

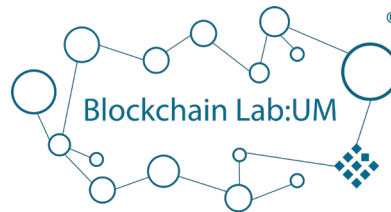


Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



UM LADIES IN
INFORMATICS

SINERGIJA PROTOKOLA IPFS IN TEHNOLOGIJE VERIŽENJA BLOKOV

Aida Kamišalić Latifić, Muhamed Turkanović,
Blaž Podgorelec, Marjan Heričko

TEHNOLOGIJA VERIŽENJA BLOKOV in IPFS

Porazdeljena & decentralizirana omrežja

- **Odpornost proti napadom**
 - Ni ene same točke vdora
- **Odpornost proti dogovarjanju**
 - Ne obstaja določeno število glavnih vozlišč, ki bi se skupaj dogovarjala v svojo korist
- **Odpornost proti napakam**
 - Kljub morebitnim napakam na določenih vozliščih, le te nimajo vpliva na celotno omrežje



Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



UM LADIES IN
INFORMATICS

IPFS (Inter-Planetary File System)

- P2P protokol za varno shranjevanje in deljenje vsebin
- P2P porazdeljen datotečni sistem
 - Uporablja sistem, ki naslavlja vsebino za razliko od sistema, ki temelji na lokaciji HTTP



Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



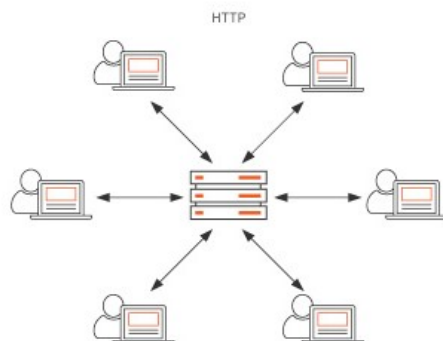
**UM LADIES IN
INFORMATICS**

IPFS (Inter-Planetary File System)

- P2P protokol za varno shranjevanje in deljenje vsebin
- P2P porazdeljen datotečni sistem
 - Uporablja sistem, ki naslavlja vsebino za razliko od sistema, ki temelji na lokaciji HTTP

sistem, ki temelji na lokaciji HTTP

<http://15.20.35.40/folder/file.txt>

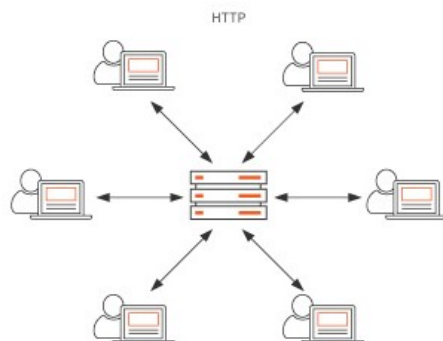


IPFS (Inter-Planetary File System)

- P2P protokol za varno shranjevanje in deljenje vsebin
- P2P porazdeljen datotečni sistem
 - Uporablja sistem, ki naslavlja vsebino za razliko od sistema, ki temelji na lokaciji HTTP

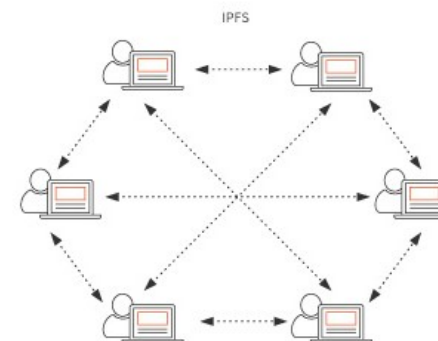
sistem, ki temelji na lokaciji HTTP

<http://15.20.35.40/folder/file.txt>



sistem, ki naslavlja vsebino

<https://ipfs.io/ipfs/QmF5NvKtoM5s/folder/file.txt>





IPFS (Inter-Planetary File System)

