- APDU – 255 B



Iné vektor-komitment schémy

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

Rozšírenie inštrukcie

(**konštantná hlavička**, variabilné dáta)

$\downarrow$

((**konštanta** C_1, **. . . , konštanta** C_c), variabilné dáta)

Príklad: (("**POŠLI HODNOTU**", "**množstvo**"), 1234)

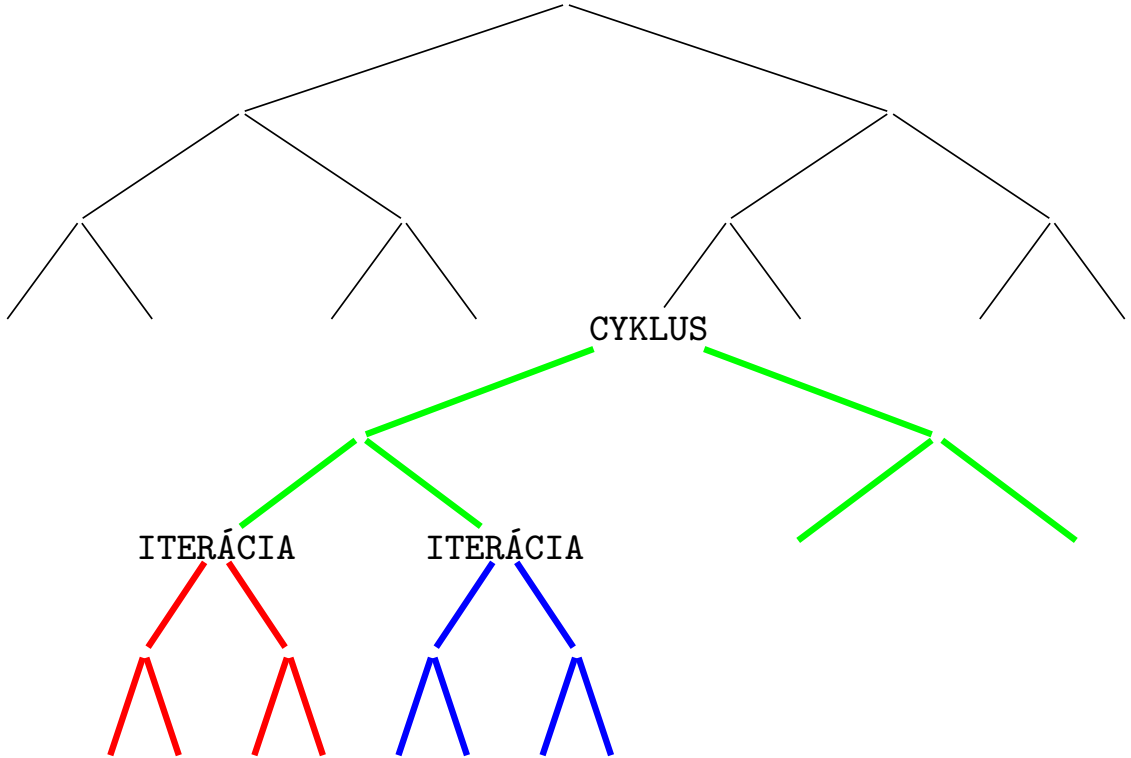
$\parallel$

`POŠLI_HODNOTU`("**množstvo**", 1234)

Polia

- Potreba heterogénnych polí variabilnej veľkosti
- Vnorené polia

Hashovacie stromy + polia



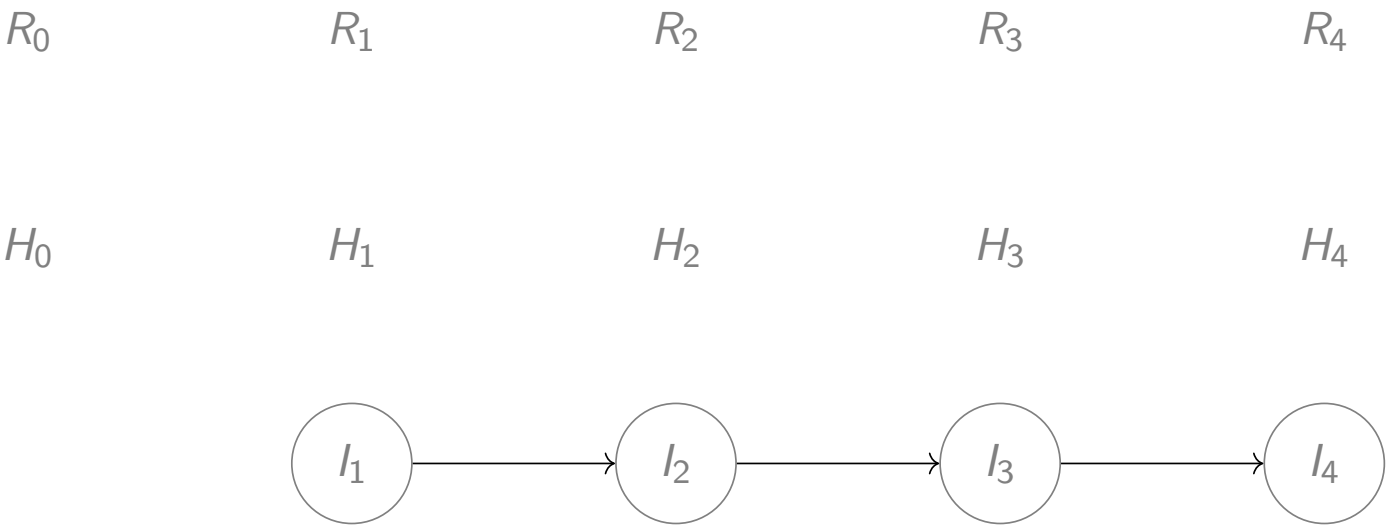
Efektívnejšie riešenie

Typy hashov

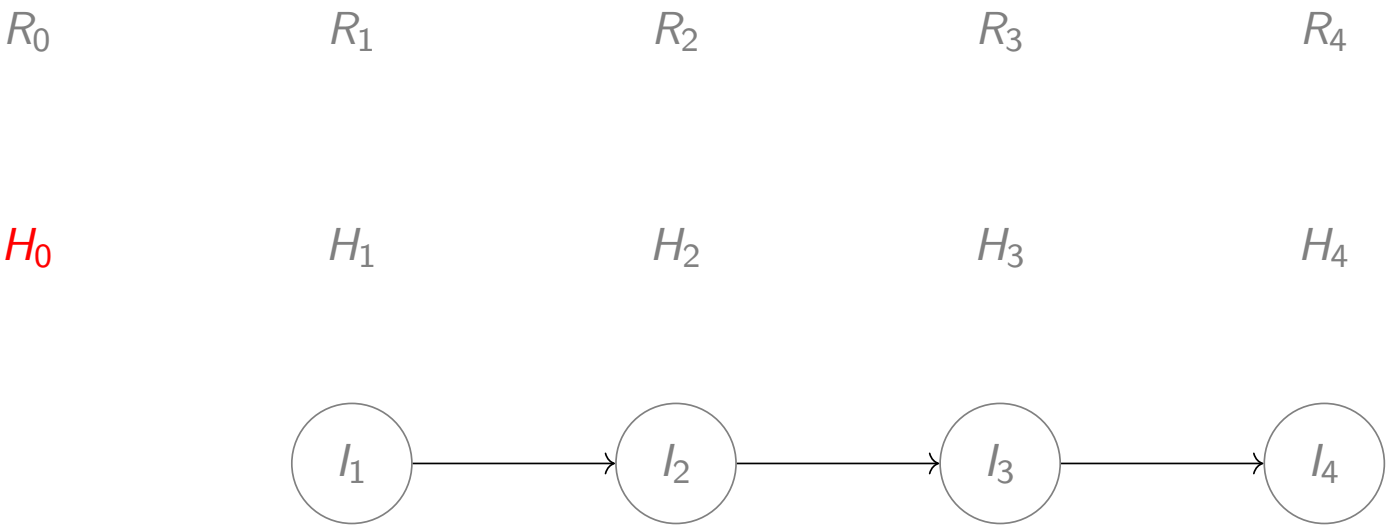
[POŠLI_DÁTA("**príjemca**", "xyz"), POŠLI_DÁTA("**množstvo**", 1234)]

- H_i – hash konštantných častí prvých i inštrukcií
  - $H_0 = hash(0x00)$
  - $H_i = hash(H_{i-1}, \text{hlavička}_i)$
- R_i – reverzný hash $H_i, H_{i+1}, ..., H_n$
  - $R_n = hash(0x01)$
  - $R_i = hash(R_{i+1}, H_{i+1})$

