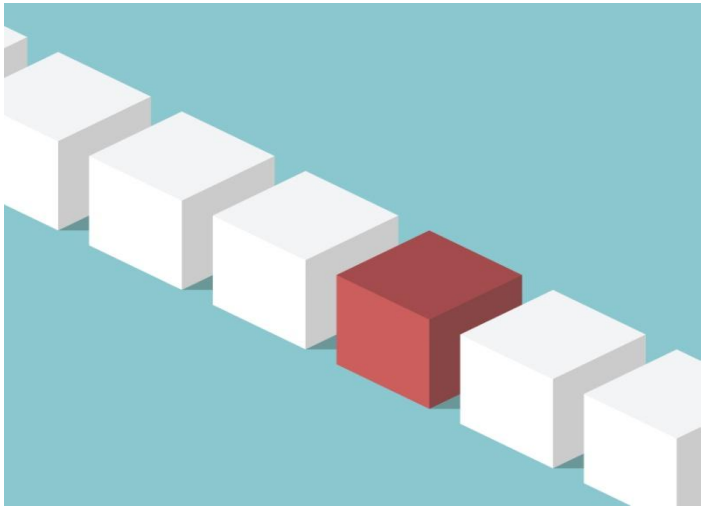
Veleučilište u Bjelovaru

Pohrana diploma studenata Veleučilišta u Bjelovaru na blockchain

Homer Simpson, master of the Blockchain.

Osnove blockchain-a

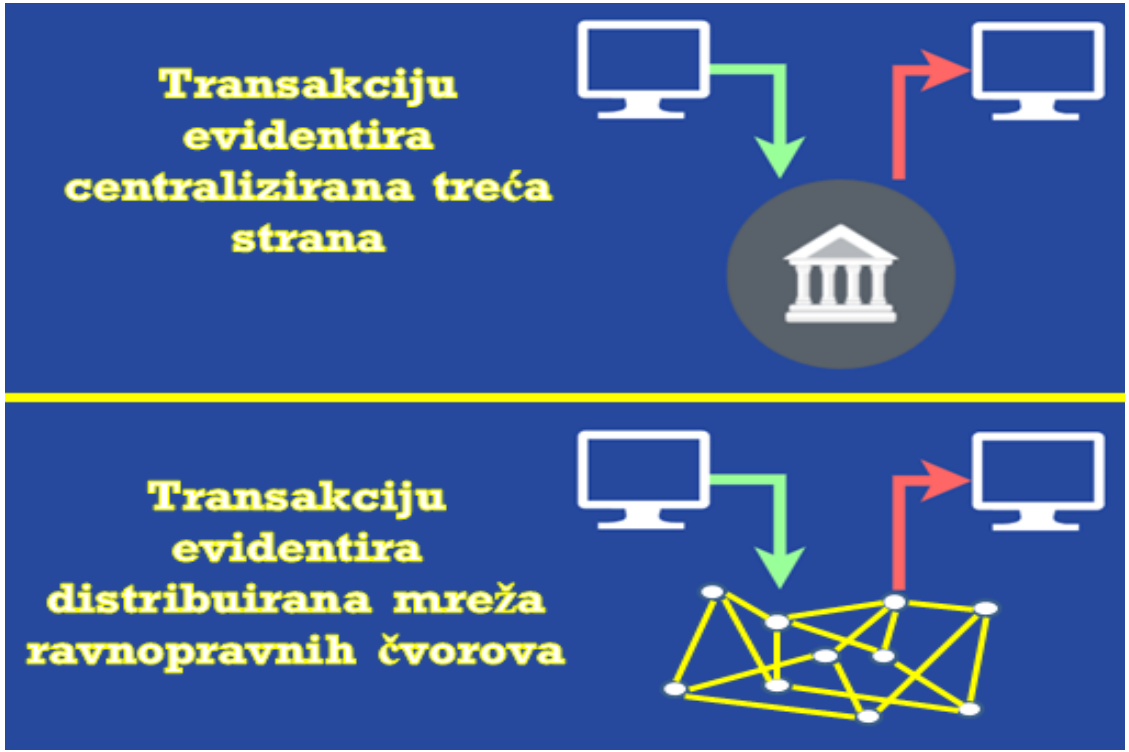
- Pojam **blockchain** – lanac podatkovnih blokova
- Svaki blok sadrži podatke o izvršenim transakcijama



- **Blockchain ledger** – knjiga transakcija na blockchainu – sačinjena od blokova podataka

