IZBORNI PROJEKT

Usporedba hash algoritama u kriptovalutama

Petra Avsec

Algoritmi i strukture podataka
Zavod za računarstvo
prof. Kristijan Lenac
Tehnički fakultet Sveučilišta u Rijeci
Kolovoz 2020.

Sadržaj

1 Kriptovaluta

Kriptovaluta je vrsta digitalnog novca, elektronski način razmjene novca i zapisivanja transakcija na računalu. To je sredstvo razmjene koje koristi kriptografiju kako bi stvorilo i osiguralo prijenos novca.[1] Za razliku od banaka, kriptovalute su decentralizirani sustav što znači da nema središnje organizacije koja kontrolira vrijednost, provjerava transakcije ili na bilo koji drugi način utječe na razmjenu novca. Kriptovaluta je peer-to-peer sustav razmjene što znači da za svoje funkcioniranje koristi rad svojih korisnika, oni su zaslužni za stvaranje novih novčanih jedinica i prijenos postojećih.
Sigurnost i integritet transakcija osigurava zajednica rudara (*miners*) koji svojim računalima ovjeravaju transakcije dodavanjem vremenske oznake i ubacivanjem u tzv. glavnu knjigu svih transakcija (*ledger*). Transakcije su računalno zahtjevne i nepraktične za poništiti ili promijeniti što kriptovalutu čini vrlo sigurnim načinom prijenosa novca.
Sustav je siguran dok god većinu čvorova kontroliraju "pošteni" (*honest*) korisnici, a ne napadači (*attackers*).
Ispravnost svake jedinice kriptovalute osigurava blockchain.[2]

1.1 Blockchain

Sustav koji kriptovalute koriste za spremanje podataka o transakcijama je blockchain, decentralizirani mehanizam pohranjvanja informacija o transakcijama. Blockchain je distribuirana glavna knjiga u kojoj se spremaju i čuvaju podaci o transakcijama tako da svi korisnici imaju svoju kopiju, nema osobe ili organizacije koja ima popis transakcija te ih može mijenjati ili brisati. Sve informacije su vidljive svima koji koriste tu valutu te nije moguća manipulacija podataka.
Blockchain je realiziran kao rastuća lista podataka raspoređenih u blokove. Svaki blok je povezan s prethodnim tako što sadrži hash vrijednost tog bloka. Osim hash vrijednosti, blokovi sadrže i: index bloka, hash prethodnog bloka, vremenske oznaku, podatake, koji su u slučaju kriptovaluta, transakcije.
Transakcije su strukturirane u obliku Merkle stabla koje se stvara hashiranjem po-

dataka u više navrata. Prvo se hashiraju same transakcije, zatim upare dva hasha koji se ponovno hashiraju. Postupak se ponavlja dok ne dobijemo samo jedan hash, hash korijen (*root hash*) ili merkle korijen. Svaki list je hash transakcije, a svaki čvor hash prethodnih hasheva. Kada su podaci spremljeni u ovakvoj strukturi podataka, lako se može provjeriti da li je transakcija spremljena u tom setu podataka.
Potvrda da su transakcije određenog bloka prihvaćeni od strane ostalih čvorova i time ispravni, dobije se kada novi čvorovi počnu koristiti hash tog bloka u potrazi za novim.

1.1.1 Proof of Work

Proof of work je mehanizam kontrole pristupa koji koristimo kada želimo ograničiti, ali ne i zabraniti pristup resursu. Ovaj mehanizam od korisnika zahtjeva neku vrstu rada, najčešće procesorko vrijeme, i tako odvraća denial-of-service napade i druge vrste iskorištavanja usluga kao što je spam. Proof of work traži od korisnika da izračuna neku funkciju, tzv. *pricing function*.
Kriptovalute primjenjuju proof of work tako što miner mora pronaći nonce vrijednost koja hashirana zajedno sa ostalim parametrima koji ulaze u blok, zadovoljava neke uvjete. Kao primjer se može uzeti kriptovaluta Bitcoin, kod koje hashirana vrijednost mora imati određen broj bitova na početku hasha nula. Što je više nula u tom zahtjevu to je teže naći pripradajući hash.
Proof of Work se koristi u blockchainu kako bi se stvorio zapis transakcija koji se ne može lako promijeniti, tj. trebalo bi ponoviti potreban rad za sve transakcije koje su bile nakon te koju bi htjeli promijeniti. Najdulji lanac služi kao dokaz svih događaja u lancu i dokaz najveće potrošene procesorske snage.[3]

1.1.2 Hash funkcija

Hash funkcije su funkcije koje ulazne podatke proizvoljne dužine sažimaju u izlaz određenog formata i veličine. Idealni algoritmi neće imati kolizija, tj. za svaki ulaz, izlaz algoritma je različit, neovisno o veličini promjena ulaznih podataka.
Hash funkcije koje se koriste u blockchainu, kriptovalutama i općenito kriptografiji

moraju biti jednostrane što znači da ne možemo lako iz izlaza dobiti odgovarajući ulaz.
Svojstva optimalnih hash funkcija:

- determinističke su - ista poruka (ulazna vrijednost) uvijek rezultira istim hashom
- velikom brzinom računaju hash vrijednost bilo koje poruke
- teško je i nepraktično generirati poruku koja daje određeni hash
- teško je pronaći dvije različite poruke sa istom hash vrijednosti
- mala promjena poruke treba imati veliki utjecat na izalznu hash vrijednost kako se te dvije poruke ne bi mogle povezati na temelju sličnih izlaznih vrijednosti (učinak lavine)[4]

Sigurne hash funkcije su otporne na sve vrste kriptoanalitičkih napada:

- preimage attack - napad u kojem se nastoji pronaći ulaz određenog hasha ukoliko znamo duljinu ulaza. Brute forceom (napad na koristeći grubu silu, u ovom kontekstu slanje svih mogućih ulaza u hash funkciju dok se ne dobije željeni hash) se ulaz može pronaći u 2^N evaluacija, ako je N duljina ulaza
- birthday attack - pokušaj pronalaska dva različita ulaza hash funkcije koji rezultiraju istim izlazom (kolizija) - $2^{L/2}$ evaluacija

2 Pregled hash algoritama

Puno kriptovaluta, različita svojstva blabla.

2.1 SHA-256

2.2 X11

2.3 SCRYPT

Literatura

[1] Kriptovaluta. https://en.wikipedia.org/wiki/Cryptocurrency. 09.08.2020.

[2] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks. A brief survey of cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 745–752, 2016.

[3] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. Springer, 1992. doi: 10.1007/3-540-48071-4_10.

[4] Saif Al-Kuwari, James H. Davenport, and Russell J. Bradford. Cryptographic hash functions: Recent design trends and security notions. Cryptology ePrint Archive, Report 2011/565, 2011. https://eprint.iacr.org/2011/565.