

Univerza v Ljubljani  
Fakulteta za računalništvo  
in informatiko



# Kripto glavna knjiga

*ali*  
*Glavna knjiga malo drugače*

Andrej Brodnik

UL FRI, UP FAMNIT  
[andrej.brodnik@fri.uni-lj.si](mailto:andrej.brodnik@fri.uni-lj.si)

19. mali traven  
2018



# Itinerar

**Nanos gigantum humeris insidentes.**

*Bertrand iz Chartresa, 12. stoletje*

- Osnovna orodja kriptografije.
- Carigrajski (bizantinski) generali.
- Od glavne knjige do verige blokov.
- Veriga blokov v porazdeljenem okolju.

Viri slik v predstavitvi: Wiki, Coindesk, MNZ; Satoshi Nakamoto, Ethereum



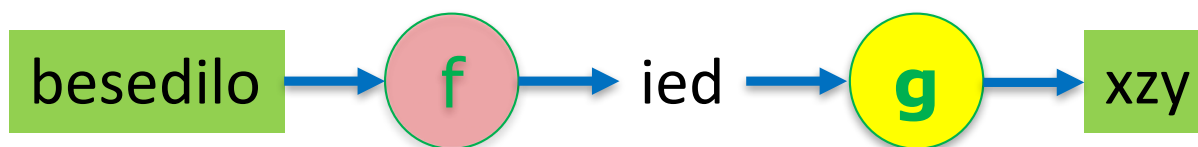
# Pečatenje



- **Zaupamo** tistemu, ki je pečatil
- Na osnovi česa?
  1. Ker **poznamo** njegov pečat.
  2. Ker ima interes/dolžnost pečatiti.