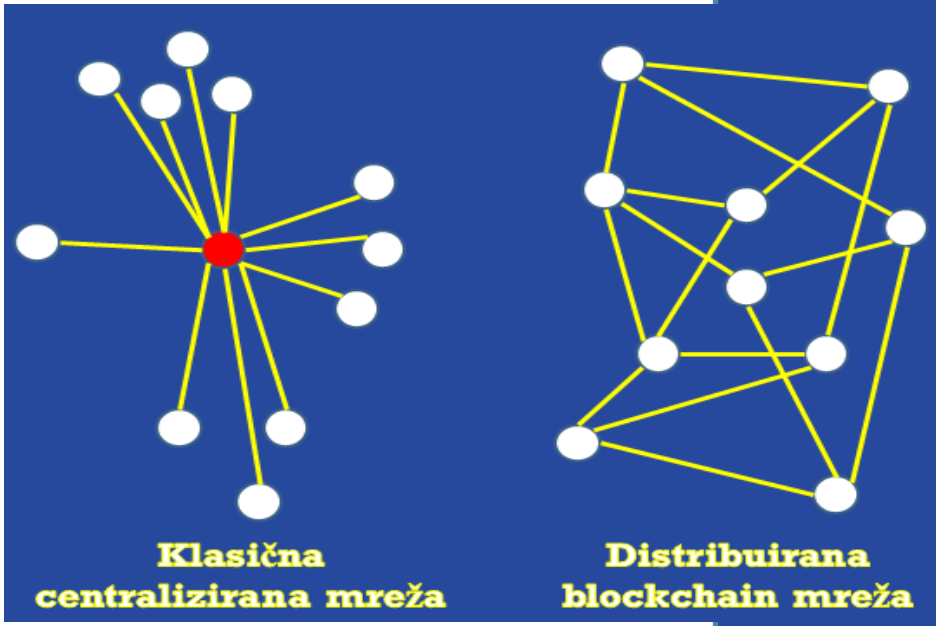
Osnove blockchain-a

- Problem povjerenja na internetu



Osnove blockchain-a

- **Distribuiran sustav za bilježenje transakcija**
- Temeljen na kriptografskim algoritmima i principima P2P arhitekture
- Velik broj dobrovoljnih sudionika u mreži– čvorovi



Osnove blockchain-a

Nekoliko vrsta čvorova:

Mining nodes

zapisuju nove transakcije u blockchain

Full nodes

Sadrže podatke o svim transakcijama - cijelu knjigu transakcija

Light nodes

Sadrže manje dijelove knjige transakcija - zapisi koji u tom trenu interesiraju korisnika - mogu slati u mrežu korisnikove zahtjeve za novim transakcijama

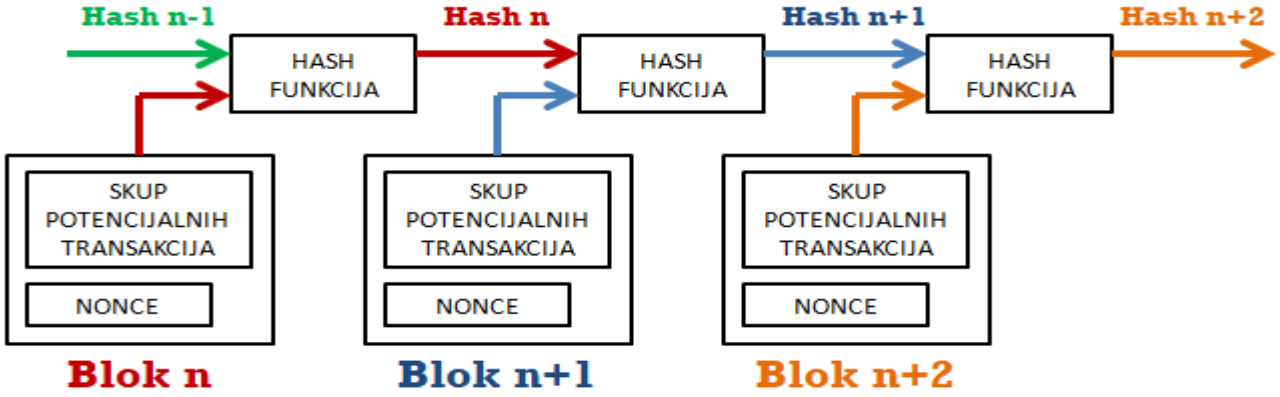
Osnove blockchain-a

- U lanac nije moguće dodati bilo kakav blok
- Svakom potencijalnom bloku se računa takozvani “hash kod”
- Mining node-ovi traže hash kod određenih karakteristika -> prvih n znamenki hash koda moraju biti nule
- SHA-256 algoritam kao rezultat uvijek daje HASH kod od 64 heksadecimalna znaka

