Raspodijeljene glavne knjige i kriptovalute

Anonimnost, skalabilnost i regulativa

Stjepan Begušić, Ante Đerek, Zvonko Konstanjčar

11. siječnja 2024.

Ponavljanje: Bitcoin vs Ethereum

S pozicije primjene

- Bitcoin primarno služi kao digitalni novac
  - Plaćanja
  - Prijenos kapitala
- Na Ethereum platformi možemo
  - Kreirati pametne ugovore
  - Kreirati digitalne novčiće (tokeni)

Izazovi u kripto sustavima

Glavni problemi proof-of-work sustava

- Ogromna potrošnja energije
- Rudarenje se svelo na velike bazene – opasnost od centralizacije

Ostali izazovi

- Anonimnost
- Skalabilnost
- Regulativa
- ...

Je li Bitcoin anoniman?

"Bitcoin is a secure and anonymous digital currency" - WikiLeaks donations page

"Bitcoin won't hide you from the NSA's prying eyes" - Wired UK

"Bitcoin Transactions Aren't as Anonymous as Everyone Hoped" - MIT Technology Review

Teška pitanja

- Želimo li kriptovalutu koja je potpuno anonimna?
- Je li anonimna kriptovaluta dobra za društvo?
- Možemo li zadržati samo pozitivne strane anonimnosti?

Osnove anonimnosti

Doslovno: anonimno = bez imena

Dvije interpretacije

- Bez stvarnog imena
- Bez imena uopće

U kojim od sljedećih slučajeva su vaše interakcije anonimne (i po kojoj interpretaciji)?

- Twitter, Reddit, Discord?
- Plaćanje karticama?
- Plaćanje u gotovini?
- Plaćanje Bitcoinom?

Pseudonimnost

Uobičajeno korištenje identiteta koji nije pravo ime nazivamo **pseudonimnost**.

Anonimnost kriptovaluta

Problem

- Kriptovalute zasnovane na lancu blokova su potpuno, javno i trajno sljedive
- Bez anonimnosti, privatnost je bitno manja nego kod tradicionalnih bankarskih sustava
  - Želimo li da svi znaju našu plaću i na što trošimo novce?

Želimo razinu privatnosti kao kod klasičnih bankarskih sustava - ili čak višu!

Etika anonimnosti

Problemi:

- Pranje novaca, kriminalne aktivnosti – u centraliziranim sustavima banke i regulatori mogu zaustaviti transakcije
- Kritična točka – ulaz i izlaz kapitala iz kriptovaluta

Anonimnost u računarstvu

Definicija

Anonimnost = pseudonimnost + nepovezivost.

Korisnik je **anoniman** ako se njegove **različite interakcije** sa sustavom ne mogu **povezati**.

Zašto je važna nepovezivost?

- Lanac blokova je javan - svatko može pratiti svaku adresu
- Ako netko poveže stvarni identitet s adresama - zna sve transakcije te osobe

Povezivanje stvarnog identiteta s adresama je često lagano:

- Mnoge Bitcoin usluge zahtijevaju stvarne identitete (npr. burze)
- Povezani profili mogu se deanonimizirati kroz razne sporedne kanale
  - Plaćanje kriptovalutom na prodajnom mjestu - prodavač može pogledati ostale transakcije povezane s adresom s koje ste platili

Nepovezivost - ključna svojstva

1. Trebalo bi biti teško povezati različite adrese istog korisnika
2. Trebalo bi biti teško povezati različite transakcije istog korisnika
3. Trebalo bi biti teško povezati platitelja i primatelja

Treće svojstvo je teško postići **direktno**.

Ideja: otežati povezivanje platitelja i krajnjeg primatelja.

