Matematika bitcoinů

Jan Hladký
Matematický ústav
Akademie věd České republiky

Jan Hladký is supported by a Marie Curie Intra European Fellowship within the 7th European Community Framework Programme.

Bitcoiny: souhrn

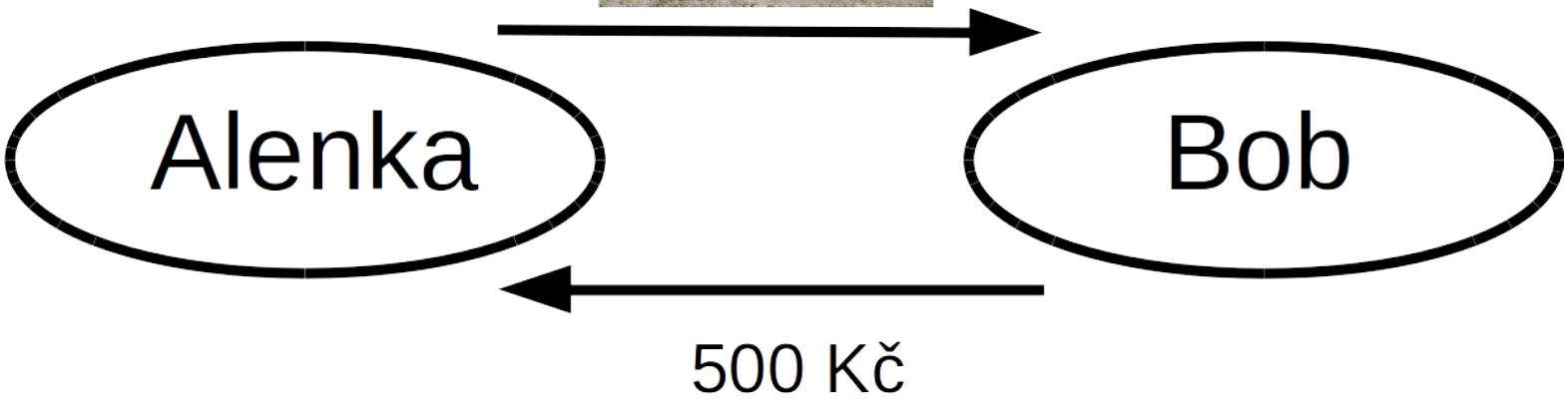
- elektronický platební systém a měna
- 2008, Satoshi Nakamoto (?)
- decentralizovaná a neregulovaná
- ฿1 $\approx$ 10 120 Kč
- v současné době ca ฿15 000 000 $\approx$ 150 miliard Kč
  (tj. ca 12% ročního rozpočtu ČR)
- fluktuace: 04/12/2013: ฿1 $\approx$ 25 000 Kč,
  07/12/2013: ฿1 $\approx$ 15 000 Kč
- výhody: anonymita
  mimo dohled státních orgánů
  malé poplatky za transakce

