

Matematika bitcoinů

Jan Hladký

Matematický ústav Akademie věd České republiky, a
Technická univerzita Drážďany

Činnost podpořena Nadací Alexandra von Humboldta.

Bitcoin: souhrn

- ▶ elektronický platební systém a měna
- ▶ 2008, Satoshi Nakamoto
- ▶ decentralizovaná a neregulovaná
- ▶ $\text{฿}1 \approx 236\,000 \text{ Kč}$
- ▶ v současné době ca $\text{฿}17\,000\,000 \approx 4\,000$ miliard Kč
(tj. ca 300% ročního státního rozpočtu ČR)
- ▶ fluktuace: 01/02/2018: $\text{฿}1 \approx 200\,000 \text{ Kč}$,
 01/01/2018: $\text{฿}1 \approx 266\,000 \text{ Kč}$
 01/12/2017: $\text{฿}1 \approx 200\,000 \text{ Kč}$
 01/11/2017: $\text{฿}1 \approx 137\,000 \text{ Kč}$
- ▶ výhody: anonymita
 mimo dohled státních orgánů
 malé poplatky za transakce

Rozklad na prvočinitele

- ▶ $15 = 3 \times 5,$
- ▶ $20 = 2 \times 2 \times 5,$

Rozklad na prvočinitele

- ▶ $15 = 3 \times 5,$
- ▶ $20 = 2 \times 2 \times 5,$
- ▶ $21 =$

Rozklad na prvočinitele

- ▶ $15 = 3 \times 5,$
- ▶ $20 = 2 \times 2 \times 5,$
- ▶ $21 = 3 \times 7,$

Rozklad na prvočinitele

- ▶ $15 = 3 \times 5,$
- ▶ $20 = 2 \times 2 \times 5,$
- ▶ $21 = 3 \times 7,$
- ▶ $278\ 790\ 330\ 979 =$

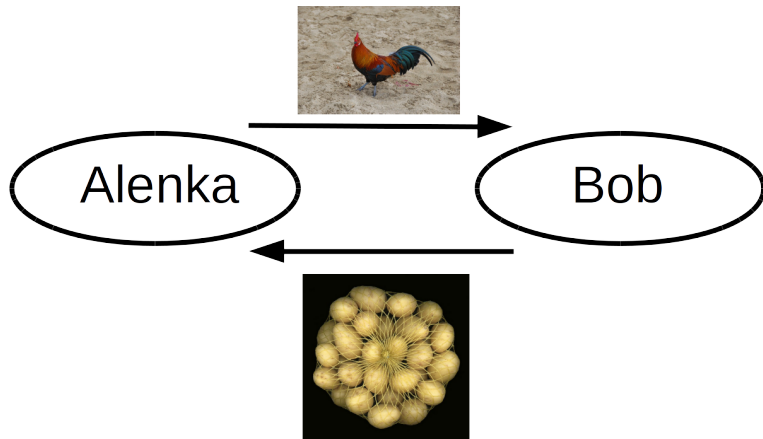
Rozklad na prvočinitele

- ▶ $15 = 3 \times 5,$
- ▶ $20 = 2 \times 2 \times 5,$
- ▶ $21 = 3 \times 7,$
- ▶ $278\,790\,330\,979 = 757\,811 \times 367\,889$