Kvantificiranje anonimnosti

Potpunu nepovezivost je teško postići

- Između svih transakcija
- Između svih adresa

Definicija

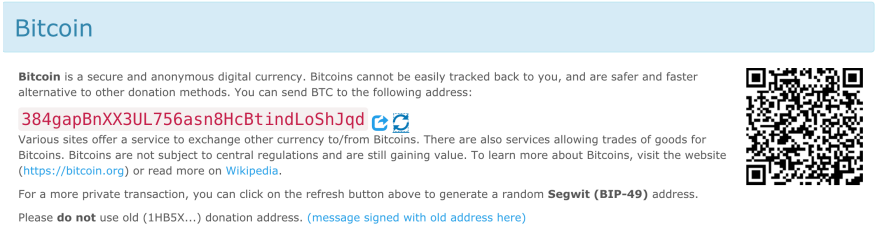
*Za danog napadača, **skup anonimnosti** (engl. anonimity set) određene transakcije je skup transakcija koje napadač ne može razlikovati od te transakcije.*

Za procjenu veličine skupa anonimnosti trebamo

- Definirati model napadača
- Definirati što napadač zna
- Definirati što napadač ne zna/ne može znati

Cilj je **maksimizirati** skup anonimnosti, tj. skup adresa i transakcija između kojih se možemo sakriti.

Generiranje puno različitih adresa



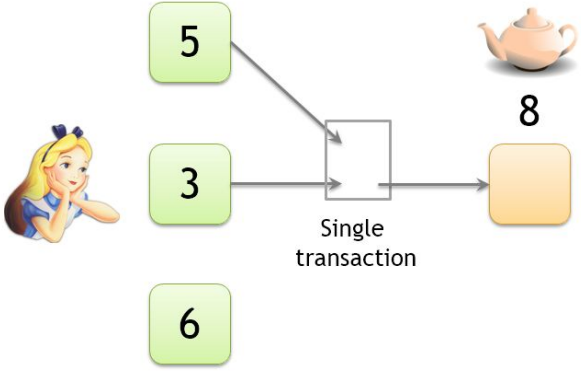
Izvor: `shop.wikileaks.org/donate`

Zadatak

Jesmo li postigli nepovezivost ako primamo Bitocine uvijek na druge adrese?

Moguće je identificirati korisnike i povezati njihove adrese koristeći heuristike za deanonimzaciju lanca blokova – tzv. **analiza grafa transakcija**.

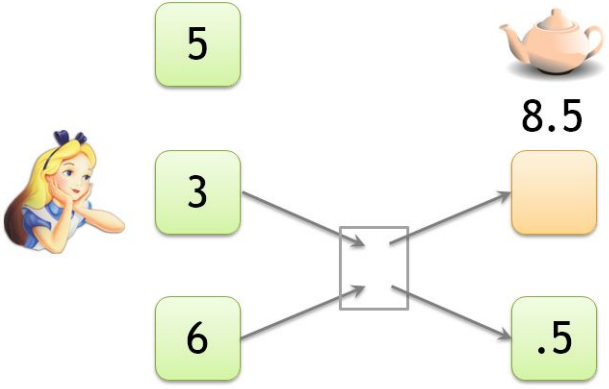
Ana kupuje čajnik



Izvor: `bitcoinbook.cs.princeton.edu`

- Zajedničko trošenje - ista kontrola
- Adrese možemo povezivati tranzitivno

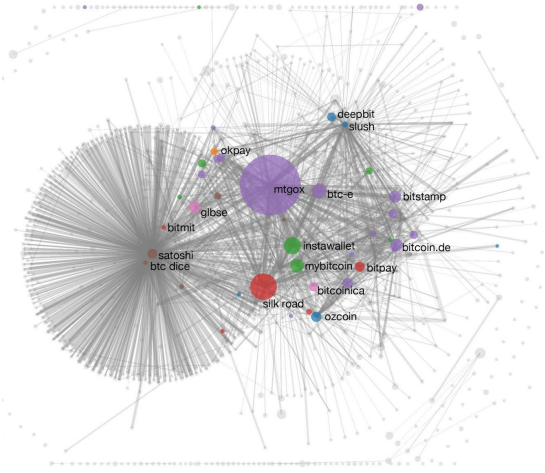
Ana kupuje čajnik - adresa ostatka



Izvor: `bitcoinbook.cs.princeton.edu`

- Adresu ostatka često definiraju novčanici - prilika za razne heuristike
- Jedna heuristika - adrese ostatka su nove

Zajedničko trošenje + heuristike = grupiranje adresa



Izvor: `bitcoinbook.cs.princeton.edu`

S. Meiklejohn, et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, Communications of the ACM, Volume 59, Issue 4, April 2016.

