nedeljainformatike v5.0

Blockchain: mit i stvarnost

David Davidović

Matematička gimnazija

NEDELJA INFORMATIKE v5.0

20. decembar 2018.

Šta je uopšte blockchain?

- Distribuirana struktura podataka
- Imutabilan, linearan zapis o nekim događajima (*jedna verzija istine*)
- Postiže ovo bez centralne organizacije koja održava tu jednu verziju istine
- Umesto toga, veliki broj učesnika postiže *konsenzus* oko toga koja verzija istine je prava

Počeci

- Prve ideje o strukturi podataka koja nalikuje blockchain-u su počele ranih 90-tih
- 28. marta 1997, *Adam Back* opisuje **Hashcash**
- 1. avgusta 2002, **Hashcash** biva donekle formalizovan u radu
- 31. oktobra 2008, misteriozna osoba ili grupa ljudi pod pseudonimom *Satoshi Nakamoto* objavljuje naučni rad koji opisuje **Bitcoin**

Svrha

- Jedini razlog: *decentralizacija*!
- **Primeri:**
  - “Ne želimo da se oslanjamo na banku za finansijske transakcije”
  - “Želimo način da izvršimo ugovore bez verovanja trećem licu”
  - ...

Šta obuhvata ova prezentacija?

- Kako izgleda blockchain (struktura podataka)
- Kako se blockchain koristi u Bitcoin mreži za implementaciju valute
- Korisne primene blockchain-a
- Beskorisne primene blockchain-a

Heš funkcije

- **Heš funkcija**: mapira ulaz proizvoljne dužine u izlaz fiksne dužine
- **Kriptografske heš funkcije** imaju dodatna svojstva:
  - Ako je dato h, nije moguće naći neko m tako da je $H(m) = h$ efikasnije od *brute-force* pretrage
  - Ako je dato m i h tako da je $H(m) = h$, nije moguće naći neko m' tako da je $H(m') = h$ efikasnije od *brute force* pretrage
  - Nije moguće naći proizvoljne m i m' za koje važi $H(m) = H(m')$ efikasnije od *brute-force* pretrage

