Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Primož Hrovat

Mikrostoritve v decentraliziranem okolju

diplomsko delo

univerzitetni študijski program
prve stopnje
računalništvo in informatika

Mentor: prof. dr. Matjaž Branko Jurič

Ljubljana, 2018

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Besedilo teme diplomskega dela študent prepiše iz študijskega informacijskega sistema, kamor ga je vnesel mentor. V nekaj stavkih bo opisal, kaj pričakuje od kandidatovega diplomskega dela. Kaj so cilji, kakšne metode uporabiti, morda bo zapisal tudi ključno literaturo.

TODO: dopolni z opisom, ko bo na voljo

Na tem mestu zapišite, komu se zahvaljujete za izdelavo diplomske naloge. Pazite, da ne boste koga pozabili. Utegnil vam bo zameriti. Temu se da izogniti tako, da celotno zahvalo izpustite.

Posvetilo

Kazalo

Seznam uporabljenih kratic

TODO: dopolni

kratica	**angleško**	**slovensko**
CA	classification accuracy	klasifikacijska točnost
DBMS	database management system	sistem za upravljanje podatkovnih baz
SVM	support vector machine	metoda podpornih vektorjev
...	...	...

Povzetek

Naslov: Mikrostoritve v decentraliziranem okolju

Avtor: Primož Hrovat

TODO: dopolni ob koncu

Ključne besede: decentralizacija, distribuirane storitve, tehnologija veriženja podatkovnih blokov.

Abstract

Title: Microservices in decentralized environment

Author: Primož Hrovat

TODO: dopolni ob koncu

Keywords: decentralization, distributed services, blockchain.

Poglavje 1

Uvod

Poslovne storitve se danes selijo v oblak. S pojavom arhitekture mikrostoritev in podporne tehnologije, kot so vsebniki in okolja za orkestracijo vsebnikov, so, nekdaj ogromni, kosi programske opreme pričeli razpadati na manjše, logično ločene sestavne dele. Razmeroma majhne in neodvisne aplikacije, specializirane za opravljanje točno določenih nalog, omogočajo hiter vzpostavitveni čas in puščajo majhen odtis na porabi strojne opreme. Neodvisnost teh aplikacij nam omogoča tudi skaliranje teh posamenznih delov celotne storitve, ko je to potrebno. Vsebniki so razmeroma stara tehnologija, ki je s pojavom okolja Docker doživela pravi razcvet. Gre za "lahko"obliko virtualizacije, virtualizacija tu poteka na nivoju procesov in ne operacijskega sistema. Pravi potencial vsebnikov izkoristimo šele z uporabo orkestratorjev, kot so Kubernetes, Amazon ECS, Google Container Engine (GKE), Docker Swarm, Azure Container Service in podobni. Ta orodja omogočajo monitoring, zaganjanje, zaustavljanje in preverjanje storitev, skladno s podanimi zahtevami. Storitve se izvajajo distribuirano (porazdeljeno) in replicirano, lahko tudi na fizično ločenih sistemih, kar zagotavlja visoko stopnjo odzivnosti in dosegljivosti. Stopnja dosegljivosti se danes meri na peti ali šesti decimalki („number of nines“).

S pojavom Bitcoina se je začel razvoj tehnologije, ki v decentraliziranem okolju omogoča varno in nespremenljivo hrambo podatkov. Veriženje

podatkovnih blokov je v zadnjih letih s pojavom različnih organizacij kot so Hyperledger in Ethereum doživelo razcvet. Nova tehnologija omogoča shranjevanje podatkov, repliciranih na vseh sodelujočih entitetah v omrežju, obenem pa ohranjajo nespremenljivost.

Tu se pojavlja vprašanje. Ali je možno tudi poslovno logiko prestaviti v decentraliziran svet na način, da bo sodelujoči v omrežju ob klicu želene storitve vedno dobil odgovor, izvedla pa ga bo katerakoli druga entiteta, obenem pa zagotoviti pravilnost izvajana? Z uresničitvijo tega cilja bi miselnost decentraliziranih podatkov prestavili nivo višje, na nivo poslovne logike. Odzivnost in dosegljivost storitve bi s številom sodelujočih v omrežju dosegla 100%, prav tako bi bilo praktično nemogoče izvesti napade DOS.

TODO: dopolni s podrobnostmi (ob koncu pisanja)

Poglavje 2

Arhitekturni koncepti mikrostoritev

Razvoj monolitov je enostaven in danes dobro podprt v vseh danes prisotnih razvojnih okoljih. Prenos in namestitev teh storitev na strežniške sisteme je enostaven, rešitev v obliki izvršljivih datotek ali s kopiranjem direktorijske strukture prenesemo v produkcijsko izvajalno okolje. Če želimo tako storitev skalirati, kot vstopno točko v naše zaledne sisteme nastavimo izenačevalnika obremenitev (ang. load balancer), ki poskrbi za enakomerno porazdeljevanje dela med posameznimi instancami storitve.

Slabosti te arhitekture se pojavijo, ko storitev postane kompleksnejša. Podaljša se zagonski čas (start up time), ob preobremenitvi le enega dela storitve je potrebno pognati celotno aplikacijo. Proces sprotne dostave (Continouos Delivery) je otežen, za posodobitev enega dela sistema, je potrebno celotno storitev zaustaviti, namestiti novo različico in jo zagnati. [5]

2.1 Arhitektura mikrostoritev

Arhitektura mikrostoritev omogoča...

