Sigurnosne prijetnje na Internetu

Kriptovalute

Matija Jelavić, 6.11.2024.

Pregled predavanja

- Komunikacija *blockchain* sustava i vanjskog svijeta
- Osnovno o *blockchainu*
- Bitcoin
- Zcash
- Monero

Pitanja za ispite

- Navedite barem dvije karakteristike decentraliziranih mjenjačnica (DEX).
- Zbog čega je Bitcoin najkorištenija kriptovaluta za kriminal?
- Od koja dva dijela se sastoji Zcash te koji funkcionira gotovo jednako kao i Bitcoin?
- Na koji način su skriveni primatelj i iznos u Moneru i Zcashu?
- Kako se zove dokaz kojime se dokazuje povjerenje bez otkrivanja gotovo nikakvih informacija?

Motivacija

- Američke policijske snage godišnje plaćaju milijune dolara firmama koje provode razne metode za deanonimizaciju transakcija kriptovalutama
- Također, bitna je informiranost o anonimnosti i oprez prilikom osobnog korištenja kriptovaluta

Uvod

- Koncept predavanja će biti upoznavanje s određenim pojmom te odmah nakon toga potencijalni načini narušavanja anonimnosti istoga
- U kontekstu anonimnosti *blockchaina,* napad je bilo koji pokušaj stjecanja dodatnog znanja o transakciji

Komunikacija *blockchain* sustava i vanjskog svijeta (1)

- Centralizirane mjenjačnice (CEX)
  - Mora se otkriti identitet kako bi se kupile kriptovalute
- Decentralizirane mjenjačnice (DEX)
  - Ne otkriva se identitet
  - Ne postoji posrednik kod kupovine
  - Mehanizmi protiv varanja
  - Banka vidi samo transakciju na drugi račun, ne vidi da se radi o kupovini kriptovaluta

Komunikacija *blockchain* sustava i vanjskog svijeta (2)

- Direktan prijenos
  - Umjesto kupovine, netko prebaci kriptovalute na adresu primatelja
- Bankomati
  - Unos gotovine ili unos kartice
  - Video nadzor

Osnovno o blockchainu

- Baza podataka pohranjena na svakom pojedinom čvoru P2P mreže (bez dopuštenja) umjesto na jednom centraliziranom poslužitelju
- Najkorišteniji je za prijenos sredstava bez centraliziranog autoriteta

Bez dopuštenja (*engl.* permissionless) označava da se svatko može pridružiti i sudjelovati u toj P2P mreži.

Koraci izvršavanja transakcije

- Stvaranje – definiranje pošiljatelja, primatelja, količine resursa i dodatnih podataka
- Potpisivanje – korištenje privatnog ključa za generiranje digitalnog potpisa
- Distribucija - slanje čvorovima u mreži kako bi transakcija bila dodana u *blockchain*

Napad kada se ne koristi posrednik

- Žrtva uključi vlastiti čvor u *blockchain* mrežu kako bi distribuirala transakciju
- Napadač svoj čvor povezuje s velikim brojem drugih čvorova te prati od kojeg čvora je prvog primio transakciju žrtve
- IP adresa tog čvora je IP adresa žrtve
- Napad ne uspijeva ako se transakcija distribuira koristeći posrednika ili Tor mrežu

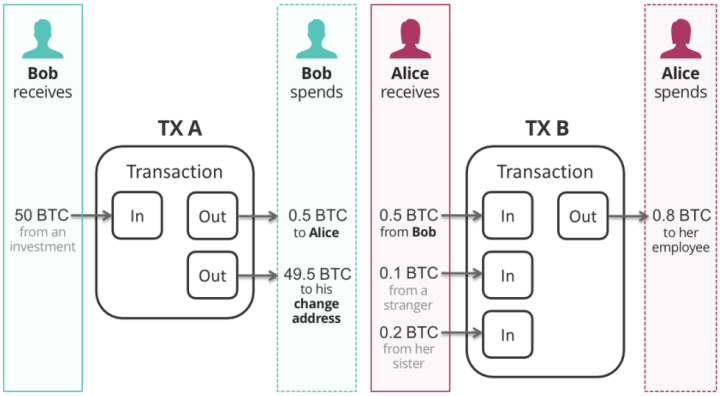
Bitcoin i kriminal

- Najkorištenija kriptovaluta za kriminal
  - Dostupan u velikom broju mjenjačnica
  - Velik broj korisnika i transakcija pa se smatra da se ilegalne transakcije "izgube u masi"
- Najčešća upotreba u slučaju *ransomware*a

Bitcoin (1)

- Ne postoji koncept jedinstvenog pošiljatelja, nego se referencira transakcija odakle su dobiveni resursi - stječe se dojam anonimnosti
- Ako se ne žele potrošiti svi resursi iz određene transakcije, višak se uplaćuje nazad pošiljatelju