Transakce

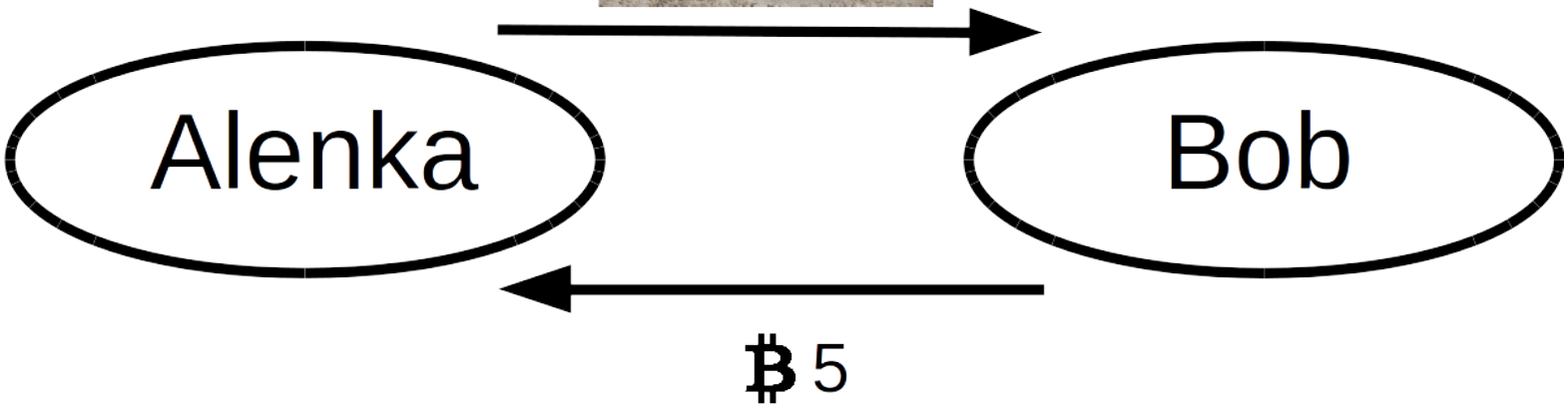
Alenka

Bob

Transakce



Transakce



- Byl to opravdu Bob, kdo odeslal ฿5 z Bobova účtu?
  → elektronický podpis
- Měl Bob ฿5?
- Může Bob těchto ฿5 použít znova?