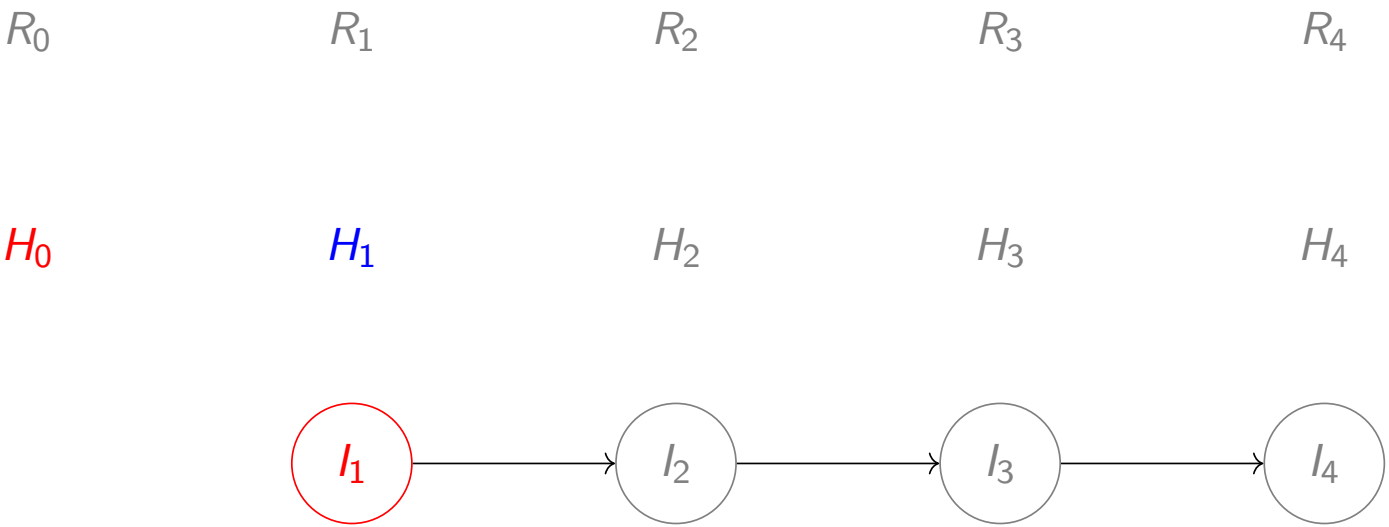
Pridanie nového typu transakcie



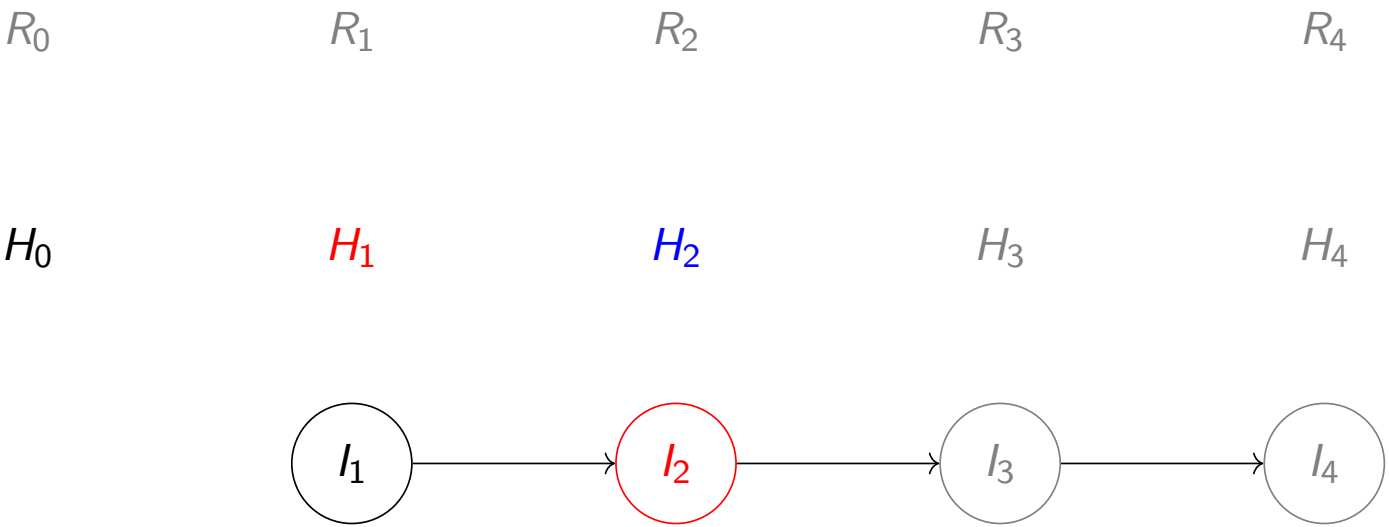
Pridanie nového typu transakcie



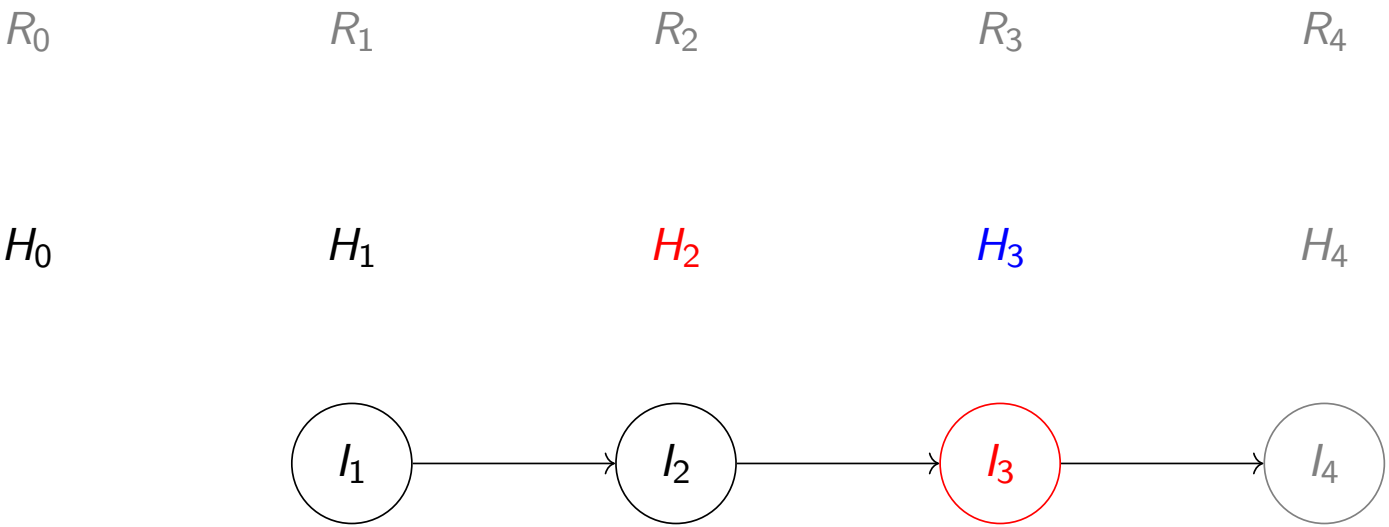
Pridanie nového typu transakcie



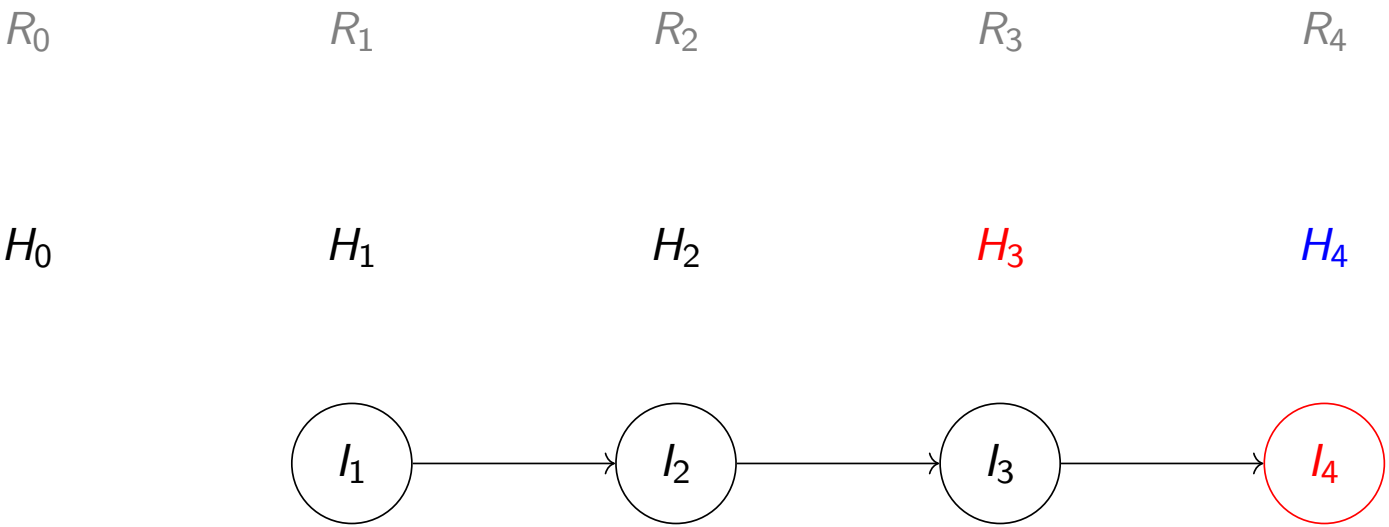
Pridanie nového typu transakcie



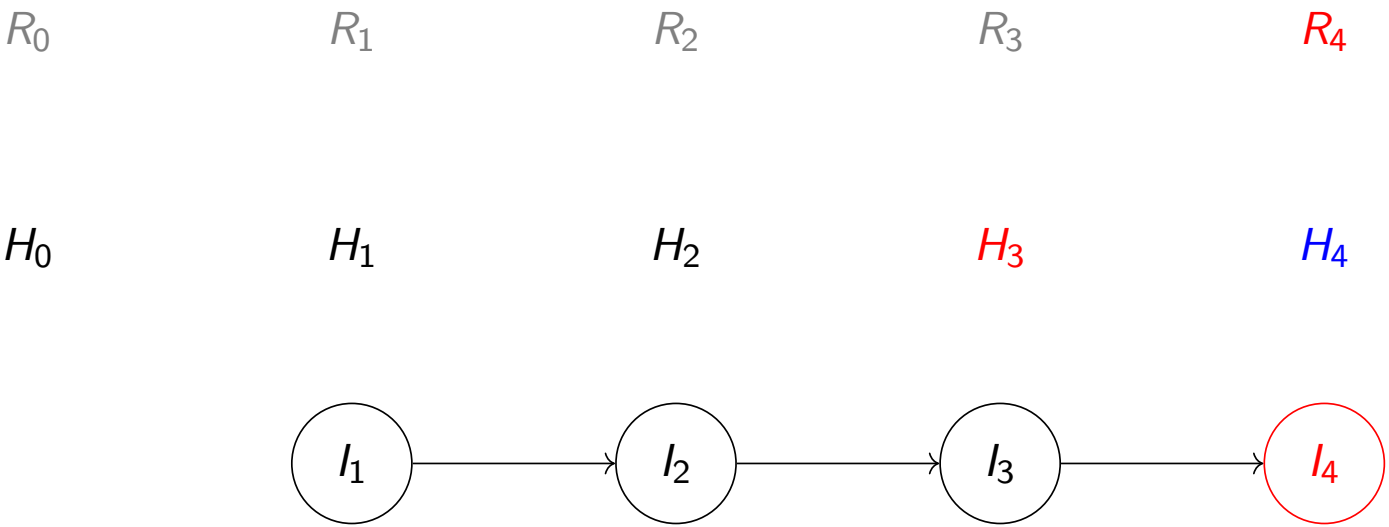
Pridanie nového typu transakcie



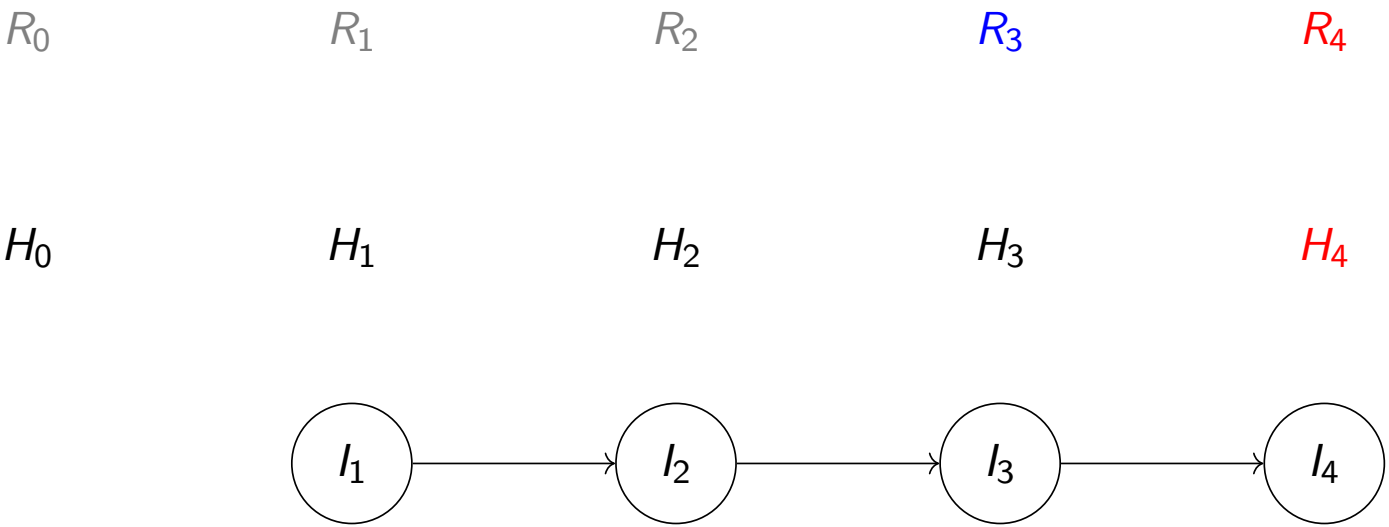
Pridanie nového typu transakcie



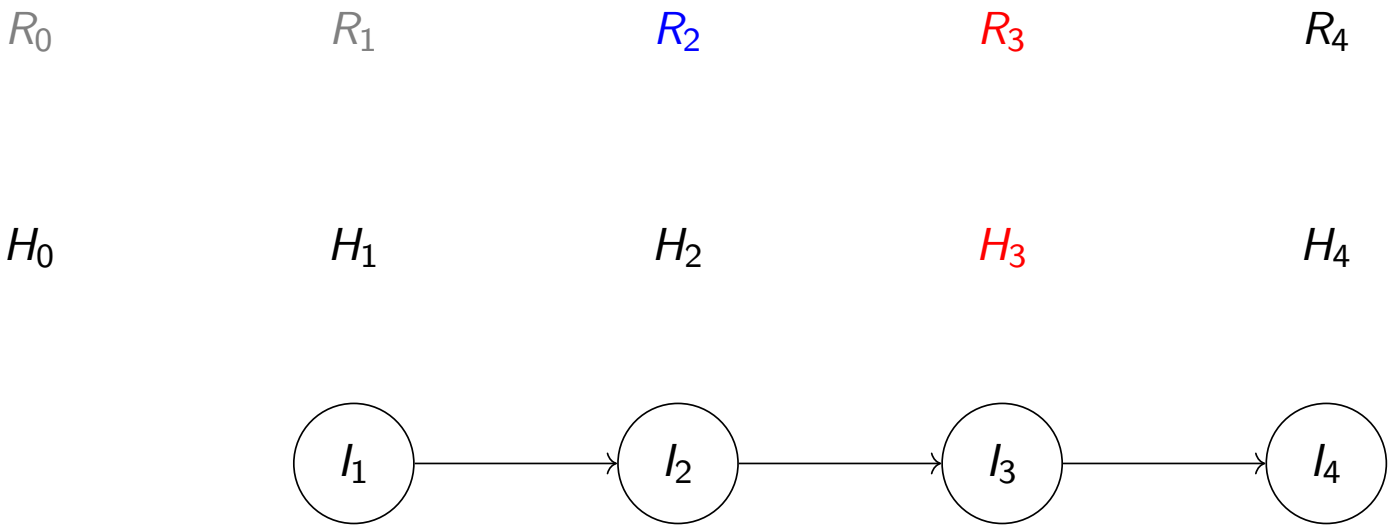
Pridanie nového typu transakcie



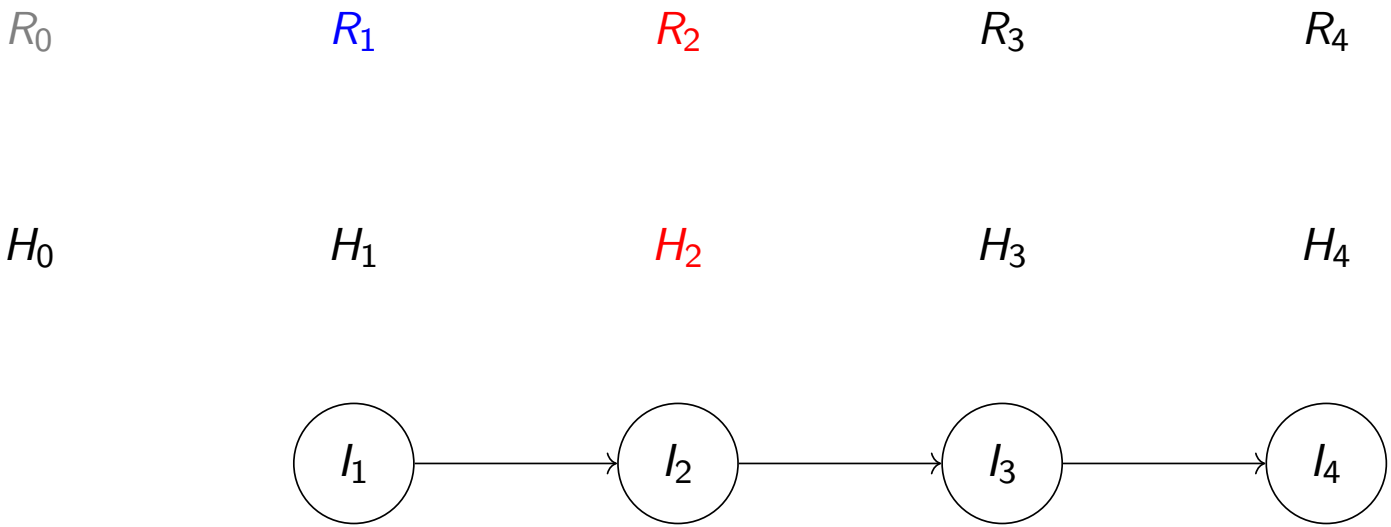
Pridanie nového typu transakcie



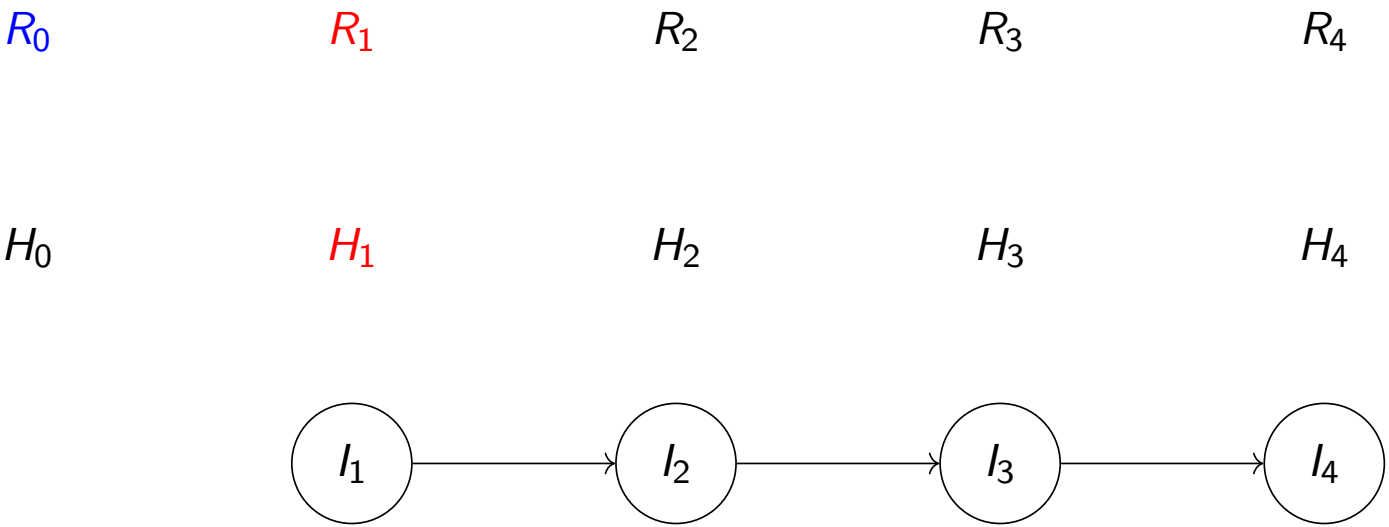
Pridanie nového typu transakcie



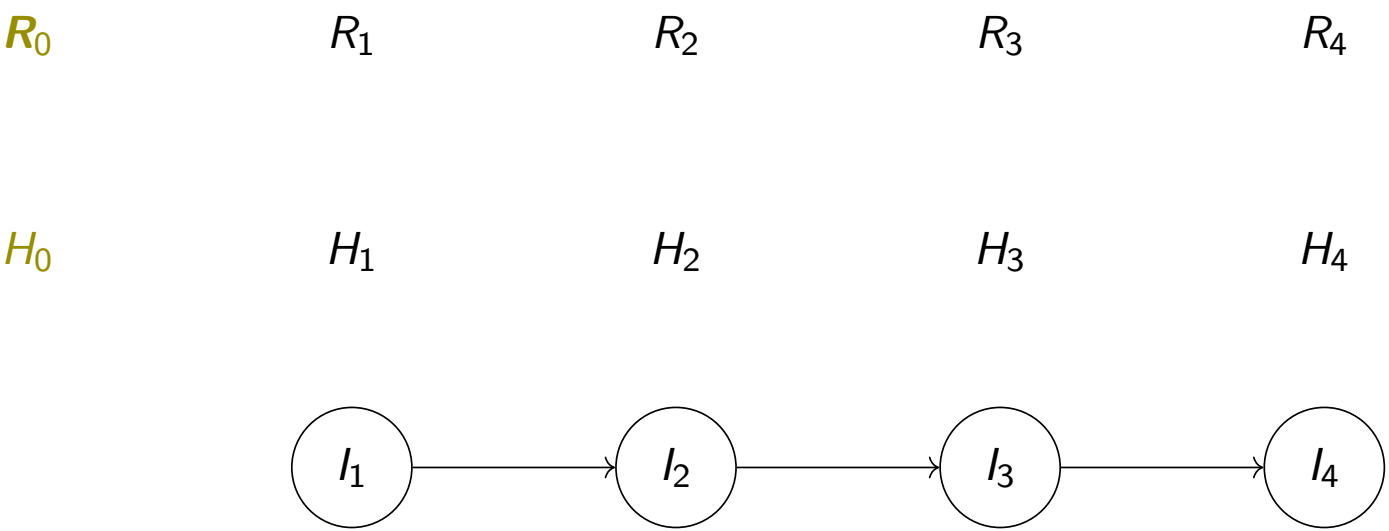
Pridanie nového typu transakcie