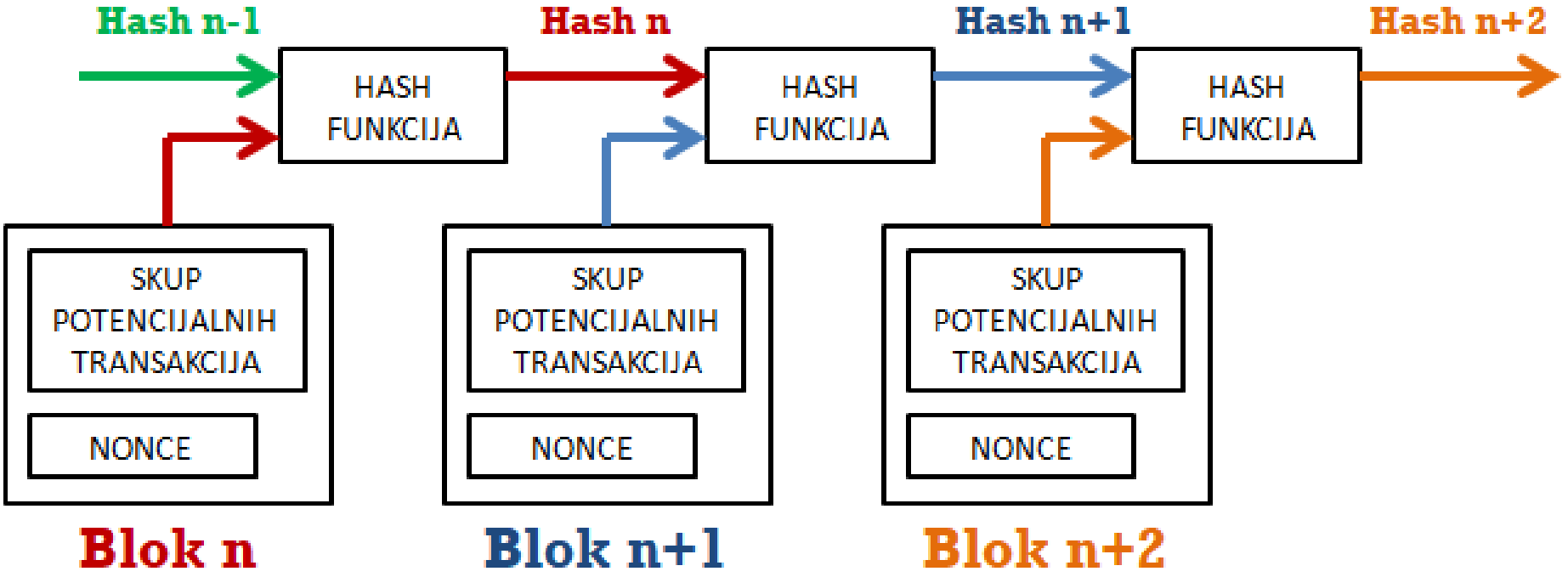
Ulazna vrijednost	A
HASH (SHA-256)	Ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

Osnove blockchain-a

Ulazna vrijednost	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
HASH (SHA-256)	2d8c2f6d978ca21712b5f6de36c9d31fa8e96a4fa5d8ff8b0188dfb9e7c171bb



Osnove blockchain-a



Osnove blockchain-a

- Blockchain je distribuirana mreža koja sadrži knjigu transakcija
- U knjigu se pohranjuju tekstualni podatci
- Ulančavanje podatkovnih blokova pomoću hash kodova osigurava nepromjenjivu povijest transakcija

KRATKA POVIJEST BLOCKCHAIN-A

1991.

Istraživački rad "How to Time-Stamp a Digital Document"

31. listopada 2008.

Satoshi Nakamoto objavljuje rad "Bitcoin: A peer-to- peer Electronic Cash System

12. siječnja 2009.

Prva Bitcoin transakcija

2010.

- Bitcoin hakiran
- Prva kupnja Bitcoin-om – pizza za 10 000 BTC

29. listopada 2013.