} účetní kniha

Elektronický podpis

20.12.2010

Vážení čtenáři MKP, přeji Vám vše nejlepší v roce 2011.
Váš ředitel,

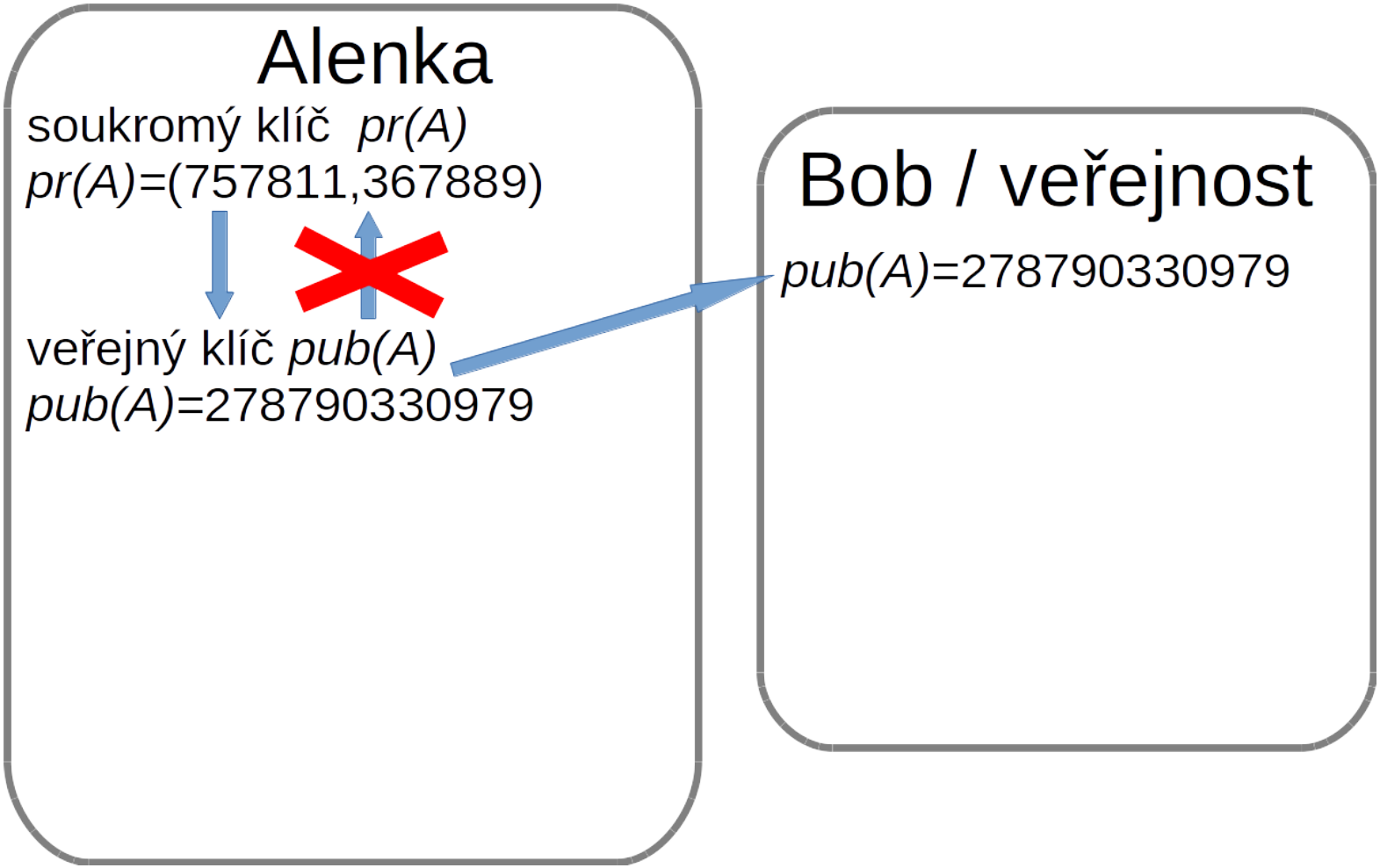
Tomáš Řehák

Elektronický podpis

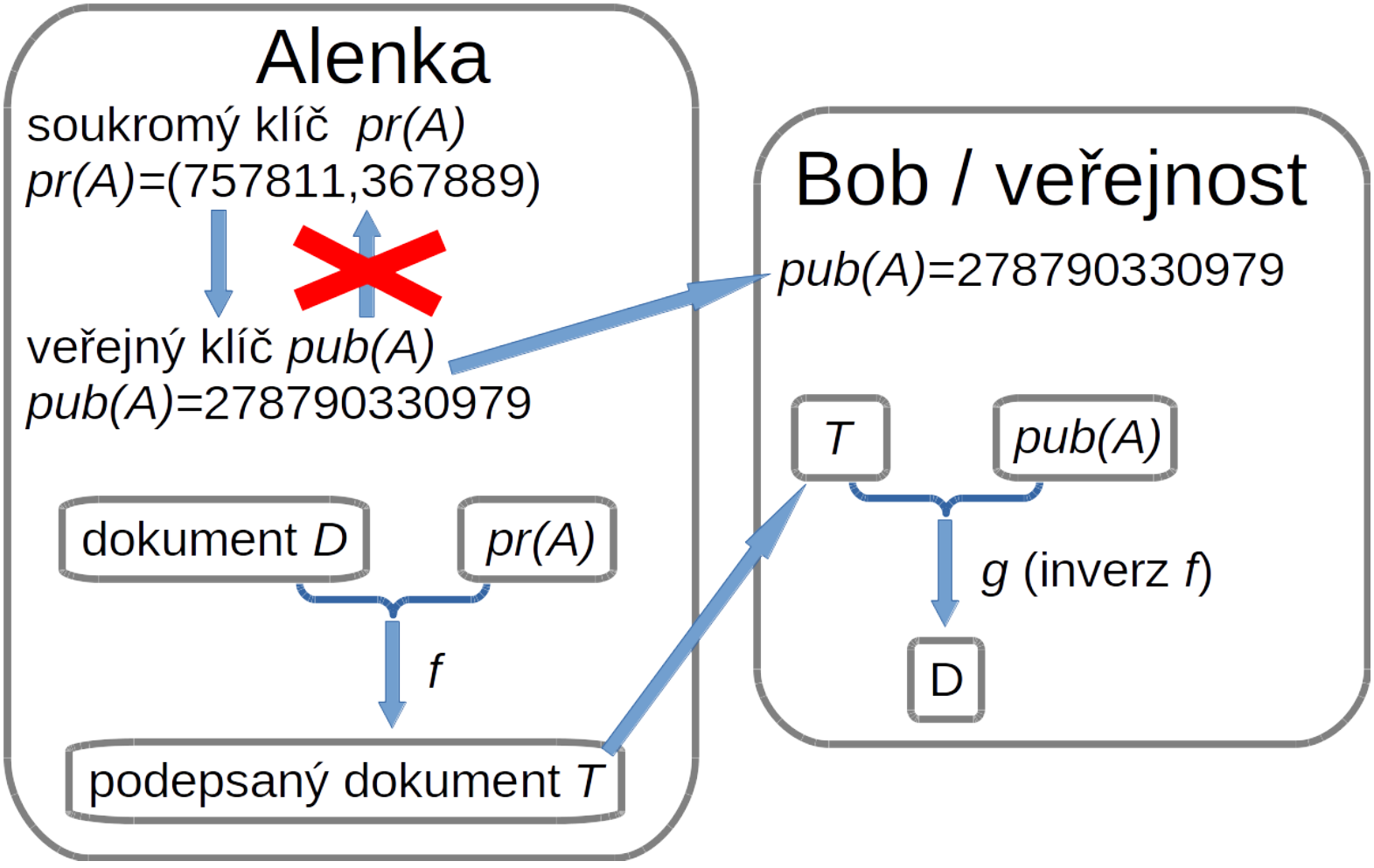
16.3.2016

Vyplaťte Janu Hladkému honorář
1 000 000 Kč za přednášku o bitcoinech

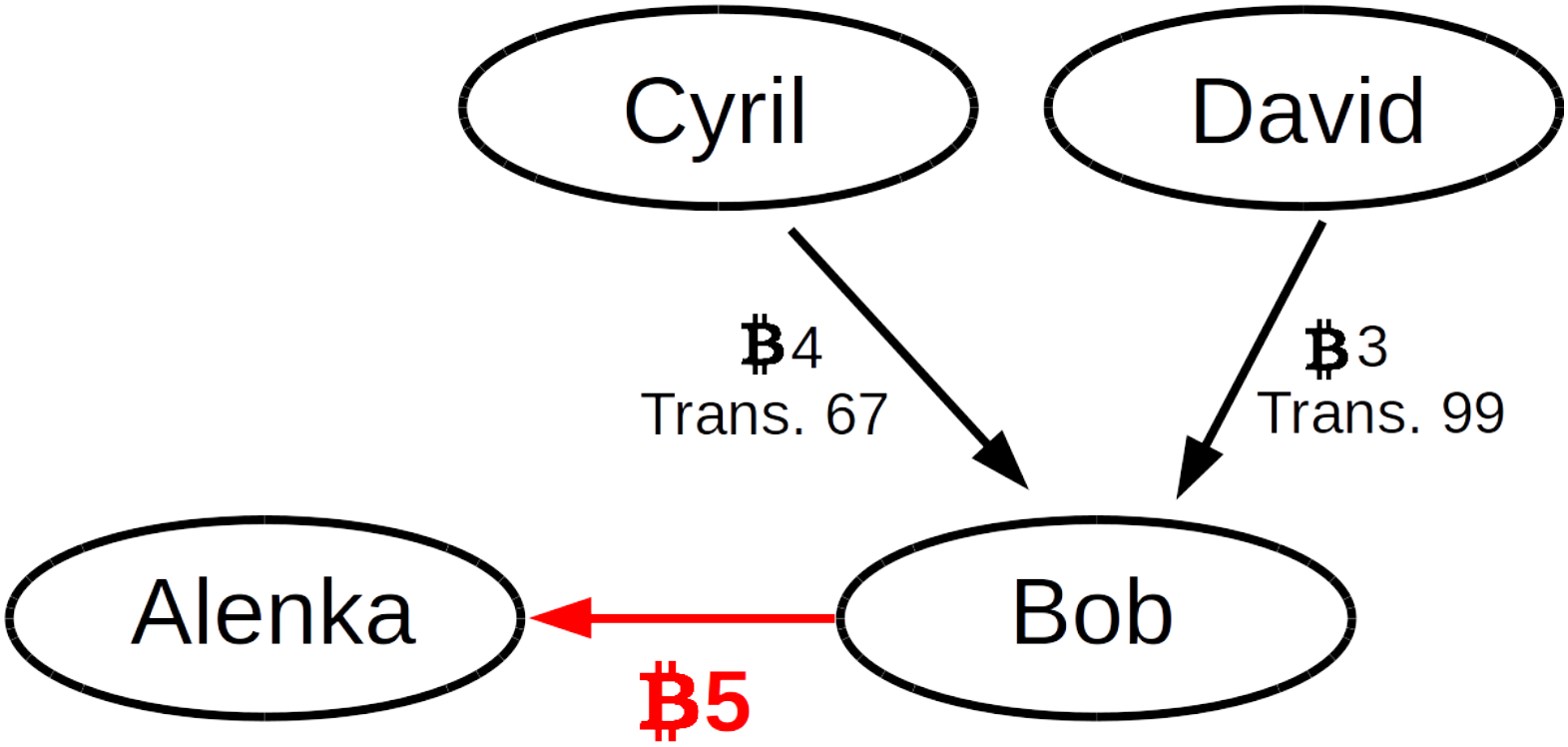
Elektronický podpis



Elektronický podpis



Účetní kniha



Bobův platební příkaz:

- Na základě Trans 67: ฿0.01 → účetní, ฿3.99 → A
- Na základě Trans 99: ฿1.01 → A, ฿1.99 → B

Účetní kniha

- Úkolem účetního je kontrolovat zda-li byla každá transakce použita jen jednou.
- Účetním (pro jeden úkol) může být každý, kdo vyřeší hádanku.
- Hádanka je složitá je vyřešení, ale jednoduchá na kontrolu.
- Konkurenční účetní zkontrolují řešení (motivovaní odměnou za vedení účetnictví).

Poznámky

- obrázky z flickr.com (licence creative commons 2.0).
  kohout: chris.murphy, Wild chicken
  pytel brambor: bartb_pt, Potatos
- dokument s podpisem RNDr. Tomáše Řeháka je fiktivní
- celá prezentace na
  `http://users.math.cas.cz/~hladky/index_personal.html`