Mathematics of bitcoins

Jan Hladký

Institute of Mathematics, Czech Academy of Sciences, and
TU Dresden

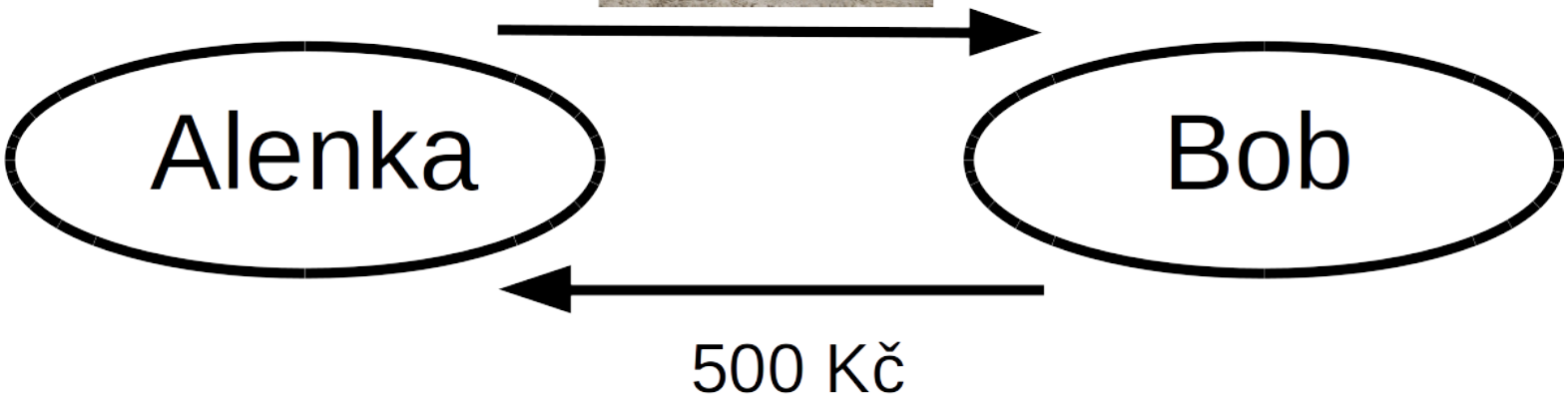
Supported by the Alexander von Humboldt Foundation.

Bitcoins: summary

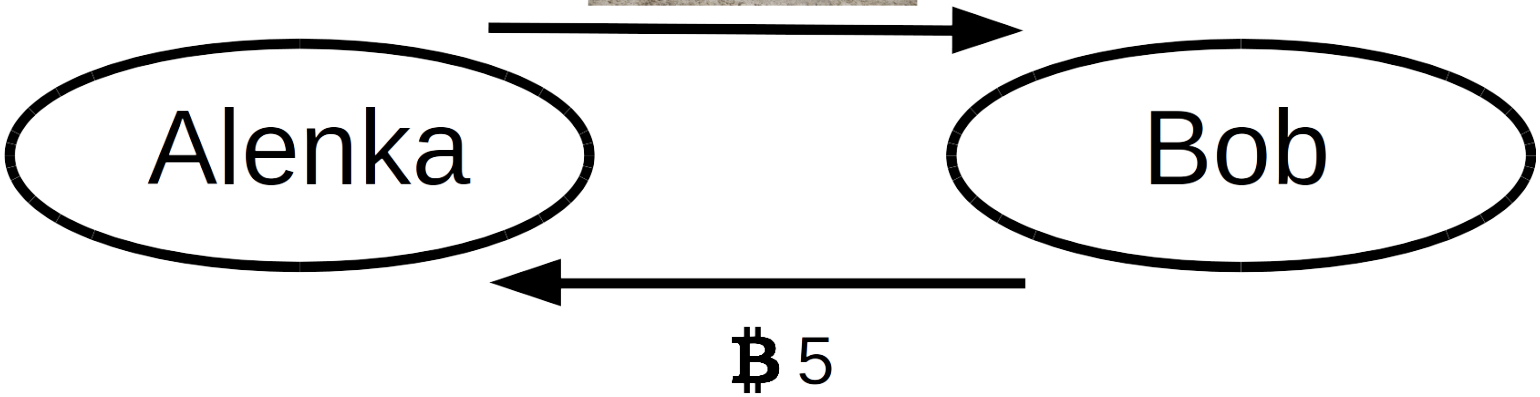
- digital payment system and currency
- 2008, Satoshi Nakamoto
- decentralized
- ฿1 $\approx$ 155 000 Kč
- currently ฿16 000 000 $\approx$ 2 480 billion Kč
  (ca 200% of the annual state budget of the Czech Republic)
- fluktuations: 04/12/2013: ฿1 $\approx$ 25 000 Kč,
  07/12/2013: ฿1 $\approx$ 15 000 Kč
- advantages: anonymity
  out of sight of state authorities
  small(ish) transaction fees