Identifikacija adresa individualaca i organizacija

Adrese organizacija:

- Burze mogu imati poznate adrese za hladnu/toplu pohranu
- Označavanje transakcijom – moguće je u interakciji s prodavateljem ili burzom (transakciji) doznati barem jednu njihovu adresu

Kad su (i kome) poznate adrese individualaca:

- Direktne transakcije interakcija pri prodaji/kupnji – prodavač zna vašu adresu
- Interakcija s burzama ili centraliziranim uslugama
- Individualci znaju odati vlastite adrese iz nemara!

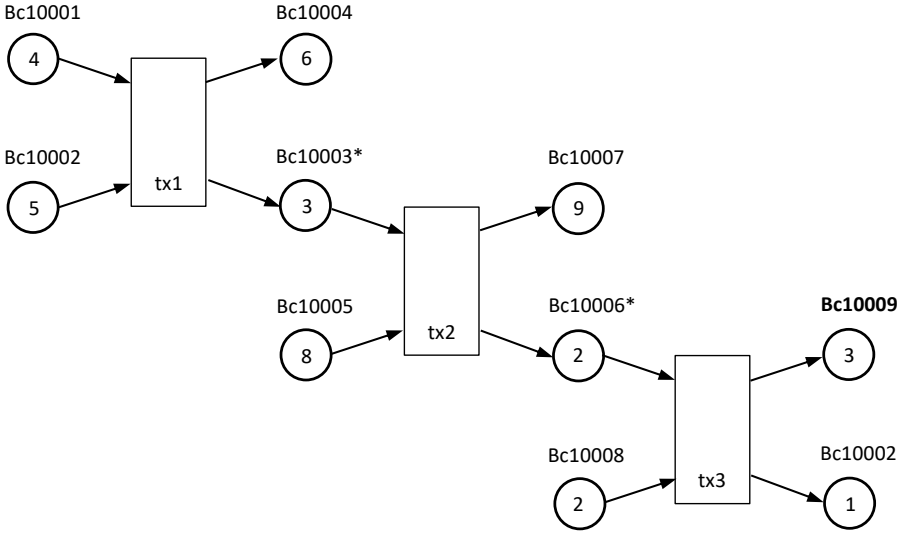
Heuristike za deanonimizaciju – primjer

Razmotrimo sljedeće transakcije. U transakciji 3 ste primili 3 BTC na adresu ***bc10009*** (prodajete biljke na internetu). Novonastale adrese označene su zvjezdicom*.

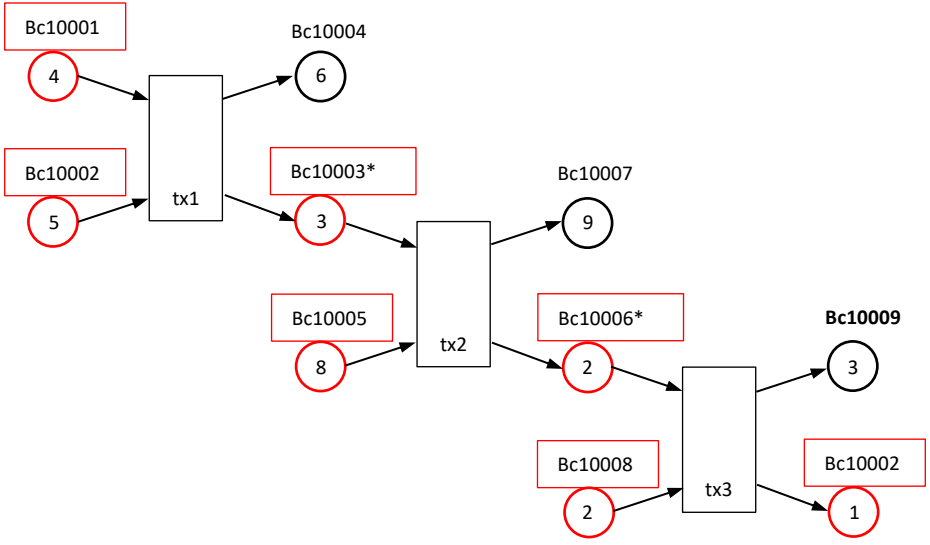
- Koje sve adrese kupca možete identificirati?
- Zbog koje greške kupca možete biti dodatno sigurni u svoju analizu?