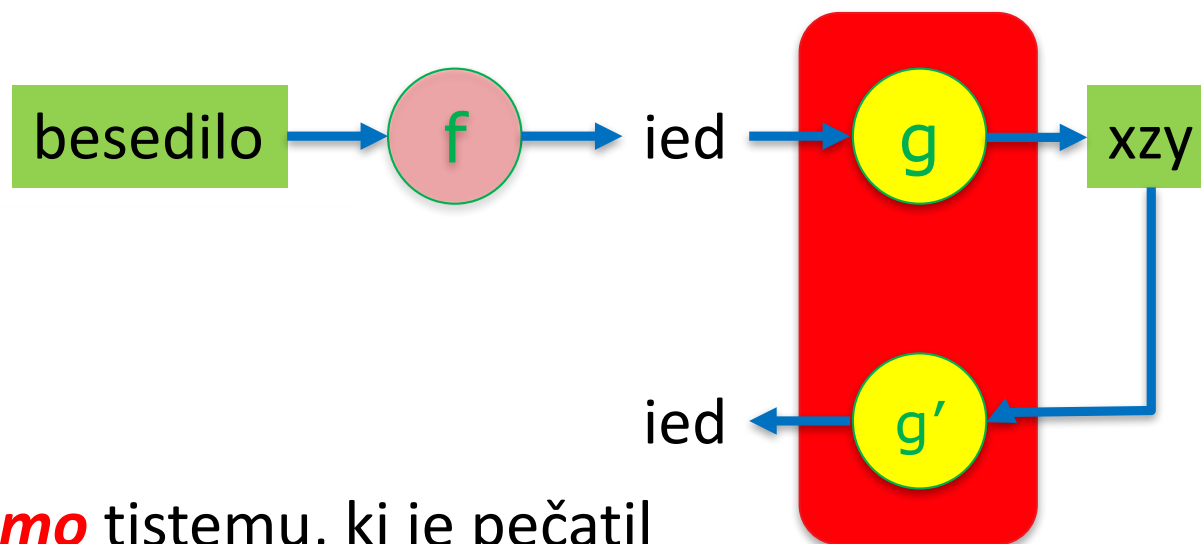
# Elektronsko pečatenje / podpisovanje



**f** – izvleček (MD5, SHA-256, ...)

**g** – podpisovanje, ki ga zna narediti samo tisti, kateri pečati (RSA)

# Preverjanje e-podpisa (RSA, 1973)



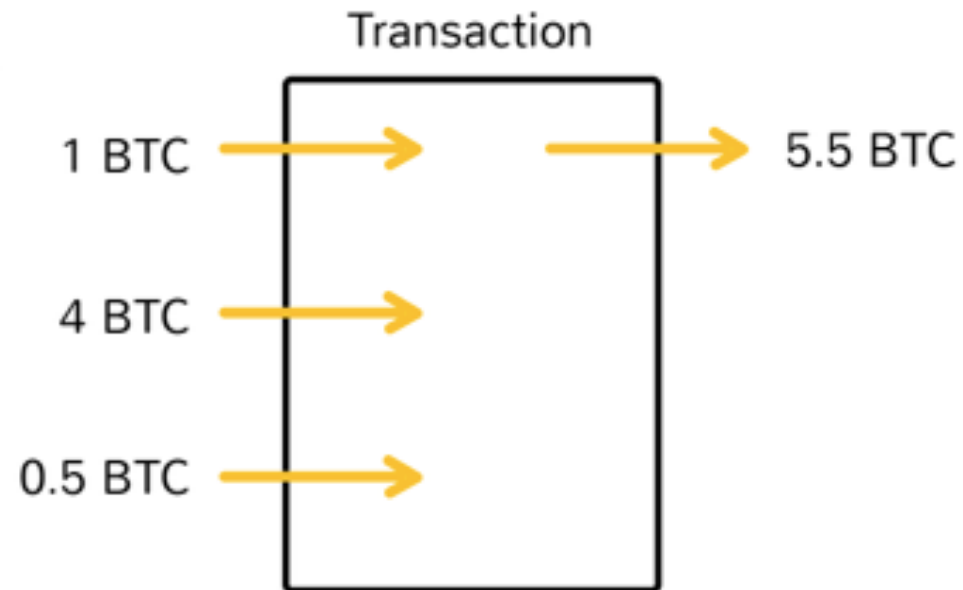
- **Zaupamo** tistemu, ki je pečatil
- Na osnovi česa?
  1. Ker **poznamo** njegov pečat.
  2. Ker ima interes/dolžnost pečatiti.

če ima nekdo interes, da se verjame, tistemu, kar je objavil,  
to lahko naredi z e-podpisom (digitalnim podpisovanjem)



# Transakcije

- Ima več virov (denarnic), od kjer prihajajo sredstva in več ponorov (denarnic), kam odhajajo sredstva





# Beleženje transakcij

- Vse transakcije od začetka stvarstva javno beležimo v ***javni glavni knjigi***, s čimer dokazujemo kje so sredstva v določenem trenutku

Accounts for Demo

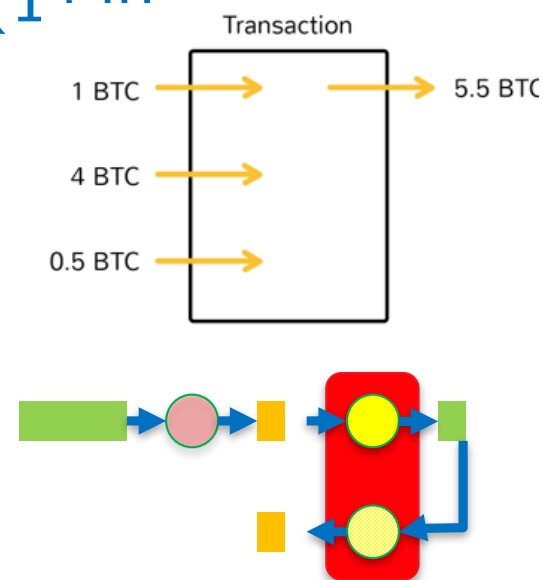
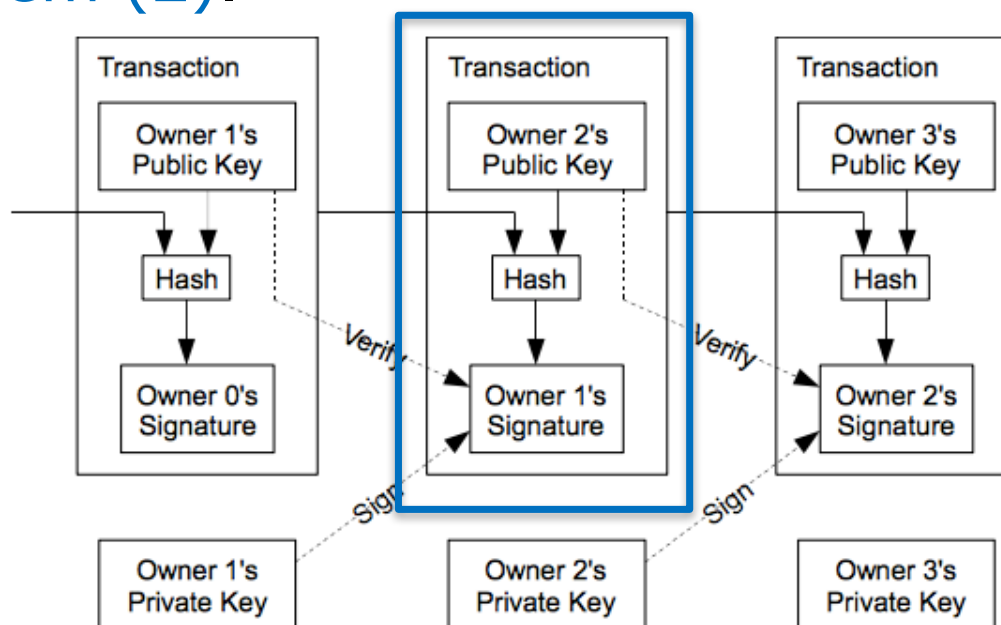
CASH ACCOUNT From 01/03/2003 to 29/02/2004