Bitcoin (2)



Izvor: https://thecoinrise.com/how-do-bitcoin-transactions-work/

13/25

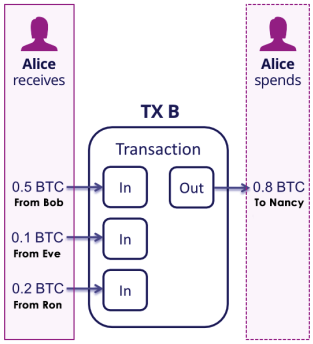
Na primjeru TX A, možemo vidjeti da kao ulaz prima 50 bitcoina, a kao izlaz 0.5 bitcoina ide Alice te 49.5 bitcoina viška se vraća nazad Bobu *(change address).* Iako adresa viška (adresa na koju ide 49.5 bitcoina) može biti različita od adrese s koje je poslano 50 bitcoina, obje su u vlasništvu Boba te ćemo kasnije u predavanju vidjeti da se one mogu grupirati kako bi se narušila anonimnost.

Napad adrese viška

- Ako se adresa u izlazu prvi puta pojavljuje smatra se da je to adresa viška i grupira se zajedno s adresom pošiljatelja
- Točnije, obje pripadaju istom entitetu

Napad grupiranja adresa

- Svi ulazi su pod kontrolom istog entiteta
- Ulazi se grupiraju te se dovode u povezanost s jednim entitetom

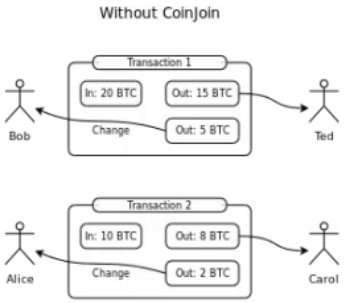


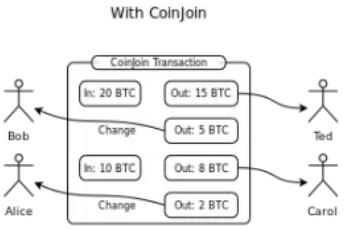
Izvor:
https://blog.areabitcoin.co/bitcoin

Kao što je rečeno na jednom od prethodnih slajdova, u Bitcoinu ne postoji koncept jedinstvenog računa s kojeg se šalju resursi, nego se referenciraju prethodne transakcije na kojima su se dobili određeni resursi. Tako u ovom primjeru, Alice kao ulaz predaje jednu adresu (adresu transakcije) gdje je dobila 0.5 bitcoina od Boba, zatim drugu adresu gdje je dobila 0.1 bitcoina od Eve i treću adresu gdje je dobila 0.2 bitcoina od Rona. Sve tri adrese su različite, ali sve tri pripadaju Alice te se tako i mogu grupirati.

CoinJoin

- Anonimizacijska metoda za Bitcoin
- Grupiranje više transakcija u jednu
- Ne prepoznaje se razlika od klasičnih transakcija





Izvor:
https://www.mycryptopedia.com/coinjoin-explained/

Na slici je vidljivo da se u jednu CoinJoin transakciju grupira više ulaza i više izlaza različitih transakcija što dovodi do toga da nije moguće sa sigurnošću utvrditi da je, u ovom slučaju, Bob poslao transakciju Tedu ili Alice prema Carol. Uz to, tu su još i adrese viška koje se ne razlikuju od ostalih adresa.

Zcash

- Resursi su dio zaštićenog ili nezaštićenog bazena
- Nezaštićeni bazen funkcionira jednako kao Bitcoin - podložan jednakim napadima

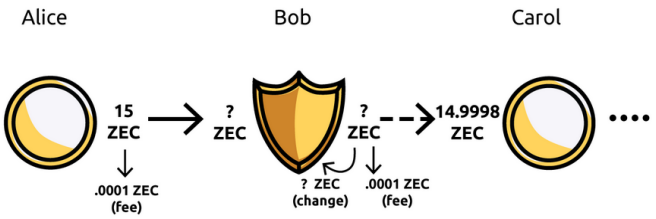
Zcash - zaštićeni bazen

- Skriva pošiljatelja, primatelja i iznos
- Kao ulaz se predaju sve adrese ikada nastale u zaštićenom bazenu
- Primatelj i iznos šifrirani javnim ključem primatelja

U Zcashu, pošiljatelj je skriven na način da se kao ulaz stave sve adrese ikada nastale u zaštićenom bazenu. Pošiljatelj sakrije adresu primatelja i iznos tako što ih šifrira javnim ključem primatelja što znači da ih može pročitati samo onaj koji ima privatni ključ. *Zero knowledge* dokaz se koristi za dokazivanje da transakcija pripada primatelju i da resurs nije potrošen što je spomenuto kasnije u predavanju.