ID	Input adrese (i iznosi)	Output adrese (i iznosi)
1	*bc10001* (4 BTC), *bc10002* (5 BTC)	*bc10003** (3 BTC), *bc10004* (6 BTC)
2	*bc10003* (3 BTC), *bc10005* (8 BTC)	*bc10006** (2 BTC), *bc10007* (9 BTC)
3	*bc10006* (2 BTC), *bc10008* (2 BTC)	***bc10009*** (3 BTC), *bc10002* (1 BTC)

Heuristike za deanonimizaciju – primjer

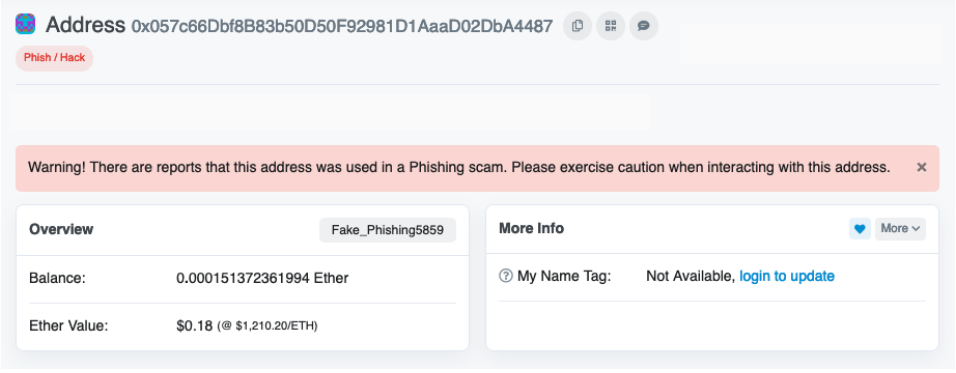


Heuristike za deanonimizaciju – primjer



Identifikacija adresa u slučaju prevara

- Adrese koje su korištene u napadima i prevarama mogu se označiti kako bi se pratio tok sredstava i onemogućile buduće prevare
- U nekim slučajevima burze mogu zamrznuti sredstva