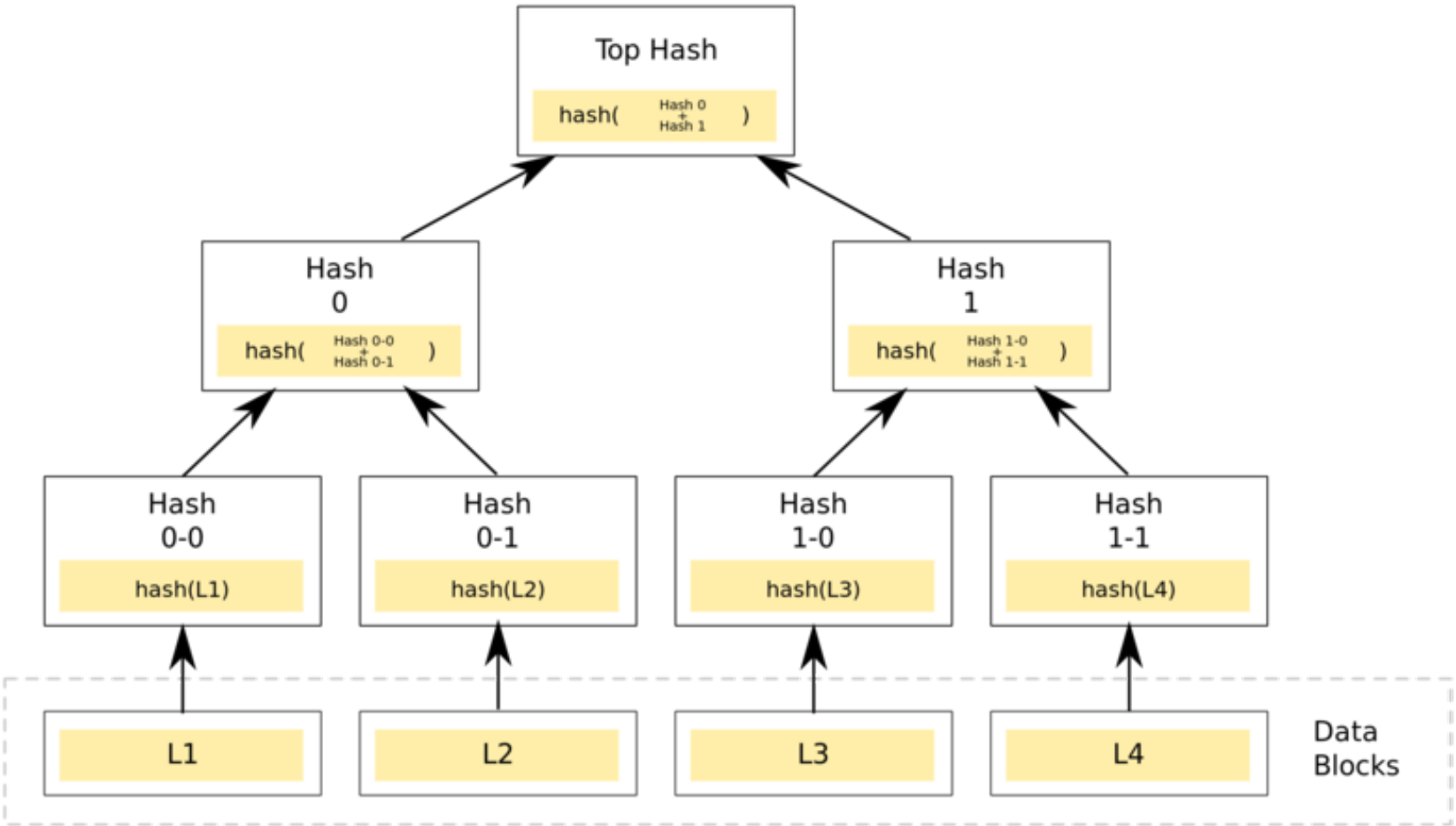
Hashcash

- Relativno jednostavna šema za pružanje dokaza o izvršenom izračunavanju (“proof-of-work”)
- Inicijalno osmišljena za sprečavanje DoS napada
- Server daje *challenge* klijentu, i klijent mora da pronađe string kome je prefiks taj *challenge* a koji se hešira u string koji počinje određenim brojem nula
- Ovo je moguće samo *brute-force* pretragom, pa time klijent dokazuje da je izvršio neko izračunavanje

Merkle stabla

- **Merkle stablo** je stablo u kome svaki čvor sadrži heširane heševe svoje dece
- Listovi stabla sadrže heševe nekih konkretnih podataka koje čuvamo u stablu
- Ukoliko je visina stabla $O(\log n)$, možemo da proverimo da li je neki podatak (heš) deo stabla u $O(\log n)$ koraka, umesto $O(n)$, koliko bi trebalo da je sve heširano zajedno
- O značaju ovoga ćemo uskoro govoriti

Merkle stabla



Public-key kriptografija

- Oblast kriptografije u kojoj kompletan ključ čine *javni* i *privatni* ključ
- *Javni* ključ je deo identiteta osobe i dostupan je svima
- Njemu odgovarajući *privatni* ključ ne sme niko drugi da vidi
- Kada se podaci šifruju javnim ključem, mogu se dešifrovati samo privatnim
  - Koristi se za tajnu komunikaciju
- Kada se podaci šifruju privatnim ključem, svako ko ima javni ključ može da ih dešifruje
  - Koristi se za dokaz o identitetu, odnosno digitalne potpise

Transakcije

- Svaki akter u Bitcoin mreži ima automatski generisan javni i privatni ključ
- Transakcije sadrže (između ostalog):
  - Pokazivač na **drugu, dolaznu transakciju** u kojoj je neki novac primljen
  - Količinu novca iz te dolazne transakcije koja se prebacuje
  - Javni ključ primaoca
- Svaka transakcija je potpisana privatnim ključem pošiljaoca
- Dakle — nema nikakvog novčanika niti “stanja na računu” u samom protokolu — odlazne transakcije samo referenciraju dolazne i “troše” ih

Transakcije

- Zbog svojstava *public-key* kriptografije, svako može da verifikuje da je transakcija validna
  - Privatni ključ kojim je potpisana mora odgovarati javnom ključu na koji je odgovarajuća dolazna transakcija adresirana!
- Međutim, potreban nam je način da nedvosmisleno ustanovimo koje transakcije su se dogodile i kojim redosledom, kako bismo imali našu jednu verziju istine

Blokovi

- **Blok** je, grubo rečeno, niz transakcija
- Svaki blok sadrži oko 2000 transakcija (trenutno), koje su organizovane u Merkle stablo
- Celokupno Merkle stablo je odvojeno od bloka (odnosno, može se preuzeti zasebno), a blok sadrži heš korenskog čvora tog stabla, što omogućuje verifikaciju
- Niz svih blokova koji opisuju svaku transakciju koja se ikad desila čine Bitcoin mrežu i valutu, i zove se *blockchain*
- Ovaj niz jednoznačno određuje ko ima koliko Bitcoin-a na raspolaganju u svakom trenutku
- Ali — i dalje — kako se svi akteri slažu oko ovog niza?

