

# Raspodijeljene glavne knjige i kriptovalute

## Uvod i osnove kriptografije

Ante Đerek, Zvonko Konstanjčar



Fakultet  
elektrotehnike i  
računarstva

5. listopada 2023.

## Nositelji

- Ante Đerek, ante.derek@fer.hr
- Zvonko Kostanjčar, zvonko.kostanjcar@fer.hr

## Predavanja

- Stjepan Begušić

## Asistenti

- Petar Paradžik
- Sven Goluža

- [https://www.fer.unizg.hr/predmet/rgkk\\_b](https://www.fer.unizg.hr/predmet/rgkk_b)
- mailing lista rgkk@fer.hr
- Konzultacije po potrebi uz najavu mailom.

## Literatura (za prvi dio predavanja)

- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder (2016.), Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, dostupna na <http://bitcoinbook.cs.princeton.edu/>
- A. M. Antonopoulos (2015.), Mastering Bitcoin: Unlocking Digital Cryptocurrencies, dostupna na <https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc>

## Slični predmeti

- Cryptocurrencies, blockchains, and smart contracts, <https://cs251.stanford.edu/>
- Bitcoin and Cryptocurrency Technologies, <https://www.coursera.org/learn/cryptocurrency>

## Bodovanje

- Međuispit – 40%
- Završni ispit – 40%
- Prva laboratorijska vježba – 10%
- Druga laboratorijska vježba – 10%

## Pragovi

- Zadovoljen minimum u obje laboratorijske vježbe.
- Ukupno 50% bodova iz svih komponenti.
  - Alternativno, ukupno 50% bodova iz pismenog ispita
- Pragovi za ocjene će biti objavljeni kasnije.

# Laboratorijske vježbe

## Prva laboratorijska vježba – Bitcoin transakcije i skripte

Planirani datumi:

- Zadatak: 26.10.2023.
- Predaja vježbe: 13.11.2023.–17.11.2023.

## Druga laboratorijska vježba – Ethereum pametni ugovori

Planirani datumi:

- Zadatak: 14.12.2023.
- Predaja vježbe: 8.1.2023.–12.1.2023.

## Osnovna pravila

- Možete raditi samostalno ili u grupi od najviše dvoje studenata. U slučaju grupnog rada oboje studenata mora biti upoznato sa svim aspektima svake vježbe.
- *Starter code* u programskom jeziku Java.
- Možete raditi u bilo kojem drugom programskom jeziku, ali bez podrške asistenata.
- U svakoj vježbi definiran minimum kojeg treba zadovoljiti za prag.

## Važno!

- Strogo kažnjavanje pokušaja plagiranja (svih sudionika).
- Tražite pomoć od nastavnog osoblja dovoljno rano.

# Glavna knjiga

**Accounts for Demo**

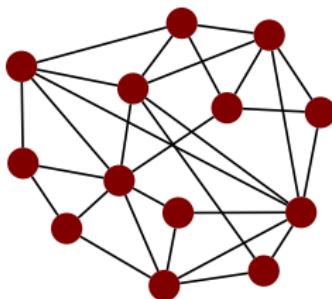
CASH ACCOUNT		From	01/03/2003	to	29/02/2004	Select current year	Select previous year	Refresh list	?	Back	
Date	Payee	Reference	Category	Actual (gross) Amount	Balance (gross)	Recon <input checked="" type="checkbox"/>	Admin. fund split GST net.	Sink. fund split GST net.	Non GST.	Non GST.	Balance (net)
25 MAY 03	Mr J Citizen	Lot 1 levy pa	Deposit	500.00	500.00	<input checked="" type="checkbox"/>	0.00	500.00	0.00	0.00	500.00
26 MAY 03	Local Insurance Bnsurance A	Insurance Bu	ninsurance Bu	-269.00	231.00	<input checked="" type="checkbox"/>	0.00	-269.00	0.00	0.00	231.00
31 MAY 03	Netbank	Govt Debit Tr	Govt Debit Tr	-2.52	228.48	<input checked="" type="checkbox"/>	0.00	-2.52	0.00	0.00	228.48
31 MAY 03	Netbank	Account Ser	Account Ser	-5.00	223.48	<input checked="" type="checkbox"/>	0.00	-5.00	0.00	0.00	223.48
31 MAY 03	Netbank	Interest	Bank Interest	0.52	224.00	<input checked="" type="checkbox"/>	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarkes Grounds	Grounds Mai	Grounds Mai	-30.00	194.00	<input checked="" type="checkbox"/>	0.00	-30.00	0.00	0.00	194.00
10 JUN 03	Electrical Engineer	Replace light	Building Maint	-22.60	171.40	<input checked="" type="checkbox"/>	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit trans	Lot 1 credit tr	Levy credit tr	0.00	171.40	<input checked="" type="checkbox"/>	0.00	-250.00	0.00	250.00	171.40
10 OCT 03	L Leahy	Terror Payou	Bank Transfe	1000.00	1171.40	<input type="checkbox"/>	909.09	0.00	0.00	0.00	1080.49
10 OCT 03	Fencers Upstand	Broken Pallin	Fencing	-120.00	1051.40	<input type="checkbox"/>	0.00	0.00	0.00	-120.00	960.49
16 OCT 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	400.00	1451.40	<input type="checkbox"/>	0.00	0.00	363.64	0.00	1324.13
6 NOV 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	25.00	1476.40	<input type="checkbox"/>	0.00	0.00	22.73	0.00	1346.86
11 NOV 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	5.00	1481.40	<input type="checkbox"/>	0.00	0.00	4.55	0.00	1351.41