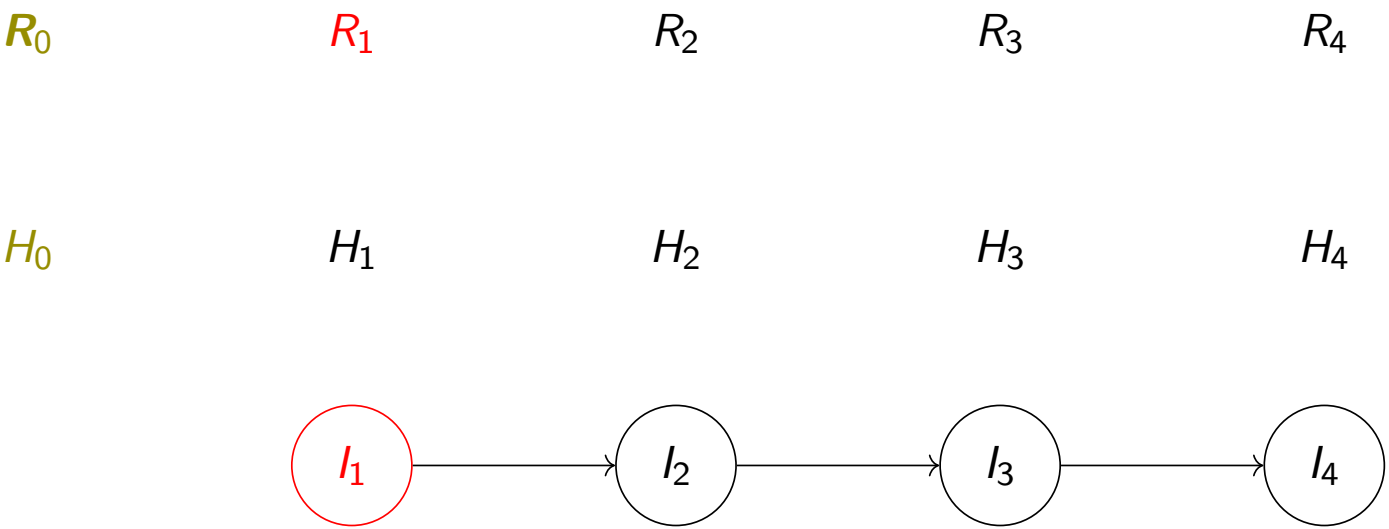
Pridanie nového typu transakcie



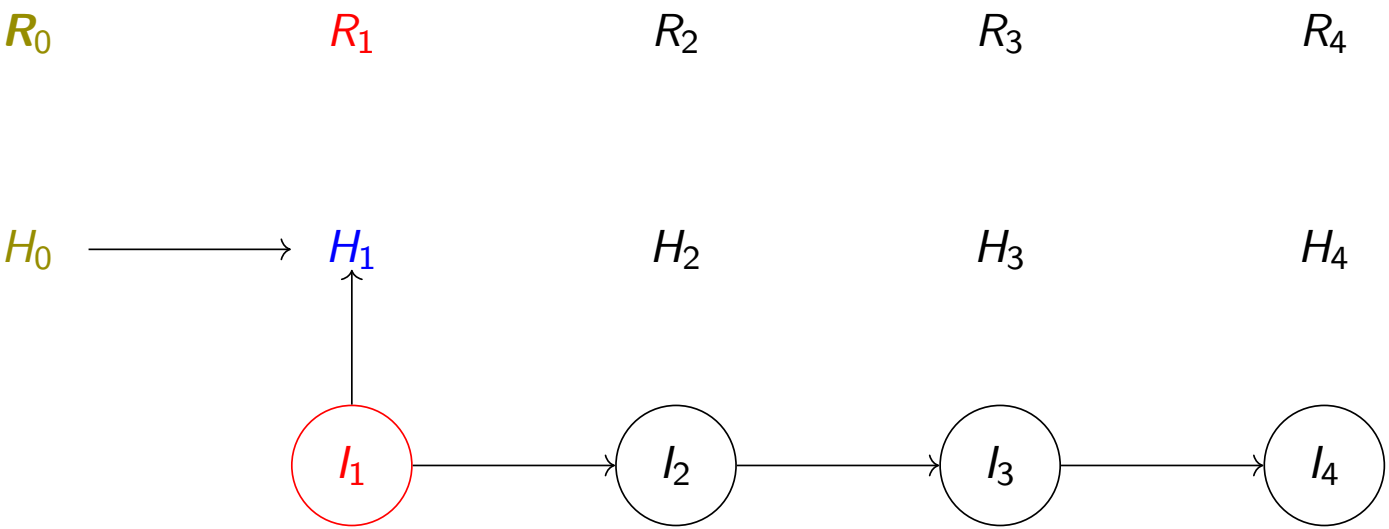
Interakcia so softvérovým klientom



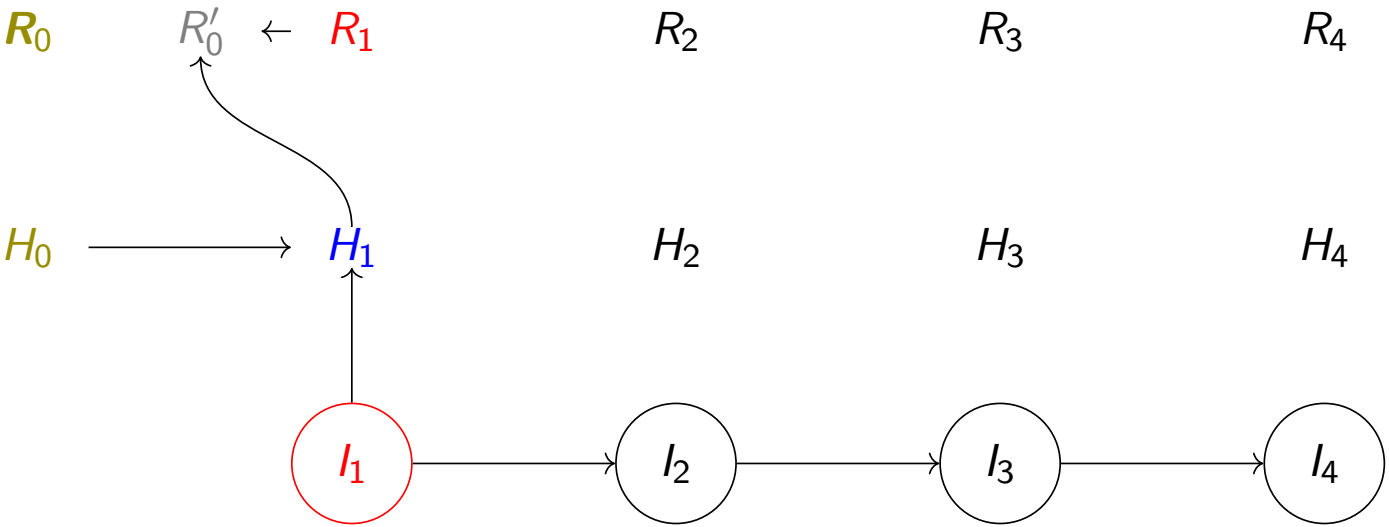
Interakcia so softvérovým klientom



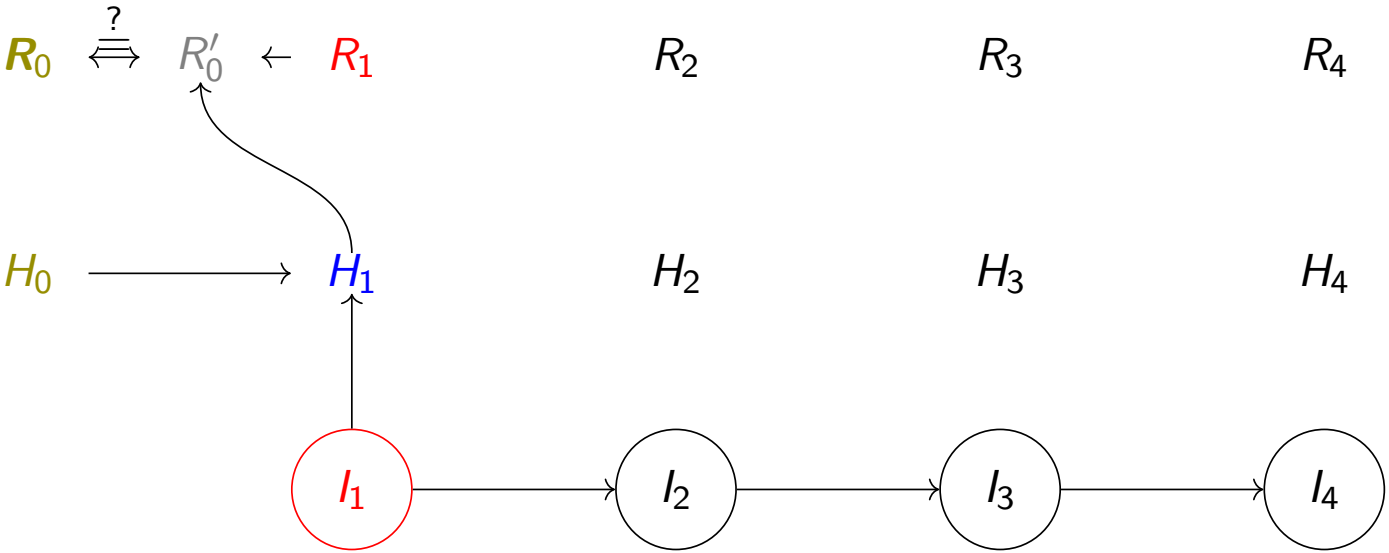
Interakcia so softvérovým klientom



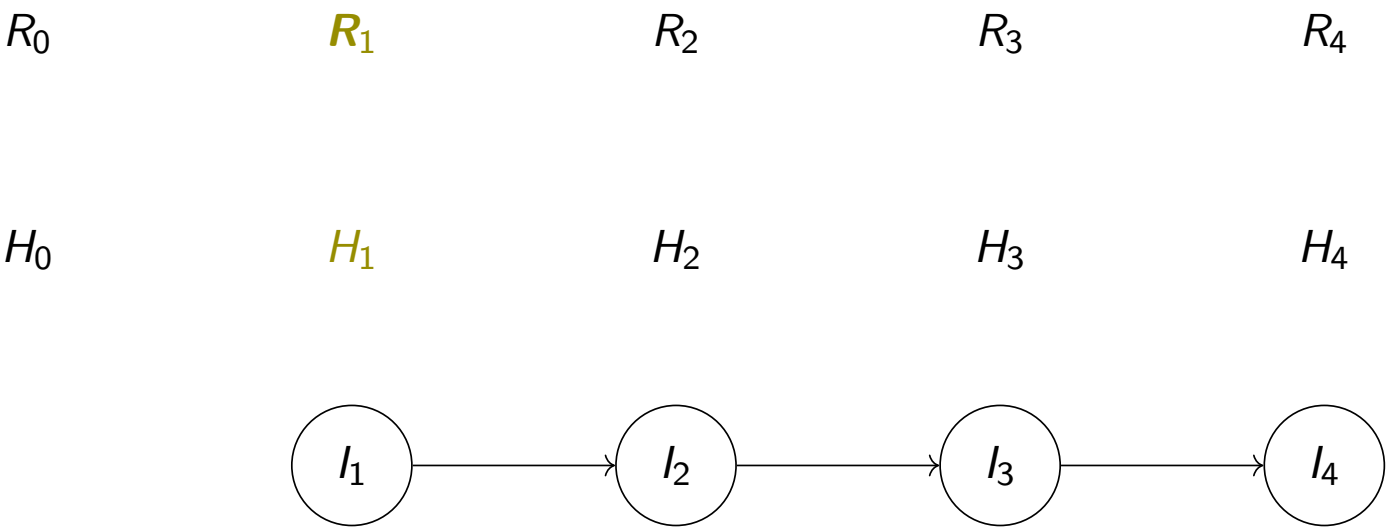
Interakcia so softvérovým klientom



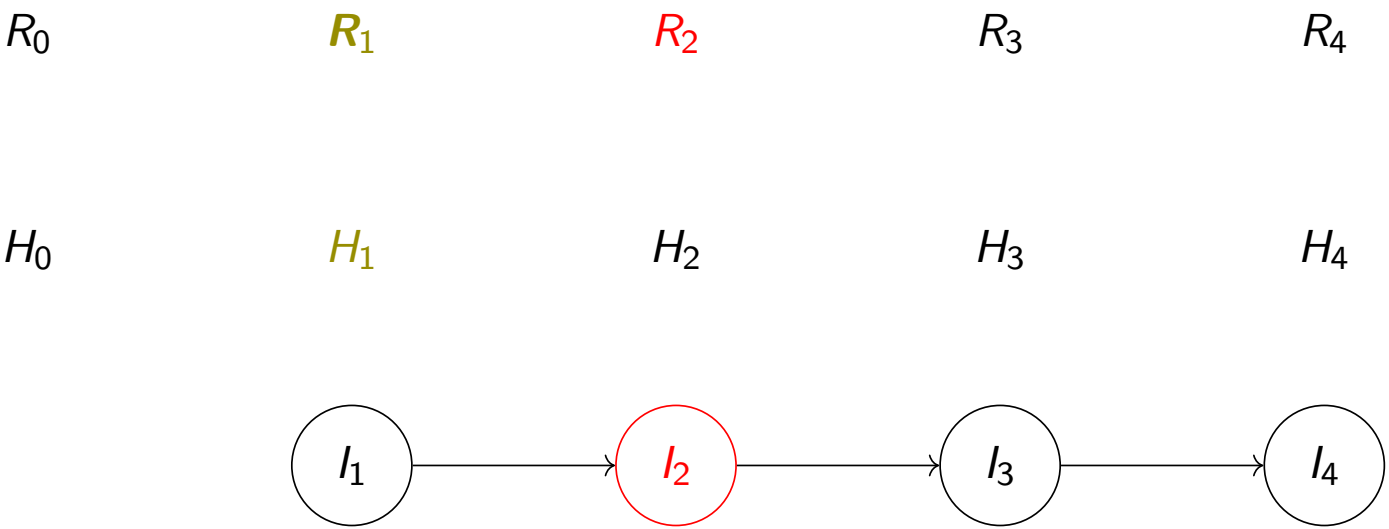
Interakcia so softvérovým klientom



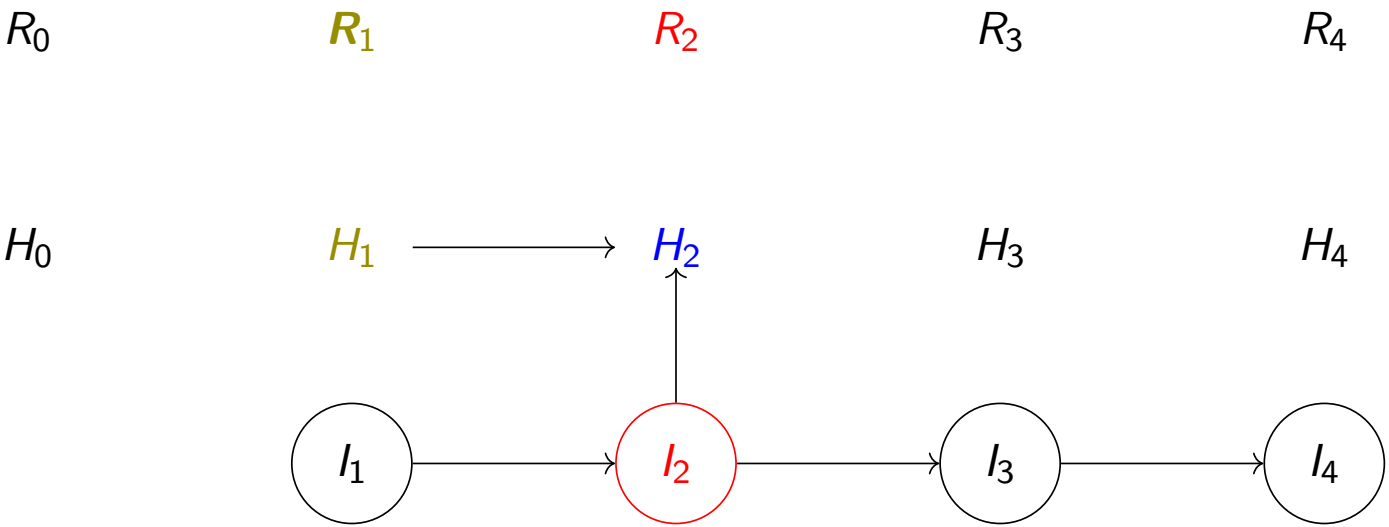
Interakcia so softvérovým klientom



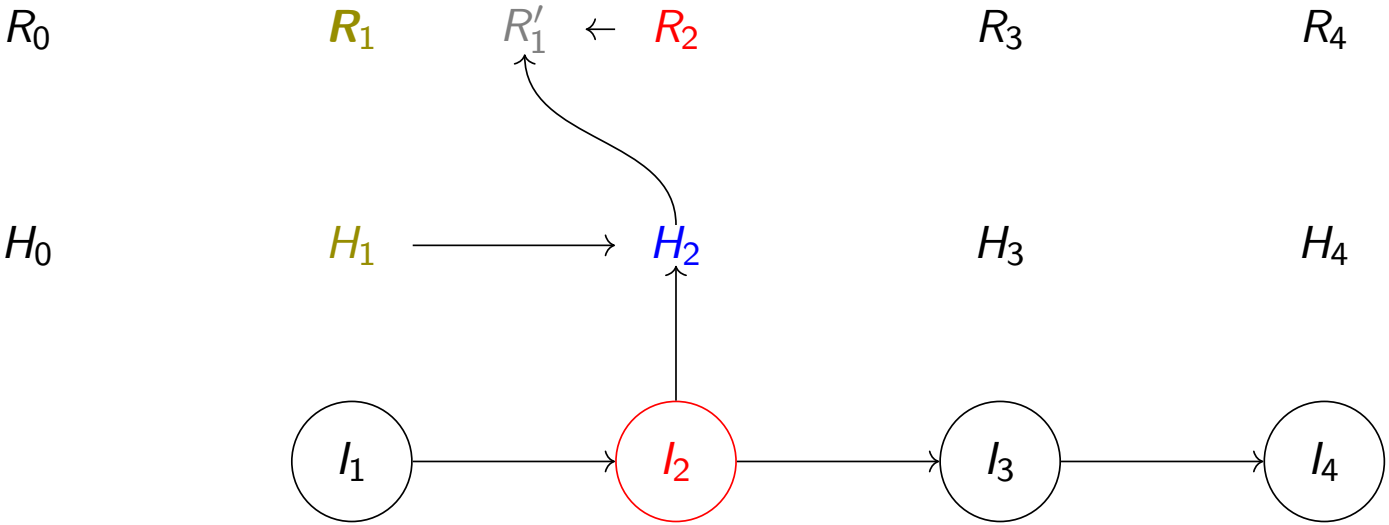
Interakcia so softvérovým klientom



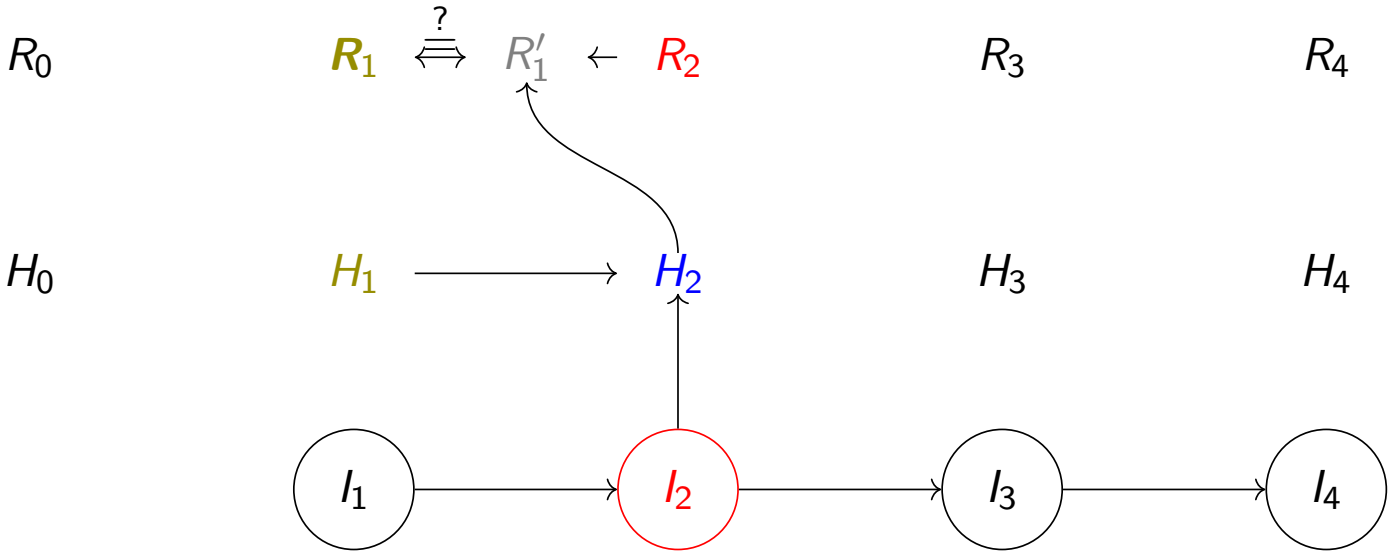
Interakcia so softvérovým klientom



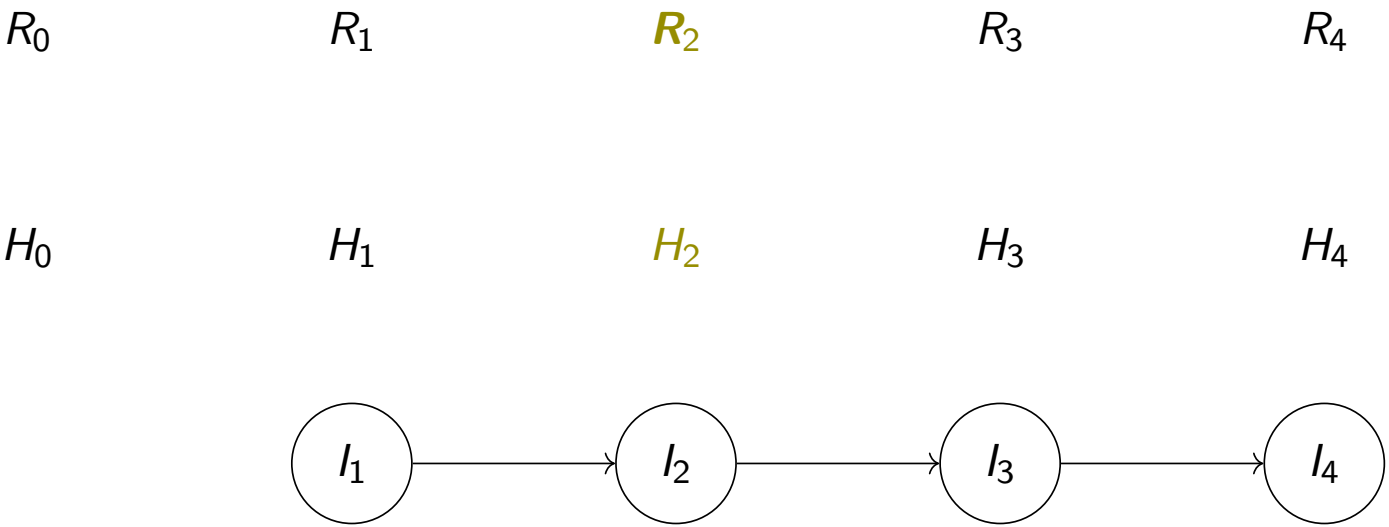