Prvi Bitcoin bankomat

2014. - danas

Nagli razvoj ostalih kriptovaluta i vezane industrije

KRATKA POVIJEST BLOCKCHAIN-A

2009.
Bitcoin

2011.
Litecoin
Namecoin
Swiftcoin

2013.
50ak kriptovaluta

2014.
Oko 300 kriptovaluta.
Stvoren Syscoin

2015.
Oko 500 kriptovaluta.
Stvoren Ethereum

2018.
Više od 1600 kriptovaluta

Syscoin protokol

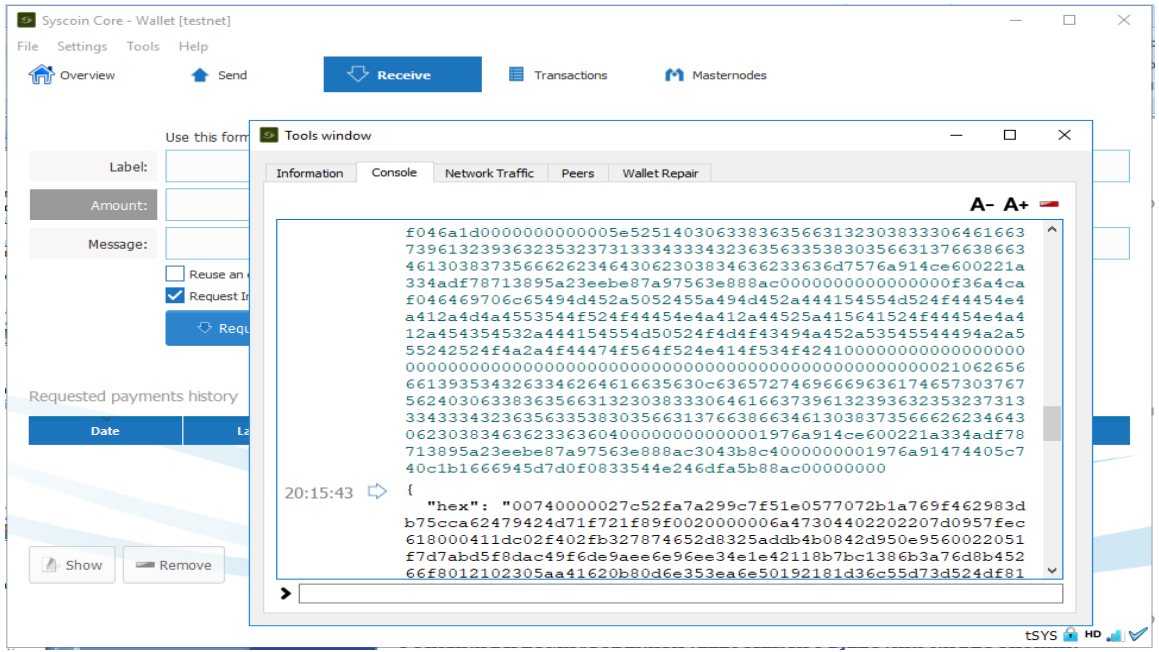
- **Syscoin – stvoren grananjem Bitcoin protokola 2014. godine**
  - Nadograđivan značajkama koje Bitcoin ne podržava
  - Prvotno zamišljen kao blockchain specijaliziran za pohranu ponuda za trgovanje – nalik na e-bay
  - Broj transakcija u sekundi(TPS):
    - Bitcoin – 5-10
    - Syscoin – 70-100
    - VISA - 1700

Syscoin protokol

- 1MB blok svakih 60s
- 60Mb/h -> 600Mb/10h -> 1Gb/17h
- 6300B – max. veličina transakcije
  - 158 transakcija u minuti za max. veličinu
  - 2,6 TPS za max. veličinu transakcije
- Veličina cijelog chain-a -> oko 1Gb

Syscoin protokol

- **Pristup Syscoin blockchain-u ostvaruje se instalacijom aplikacije Syscoin QT Wallet koja u mreži sudjeluje kao FULL NODE**



Syscoin protokol

- **Metode za pohranu podataka na Syscoin blockchain:**
  - **CREATERAWTRANSACTION**
    - 40 ASCII znakova (novije verzije BTC-a – do 83B)
  - **OFFERNEW**
    - Parametri “category” i “title” primaju svaki po 256 znakova
    - Parametar “description” prihvaća do 512 znakova
    - Ukupno do 1024 znaka