Izvor: wikipedia.org

## Što je raspodijeljena glavna knjiga?

Baza podataka koja je replicirana na mnoštvu čvorova u mreži te koja garantira određena svojstva ispravnosti i cjelovitosti podataka.

- Svaki čvor održava svoju kopiju baze, podaci u svakom čvoru su identični.
- Postoje mehanizmi koji omogućuje čvorovima da sinkroniziraju promjene i održavaju identične kopije.
- Postoje mehanizmi koji garantiraju poželjna sigurnosna svojstva.



## Poželjna svojstva

Atomarnu promjenu baze obično nazivamo *transakcija*.

- *Integritet* – detalji transakcija se ne mogu izmijeniti.
- *Neizbrisivost* – transakcije se ne mogu izbrisati.
- *Autentičnost* – transakcije su ispravno autorizirane.
- *Neporecivost* – autorizacije transakcija se ne mogu poreći.
- *Ispравност* – podaci su međusobno *konzistentni*.
- ...

## Zadatak: Sustav digitalnih diploma

Što točno znače pojedina svojstva ako gradimo raspodijeljeni sustav za evidenciju svih sveučilišnih diploma u Republici Hrvatskoj?

## Poželjna svojstva (nastavak)

- Sustav je *javan* – svatko može provjeriti ispravnost podataka, vršiti operacije na bazi, svatko može postati čvor u mreži.
- Sustav je *decentraliziran* – ne ovisi o nekom centralnom autoritetu.
- Sustav je *robustan* – funkcionira i kad je puno čvorova neispravno ili čak zlonamjerno.
- Postoji mehanizam *odgovornosti* – moguće je na neki način kazniti čvorove za neispravno ponašanje.
- ...

## Pažnja!

Nemaju svi sustavi sva poželjna svojstva.

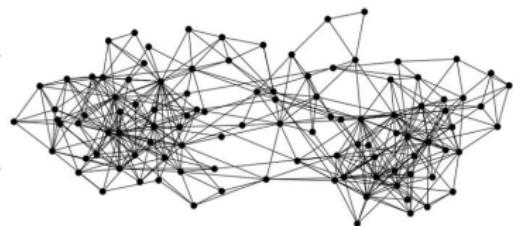
Ne znamo ostvariti sva poželjna svojstva *apsolutno*.

## Kriptovaluta

Javna i decentralizirana raspodijeljena glavna knjiga u koju spremamo digitalno potpisane transakcije, a svaka transakcija opisuje promjenu vlasništva određene količine novca.



signed by Alice  
Pay to  $pk_{Bob}$  :  $H( )$



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

## Ishodi učenja

- ① Definirati osnovne pojmove u tehnologiji raspodijeljene glavne knjige
- ② Objasniti temeljnu tehnologiju transakcija, blokova, proof-of-work te izgradnju konsenzusa
- ③ Opisati razlike između najistaknutijih struktura ulančanih blokova
- ④ Analizirati platforme poput Ethereuma za izgradnju aplikacija temeljenih na ulančanim blokovima
- ⑤ Opravdati korisnost i vrijednost digitalnih valuta
- ⑥ Ocijeniti okruženja gdje se strukture temeljene na ulančanim blokovima mogu primijeniti, njihove potencijale i ograničenja
- ⑦ Prepoznati nove izazove u monetizaciji poslovanja vezanog uz kriptovalute i tehnologiju raspodijeljene glavne knjige

Razlike između kartičnog, gotovinskog (papirnatog) plaćanja i plaćanja kriptovalutom:

- Tko sve može plaćati i primiti novčana sredstva?
- Tko sve sudjeluje u transakciji?
- Kome su sve poznati podaci o transakciji?
- Koji nivo anonimnosti imaju sudionici?
- Može li se transakcija osporiti i opovrgnuti?
- Je li potreban centralni autoritet?

## Odabrani dio povijesti

- 1988 – Chaum, Fiat, Naor, Untraceable electronic cash.
- 1989 – DigiCash.
- 1990's – Mondex, Visa Cash.
- 1998 – HashCash (*proof-of-work* kao zaštita od spam-a).
- 2008 – Bitcoin whitepaper.
- 2009 – Prva Bitcoin transakcija.
- 2013 – Ukupna vrijednost svih Bitcoina prelazi  $\$10^9$ .
- 2014 – Blockchain 2.0 — Ethereum
- 2018 – RGKK na FER-u :)
- 2020 – The Beacon Chain, DeFi
- 2022 – Ethereum koristi *proof-of-stake*

Plan za sljedećih nekoliko predavanja:

- Kriptografska hash funkcija.
- Digitalni potpis.
- Jednostavne kriptovalute.
- Raspodijeljeni konsenzus.
- Bitcoin.