Interakcia so softvérovým klientom



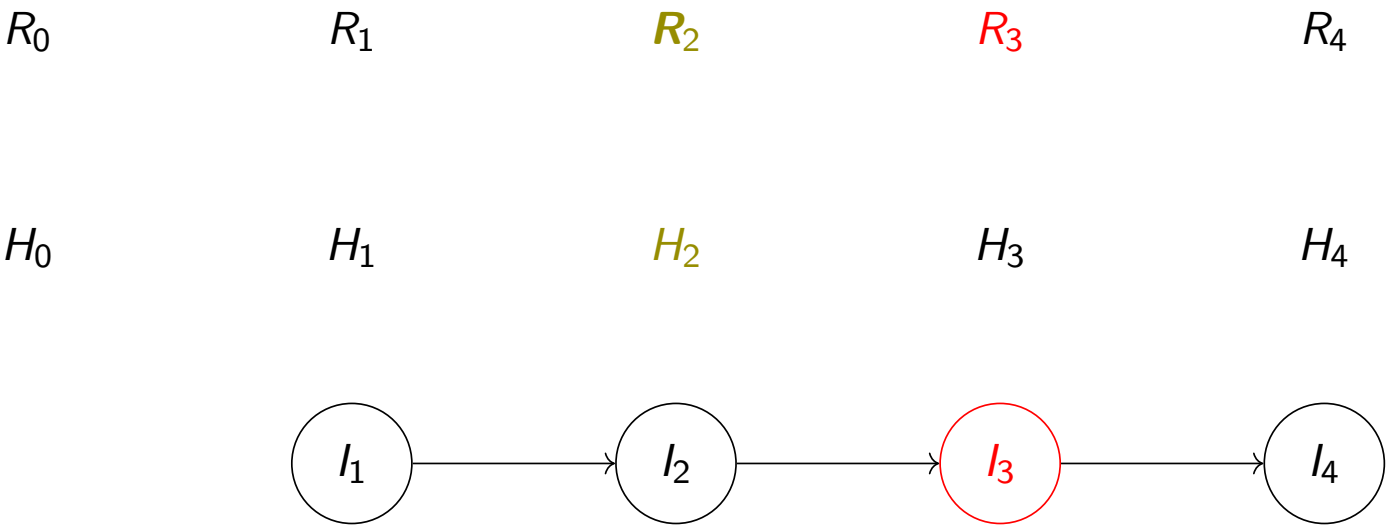
Interakcia so softvérovým klientom



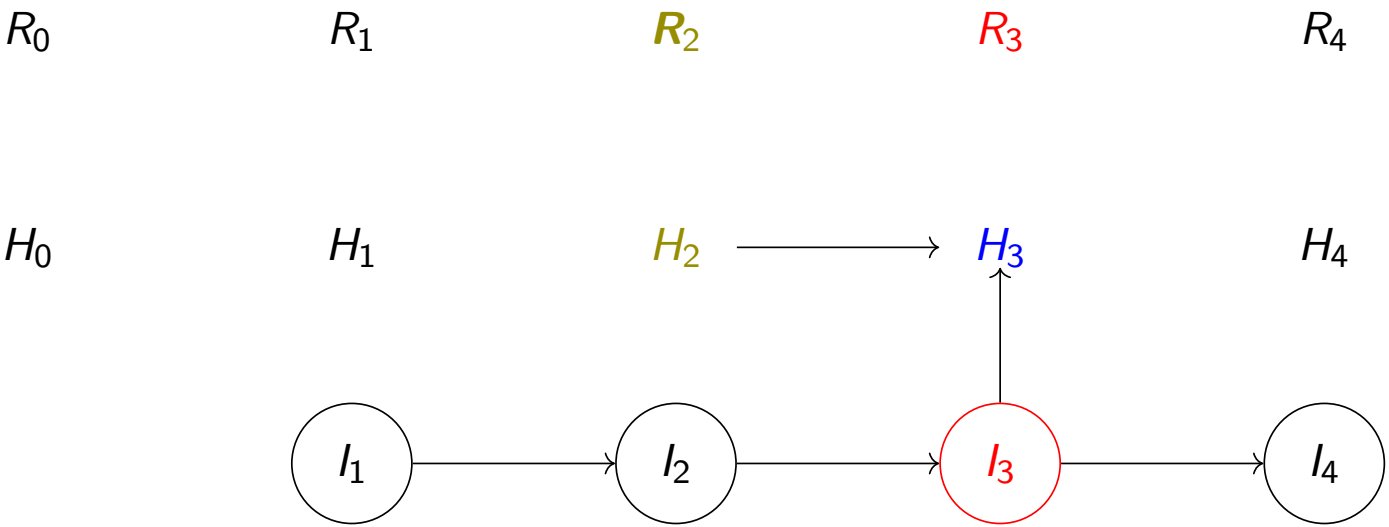
Interakcia so softvérovým klientom



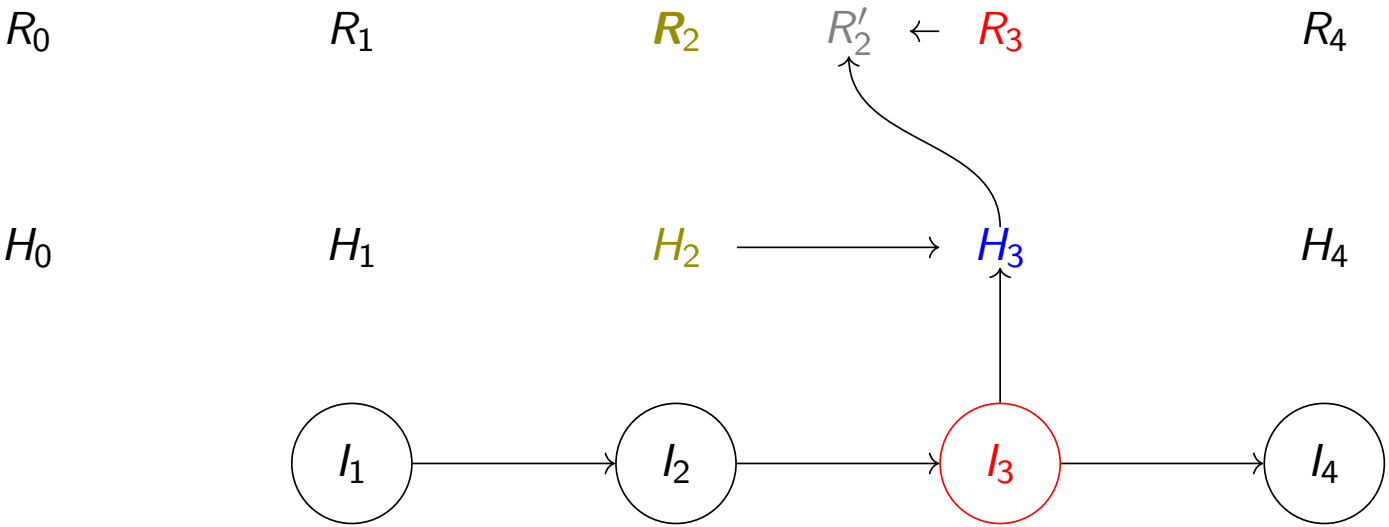
Interakcia so softvérovým klientom



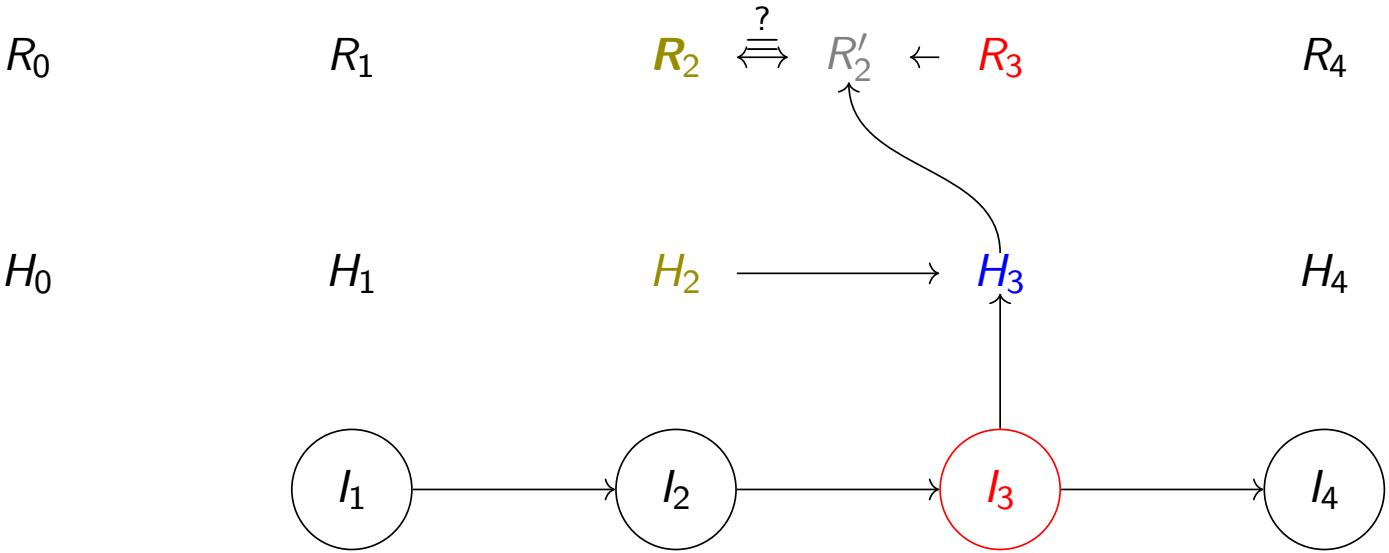
Interakcia so softvérovým klientom



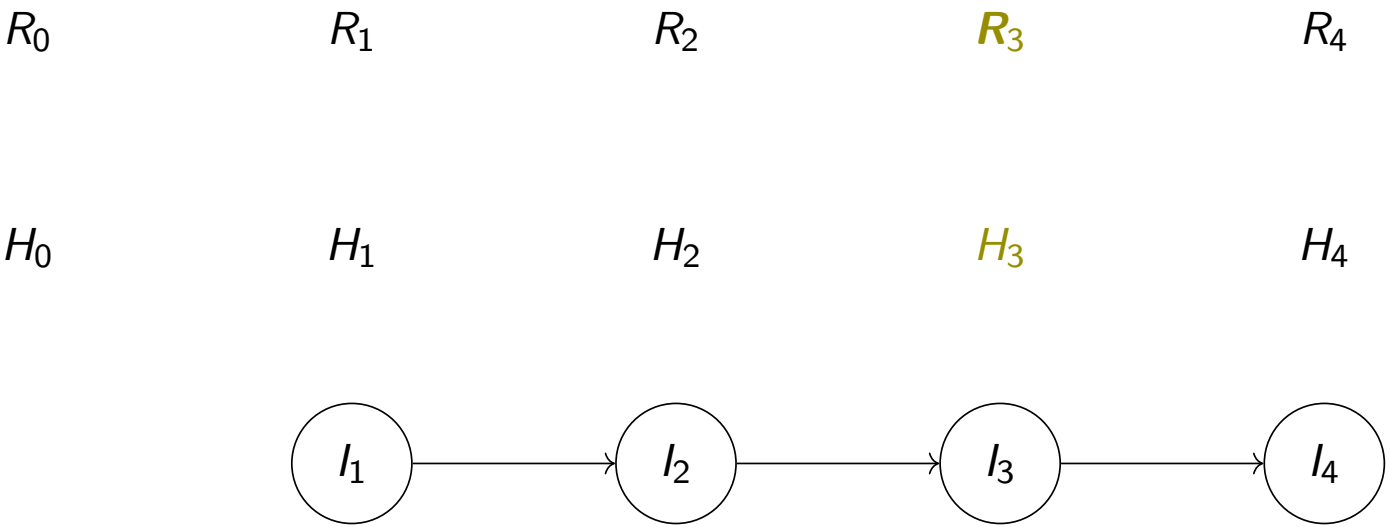
Interakcia so softvérovým klientom



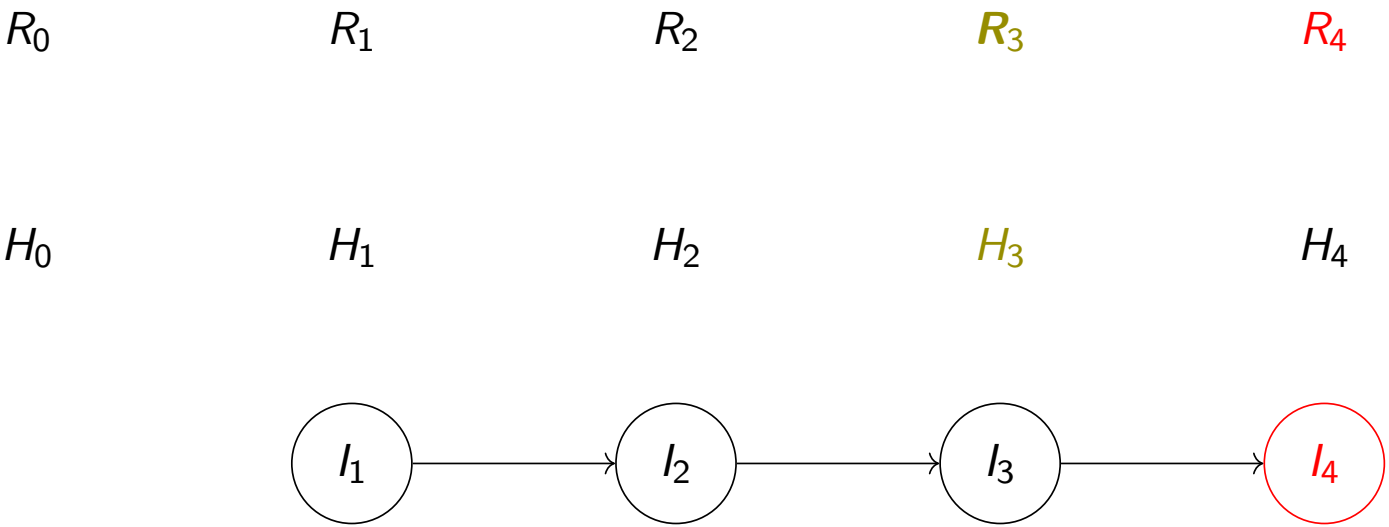
Interakcia so softvérovým klientom



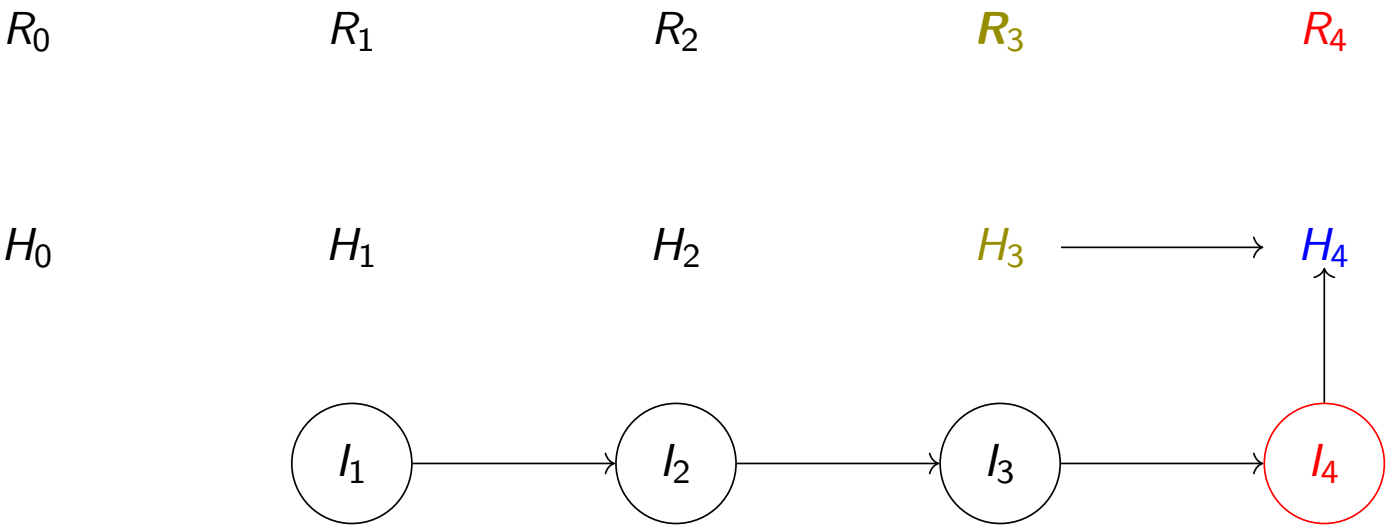
Interakcia so softvérovým klientom



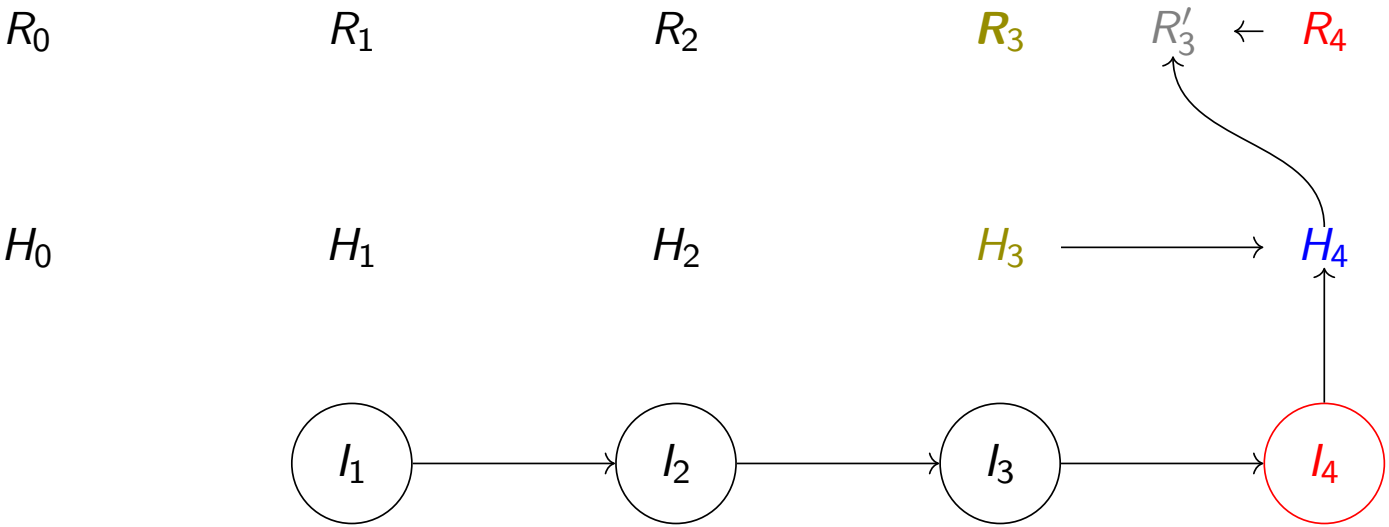
Interakcia so softvérovým klientom



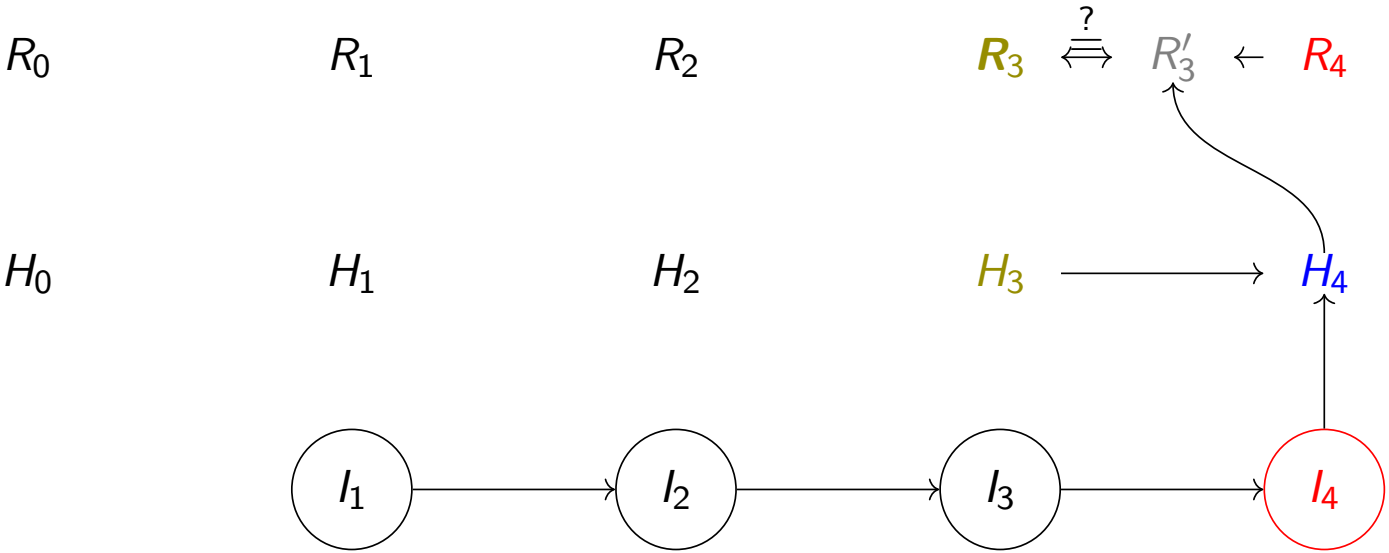
Interakcia so softvérovým klientom