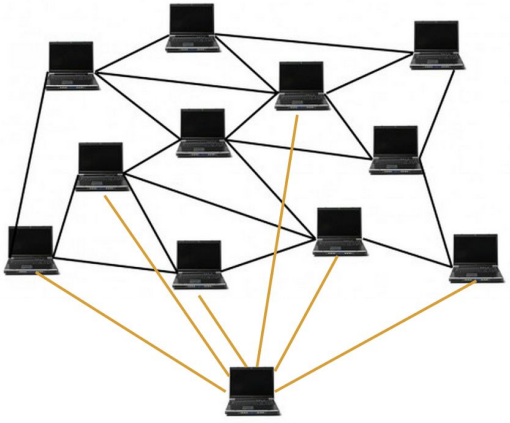
Izvor: `etherscan.io`

Identifikacija adresa u slučaju prevara

Txn Hash	Method ⓘ	Block	Age	From		To	Value	Txn Fee
0x6d07740f862bbc650e…	Transfer	15038098	175 days 5 hrs ago	Fake_Phishing5859	OUT	KuCoin 10	10.78710825 Ether	0.00071825
0x1d0e20df65df320305c…	Transfer	15035908	175 days 15 hrs ago	0x2441c77af3727dc7e9…	IN	Fake_Phishing5859	0.020481 Ether	0.001281
0x1b3a99ec3400646866…	Transfer	15034889	175 days 20 hrs ago	0x33e2d9bd0e1ce98113…	IN	Fake_Phishing5859	10.76725614 Ether	0.00103905
0xdf66718edcef7c9012c…	Transfer	15030220	176 days 17 hrs ago	Fake_Phishing5859	OUT	KuCoin 10	99.66612182 Ether	0.00116922
0x2e695bb42a325bdb21…	Transfer	15030084	176 days 17 hrs ago	0xfc99d4821e67e4e767…	IN	Fake_Phishing5859	48.9165 Ether	0.00178094
0x3c0f5c1cfdd26077fb76…	Transfer	15029914	176 days 18 hrs ago	0xfc99d4821e67e4e767…	IN	Fake_Phishing5859	50.75034434 Ether	0.00098213
0x1109984da7a16411bb…	Transfer	15026047	177 days 12 hrs ago	Fake_Phishing5859	OUT	KuCoin 10	0.21478315 Ether	0.00165973
0x15fe7432621d194612…	Transfer	15025375	177 days 15 hrs ago	0x1c727a55ea3c11b0ab…	IN	Fake_Phishing5859	0.103979 Ether	0.00161896
0x05cc03240bc9c5369c…	Transfer	15025055	177 days 16 hrs ago	Gemini	IN	Fake_Phishing5859	0.095459 Ether	0.0011603
0x44cf38c1877bb76fabd…	Transfer	15024619	177 days 18 hrs ago	Coinbase 4	IN	Fake_Phishing5859	0.01760571 Ether	0.00067684
0xad8fcf7b0a20c3dc0b5…	Transfer	15020717	178 days 12 hrs ago	Fake_Phishing5859	OUT	KuCoin 10	54.54825322 Ether	0.00053827
0x8f6ccf4d3e9ca8cd260…	Transfer	15020187	178 days 14 hrs ago	0x31264ca6ee7b3ab6d9…	IN	Fake_Phishing5859	16 Ether	0.0008862
0x06ab7cfa7cb1b95b25…	Transfer	15020065	178 days 14 hrs ago	0x31264ca6ee7b3ab6d9…	IN	Fake_Phishing5859	8 Ether	0.001029
0xc64e172b0f943154cb…	Transfer	15019974	178 days 15 hrs ago	0x31264ca6ee7b3ab6d9…	IN	Fake_Phishing5859	5 Ether	0.0009366
0x6f46d9e2476e65afc3f…	Transfer	15019921	178 days 15 hrs ago	0x31264ca6ee7b3ab6d9…	IN	Fake_Phishing5859	17.480198 Ether	0.0010794

Izvor: `etherscan.io`

Deanonimizacija na mrežnom sloju

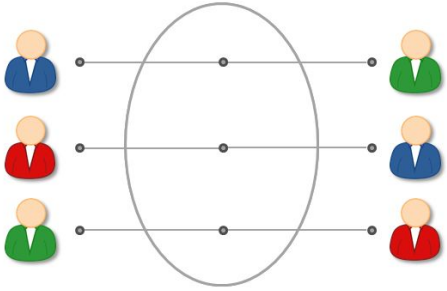


Izvor: bitcoinbook.cs.princeton.edu

Čvor u mreži koji stvara transakciju poslat će je svim svojim susjedima – čvor koji je prvi poslao transakciju vjerojatno ju je i stvorio.

Kako povećati anonimnost?

Direktno povezano s povećanjem nepovezivosti, tj. s otežanjem analize grafa transakcija.



Izvor: `bitcoinbook.cs.princeton.edu`

Jedno rješenje - tehnika koju nazivamo **miješanje**.

Intuicija: **uvođenje posrednika** povećava nepovezivost.

Online novčanici i burze

- Pružaju usluge spremanja kriptovaluta online (između ostalog)
- Novčići koje povlačimo nisu nužno isti oni koje smo pohranili
- Prednosti:
  - Donekle povećavaju nepovezivost i otežavaju analizu grafa transakcija
- Nedostatci:
  - Ne garantiraju da će miješati sredstva korisnika
  - I da miješaju, kod sebe drže zapise o tome
  - Regulirani novčanici i burze traže identitete osoba s kojima surađuju

Zadatak

Koliki je skup anonimnosti ukoliko je napadač netko izvan burze? Što ako je kompromitirana sama burza?

Očigledno je **anonimnost slična** (vjerojatno manja) kao kod **tradicionalnih banaka**. **Je li nam to dovoljno**?