Date	Payee	Reference	Category	Actual (gross)		Recon	Admin. fund split		Sink. fund split		Balance (net)
				Amount	Balance (gross)		GST net.	Non GST.	GST net.	Non GST.	
				0.00	0.00	<input checked="" type="checkbox"/>	0.00	0.00	0.00	0.00	0.00
25 MAY 01	Mr J Citizen			500.00	500.00	<input checked="" type="checkbox"/>	0.00	500.00	0.00	0.00	500.00
26 MAY 01	Local Insurance B			-269.00	231.00	<input checked="" type="checkbox"/>	0.00	-269.00	0.00	0.00	231.00
31 MAY 01	Netbank			-2.52	228.48	<input checked="" type="checkbox"/>	0.00	-2.52	0.00	0.00	228.48
31 MAY 01	Netbank			-5.00	223.48	<input checked="" type="checkbox"/>	0.00	-5.00	0.00	0.00	223.48
31 MAY 01	Netbank			0.52	224.00	<input checked="" type="checkbox"/>	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarke's Grounds			-30.00	194.00	<input checked="" type="checkbox"/>	0.00	-30.00	0.00	0.00	194.00
10 JUN 03	Electrical Enginee			-22.60	171.40	<input checked="" type="checkbox"/>	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit trans			0.00	171.40	<input checked="" type="checkbox"/>	0.00	-250.00	0.00	250.00	171.40
10 OCT 01	Leahy			1000.00	1171.40	<input type="checkbox"/>	909.09	0.00	0.00	0.00	1080.49
10 OCT 01	Fencers Upstand			-120.00	1051.40	<input type="checkbox"/>	0.00	0.00	0.00	-120.00	960.49
16 OCT 01	Mr P D Jakeson			400.00	1451.40	<input type="checkbox"/>	0.00	0.00	363.64	0.00	1324.13
6 NOV 03	Mr P D Jakeson			25.00	1476.40	<input type="checkbox"/>	0.00	0.00	22.73	0.00	1346.86
11 NOV 01	Mr P D Jakeson			5.00	1481.40	<input type="checkbox"/>	0.00	0.00	4.55	0.00	1351.41



# E-glavna knjiga

1. Zaupati moramo, da se je transakcija v resnici zgodila => **pogodba med prodajalcem (1) in kupcem (2).**



2. Zaupati moramo, da sredstva niso bila porabljena dvakrat => osrednja avtoriteta, ki ju zaupamo.





# Časovne značke

- Vsaki transakciji dodamo časovno značko.
- Ker je glavna knjiga javna, lahko **kupec vedno preveri, ali je denar še neporabljen**.
- Potrditi časovno značko ne sme biti preprosto – mora obstajati nekaj, kar si potrjevalec želi imeti
  - potrjevalec mora vložiti delo, za katerega je nagrajen (*proof-of-work*) (Back, Hashcash 1997)
- Še vedno zaupamo osrednji avtoriteti, ki vodi glavno knjigo: pravilno dodaja časovne značke in pravilno časovno overovlja posamezne transakcije.