## Osnovna svojstva

- Ulaz je niz bitova proizvoljne duljine.
- Izlaz je niz bitova fiksne duljine (npr. točno 256 bita).
- Funkcija je deterministička i može se brzo i efikasno izračunati.
- Funkcija je javna.

```
$ echo -n "fer" | sha1sum  
cef48cb4569d34364e0e86067efa14fbe9b4591e  -  
$ echo -n "fer" | sha1sum  
cef48cb4569d34364e0e86067efa14fbe9b4591e  -  
$ sha1sum big.txt  
0c496df552232e34beaba1e15046f87e147d14f6  big.txt  
$ sha1sum empty.txt  
da39a3ee5e6b4b0d3255bfef95601890afd80709  empty.txt
```

# Kriptografska hash funkcija

Izlazi kriptografske hash funkcije "izgledaju slučajno"...

```
$ echo -n "fer" | sha1sum  
cef48cb4569d34364e0e86067efa14fbe9b4591e -  
$ echo -n "fera" | sha1sum  
e63c831418b7db691a469df5c15f405ecdade29a -  
$ echo -n "Fer" | sha1sum  
4514751a6511a102351de1f2b6abf0d6633c401f -  
$ echo -n "fes" | sha1sum  
a05b39a713e206dfa099e81182b9511af8b707f5 -
```

Hash funkcija  $H$  je . . .

## Otporna na kolizije

Ako je “praktički nemoguće” pronaći dvije različite poruke  $x$  i  $y$  takve da vrijedi  $H(x) = H(y)$ .

## Korisna za slagalice

Ako je za svaki  $n$ -bitni sažetak  $y$  i za slučajno odabrani prefix  $k$  potrebno red veličine  $2^n$  operacija kako bi se pronašao  $x$  takav da vrijedi  $H(k||x) = y$  (dokle god  $k$  ima “dovoljno entropije”).

Kolizije uvijek postoje!

Ima beskonačno mogućih poruka, a  $2^n$  mogućih sažetaka pa neke poruke moraju imati isti sažetak.

Za dobru kriptografsku hash funkciju vrijedi:

Jako je teško *pronaći* jednu jedinu koliziju, čak ako napadač ima na raspolaganju ogromne računalne resurse i puno vremena.

## Napad grubom silom

- ① Odaberite slučajnu poruku  $x$ .
- ② Izračunajte  $y \leftarrow H(x)$ .
- ③ Zapamtiti par  $(y, x)$
- ④ Ako je  $(y, x')$  već viđen za neki  $x' \neq x$  onda smo našli koliziju.
- ⑤ Inače, idite na prvi korak.

Iz *paradoksa rođendana* slijedi da je potrebno red veličine  $2^{n/2}$  koraka kako bi algoritam pronašao koliziju za hash funkciju čiji je sažetak veličine  $n$  bita.

# Kriptografska hash funkcija – primjene

## Zadatak: Pohrana u oblaku

Spremate važnu datoteku na FER web kako bi je dohvatili s drugog računala. Kako možete biti sigurni da administratori nisu promijenili vašu datoteku?

## Zadatak: Backup svih datoteka

Odredite koliko različitih datoteka postoji na disku vašeg računala i pronađite sve duplike.

- Zaštita integriteta poruka.
- Zaštita zaporki.
- Generiranje pseudo-slučajnih brojeva.
- Digitalni potpis.
- ...

# Hash pokazivač

## Definicija

*Hash pokazivač je pokazivač na neku poruku  $x$  zajedno s kriptografskim sažetkom te poruke  $H(x)$ . Dereferenciranje pokazivača uključuje ponovno računanje sažetka i uspoređivanje sa spremlijenim.*

```
path: /home/user/big.txt
```

```
sha1: 0c496df552232e34beabae1e15046f87e147d14f6
```

```
block_id: 4541244, transaction_id: 3426
```

```
sha256: f6f0748717aca736bf18d5014279033f331a802348409ce305f908024fb2db46
```