Syscoin protokol

- **Metode za pohranu podataka na Syscoin blockchain:**
  - **ALIASNEW**
    - Stvara pseudonim koji je moguće koristiti umjesto blockchain adresa
    - Alias je jedinstven u Syscoin mreži
    - Parametar “public value” uz alias može spremiti do 256 znakova na blockchain

ALIAS	ADRESA
Janko	ShBFzP3YC9fxYSjTgvnGyTKdhPp9sL2LAH

Syscoin protokol

- **Metode za pohranu podataka na Syscoin blockchain:**
  - **CERTNEW**
    - **certnew [alias] [title] [public value] [category=certificates] [witness]**
    - Parametar “title” prima 256 znakova, kao i parametar “public value”
    - Prije korištenja ove metode potrebno je registrirati alias koji se šalje kao prvi argument -> jamstvo vlasništva certifikata

Primjena Syscoin platforme za pohranu diploma

Metode korištene za upis diplome:

1 **CERTNEW vub dipl “podatci” “certificates” “”**

Poziv ove metode vraća dvije vrijednosti:

- serijalizirani podatci o certifikatu u obliku heksadecimalnog niza
- Guid certifikata – globalni jedinstveni identifikator certifikata

GUID se koristi za dohvaćanje certifikata i pripadajućih podataka s blockchain-a

Primjena Syscoin platforme za pohranu diploma

1 Metoda CERTNEW

```
certnew vub dipl "IME*PREZIME*DATUMRODENJA*MJESTORODENJA*DRZAVARODENJA*EC
TS*DATUMPROMOCIJE*STUDIJ*URBROJ*ODGOVORNAOSOBA" "certificates" ""
[
  "00740000017c52fa7a299c7f51e0577072b1a769f462983db75cca62479424d71f721f
89f00200000035515203767562103330326635623366326232623066353700006d6d6d76a
914ce600221a334adf78713895a23eebe87a97563e888acffffffff036a1d000000000000
5e525140306338363566313230383330646166373961323936323532373133343334323633
56335383035663137663866346130383735666262346430623038346362336360d7576a914
ce600221a334adf78713895a23eebe87a97563e888ac0000000000000000f36a4caf04646
9706c65494d452a5052455a494d452a44415455 4d524f44454e4a412a4d4a4553544f524f
44454e4a412a44525a415641524f44454e4a412a454354532a44415455 4d50524f4d4f434
94a452a53545544494a2a555242524f4a2a4f44474f564f524e414f534f42410000000000
0000000000000000000000000000000000000000000000000000000000210626566613935 3
43263346264616635630c6365727469666963617465730376756240306338363566313230
38333064616637396132393632353237313334333432363563353830356631376638663461
13038373566626234643062303834636233636040000000000001976a914ce600221a334
adf78713895a23eebe87a97563e888ac00000000",
  "befa9542c4bdaf5c"
]
```

GUID

Primjena Syscoin platforme za pohranu diploma

Metode korištene za upis diplome:

2 **SYSCOINTXFUND <hex zapis iz prethodne metode>**

Pridružuje certifikatu novčana sredstva

Poziv ove metode vraća:

- Heksadecimalni niz u koji su dodane informacije o adresi koja plaća transakciju

Primjena Syscoin platforme za pohranu diploma

2 Metoda SYSCOINTXFUND

```
syscointxfund 00740000017c52fa7a299c7f51e0577072b1a769f462983db75cca62479424d71f721f89f
00200000035515203767562103330326635623366326232623066353700006d6d6d76a914ce600221a334ad
f78713895a23eebe87a97563e888acffffffff036a1d0000000000005e525140306338363566313230383333
064616637396132393632353237313334333432363563353830356631376638663461303837356662623464
306230383463623363 6d7576a914ce600221a334adf78713895a23eebe87a97563e888ac000000000000000
0f36a4caf046469706c65494d452a5052455a494d452a444154554d524f44454e4a412a4d4a4553544f524f
44454e4a412a44525a415641524f44454e4a412a454354532a444154554d50524f4d4f43494a452a5354554
4494a2a555242524f4a2a4f44474f564f524e414f534f4241000000000000000000000000000000000000000
000000000000000000000000000000210626566613935343263346264616635630c6365727469666696361746
573037675624030633836356631323038333064616637396132393632353237313334333432363563353830
356631376638663461303837356662623464306230383463623363604000000000000001976a914ce600221a
334adf78713895a23eebe87a97563e888ac00000000
```

```
[
  "00740000027c52fa7a299c7f51e0577072b1a769f462983db75cca62479424d71f721f89f00200000035
515203767562103330326635623366326232623066353700006d6d6d76a914ce600221a334adf78713895a2
3eebe87a97563e888acffffffffb47c39d740714fcb57c65f651fe23c1d9b588997dcf7063fb6aed4ae7158
e9c9010000001976a914b78da58b42853a9ebcfdb6ed3183638a6008ab3b88acffffffff046a1d000000000
0005e525140306338363566313230383330646166373961323936323532373133343334323635633538303 5
663137663866346130383735666262346430623038346362336360 6d7576a914ce600221a334adf78713895a2
3eebe87a97563e888ac0000000000000000f36a4caf046469706c65494d452a5052455a494d452a44415455
4d524f44454e4a412a4d4a4553544f524f44454e4a412a44525a415641524f44454e4a412a454354532a444
154554d50524f4d4f43494a452a53545544494a2a555242524f4a2a4f44474f564f524e414f534f42410000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
264616635630c6365727469666696361746573037675624030633836356631323038333064616637396132 39
363235323731333433343236356335383035663137663866346130383735666262346430623038346362336
360400000000000001976a914ce600221a334adf78713895a23eebe87a97563e888ac3043b8c40000000019
76a91474405c740c1b1666945d7d0f0833544e246dfa5b88ac00000000"
]
```