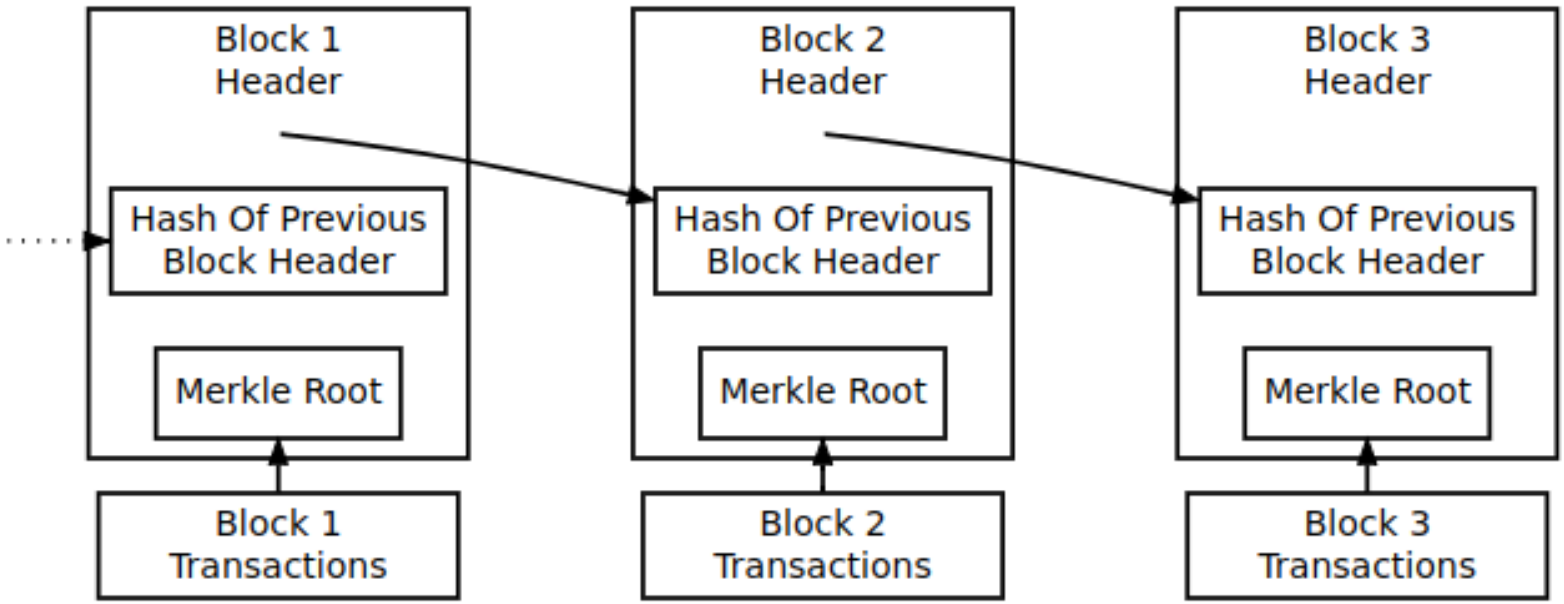
Lanac blokova i “proof-of-work”

- Ključna obzervacija idejnih tvoraca Bitcoin-a je da protokol može da zahteva neki značajan računski napor kako bi se transakcija “aminovala”
- *Hashcash*, koji smo ranije pominjali, nam daje način da dokažemo da je neki računski napor uložen
- **Glavna ideja:**
  - Blok mora da sadrži heš prethodnog bloka
  - Blok je validan samo ako sadrži string kome je prefiks sadržaj bloka a njegov heš počinje sa nekim brojem nula (*Hashcash* ideja u kojoj je “challenge” zamenjen samim sadržajem bloka)
- Rezultat: blokovi formiraju lanac koji u sebi sadrži kumulativan dokaz svog računskog napora uloženog u njega

Lanac blokova i “proof-of-work”