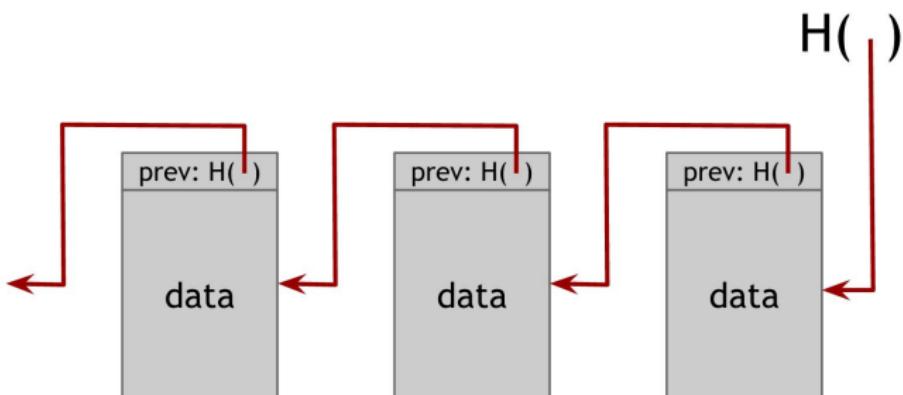


Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

# Kriptografski lanac blokova

## Definicija

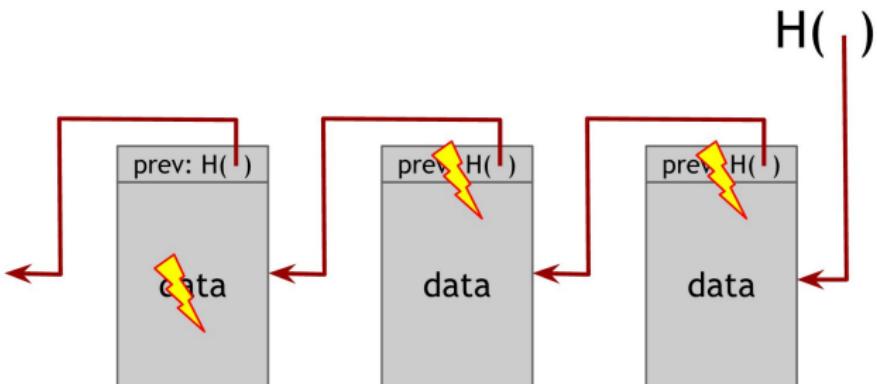
*Kriptografski lanac blokova je jednostruko povezana lista u kojoj svaki element (uz neke podatke) sadrži hash pokazivač na prethodni element.*



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

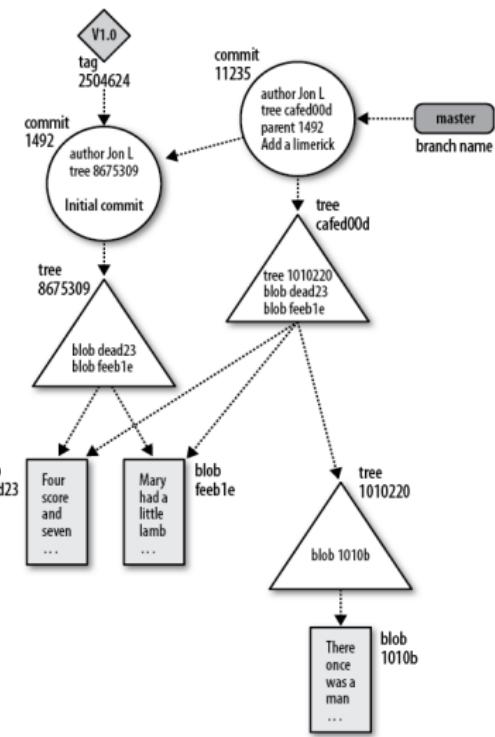
## Važno!

Hash pokazivač sadrži sažetak *cijelog* prethodnog bloka uključujući i njegov hash pokazivač.



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

# Digresija – git



Izvor: Jon Loeliger, Matthew McCullough, Version Control with Git

# Kriptografski lanac blokova – primjer

[https://www.fer.hr/lanac\\_diploma/master/2017.yaml](https://www.fer.hr/lanac_diploma/master/2017.yaml)

```
- previous_block:  
  block_id: 2016  
  block_uri: https://www.fer.hr/lanac_diploma/master/2016.yaml  
  block_hash: ade6629cd9b1fc5d55b88d7b09a82d621d9e513  
- block_id: 2017  
- student:  
  name: "Mirko Mirić"  
  oib: 123456789  
  graduation_date: "Sep 28 2017"  
- student:  
  name: "Slavko Slavić"  
  oib: 986198232  
  graduation_date: "Jul 01 2017"
```

Narodne novine, listopad 2017

FER čestita svim novim magistrima inženjerima!

Block: [https://www.fer.hr/lanac\\_diploma/master/2017.yaml](https://www.fer.hr/lanac_diploma/master/2017.yaml)

Hash: a6d6be112ab1a22baebf38a6fe26674bb44e16b0

## Zadatak

*Kako poslodavac može provjeriti je li kandidat stvarno diplomirao na FER-u? Što ako je poslodavac stvarno paranoičan?*

## Zadatak

*Ako [www.fer.hr](http://www.fer.hr) nije dostupan, kako student može dokazati da je stvarno diplomirao?*