Primjena Syscoin platforme za pohranu diploma

Metode korištene za upis diplome:

3 **SIGNRAWTRANSACTION <hex zapis iz prethodne metode>**

Potpisuje transakciju s privatnim ključem kako bi se moglo pristupiti novčanim sredstvima

Poziv ove metode vraća:

- Heksadecimalni niz u koji su dodane informacije o adresi koja plaća transakciju i potpis

3 Metoda SIGNRAWTRANSACTION

```
signrawtransaction 00740000027c52fa7a299c7f51e0577072b1a769f462983db75cca62479424d71f721f89f00200
000035515203767562103330326635623366326232623066353700006d6d6d76a914ce600221a334adf78713895a23eeb
e87a97563e888acffffffffb47c39d740714fcb57c65f651fe23c1d9b588997dcf7063fb6aed4ae7158e9c90100000019
76a914b78da58b42853a9ebcfdb6ed3183638a6008ab3b88acffffffff046a1d000000000005e525140306338363563
1323038333064616637396132393632353237313334333432363563353830356631376638663461303837356662623464
306230383463623363 6d7576a914ce600221a334adf78713895a23eebe87a97563e888ac0000000000000000f36a4caf0
46469706c65494d452a5052455a494d452a444154554d524f44454e4a412a4d4a4553544f524f44454e4a412a44525a41
5641524f44454e4a412a454354532a444154554d50524f4d4f43494a452a53545544494a2a555242524f4a2a4f44474f5
64f524e414f534f42410000000000000000000000000000000000000000000000000000000000000000021062656661
393534326334626461663563 0c63657274696669636174657303767562403063383635663132303833306461663739613
2393632353237313334333432363563353830356631376638663461303837356662623464306230383463623363604000
0000000001976a914ce600221a334adf78713895a23eebe87a97563e888ac3043b8c4000000001976a91474405c740c1
b1666945d7d0f0833544e246dfa5b88ac00000000
```


```
{
  "hex": "00740000027c52fa7a299c7f51e0577072b1a769f462983db75cca62479424d71f721f89f0020000006a473
04402202207d0957fec618000411dc02f402fb327874652d8325addb4b0842d950e9560022051f7d7abd5f8dac49f6de9
aee6e96ee34e1e42118b7bc1386b3a76d8b45266f8012102305aa41620b80d6e353ea6e50192181d36c55d73d524df81e
5554f29afdb7437ffffffffb47c39d740714fcb57c65f651fe23c1d9b588997dcf7063fb6aed4ae7158e9c9010000006b
483045022100a23943d3ad3ab1881f6d14b1d39199ead8c768d5823ab7b312d7bca9b02c0109022055ba66251a0c96ac1
bb833f4508340e8deabfca3d8020388fc1670638f893bb7012102c01dbe2f3aeefc0f079718adf824916136e73bdfb995
cf773bc3dfb479074dbcffffffff046a1d000000000005e525140306338363566313230383330646166373961323936 3
2353237313334333432363563353830356631376638663461303837356662623464306230383463623363 6d7576a914ce
600221a334adf78713895a23eebe87a97563e888ac0000000000000000f36a4caf046469706c65494d452a5052455a494
d452a444154554d524f44454e4a412a4d4a4553544f524f44454e4a412a44525a415641524f44454e4a412a454354532a
444154554d50524f4d4f43494a452a53545544494a2a555242524f4a2a4f44474f564f524e414f534f42410000000000000
00000000000000000000000000000000000000000000000000021062656661393534326334626461663563 0c6365
727469666963617465730376756240306338363566313230383330646166373961323936323532373133343333432363 56
3353830356631376638663461303837356662623464306230383463623363604000000000000001976a914ce600221a334
adf78713895a23eebe87a97563e888ac3043b8c4000000001976a91474405c740c1b1666945d7d0f0833544e246dfa5b8
8ac00000000",
  "complete": true
}
```