- Transakcije koje korisnici Bitcoin-a žele da izvrše se šalju akterima koji od njih formiraju blokove i ulažu računski napor kako bi našli heš koji bi učinio blok validnim
- Ovi akteri se zovu *miners* (rudari?)
- *Miner-i* šalju ispravne blokove svim ostalim akterima koji mogu ručno da se uvere da su blokovi validni, prateći lanac do početka
- Bilo kakva promena bilo gde u lancu se odmah detektuje i automatski odbacuje, jer se heševi više ne mogu pratiti
- U svakom trenutku može postojati više aktivnih lanaca, ali je važeći onaj koji je najduži

Lanac blokova i “proof-of-work”



Lanac blokova i “proof-of-work”

- *Miner*-i se takmiče međusobno da baš oni budu ti koji će uspeti da naprave sledeći validan blok u lancu
- Kada krajnji korisnik započne transakciju, obično se čeka da ona završi u nekoliko sukcesivnih blokova kako bi se smatrala “izvršenom”
- Posle određenog broja blokova koji su nanizani posle bloka sa tom transakcijom, smatra se da je mala verovatnoća da se desi račvanje negde pre koje će ukloniti transakciju iz jednog izvora istine
- Pošto su transakcije organizovane u potpuno binarno Merkle stablo, klijenti mogu efikasno, u $O(\log n)$ vremena, da provere da li je njihova transakcija u nekom bloku
- Ali zašto bi iko bio *miner*?

Blokovna nagrada

- **Blokovna nagrada** ili **block reward** odgovara na dva pitanja: (1) zašto bi neko bio *miner* i (2) kako novac nastane, ako svaka transakcija mora da referencira prethodnu, dolaznu transakciju?
- Dok *miner* validira blok, dozvoljeno mu je da ostavi svoj javni ključ kako bi dobio nagradu za validaciju bloka
- Ova nagrada se postepeno smanjuje sa brojem transakcija u mreži (po dizajnu)
- Može se iskoristiti kao referencirana dolazna transakcija

Troškovi transakcija

- **Troškovi transakcija** ili **transaction fees** su drugi bitan element koji osigurava profitabilnost *mining*-a
- Prilikom iniciranja transakcije, korisnik može da odredi koliko želi da plati procesiranje *miner*-u koji validira blok sa tom transakcijom
- *Miner*-i imaju slobodu da biraju koje transakcije žele da uključe u koji blok, tako da transakcije sa većim troškovima budu odabrane prve
- *Miner* prosto unosi svoj javni ključ i dobija ove troškove transakcija

Troškovi transakcija

- **Troškovi transakcija** ili **transaction fees** su drugi bitan element koji osigurava profitabilnost *mining*-a
- Prilikom iniciranja transakcije, korisnik može da odredi koliko želi da plati procesiranje *miner*-u koji validira blok sa tom transakcijom
- *Miner*-i imaju slobodu da biraju koje transakcije žele da uključe u koji blok, tako da transakcije sa većim troškovima budu odabrane prve
- *Miner* prosto unosi svoj javni ključ i dobija ove troškove transakcija

Difficulty

- **Teškoća** ili **difficulty** je promenljiva koja govori koliko je teško validirati jedan blok
- Informalno, teškoća definiše sa koliko nula je potrebno da počinje heš kako bi blok bio validan
- Kako se sve više i više ljudi uključuje u proces, potrebno je održati sličnu globalnu brzinu izbacivanja novih blokova, kako sistem ne bi postao nestabilan
- O ovome se razmišljalo i u inicijalnoj verziji protokola, pa se tako teškoća menja na svakih N blokova u zavisnosti od toga koliko vremena je bilo potrebno za *mining* prethodnih N blokova

51% napad

- Jedna fundamentalna slabost ovakve decentralizovane mreže je da zlonamerni akter koji kontroliše većinu čvorova može da dovede mrežu u opasnost
- Ovakav napad se zove **51% napad** ili **većinski napad** (**majority attack**)
- Sastoji se u tome da neko dobije kontrolu nad više od 50% Bitcoin mreže
- Takav akter može da izvede transakciju i onda je u proizvoljnom trenutku poništi, račvajući novi blockchain, pošto ima monopol nad *mining* procesom
- Na ovaj način, ukoliko bi transakcija bila npr. za konverziju Bitcoin-a u USD, u trenutku kada napadač dobije pristup USD iznosu, može da poništi transakciju i dobije Bitcoin nazad

Ne samo Bitcoin!