Usluge specijalizirane za miješanje

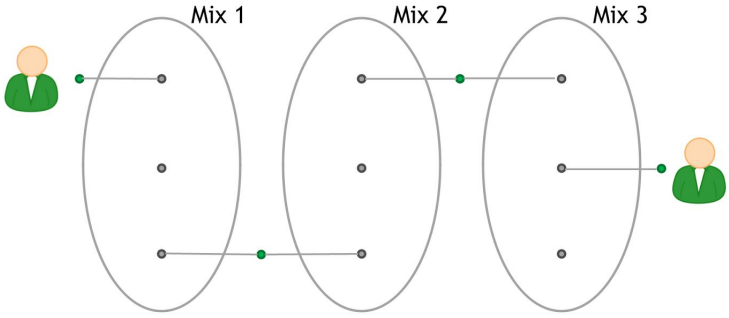
Svojstva

- Garantirano ne čuvaju zapise
- Ne traže identitet (niti username)
- Korisnik šalje Bitcoine i ciljanu adresu na adresu koju dobije od davatelja usluge miješanja
- Problematično **povjerenje u uslugu miješanja** - što ako ne rade što bi trebali?

Zadatak

Kako bi dodatno povećali anonimnost?

Usluge specijalizirane za miješanje - naprednija rješenja



Izvor: `bitcoinbook.cs.princeton.edu`

Svojstva

- Korištenje niza usluga miješanja
- Uniformne transakcije – potrebno dogovoriti adekvatni iznos

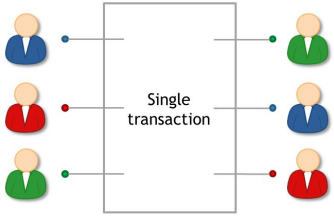
IDEJA: **Zamijeniti uslugu miješanja** s peer-to-peer **protokolom** pomoću kojeg grupa ljudi može miješati svoje novčiće.

Prednosti

- Korisnici ne moraju čekati davatelja usluge miješanja s adekvatnom reputacijom
- Krađa nije moguća u raspodijeljenom miješanju (osigurava protokol)
- Na neki način osigurava bolju anonimnost

Raspodijeljeno miješanje - združeni novčić (*engl. coinjoin*)

IDEJA: U ovom protokolu različiti korisnici stvaraju zajedničku transakciju koja kombinira sve njihove ulaze.



Izvor: `bitcoinbook.cs.princeton.edu`

Protokol - idejno rješenje

- Svaki korisnik zasebno dostavlja ulazne i izlazne adrese
- Poredak ulaznih i izlaznih adresa u tx se slučajno izmiješa
- Kada korisnici vide da je sve s njihovim iznosima i adresama u redu, potpisuju transakciju

Raspodijeljeno miješanje - Tornado cash (Ethereum)

- Tornado Cash – pametni ugovor i decentralizirana organizacija na Ethereum lancu (i nekim drugima), koristi kriptografiju za decentralizirano miješanje
- Sudjelovao u miješanju preko 7 mlrd. USD vrijednosti ETH-a
- Kolovoz 2022. - Ured za kontrolu strane imovine (OFAC) ministarstva financija SAD-a proglasio ilegalnim korištenje Tornado Cash-a
  - Svi građani SAD-a koji su na svoje adrese primili ETH koji je u prethodnim transakcijama došao iz Tornado Casha moraju to prijaviti


U.S. DEPARTMENT OF THE TREASURY

HOME › NEWS › PRESS RELEASES

PRESS RELEASES

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

August 8, 2022

Izvor: treasury.gov.

Anonimnost - pregled rješenja

System	Type	Anonymity attacks	Deployability
Bitcoin	pseudonymous	transaction graph analysis	default
Manual mixing	mix	transaction graph analysis, bad mixes/peers	usable today
Chain of mixes or coinjoins	mix	side channels, bad mixes/peers	bitcoin-compatible
Zerocoin	cryptographic mix	side channels (possibly)	altcoin, trusted setup
Zerocash	untraceable	none known	altcoin, trusted setup

Izvor: `bitcoinbook.cs.princeton.edu`

Skalabilnost

Problemi

- Transakcije nisu trenutne
- Mikroplaćanja ne funkcioniraju - visoki transakcijski troškovi
- S porastom korisnika, funkcionalnost sve lošija