Napad ulaza i izlaza

- Ako se dogodi transakcija iz nezaštićenog u zaštićeni bazen te potom iz zaštićenog u nezaštićeni s jednakim iznosom, smatra se da su transakcije povezane



Na slici Alice prebacuje 15 ZEC-a u zaštićeni bazen do Boba. Zatim, Bob iz zaštićenog bazena prebacuje 15 ZEC-a do Carol. Ako se ove dvije transakcije dogode u određenom vremenskom intervalu, smatra se da su transakcije od Alice prema Bobu i od Boba prema Carol na neki način povezane.

Monero

- Sustav sličan zaštićenom bazenu u Zcashu, ne postoji "nezaštićeni dio"
- Što znači da su skriveni pošiljatelj, primatelj i iznos

U Moneru, pošiljatelj je skriven na način da se kao ulaz predaju razne *dummy* adrese prema gama razdiobi. Pošiljatelj sakrije adresu primatelja i iznos tako što ih šifrira javnim ključem primatelja što znači da ih može pročitati samo onaj koji ima privatni ključ. *Zero knowledge* dokaz se koristi za dokazivanje da transakcija pripada primatelju i da resurs nije potrošen što je spomenuto kasnije u predavanju.

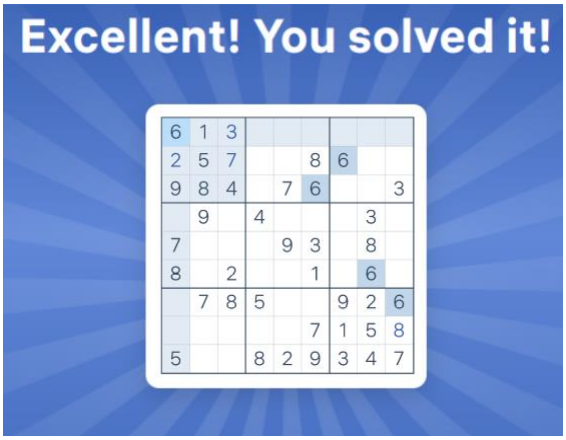
Zero knowledge dokaz (1)

- Tko misli da znam riješiti zagonetku?

6	1	3						
2	5	7			8	6		
9	8	4		7	6			3
	9		4				3	
7				9	3		8	
8		2			1		6	
	7	8	5			9	2	6
					7	1	5	8
5			8	2	9	3	4	7

Zero knowledge dokaz (2)

- A sada?



Iz ovog primjera se daje prikaz rada *zero knowledge* dokaza na vrlo visokoj razini apstrakcije. Bez pokazivanja pravila rješavanja Sudoku zagonetki ili evenutalnog pokazivanja cijelog ili djelomičnog rješenja sam dokazao da ipak znam riješiti zagonetku s prethodnog slajda te da mi se može vjerovati. U stvarnoj primjeni, *zero knowledge* dokazi funkcioniraju na kompleksnim principima matematike i kriptografije.

Zaključak

- Nije nimalo jednostavno narušiti anonimnost unutar *blockchain* sustava
- Svi opisani napadi su samo pokušaji stjecanja dodatnog znanja, ali gotovo nijedan ne pruža skroz pouzdane podatke
- Veća vjerojatnost identifikacije kriminalaca kroz komunikaciju *blockchain*a s vanjskim svijetom

Literatura

- Deuber, Dominic, Viktoria Ronge, and Christian Rückert. "Sok: Assumptions underlying cryptocurrency deanonymizations." Proceedings on Privacy Enhancing Technologies 3 (2022): 670-691.
- Silfversten, Erik, et al. Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. Santa Monica, CA, USA: RAND, 2020.
- Internet Organised Crime Threat Assessment (IOCTA), 2024. URL https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024, pristupio: 22.10.2024.
- How Does a Blockchain Transaction Work?, 2022. URL https://www.ledger.com/academy/how-does-a-blockchain-transaction-work, pristupio: 22.10.2024.
- CoinJoin Explained, 2019. URL https://www.mycryptopedia.com/coinjoin-explained/, pristupio: 22.10.2024.
- Gomez, Gibran, Kevin van Liebergen, and Juan Caballero. "Cybercrime bitcoin revenue estimations: Quantifying the impact of methodology and coverage." Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023.

Dodatna literatura

- Petkus, Maksym. "Why and how zk-snark works." *arXiv preprint arXiv:1906.07221* (2019).
- Kaloudis, George. "A Deep Dive Into Lightning as a Bitcoin Scaling Solution" (2021).

Hvala!