Primjena Syscoin platforme za pohranu diploma

Metode korištene za upis diplome:

4 **SYSCOINSENDRAWTRANSACTION <hex zapis iz prethodne metode>**

Objavljuje transakciju mreži

Poziv ove metode vraća:

- ID transakcije - 64 heksadecimalna znaka

Primjena Syscoin platforme za pohranu diploma

4 Metoda SYSCOINSENDRAWTRANSACTION

```
syscoinsendrawtransaction 00740000027c52fa7a299c7f51e0577072b1a769f462983db75cca6247942
4d71f721f89f0020000006a4730440220207d0957fec618000411dc02f402fb327874652d8325addb4b084
2d950e9560022051f7d7abd5f8dac49f6de9aee6e96ee34e1e42118b7bc1386b3a76d8b45266f8012102305
aa41620b80d6e353ea6e50192181d36c55d73d524df81e5554f29afdb7437ffffffffb47c39d740714fcb57
c65f651fe23c1d9b588997dcf7063fb6aed4ae7158e9c9010000006b483045022100a23943d3ad3ab1881f6
d14b1d39199ead8c768d5823ab7b312d7bca9b02c0109022055ba66251a0c96ac1bb833f4508340e8deabfc
a3d8020388fc1670638f893bb7012102c01dbe2f3aeefc0f079718adf824916136e73bdfb995cf773bc3dfb
479074dbcfffffff046a1d0000000000005e525140306338363566313230383330646166373961323936323
353237313334333432363563353830356631376638663461303837356662623464306230383436236336d7
576a914ce600221a334adf78713895a23eebe87a97563e888ac0000000000000000f36a4caf046469706c65
494d452a5052455a494d452a444154554d524f44454e4a412a4d4a4553544f524f44454e4a412a44525a415
641524f44454e4a412a454354532a444154554d50524f4d4f43494a452a53545544494a2a555242524f4a2a
4f44474f564f524e414f534f4241000000000000000000000000000000000000000000000000000000000000
000000002106265666139353432633462646163563 0c6365727469666963617465730376756240306338363
566313230383330646166373961323936323532373133343334323635633538303566313766386634613038
373566626234643062303834636233636040000000000001976a914ce600221a334adf78713895a23eebe
87a97563e888ac3043b8c4000000001976a91474405c740c1b1666945d7d0f0833544e246dfa5b88ac00000
000
{
  "txid": "a21b06b369aaadf16982f2ad3566263391d9261f78a7e59e5f7fce0f11ee32de"
}
```

Dohvat diploma

- Transakcija je zapisana na blockchain tek kada ju mining node uključi u blok i doda u lanac
- Dohvat certifikata s podatcima o diplomi pomoću GUID-a i metode CERTINFO

Dohvat diploma

- **Dohvat većeg broja zapisa:**

  listcerts [count] [from] [{options}] - scan through all certificates.
  [count] (numeric, optional, unbounded=0, default=10) The number of results to return, 0 to return all.
  [from] (numeric, optional, default=0) The number of results to skip.
  [options] (object, optional) A json object with options to filter results

  listcerts 0 0 '{"alias":"vub", "title":"diploma"}‘

  - **dohvaća sve certifikate koje je upisao alias “vub” i koji imaju naslov “diploma”**

Financije

- **Cijena upisa diplome: 0.0000753 SYS**

  → 0.0000196kn

- **0.00010000 SYS/kB**

  0.000025984kn → 1Gb → 26kn

0.000025984kn	1 kB
0.00025984kn	10 kB
0.0025984kn	100 kB
0.025984kn	1 000 kB
0.25984kn	10 000 kB

Performanse

- Stvaranje i upis certifikata na blockchain traje 10ak sekundi – paralelan upis preko istog čvora je problem
- Dohvat certifikata je trenutan