Transakcije u sekundi

- Bitcoin obrađuje oko 7 transakcija u sekundi (uz veličinu bloka 1MB i 250 bytes/tx)
- Trebalo bi biti dovoljno za čitav svijet?
- Visa obrađuje oko 2.000 transakcija u sekundi (max preko 40.000 tps)
- Uz 7 milijardi ljudi i prosječno 2 transakcije na mjesec, veličina bloka bi trebala biti 0.8 GB (5.400 tps)

Izvor: https://en.bitcoin.it/wiki/Scalability

Problem povećanja veličine blokova

- Skupo validirati - malo punih čvorova
- Za veličinu blokova 1GB - za validaciju potrebni resursi na razini data centra - barijera za male čvorove
- Propagacija postaje problematična
- Stalna debata o tome kolika bi veličina blokova trebala biti

"Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient." - Hal Finney, Dec 2010.

Layer 2 rješenja i protokoli – ideja

- Izuzeti male transakcije iz lanca blokova (izvan lanca, engl. off chain)
- Slično na burzama - transakcije bez izmjene na lancu blokova
- Najznačajniji *layer 2* protokol za Bitcoin – Lightning Network

Primjer

- Ana ide na ručak redovito u Cassandru
- Neefikasno je koristiti lanac blokova za male transakcije
- Rješenje je uspostava multisig adrese dijeljene između Ane i Cassandre
- Multisig adresa je kao sef koji se može otvoriti samo ako se obje strane slože - "kanal plaćanja" (engl. "payment channel").

Stvaranje, održavanje i zatvaranje kanala plaćanja

1. Stvaranje kanala između Ane i Branka:
   - Ana "zaključava" sredstva (npr. 10 BTC) u 2-od-2 multisig adresu (*funding transaction*) – **objavljuje se na lancu**
   - Branko odmah pošalje Ani potpisanu transakciju u kojoj se sva sredstva (10 BTC) vraćaju Ani
2. Promjena stanja kanala: npr. Ana šalje Branku 2 BTC
   - Šalje mu potpisanu transakciju (*commitment transaction*) u kojoj se sredstva troše po novom stanju (Ani 8 BTC, Branku 2 BTC)
   - Sva iduća plaćanja u kanalu uključuju slanje potpisane *commitment* transakcije s novim stanjem
3. Kanal se zatvara kad bilo tko od strana zadnju potpisanu *commitment* transakciju (c.t.) objavi na lancu blokova

Zadatak

Koji je potencijalni problem s ovakvim dizajnom kanala plaćanja?

Primjer: zašto Ana ne bi jednostavno objavila prvotnu c.t. u kojoj uzima svih 10 BTC?

- Potrebno je stare c.t. na neki način opozvati ili poništiti – to nije moguće!

Mehanizam kažnjavanja pokušaja objave starih c.t.:

- Načelo: svaka nova c.t. sadrži informacije koje omogućavaju drugoj strani da potroši sva sredstva iz outputa prethodne c.t.
- Na taj način svaka nova c.t. čini prethodnu neupotrebljivom ("poništava" je)

Lightning Network - usmjeravanje preko kanala plaćanja (*routing*)

Što ako Ana želi platiti Cassandri a ne postoji direktni kanal plaćanja između njih?

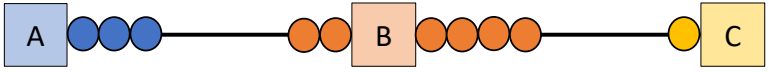
Usmjeravanje u LN (*routing*)

Ako postoji kanal između A i B, te kanal između B i C - moguće je preko ta dva kanala usmjeriti plaćanje između A i C.

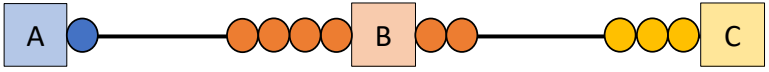
Primjer:

- Ana želi platiti Cassandri 2 BTC. Postoje kanali:
  - Kanal između Ane i Branka (stanje: Ana 3 BTC, Branko 2 BTC)
  - Kanal između Branka i Cassandre (stanje: Branko 4 BTC, Cassandra 1 BTC)
- Dvije LN transakcije:
  1. Ana šalje Branku 2 BTC
  2. Branko šalje Cassandri 2 BTC
- Mreža može pronaći najjednostavniji put kroz kanale plaćanja za obradu dane transakcije

Lightning Network - usmjeravanje preko kanala plaćanja (*routing*)



Stanje kanala plaćanja u početku.