## Zadatak

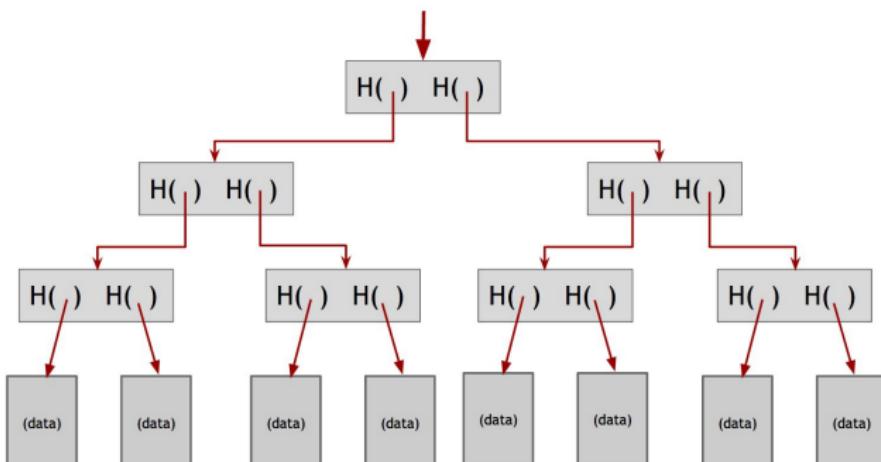
*Što napadač mora napraviti kako bi dodao (ili uklonio) podatak da je neki student diplomirao 2010. godine?*

*"The past was alterable. The past never had been altered.  
Oceania was at war with Eastasia. Oceania had always  
been at war with Eastasia."*

*George Orwell, 1984*

## Definicija

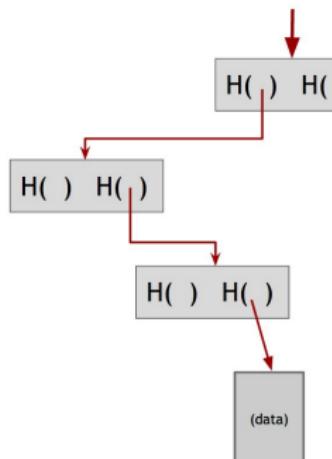
*Merkleovo stablo je potpuno binarno stablo u kojem svaki unutarnji čvor sadrži hash pokazivače na svoja dva djeteta.*



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

## Zadatak

Kako možemo nekoga uvjeriti da se određeni list stvarno nalazi u stablu?



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

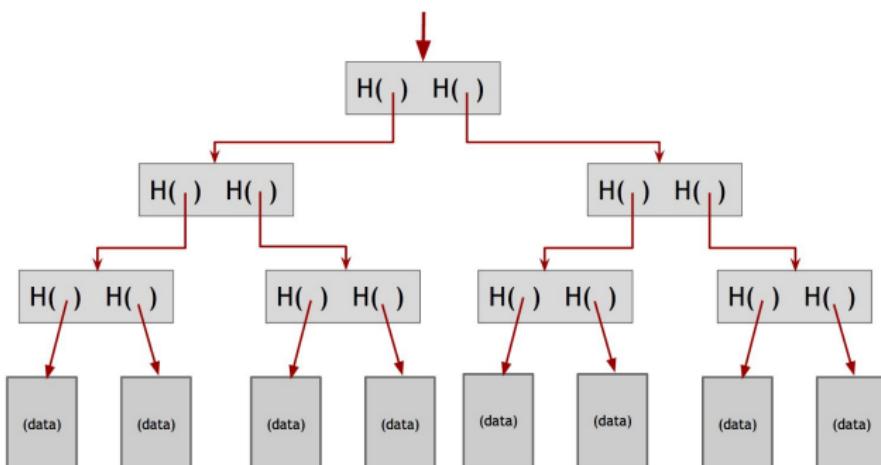
Izazov

*Kako možemo nekoga uvjeriti da element nije dio stabla?*

# Merkleovo stablo – dokaz nepripadnosti

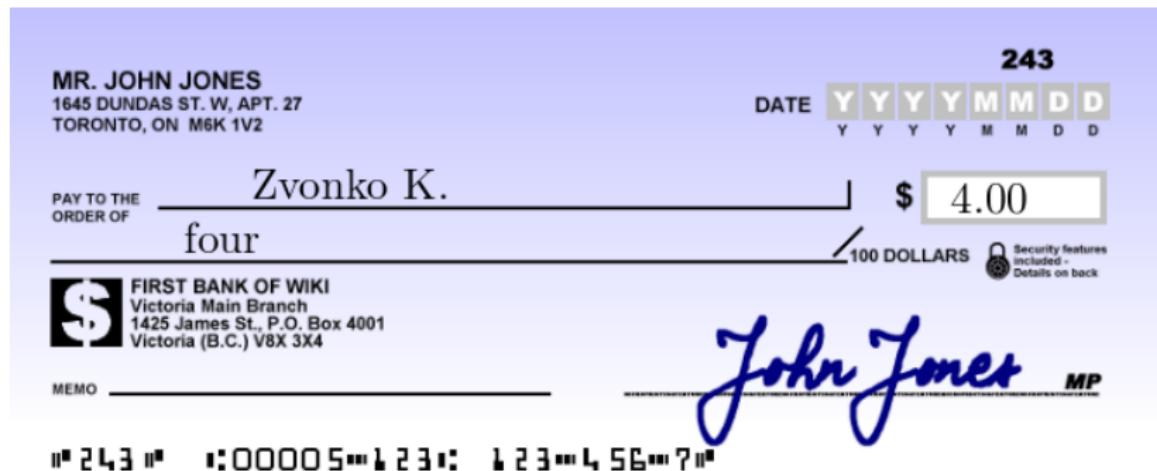
Izazov

Kako možemo nekoga uvjeriti da element nije dio stabla?



