Metastabilné protokoly na dosiahnutie konsenzu

Bc. Matej Štubniak

doc. RNDr. Martin Stanek, PhD.

Rodina protokolov Snow

- komunikačná zložitosť - $O(\log n)$ až $O(1)$
- vysoká priepustnosť
- dobrá škálovateľnosť
- nehybnosť

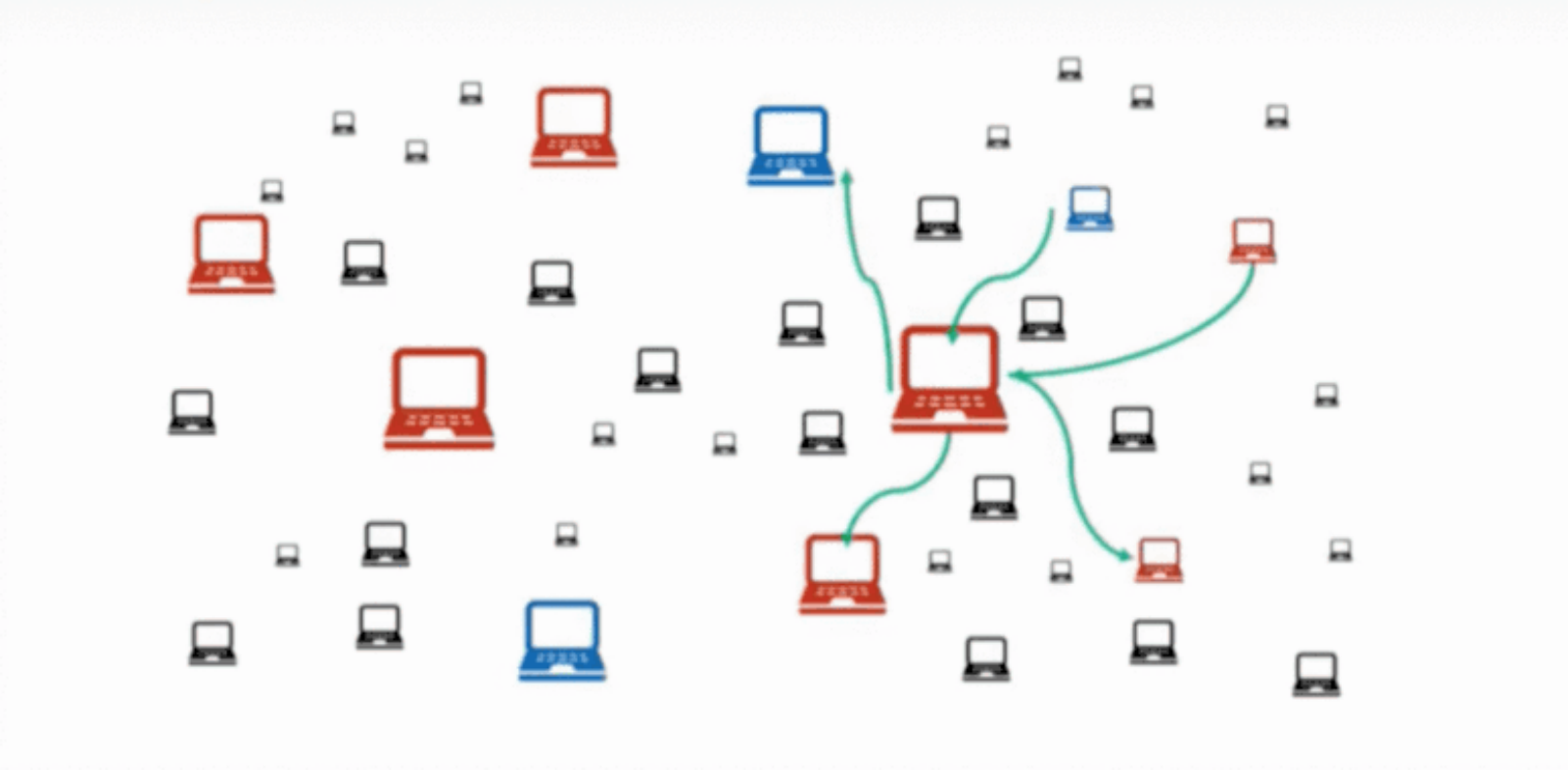
Garancie

- 1. 2 korektné uzly sa rozhodnú naopak len so zanedbateľnou pravdepodobnosťou ($\leq \epsilon$)
- 2. beh protokolu skončí v rámci $\omega(\log n)$ kôl so striktne kladnou pravdepodobnosťou
- 3. ak počet nepriateľských uzlov $f \in O(\sqrt{n})$, potom beh protokolu skončí s vysokou pravdepodobnosťou ($\geq 1 - \epsilon$) v rámci $O(\log n)$ kôl

Slush

- kvôli jednoduchosti - rozhodovanie medzi červenou a modrou farbou
- kľúčová idea - voľba náhodnej podmnožiny uzlov veľkosti k, ktorým sa posiela žiadosť
- hranica $\alpha.k$, kde $k \leq n$, $\alpha > \lfloor k/2 \rfloor$
- m kôl
- nie je odolný voči prítomnosti nepriateľských uzlov

Slush



Snowflake

- každý uzol má svoje počítadlo - počet po sebe idúcich kôl, ktoré vrátia tú istú farbu
  - pri zmene farby je počítadlo resetované
  - ináč zvýšime o 1
- ak počítadlo $> \beta$, akceptujeme

Snowball

- ďalšie počítadlo, pre obe farby, zvýšené pri každej úspešnej žiadosti
- uzol zmení farbu, len ak sa toto počítadlo pre druhú farbu stane väčším

Avalanche

- udržiavanie orientovaného acyklického grafu všetkých známych transakcií (so spoločným koreňom)
- problémom sú konfliktné transakcie
- žiadosť ohľadom jednej transakcie sa týka všetkých tých, ktoré sú z nej v danom grafe dosiahnuteľné
  - uzol odpovie kladne, ak sú všetci jeho predkovia preferovanou možnosťou v jednotlivých konfliktných množinách
- úspešné hlasovanie o transakcii - dostane žetón (prebieha len raz)
  - mieru dôvery pre danú transakciu udáva suma žetónov jej potomstva

Eclipse útok

- monopolizácia spojení niektorého uzlu
- vyžaduje reštart a dostatočný počet IP adries
- útok na peer-to-peer sieť
- funguje na Bitcoin aj Ethereum (asi staršie verzie)

Eclipse útok na Avalanche

- doteraz 2 typy účastníkov protokolu - korektní a zlomyseľní
- nový 3. typ - korektní, ktorí sú monopolizovaní zlomyseľnými

Plány

- analýza garancií protokolu voči rôznym útokom (Eclipse a pod.)
- návrh fungovania útočníka

Ďakujem za pozornosť