- Mi smo razmatrali Bitcoin, s obzirom na to da je to prva prava konceptualizacija i implementacija blockchain tehnologije
- Daleko od toga da je Bitcoin jedina primena
- Prava upotreba blockchain-a se uglavnom svodila na:
  - **Kriptovalute**: Ubedljivo najviše. Svaka kriptovaluta ima svoj blockchain, i uglavnom se razlikuju po nekim bitnim ili manje bitnim karakteristikama; na primer, heš funkcija koja se koristi.
  - **Pametni ugovori**: Pametni ugovori su programi čije se izvršavanje vrši na mašinama *miner*-a i može se verifikovati; reći ćemo nešto više o njima uskoro.
  - **Druge primene**: Predloženo je ili postoje pokušaji da se blockchain tehnologija iskoristi za praćenje inventara, glasanje, i sl.

Ethereum i EVM

- **Ethereum** je kriptovaluta koja u svom blockchain-u može da drži stanje izvršavanja nekog programa
- Programi se izvršavaju na arhitekturi koja se zove **Ethereum virtuelnoj mašini (EVM)**
- Svaki *miner*, sem obične validacije blokova, takođe treba da izvrši i unese stanje izvršavanja programa u blok pre validacije
- Ovo stanje se može validirati ponovnim izračunavanjem i upoređivanjem
- Postiže se mogućnost izvršavanja proizvoljne logike, gde se ne zavisi od centralnog entiteta

Ethereum i EVM

- Ovi programi se najčešće koriste za **pametne ugovore** ili **smart contracts**, što su programi koji interaguju sa Ethereum “novčanicima” nekih ugovornih strana
- Na ovaj način se može, na primer, bezbedno izvršiti transfer novca uz neki eksterni uslov, gde nijedna strana ne mora da veruje drugoj strani niti centralnom entitetu
- Koristi se za kredite, kockanje, štedne račune, i sl.

Problemi decentralizacije

- Ipak, i pored svog entuzijazma za blockchain tehnologije, nešto je pošlo po zlu
- Bitcoin, i mnogo drugih kriptovaluta, danas se skoro i ne koristi za platni promet
- I pored obećanja, nije se naišlo na veliku primenu blockchain tehnologije van oblasti kriptovaluta, i donekle pametnih ugovora
- Postavlja se pitanje zbog čega se ovo desilo, i da li odatle može nešto da se nauči?

Problemi decentralizacije

- Ispostavlja se da banke, iako su centralizovan entitet, pružaju mnogo pogodnosti korisnicima koje kriptovalute ne pružaju
- Za transakcije kriptovalutama nije potrebno poverenje centralnom entitetu, ali je potrebno veće poverenje među partijama nego pomoću konvencionalnih transakcija!
- Ukoliko platite proizvod pomoću kreditne kartice, uživate zaštitu ukoliko vam prodavac, na primer, prosto ne dostavi proizvod
- Sa kriptovalutama, ovakvih garancija nema — sve je anonimno
- Ispostavlja se da su potrošačima ovakve garancije mnogo bitnije...

Problemi decentralizacije

- Prosečnoj osobi decentralizacija nije bitna — procenat ljudi koji zaista ne veruje finansijskim institucijama dovoljno da koristi nešto poput Bitcoin-a je mali
- Ljudi više cene činjenicu da je neko, makar i multinacionalna korporacija, odgovoran za njihov novac
- Veliki entuzijazam među generalnom populacijom je bio rezultat pohlepe, ne verovanja u “ideale” kriptovaluta
- I van finansijskog sveta, potreba za apsolutno decentralizovanim zapisom podataka nije velika

Kriptogroznica i prodavanje magle

- Pre oko godinu dana kriptovalute su doživele eksploziju neviđenih razmera, neke se udesetostručujući u vrednosti
- Veliki broj laika je počeo da kupuje Bitcoin i druge kriptovalute u nadi da će lako zaraditi
- Kada god se ovako nešto desi, uvek se pojave trgovci maglom koji žele da profitiraju na neukosti novopridošlih
- **Initial Coin Offering** ili **ICO**: nova kompanija daje bezvrednu kriptovalutu u zamenu za pravi novac, uz obećanje da će ga koristiti da kriptovalutu učini vrednom
  - Oko 50% svih ICO-ova koji su se dogodili krajem 2017. nije preživeo do februara 2018
  - I pored toga, oko $7 * 10^9$ dolara je sveukupno uzeto na njima