Interakcia so softvérovým klientom

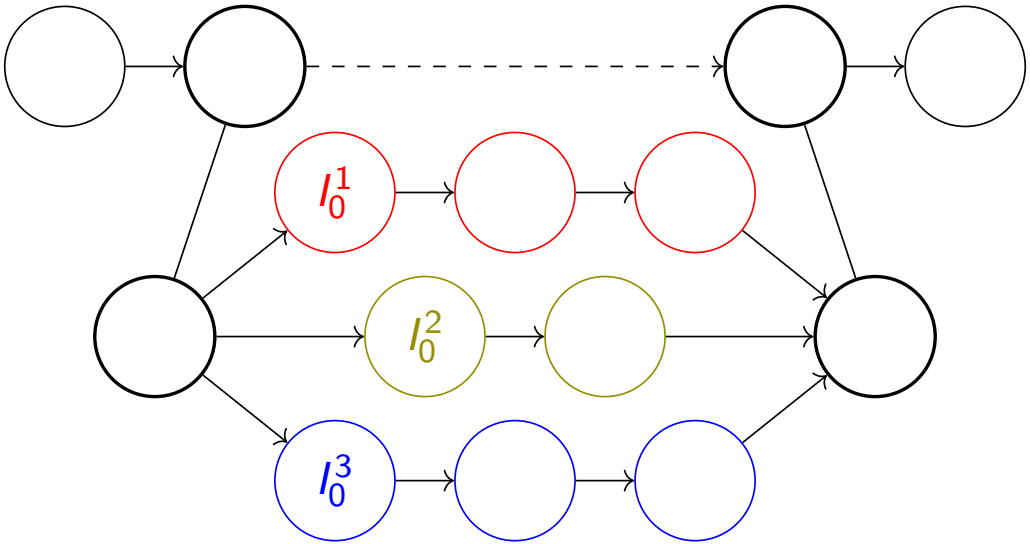


Interakcia so softvérovým klientom



Transakcia obsahujúca pole

```
ZAČNI_CYKLUS([R_0^1, R_0^2, R_0^3])
   ZAČNI_ITERÁCIU(3), ..., UKONČI_ITERÁCIU()
   ...
   ZAČNI_ITERÁCIU(3), ..., UKONČI_ITERÁCIU()
   ZAČNI_ITERÁCIU(1), ..., UKONČI_ITERÁCIU()
UKOČI_CYKLUS()
```



Zdôvodnenie bezpečnosti

- Vývojár vytvorí šablónu transakcie, vypočíta R_0
- Postupnosť inštrukcií ***spĺňa šablónu*** – rekurzívna definícia
  - Intuitívne
- Postupnosť inštrukcií ***hashovo spĺňa šablónu*** – overenie proti R_0

Veta

Pre útočníka je neuskutočniteľné vypočítať postupnosť inštrukcií, ktorá **hashovo spĺňa** šablónu a zároveň túto šablónu **nespĺňa**.

Krok späť (undo / redo)