Primjena Syscoin platforme za pohranu diploma

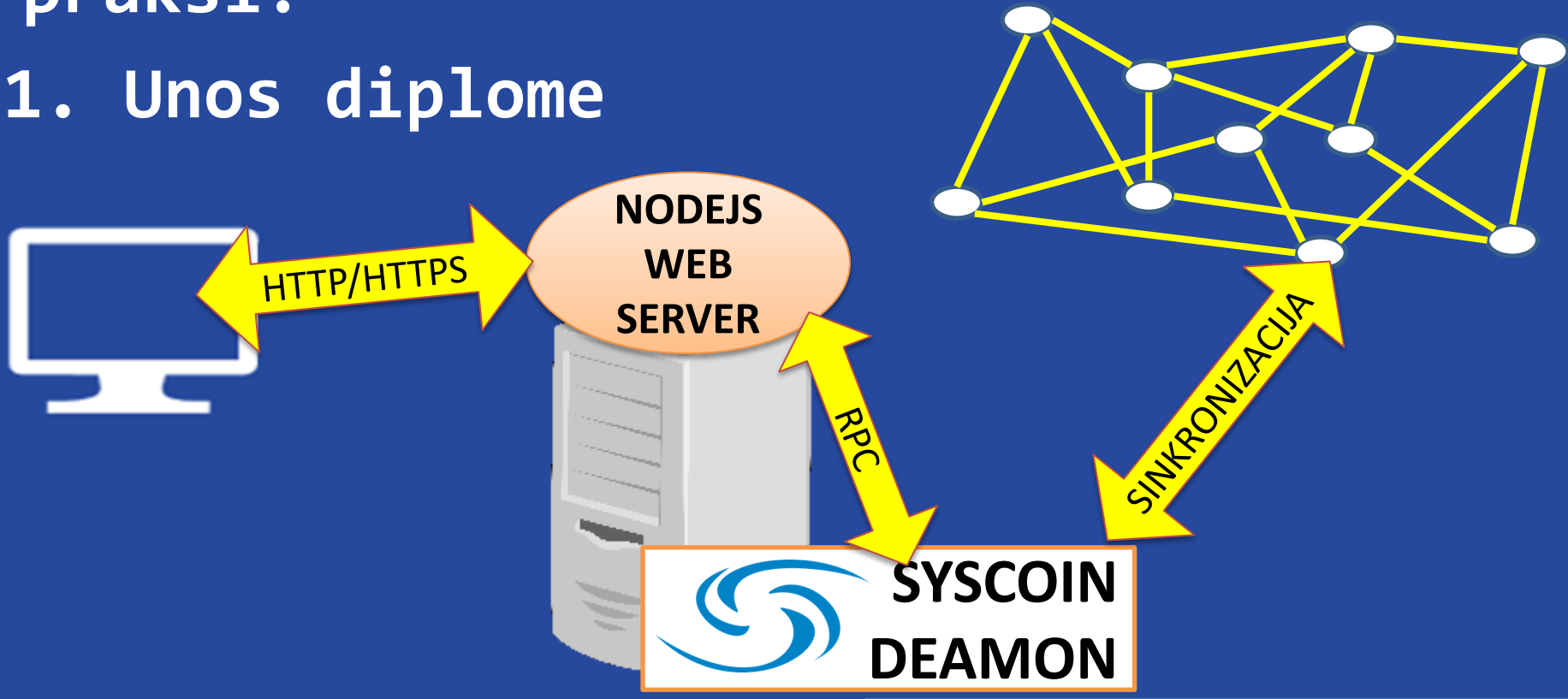
U praksi:

1. Unos diplome
   - nodejs web server komunicira s lokalnim syscoin servisom(syscoin-deamon)
   - syscoin servis služi kao ulazna točka prema syscoin blockchain mreži
   - servis mora imati pridružen wallet sa syscoin tokenim-a za plaćanje upisa transakcija na blockchain

Primjena Syscoin platforme za pohranu diploma

U praksi:

1. Unos diplome



Primjena Syscoin platforme za pohranu diploma

U praksi:

2. Provjera diplome: vub.hr/diploma

Primjena Syscoin platforme za pohranu diploma

U praksi:

2. Provjera diplome: vub.hr/diploma
   - Web stranica šalje upit s GUID-om syscoin servisu instaliranom na udaljenom poslužitelju
   - Poslužitelj dostavlja informaciju o postojanju diplome na blockchain-u
   - Web stranica prezentira informaciju