- IPFS uporablja zgostitev (hash) vsebine, da naslovi vsebino
- Namesto komunikacije s strežnikom, dobimo dostop do ‚začetne točke‘ podatka
 - Uporaba fizične bližine
- Vsako vozlišče hrani zgolj vsebino, ki ga zanima
- Združuje uspešne ideje obstoječih sistemov P2P (DHTs, BitTorrent, Git, SFS)
 - Porazdeljena zgoščevalna tabela
 - Izmenjava blokov s protokolom BitSwap
 - Sistem za nadzor različic za sledenje vsebini (Merkle DAG)
 - Lastno potrjevanje imenskega prostora



IPFS (Inter-Planetary File System)

PREDNOSTI

- Ni enojne točke vdora (no single point of failure)
- Med vozlišči ni nujno zaupanje
 - Shranjujejo objekte v lokalni shrambi
 - Se povezujejo in prenašajo objekte (datoteke in druge podatkovne strukture)
- Ni omejitve glede velikosti podatkov

SLABOSTI

- Vsebina ni nujno trajno shranjena v omrežju
 - Vozlišča lahko brišejo podatke, da prihranijo na prostoru
 - Potrebna finančna spodbuda za hranjenje velikih količin podatkov
 - FileCoin
- Ni popolne replikacije
 - Počasno pridobivanje vsebin, ki niso zelo iskane

TEHNOLOGIJA VERIŽENJA BLOKOV

- Temelji na naslednjih konceptih:
 - **Kriptografiji**
 - **Porazdeljenem omrežju**
 - **Porazdeljeni podatkovni bazi**
 - **Porazdeljenem soglasju**



Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



**UM LADIES IN
INFORMATICS**



TEHNOLOGIJA VERIŽENJA BLOKOV

PREDNOSTI

- Ni enojne točke vdora (no single point of failure)
 - Varnost in zanesljivost
- Podatki in transakcije so varni, celoviti in zaupanja vredni
 - Nespremenljivost, transparentnost
- Upravljanje porazdeljeno med vozlišča
 - Ni centralne avtoritete
 - Zaupanje med vozlišči vzpostavljeno z algoritmi porazdeljenega soglasja

SLABOSTI

- Skalabilnost
- Omejena velikost podatkov



Sinergija tehnologije veriženja blokov in IPFS

- Rešujemo problem omejene velikosti podatkov, ki jih lahko pri opravljanju transakcije shranimo na verigo blokov
 - Naslovi velike količine podatkov z IPFS
 - Nespremenljive, trajne povezave na IPFS pa pošlje v transakcijo na verigo blokov
 - Označi s časovnim žigom in zavaruje vsebino, čeprav vsebina ni shranjena v verigi

Sinergija tehnologije veriženja blokov in IPFS

Primer EduCTX

- Decentralizirana platforma za upravljanje digitalnih mikro-certifikatov
- Žetoni in transakcije ECTX predstavljajo zaupanja vreden in transparenten dokaz o pridobljenih veščinah in znanjih posameznikov v obliki digitalnih mikro certifikatov



