

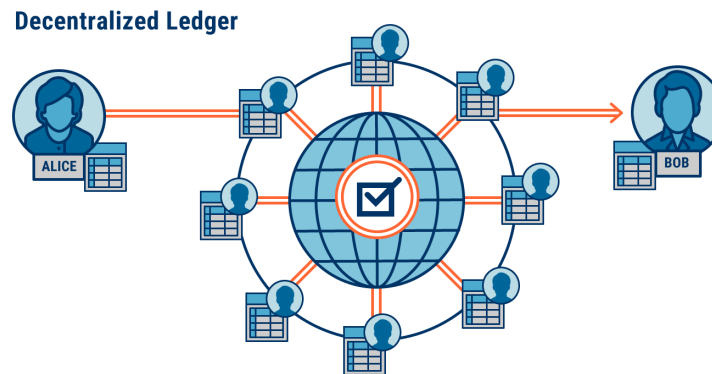


UPORABA TEHNOLOGIJE VERIŽENJA BLOKOV NA PODROČJU ZDRAVSTVA

Marko Hölbl, Marko Kompara, Aida Kamišalić Latifić in Lili Nemec Zlatolas
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko

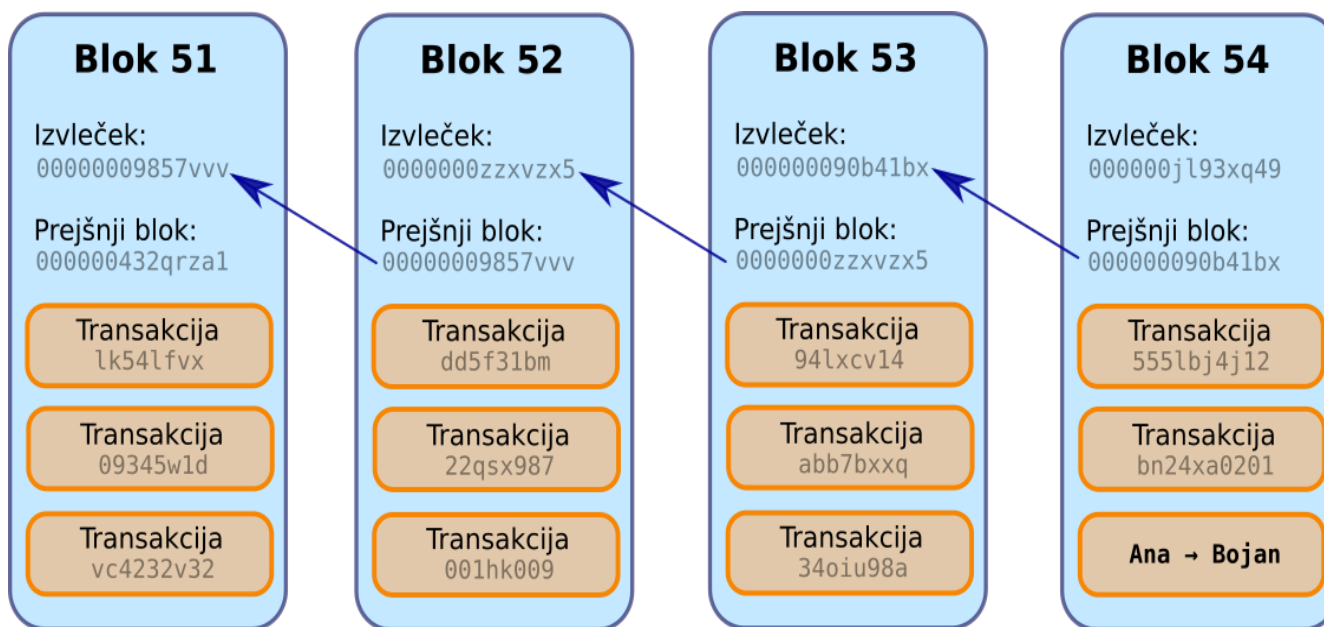
Tehnologija veriženja blokov (TVB) - blockchain

- nov način vzdrževanja dogovorov med deležniki.
- shranjeni dogovori med deležniki ne vodijo centralno
- Vsak deležnik ima natančno enako kopijo dogovora
- Za zaupanje med deležniki in verodostojnost podatkov skrbi **protokol** veriženja tehnologije podatkovnih blokov (mehanizem soglasja)