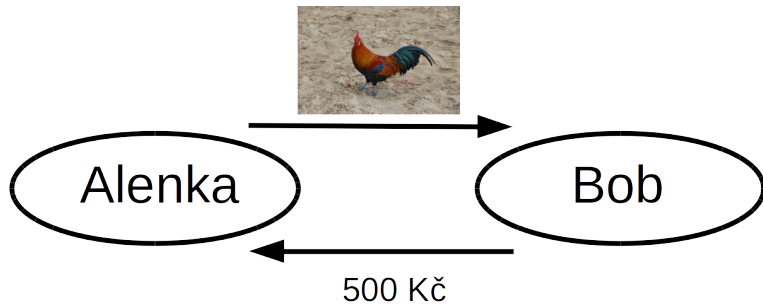
Asymetrie

Ve skutečnosti se používají **eliptické křivky**

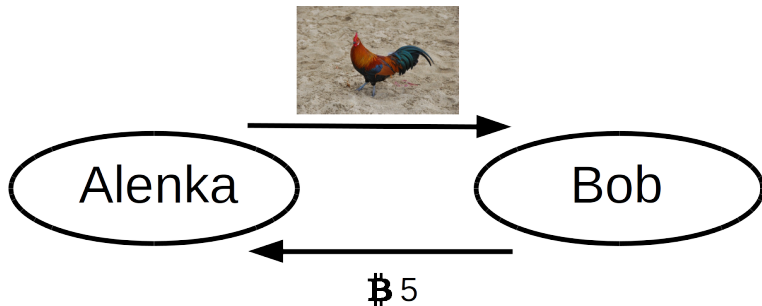
Transakce



Transakce



Transakce



- Byl to opravdu Bob, kdo odeslal ₿5 z Bobova účtu?
 - Měl Bob ₿5?
 - Může Bob těchto ₿5 použít znova?
- elektronický podpis*
- účetní kniha*

20.12.2015

Vážený zaměstnanci, přeji Vám
vše nejlepší do nového roku.

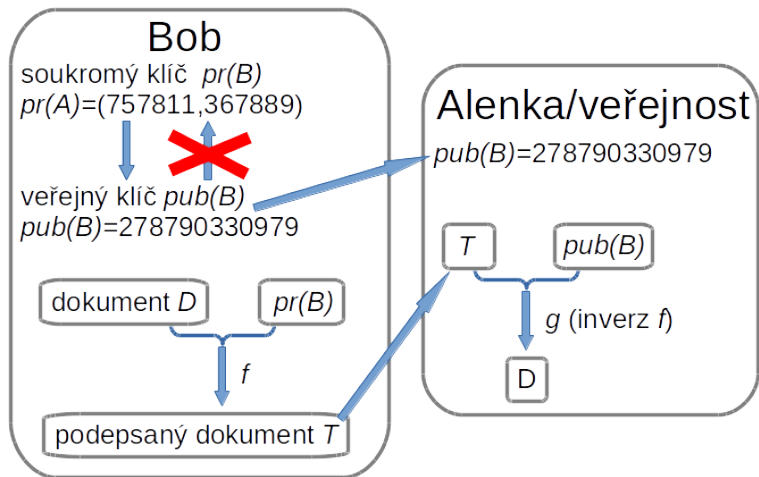
J. Rákosník

20.2.2018

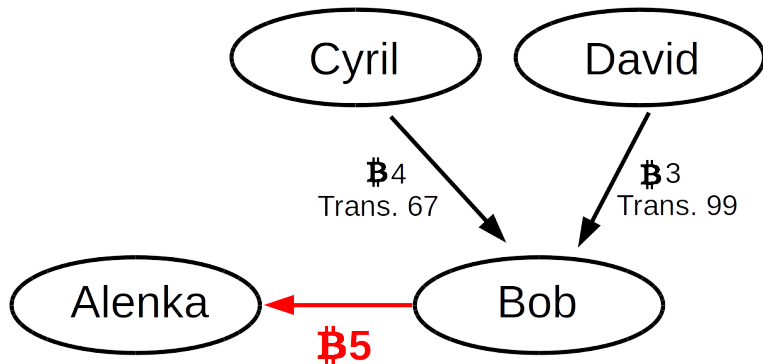
Vyplat'te Janu Hladkému honorář
1 000 000 Kč za přednášku o bitcoinech



Elektronický podpis



Účetní kniha ("blockchain")



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 ("blockchain")

- ▶ 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).

Sudoku

The world's hardest sudoku

8								
		3	6					
	7			9		2		
	5				7			
				4	5	2		
			1				3	
		1					6	8
		8	5				1	
	9					4		

Sudoku

The world's hardest sudoku with solution

8	1	2	7	5	3	6	4	9
9	4	3	6	8	2	1	7	5
6	7	5	4	9	1	2	8	3
1	5	4	2	3	7	8	9	6
3	6	9	8	4	5	7	2	1
2	8	7	1	6	9	5	3	4
5	2	1	9	7	4	3	6	8
4	3	8	5	2	6	9	1	7
7	9	6	3	1	8	4	5	2

Poznámky

- ▶ obrázky z flickr.com (licence creative commons 2.0).
kohout: chris.murphy, Wild chicken
pytel brambor: bartb_pt, Potatos
- ▶ celá prezentace na
http://users.math.cas.cz/~hladky/index_personal.html