Izvor: [bitcoinbook.cs.princeton.edu](http://bitcoinbook.cs.princeton.edu)

# Ponavljanje: digitalni potpis



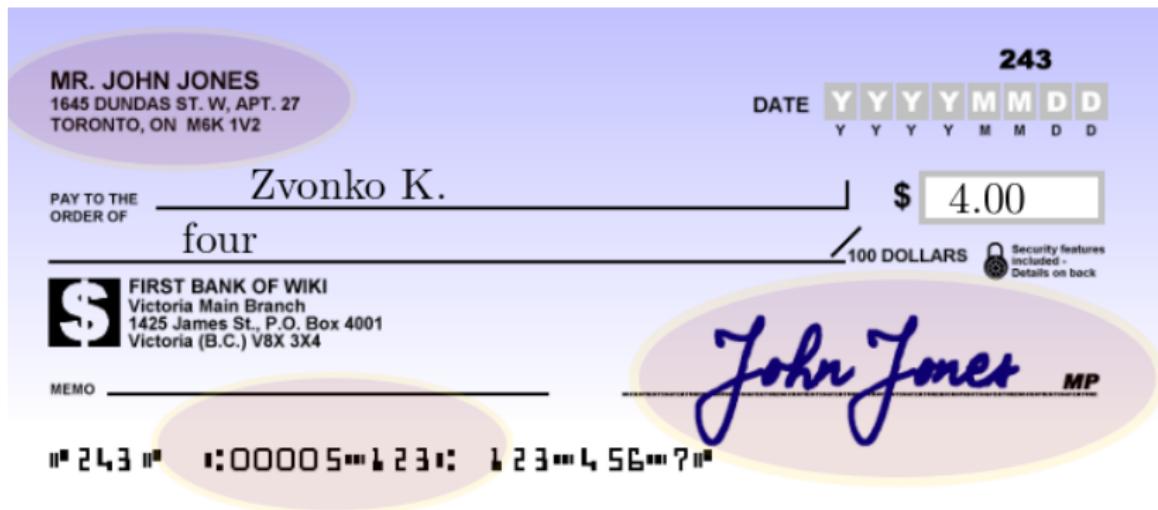
Izvor: wikipedia.org

- ➊ Ana generira par ključeva  $(sk, pk)$  — redom njezin *privatni* i *javni* ključ. Ana objavi svoj javni ključ, privatni ključ dobro čuva. Branko dohvata i sprema Anin javni ključ.
- ➋ Ana želi poslati poruku  $m$  Branku.
- ➌ Ana za poruku  $m$  računa potpis  $\sigma \leftarrow S(sk, m)$ .
- ➍ Ana šalje Branku poruku  $m$  i potpis  $\sigma$ .
- ➎ Branko računa  $V(pk, m, \sigma)$  i prihvata poruku samo ako je provjera uspješna.

## Zadatak

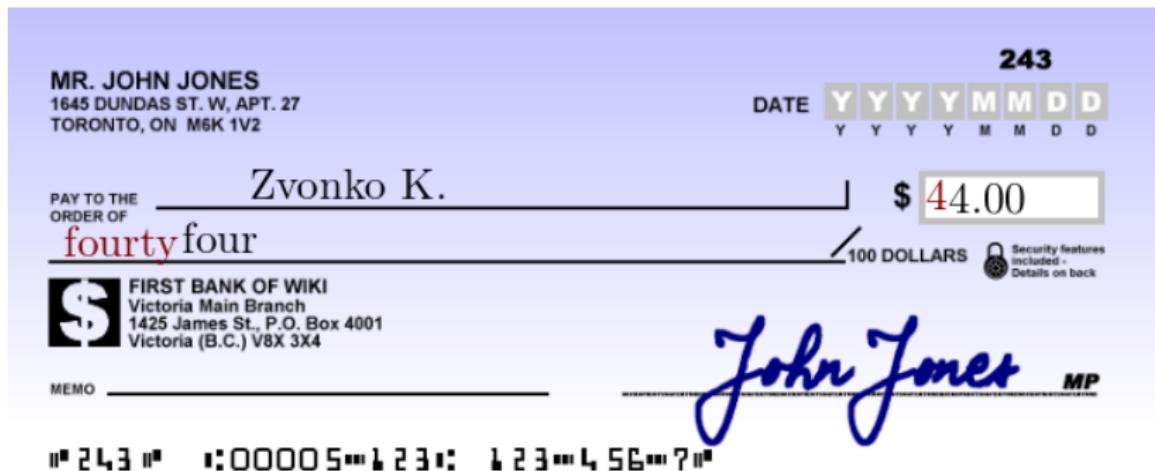
Recimo da je Branko Anin osobni bankar, a poruka  $m$  upute za bankovnu transakciju. Koja svojstva treba pružati digitalni potpis?