Stanje kanala plaćanja nakon što A pošalje C iznos od 2 BTC.

Lightning Network

Lightning network je **protokol za plaćanje** koji funkcionira na aplikacijskom sloju (*layer 2*) koji se nalazi iznad lanca blokova.

Posljedice

- Velika brzina transakcija
- Niske naknade
- Moguće koristiti za mikro plaćanja

- Lightning Network je krenuo u produkciju 2018. godine
- 2021. godine El Salvador uvodi BTC kao službenu državnu valutu, a novčanik podržava Lightning Network mikrotransakcije
- Tehnologija još uvijek u razvoju – trenutno postoji preko 15.000 LN čvorova s ukupno preko 5.000 BTC zaključano u kanalima
- Slična L2 rješenja dostupna i za Ethereum blockchain

Upravljanje – tko su dionici?

Core developeri

- Definiraju pravila
- Svi koriste njihov kod

Rudari

- Određuju koje transakcije su ispravne
- Grade povijest

Investitori, trgovci i korisnici

- Generiraju potražnju
- Određuju vrijednost valute

Za uspjeh kriptovalute - tri vrste konsenzusa

Konsenzus oko pravila

- Dogovor oko protokola i formata
- Što definira ispravnost transakcija, blokova

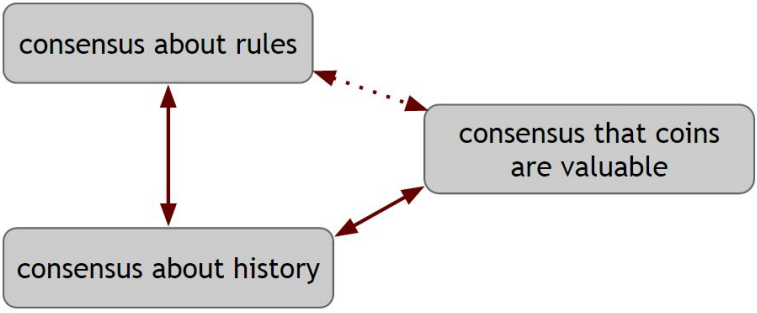
Konsenzus oko povijesti

- Dogovor oko sadržaja lanca blokova
- Koji novčići postoje i tko su njihovi vlasnici

Konsenzus oko vrijednosti

- Dogovor da novčići imaju vrijednost
- Cijena određena trgovanjem

Za uspjeh kriptovalute - tri vrste konsenzusa



Izvor: bitcoinbook.cs.princeton.edu

Regulativa – motivacija

Kontrola kapitala

- Iznošenje kapitala izvan države - postoje pravila i zakoni
- Trud usmjeren na odsijecanje (reguliranje) fiat valuta od kripto valuta

Kriminal

- Kriptovalute potencijalno olakšavaju neke vrste kriminala, npr. plaćanje otmičarima, trgovina drogom itd.
- Nastaju i novi oblici prevara i kriminala

Pranje novca

- Općeniti cilj: kontrolirati tokove novca i spriječiti prelijevanje velike količine novca između legalnog dijela gospodarstva i ilegalnih aktivnosti

Regulativa – AML i KYC

Anti-money laundering (AML)

- Novac zarađen od kriminalnih aktivnosti (uglavnom organizirani kriminal) ne smije se moći lako pretočiti u legalni dio gospodarstva
- U sklopu AML procedura traže se informacije o klijentu, porijeklu imovine...

Know your customer (KYC)

- Identifikacija i autentifikacija klijenata
- Procjena rizika klijenta (rizik od toga da je klijent uključen u kriminalne aktivnosti)
- Praćenje aktivnosti klijenta u potrazi za anomalijama u ponašanju

Burze kriptovaluta koje posluju s fiat valutama danas u velikoj većini imaju stroge KYC procedure.