- Používateľ sa môže chcieť vrátiť k už potvrdeným dátam.
- Riešenie:
  - Použitie dopredných a reverzných hashov
  - Hashe musia zahŕňať aj variabilné dáta z inštrukcií
  - Aplikácia počas behu tieto hashe vypočítava

Zhrnutie

Hlavné výsledky práce:

- Návrh 2 riešení pre overovanie transakcie po každom kroku
  1. Hashovacie stromy
  2. Dopredné a reverzné hashe
     - Klient musí okrem dát poslať iba 1 hash
- Zdôvodnenie neuskutočniteľnosti vytvorenia podpisu nepovolenej transakcie
- Návrh riešenia problému vracania sa späť

Možnosti rozpracovania:

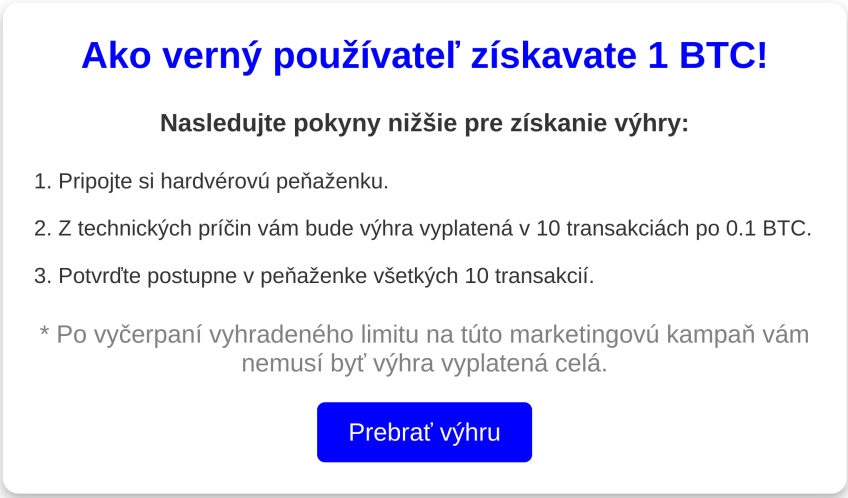
- Skúmanie iných aplikácií metódy dopredných a reverzných hashov
- Implementácia

Otázka od oponenta

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