# Digitalni vs. analogni potpis – autentifikacija



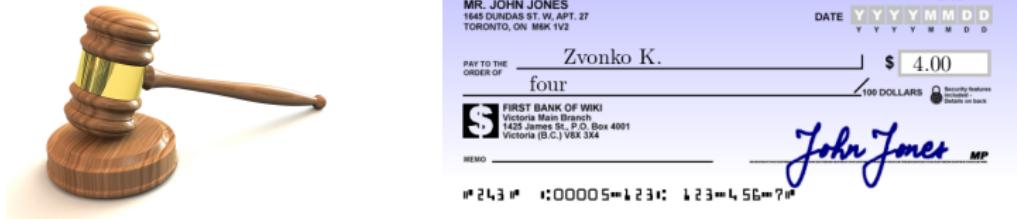
Izvor: wikipedia.org

# Digitalni vs. analogni potpis – integritet



Izvor: wikipedia.org

# Digitalni potpis – neporecivost



Izvor: wikipedia.org

## Sustav digitalnog potpisa

Trojka algoritama:

- $G()$  – algoritam koji generira par ključeva  $(sk, pk)$ .
- $S(sk, m)$  – algoritam koji na temelju privatnog ključa  $sk$  i poruke  $m$  generira potpis  $\sigma \leftarrow S(sk, m)$ .
- $V(pk, m, \sigma)$  – algoritam koji prima javni ključ, poruku i njezin tobožnji potpis i vraća `true` ako je  $\sigma$  ispravan potpis poruke  $m$  odgovarajućim privatnim ključem, a `false` ako nije.

## Svojstvo korektnosti: Ispravni potpisi prolaze provjeru

Ako je  $(sk, pk) \leftarrow G()$ , onda za svaku poruku  $m$  vrijedi  
 $V(pk, m, S(sk, m)) = \text{true}$ .

## Praktički je nemoguće krivotvoriti potpis

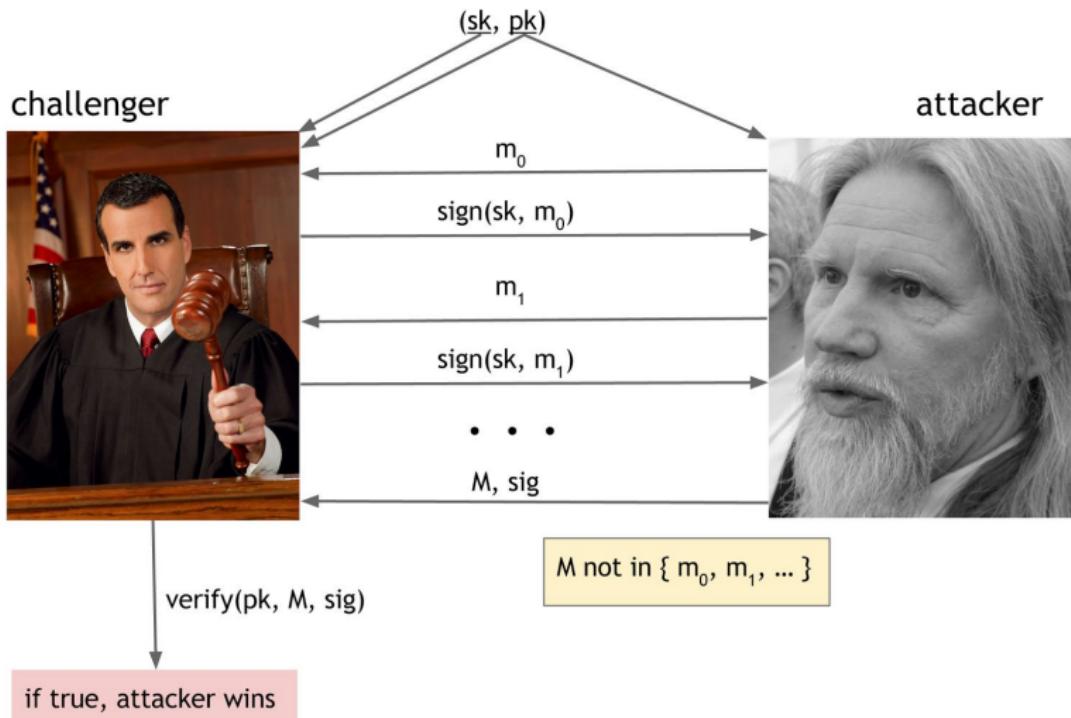
Napadač koji nema privatni ključ ne može konstruirati niti jednu *novu* poruku  $m$  i njezin potpis  $\sigma$  koji prolazi postupak provjere, tj. za koje vrijedi  $V(pk, m, \sigma) = \text{true}$ .