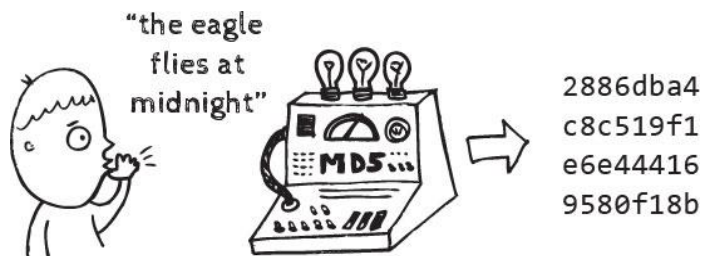
Veriga

- Povezovanje blokov v verigo
 - nespremenljivost



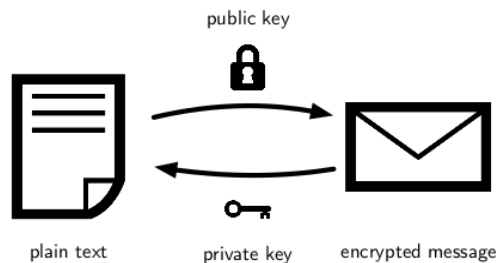
Gradniki, povezani z verigo

- Zgoščevalne funkcije



- kriptografija javnega ključa

– elektronski podpis

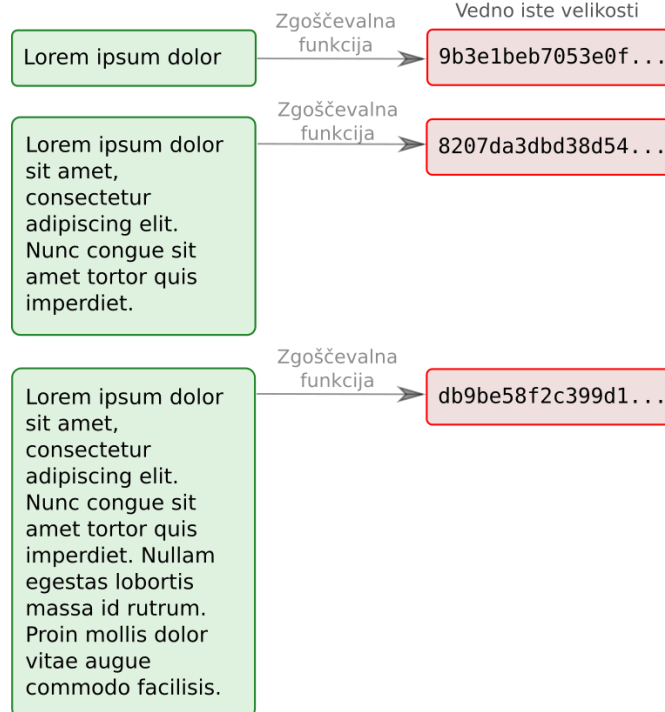


Koncepti in gradniki

Izvorno sporočilo

Izvleček

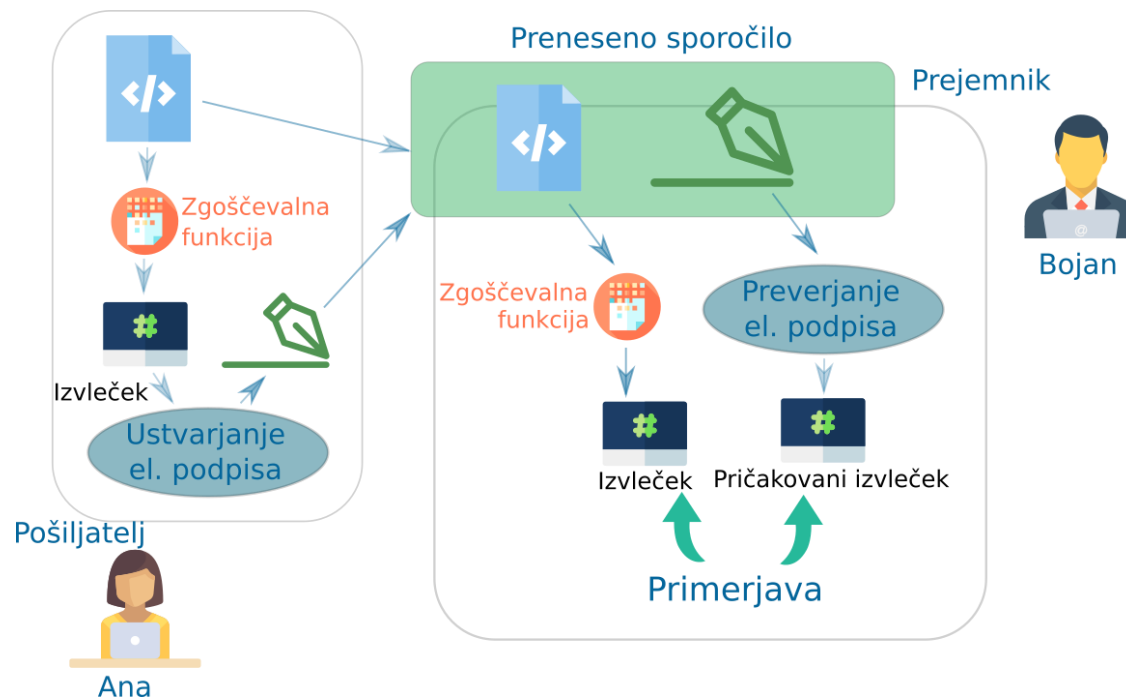
Vedno iste velikosti



- Uporaba pri reševanju uganke

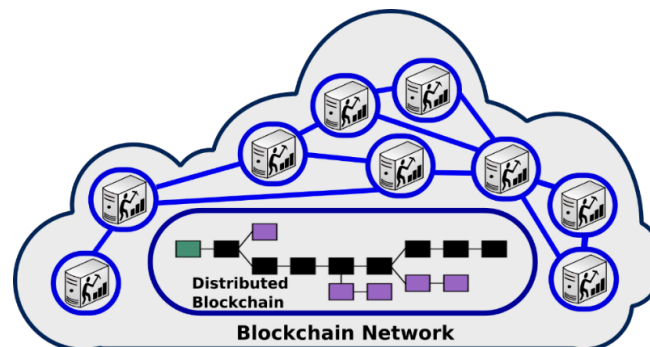
kriptografija javnega ključa in elektronski podpis

- Naslov denarnice -> javni ključ
- Zasebni ključ je kot geslo
 - Različno za vsako transakcijo



Vozlišča

- naloge:
 1. povezovanje v omrežje
 2. shranjevanje trenutne različice glavne knjige
 3. spremljanje transakcij
 4. posredovanje potrjenih transakcij v omrežje
 5. spremljanje in validacija na novo potrjenih blokov – potrjevanje transakcij
 6. ustvarjanje in posredovanje novih (nepotrjenih) blokov



Algoritmi soglasja

- kako se deležniki omrežja poenotijo v porazdeljenem okolju
- V javnih omrežij tehnologije veriženja blokov
 - »dokaz o delu« (ang. Proof of Work – PoW)

PROOF OF WORK



Algoritmi soglasja

- dokaz o vložku (Proof of Stake - PoS)

Differences/implementations



- delegiran dokaz o vložku (Delegated Proof of Stake – DPoS)
- dokaz o avtoriteti (Proof of Authority - PoA)

Tipi TVB

- Tako javna kot poslovna (zasebna in javna) omrežja TVB imajo uporabne aplikacije, podobno kot internet in intraneti organizacij.

JAVNA OMREŽJA BREZ DOVOLJENJ



ZASEBNA OMREŽJA Z DOVOLJENJEM



MOŽNOSTI UPORABE V ZDRAVSTVU

- Trenutna podatkovna infrastruktura v zdravstvu je večinoma odvisna od zaupanja vrednih tretjih strani.
- Medtem ko tehnologija veriženja blokov temelji na soglasju in ne potrebuje TTP-ja.