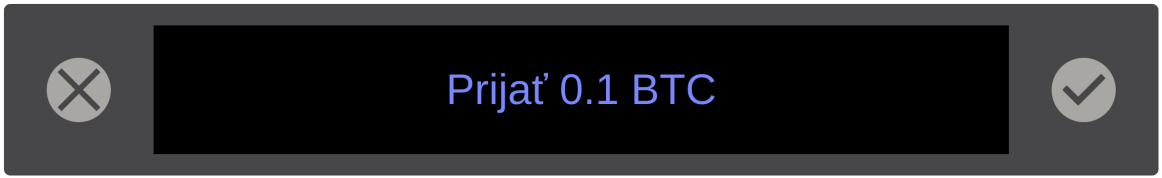
Otázka od oponenta

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?



Otázka od oponenta – fiktívna transakcia 1/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?



Otázka od oponenta – fiktívna transakcia 1/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 1/10

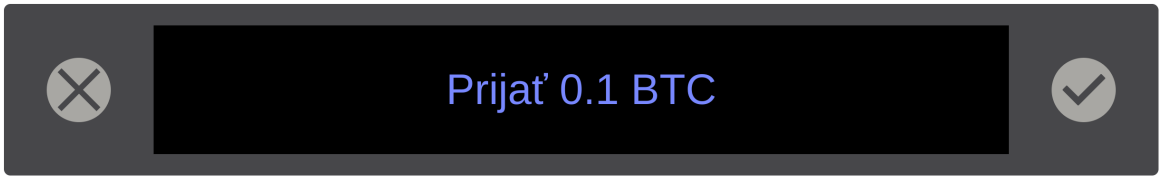
Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 1/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 2/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?



Otázka od oponenta – fiktívna transakcia 2/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 2/10

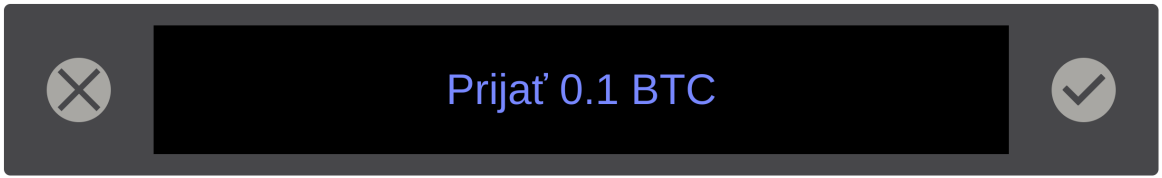
Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 2/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 3/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?



Otázka od oponenta – fiktívna transakcia 3/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 3/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – fiktívna transakcia 3/10

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – podvrhnutá skutočná transakcia

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – podvrhnutá skutočná transakcia

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – podvrhnutá skutočná transakcia

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?

Otázka od oponenta – podvrhnutá skutočná transakcia

Ste si vedomý konkrétneho útoku, ktorý by využíval neskorú validáciu inštrukcií v existujúcich riešeniach?