- Čak i ako napadač zna odgovarajući javni ključ  $pk$ .
- Čak i ako napadač ima mogućnost da dobije potpis  $\sigma' \leftarrow S(sk, m')$  proizvoljne poruke  $m'$ .

## Izazov

*Kakve veze naša definicija sigurnosti ima sa svojstvima autentifikacije, integriteta i neporecivosti?*

# Digitalni potpis – sigurnost



Sve konstrukcije koje znamo su bazirane na matematici:

- RSA
- DSA
- ECDSA
- ...

Bitcoin koristi ECDSA sustav s "secp256k1" krivuljom:

- Privatni ključ: 256 bita
- Javni ključ: 520 bita ("kompresirani" javni ključ 264 bita)
- Potpis: 512 bita
- Efektivna veličina ključa: 128 bita
- Hash funkcija SHA256 je dio algoritma potpisivanja.

- Potpisivanje elektronskih dokumenata.
- Sigurnosni protokoli (TLS, ...).
- Autentifikacija email-a.
- Provjera integriteta software-a (apk, exe, firmware, ...).
- Kriptovalute.
- ...

# Digitalni potpis – primjene

 <b>REPUBLIKA HRVATSKA MINISTARSTVO ZNANOSTI I OBRAZOVANJA</b>	Vrijeme izdavanja: 18.05.2017. 21:52:12
Izdavatelj certifikata:	CN=STATUS STUDENTA, L=ZAGREB, O=SVEUČILIŠTE U ZAGREBU SVEUČ.RAČUN.CENTAR HR34016189309, C=HR
Serijski broj:	1234567890
Algoritam potpisa:	SHA1withRSA
Broj zapisa:	2017-1245-67
Kontrolni broj:	123-144-5444
Elektronički pečat:	UHJ2aSBzdHVkZW50IGivamkgdSBha2FkZW1za29qIGdvZGluaSAyMDE4LzlwMTkgeG/FoWFsamUgc2xqZWRIxIdpIGtvZApYSBhbnsRlLmRlcemVrQGZlci5ociBkb2JpdmEgMTAgYm9kh3ZhOtbjYmQ3Y2M2MzM0NjQ0NGI2Mzk3YTRhN2UyZT12Zgo=
Informacije za provjeru dokumenta:	Na Internet adresi <a href="https://isspp.srce.hr/e-potvrda/provjera">https://isspp.srce.hr/e-potvrda/provjera</a> možete provjeriti točnost podataka navedenih u ovom elektroničkom zapisu. Upisivanjem broja zapisa i kontrolnog broja sustav će prikazati izvornik ovog elektroničkog zapisa.
Napomena:	Elektronički pečat kreiran je certifikatom Ministarstva znanosti, obrazovanja i sporta.

## Izazov

*Koja je razlika između ovakvih diploma i sustava baziranom na lancu blokova?*

# Digitalni potpis – identitet i javni ključ

Većina primjena digitalnog potpisa

Bitna je veza između identiteta i javnog ključa!

Certificate Viewer: \*.fer.unizg.hr

**General** Details

This certificate has been verified for the following usages:

SSL Server Certificate

**Issued To**

Common Name (CN)	*.fer.unizg.hr
Organization (O)	Sveučilište u Zagrebu
Organizational Unit (OU)	CIP

**Issued By**

Common Name (CN)	TERENA SSL CA 3
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>

**Validity Period**

Issued On	Sunday, May 13, 2018 at 2:00:00 AM
Expires On	Wednesday, May 20, 2020 at 2:00:00 PM

**Fingerprints**

SHA-256 Fingerprint	40 3C 93 37 41 0E 46 A0 50 7E BC 01 A8 2C 17 A9 97 06 C9 09 3F 9B 3B BF 69 51 A6 B9 E9 F3 SD 8A
SHA-1 Fingerprint	B8 EB B1 FA 0D 60 90 BA 67 56 45 72 9A E0 E2 2F BA DA 59 4C

# Digitalni potpis – identitet i javni ključ

## Kriptovalute

Nema veze između identiteta i javnog ključa!

Identitet = Javni ključ!

The screenshot shows a transaction on the Block Explorer. It has one input (4c3f852fa645148cf... ) and two outputs:

- Output 1: 1GjL2pzK4Ycd... 0.00059274 BTC
- Output 2: 179aKQAbwJZjUbqdWT... 0.00005176 BTC (U)
- Output 3: 1GjL2pzK4Ycd... 0.0005342 BTC (S)

Below the transaction details, it shows:  
FEE: 0.00000678 BTC      UNCONFIRMED TRANSACTION!      0.00058596 BTC

Izvor: [blockexplorer.com](https://blockexplorer.com)