Transactions

Transactions



Transactions



- Was it really Bob, who authorized ฿5 to be sent?
  - Digital signature
- Did Bob own ฿5?
- Will Bob be unable to re-use the ฿5?

} ledger

Digital signature

20.12.2015
Dear members of the Institute,
I wish you all the best in
New Year.

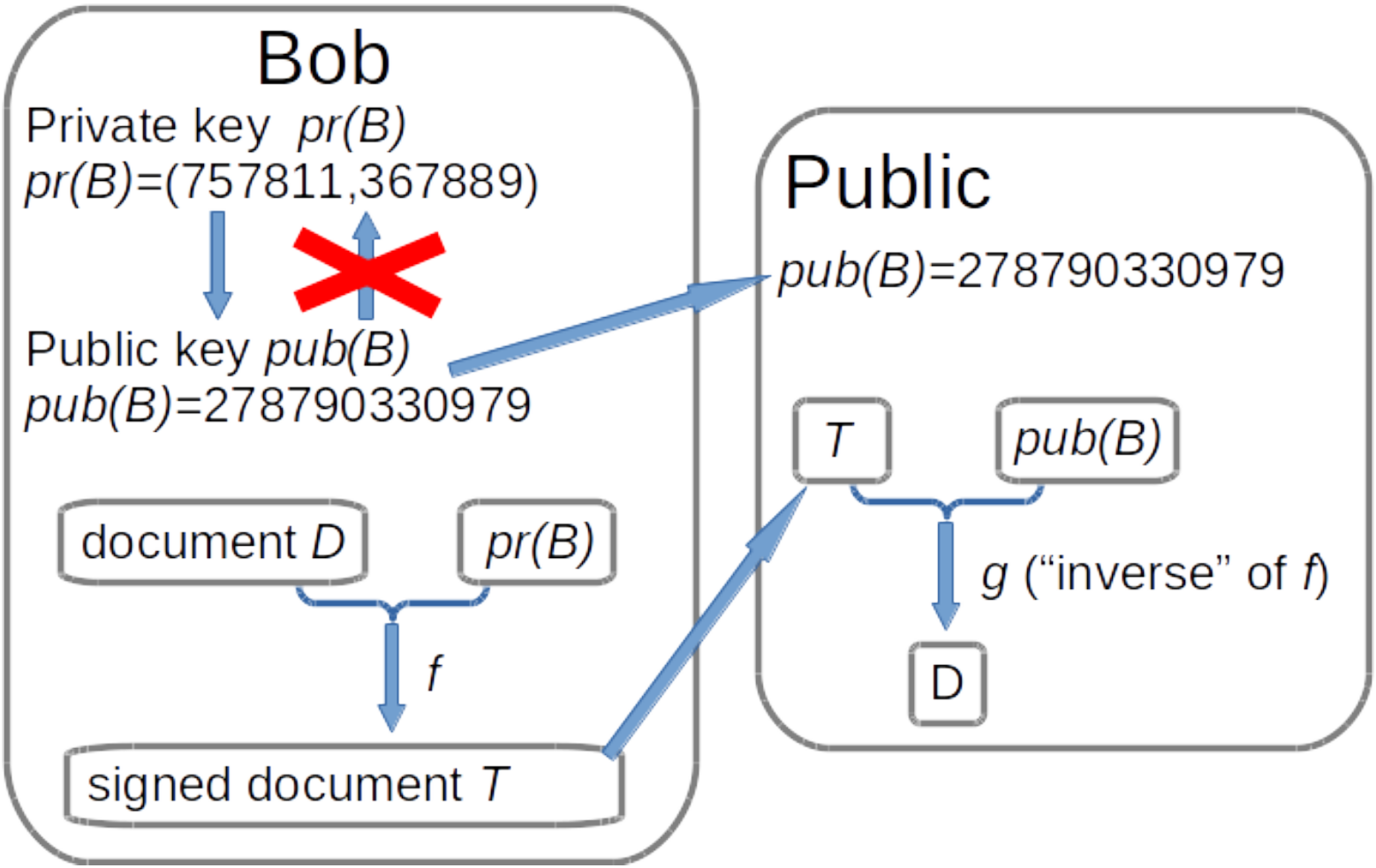
J. Rákosník

Digital signature

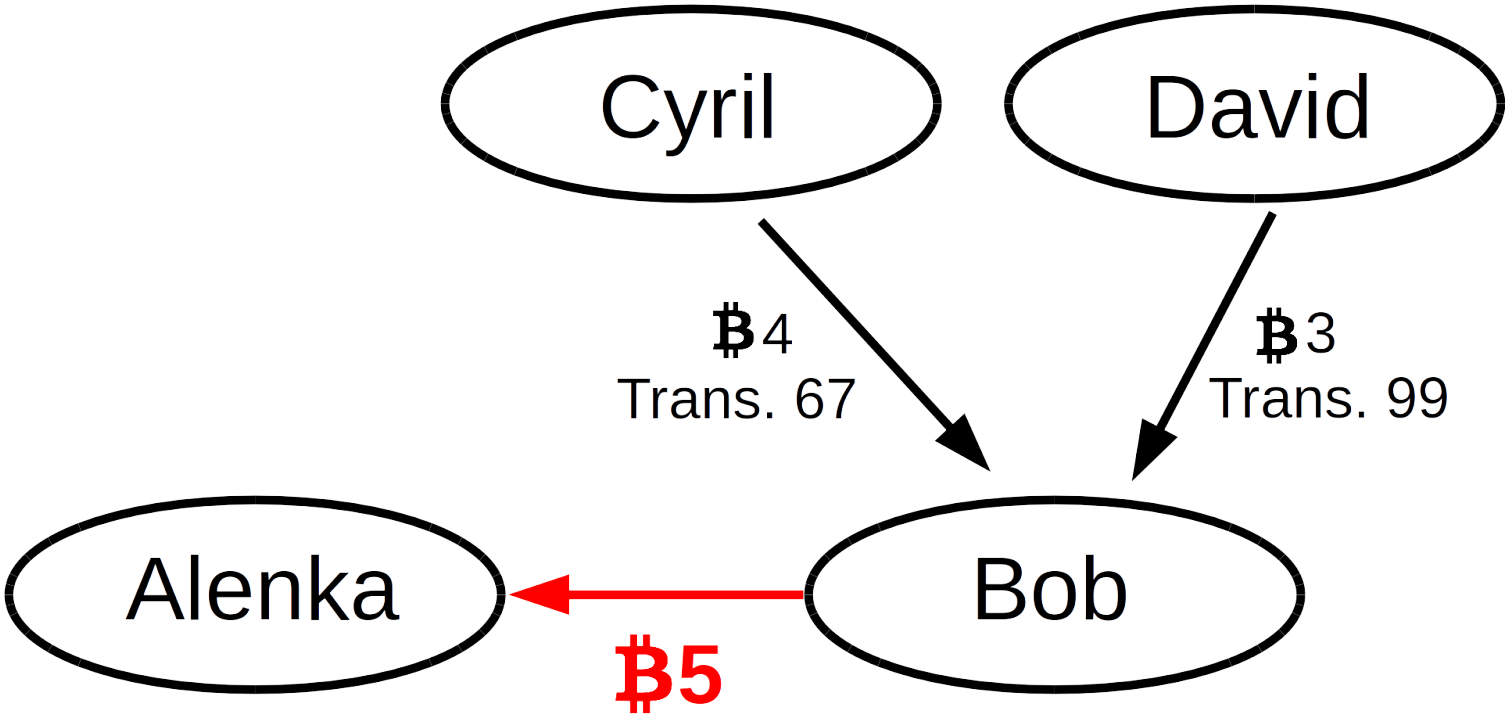
10.11.2017

Pay a honorarium of 1,000,000 Kč
to Jan Hladký for the bitcoin talk.

Digital signature



The ledger



Bob's payment order:

- Based on Trans 67: ฿0.01 → fee, ฿3.99 → A
- Based on Trans 99: ฿1.01 → A, ฿1.99 → B

The ledger

- The task of the accountant is to check that each transaction was used once.
- An accountant (for one task) can be anyone who solves a math puzzle.
- The puzzle is difficult but the solution is simple to check.
- Competing accountants review solutions (motivated by remuneration for accounting).

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`