- Smiselnost uporabe TVB:
 - Uporaba modelov za odločevanje – npr. Würst-Gervaisov odločitveni model



SISTEMATIČEN PREGLED



Podatkovna zbirka	Število rezultatov	Število primernih publikacij
Google Scholar	5500 (200)	53
Web of Science (WoS)	58	36
IEEE Xplore	49	22
PubMed	25	20
Medline EBSCO	30	16
SpringerLink	695 (200)	5
Elsevier ScienceDirect	9	3
MDPI	3	2
ACM Digital Library	6	1
Skupaj	6375 (580)	158

Analiza

	Število publikacij
strukturna zasnova	27
algoritem ali protokol	4
algoritem soglasja	1
nova metrika	1

področje	število publikacij
izmenjava podatkov	20
zdravstvene evidence	18
nadzor dostopa	15
vodenje revizijske sledi	6
oskrbovalna veriga	2
drugo	8



Analiza

		Število publikacij
Platforma	Ethereum	10
	Hyperledger Fabric	5
	Gcoin	1
	Nedefinirano	15
Algoritem soglasja	proof-of-work	7
	proof-of-information	1
	proof-of-interoperability	1
	proof-of-stake	1
	Practical Byzantine Fault Tolerance	1
	QuorumChain	1
	Nedefinirano	21
Uporaba pametnih pogodb	Da	15
	Nedefinirano	18



ethereum



HYPERLEDGER



**HYPERLEDGER
FABRIC**

Ugotovitve

- Večinoma predstavljena strukturna zasnova
 - ogrodje, arhitektura ali model
- večina ne podaja tehničnih podrobnosti
- najbolj priljubljeni platformi Ethereum in Hyperledger fabric
- najpogosteje uporabljen algoritem soglasja je »dokaz od delu«
 - deloma presenetljivo, predvsem zaradi dejstva, da gre za počasen postopek, ki zahteva veliko računalniških virov



Zaključek

- raziskave uporabe TVB v zdravstvu povečujejo
- večinoma uporablja za izmenjavo podatkov, zdravstvene evidence in nadzor dostopa, vendar le redko za druge scenarije, kot je na primer upravljanje oskrbovalne verige
- veliko še neizkoriščenega potenciala





HVALA ZA VAŠO POZORNOST!

VPRAŠANJA/PRIPOMBE/PREDLOGI