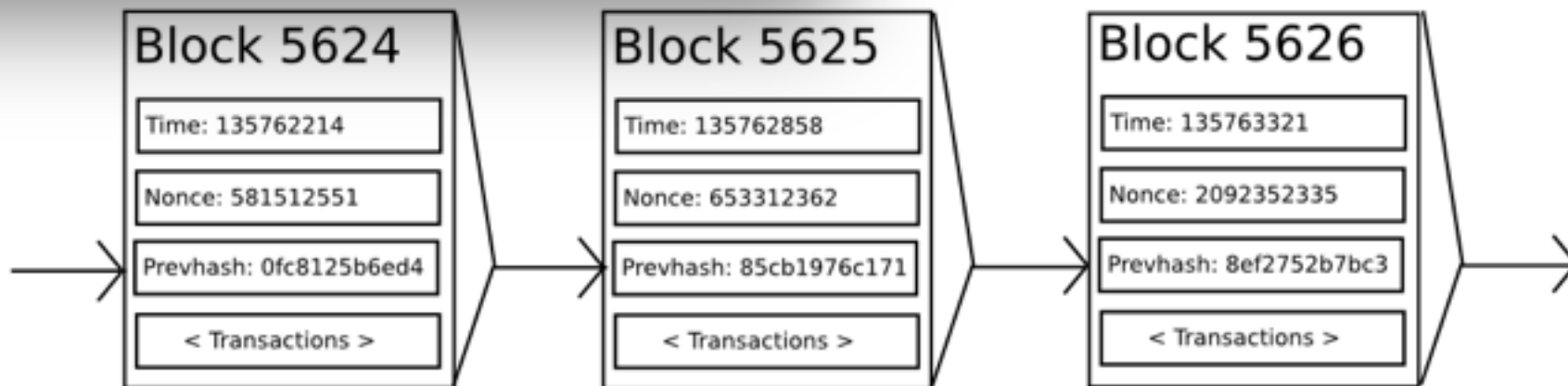
# Porazdeljeni sistem

- Problem carigrajskih (bizantinskih) generalov (Lamport, 1982)
  - Imamo  $n$  generalov, ki morajo usklajeno napasti nasprotnika, ker sicer bodo napadalci poraženi.
  - Kako zaznato napako v sistemu, ki lahko razpade.
- Rešitev:
  - vsaj polovica se mora strinjati in
  - manj kot polovica jih sme biti povezanih.



# Združevanje transakcij

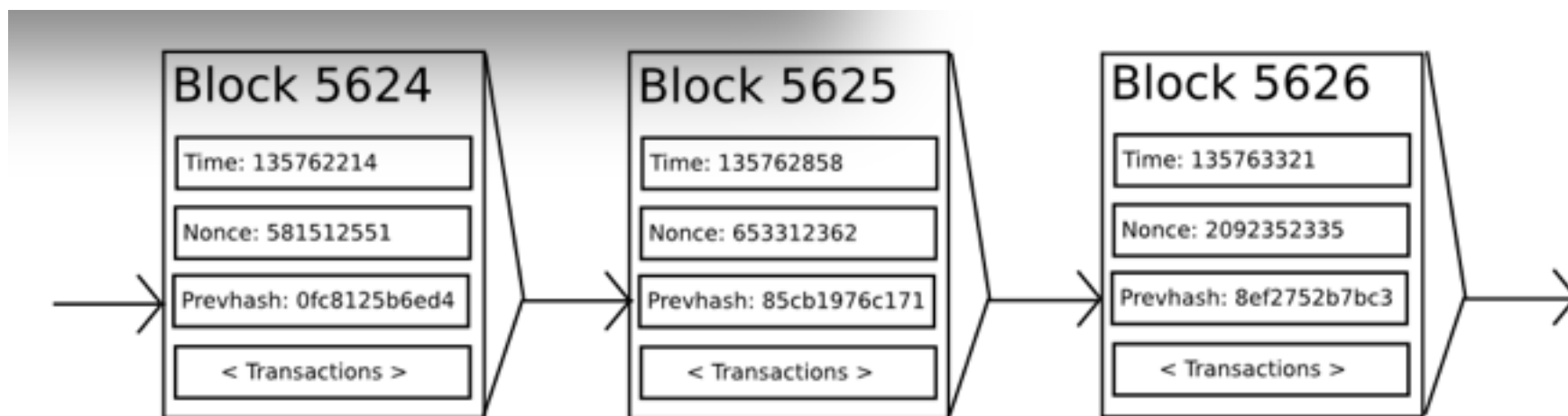
- Ekonomičneje je, da ne overovljamo vsake transakcije, ampak več transakcij, ki jih združujemo v **bloke**.
- Zaporedje blokov (**veriga**) je časovno pogojeno in potrdilo o pravilnosti bloka vključuje dokaz o pravilnosti neposredno (časovno) predhodnega bloka.





# Veriga blokov

- Če želimo **popraviti** transakcijo v bloku 5624, mora sistem na novo potrditi novi block 5624, kar zahteva popravke bloka 5625 ter nato 5626, ...
- To ni ekonomično, razen če imamo nadzor nad potrjevalci (rudarji).





# Itinerar

**In beseda je dejanje postala.**

- Od podatkov k programom.
- Je program, ki je podatek, pameten podatek.
- Veriga blokov vsebujočih pametne podatke.