Fakulteta za elektrotehniko,
računalništvo in informatiko

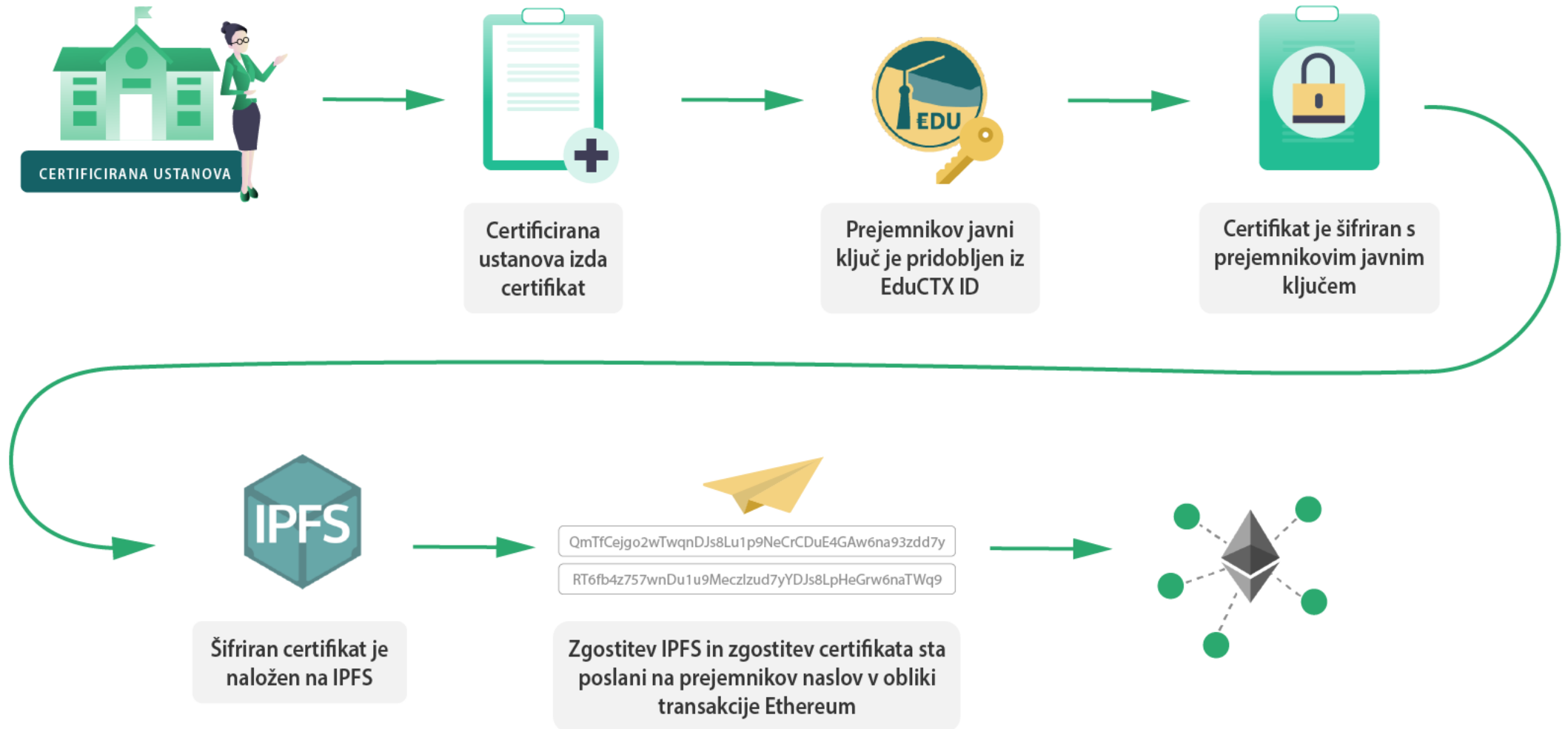


INŠTITUT ZA INFORMATIKO



**UM LADIES IN
INFORMATICS**

Izdaja certifikata



Zaključek

- Uporaba tehnologije veriženja blokov in protokola IPFS
 - Omogoča postavitev omrežja verige blokov tudi za domene in poslovne procese, ki zahtevajo obdelavo večje količine podatkov
 - IPFS omogoča princip shranjevanja izven verige blokov



Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



**UM LADIES IN
INFORMATICS**

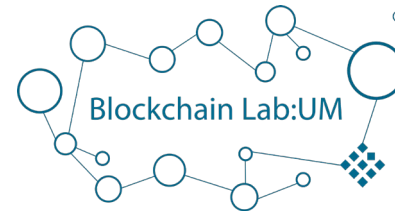


Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko



INŠTITUT ZA INFORMATIKO



UM LADIES IN
INFORMATICS

SINERGIJA PROTOKOLA IPFS IN TEHNOLOGIJE VERIŽENJA BLOKOV

Aida Kamišalić Latifić

aida.kamisalic@um.si