# Alan Turing in splošni računalnik

- Stroj, ki zna izračunati vse, kar se da izračunati.
  - Alan Turing, 1936 -> programski jeziki (*Solidity*)
  - kaj je sploh izračunljivega

## ***Nagrada Alana Turinga***

- Podeljuje ACM (*Association for Computing Machinery*).
- Nobelova nagrada v računalništvu in informatiki
- Lamport 2013, Adleman, Rivest in Shamir 2002, McCarthy 1971.



# Ali je podatek ali program?

- Vsak program je v osnovi besedilo
  - $\lambda$  račun in LISP, McCarthy 58 -> JVM, EVM
- Transakcija postane program:

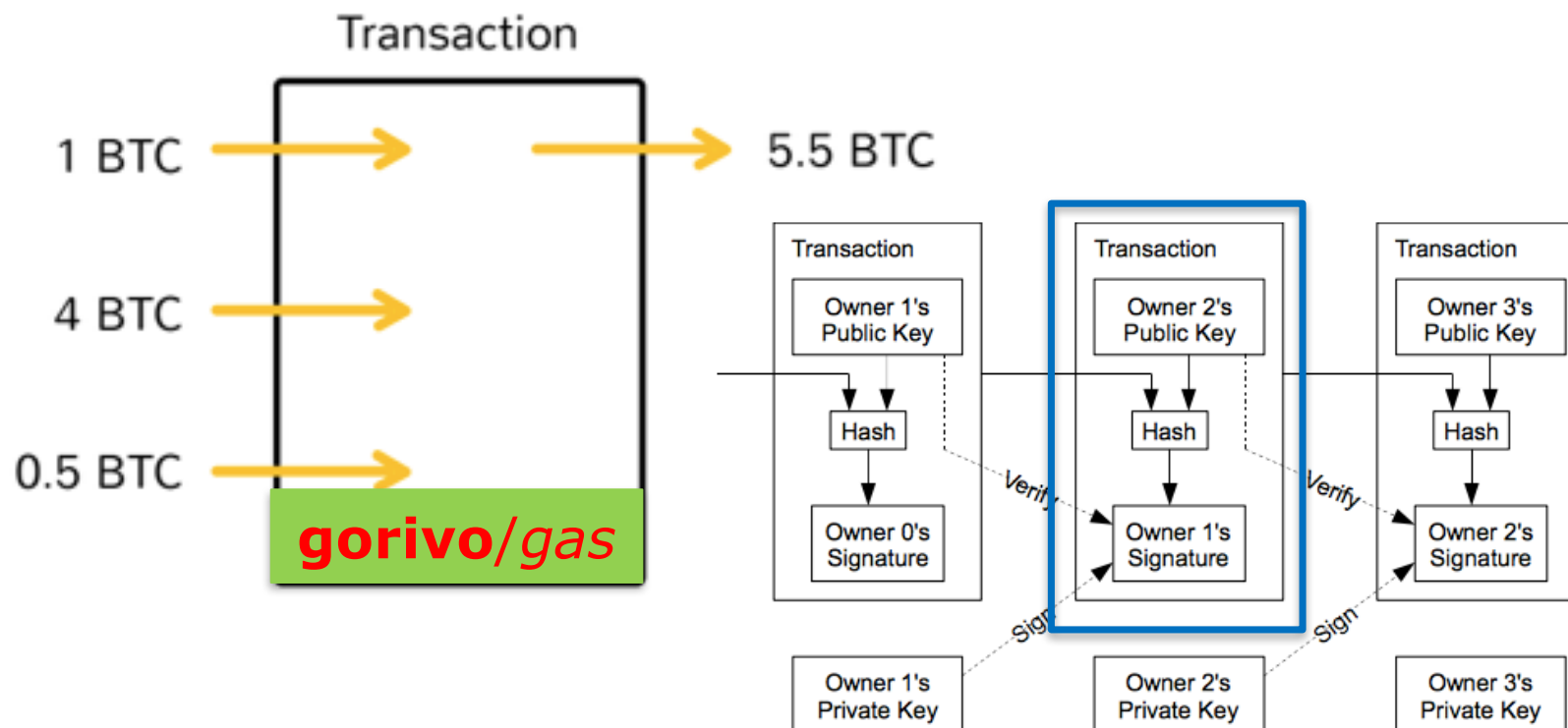
**ČE obljubljenih 68 BIC THEN  
izvedi transakcije**

- *Problem:* izvajanje lahko zahteva veliko časa (virov)
  - DoS.



# Pametni podatki – pametne pogodbe

- Poleg virov še, koliko lahko porabimo za izvajanje pogodbe







# Hvala za pozornost!

[andrej.brodnik@fri.uni-lj.si](mailto:andrej.brodnik@fri.uni-lj.si)