2.2 Vzorci

2.2.1 Metrike

2.2.2 Preverjanje (Health Check)

2.2.3 Odkrivanje storitev (Service discovery)

2.2.4 Odpornost na napake (Fault Tolerance)

2.3 Vsebniki in orkestracija

TODO: dopolni s podrobnostmi (1. in 2. teden v juniju).

Poglavje 3

Tehnologija veriženja podatkovnih blokov

Veriženje podatkovnih blokov je peer-to-peer porazdeljena podatkovna shramba, dosežena s konsenzom, sistemom "pametnih"pogodb ter drugih pomožnih tehnologij [2]. V središču omrežja je glavna knjiga "ledger", ki beleži vse transakcije, izvedene na omrežju. [4] Vsak blok v verigi predstavlja zbirko transakcij, te člene pa med seboj povezuje zgoščevalna (hash) funkcija. V verigo je blok moč le dodajati. Vsak nov blok mora biti pred zapisom potrjen s strani skupnosti in, preko vrednosti zgoščene funkcije prejšnjega člena, povezan v verigo blokov. Celotna veriga blokov je shranjena pri vsaki sodelujoči entiteti. Kombinacija teh pristopov omogoča, da nobena izmed sodelujočih entitet ne more spreminjati že zapisanih blokov. S temi mehanizmi se zagotovi veljavnost in nespremenljivost podatkov, v okolju, ki mu apriori ni potrebno zaupati. Ni več potrebe po zunanji, zaupanja vredni, entiteti.

Za interakcijo z glavno knjigo in zapisovanje novih informacij, omrežje uporablja t.i. "pametne pogodbe". [4]

TODO: dopolni s podrobnostmi

3.1 Razlaga osnovnih konceptov

3.1.1 Izvajalna okolja glede na zaupanje med udeleženci

V grobem lahko ločimo dva tipa izvajalnih okolij, glede na stopnjo zaupanja, ki ga udeleženci delijo med seboj. Imamo omrežje, kjer so udeleženci vnaprej znani, identificirani s strani tretje osebe, ki ji zaupajo vsi sodelujoči. Interakcije med njimi so varne v smislu prevzemanja odgovornosti. Morebitna škodoželjnost udeleženca je enostavno kaznovana, prav zaradi fizično overjenih oseb (pravnih ali fizičnih).

V javnih okoljih teh ugodnosti ne uživamo. V omrežju lahko sodelujo kdorkoli in to povsem anonimno. Med udeleženci tako a priori velja načelo nezaupanja. Zaupa se le stanju celotne podatkovne verige. Tipično so za potrjevanje blokov in novih transakcij uporabljene „kripto valute“, pridobljene s ti. postopkom rudarjenja. Ta omrežja večinoma temeljijo na ??? (BFT). [4]

3.1.2 Zasebnost in zaupnost

Javne podatkovne verige so replicirane na vseh sodelujočih entitetah, kar prinaša transparentnost, obenem pa poslovnim subjektom onemogoča učinkovito sklepanje dodatnih ugodnosti, aneksov ipd. s poslovnimi partnerji. Ena od možnih rešitev problema je enkripcija podatkov, ki pa v tem primeru odpove. Vsak izmed sodelujočih ima dostop do celotne glavne knjige, kar omogoča enostavne napade s silo. V nadaljanju predstavljeno omrežje Fabric tu vpeljuje koncept kanalov. Ti predstavljajo logično grupiranje posameznih entitet in omejujejo dostop do pametnih pogodb in glavne knjige na posameznem kanalu. [4]

3.2 Ethereum

Ethereum je decentralizirana platforma, ki izvaja "pametne"pogodbe (smart contracts) - aplikacije, ki se izvajajo natanko tako, kot so bile zapisane. Platforma je osnovana na verigi podatkovnih blokov, ki omogoča reprezentacijo in prenos vrednosti. Lahko si ga predstavljamo kot svetovni računalnik, izvajanje programske kode pa poteka na vseh sodelujočih računalnikih. Pametne pogodbe ponujajo možnost interakcije s podatkovno verigo, določeni deli kode pa se izvajajo le pod točno določenimi pogoji.

Stanje v Ethereum omrežju določajo objekti, znani kot uporabniški računi (accounts). Vsak račun sestavlja 20 bajtov dolg naslov, prenos sredstev in informacij med računi pa predstavlja spremembo trenutnega stanja. Uporabniške račune sestavljajo štiri polja:

- števec (nonce), ki preprečuje podvajanje transakcij
- trenutno stanje Ethra (ether balance) trenutna količina ethra v lasti računa
- pogodbena koda (contract code) opcijska
- shramba (storage) privzeto prazno

Ether je interno plačilno sredstvo v omrežju. Uporablja se kot nadomestilo za izvrševanje transakcij. Ethereum pozna dva tipa uporabniških entitet: zunanje (externally owned), določenih s privatnimi ključi in pogodbene (contract accounts), določenih s kodo. Zunanji računi ne obvladujejo kode, z ostalimi entitetami v omrežju pa lahko komunicirajo preko digitalno podpisanih transakcij. Pametne pogodbe so entitete, ki se v omrežju odzivajo na vnaprej določena sporočila: izvedejo del logike, berejo in pišejo v glavno knjigo oziroma pošljejo novo sporočilo v omrežje.

3.2.1 Komunikacija med entitetami

V omrežju obstajata dva načina komunikacije: sporočila (messages) in transakcije (transactions). Transakcije so podpisani podatkovni bloki, ki jih ustvarijo zunanji uporabniški računi. Sestavni deli transakcije so:

- prejemnik
- podpis pošiljatelja
- količina prenesenega ethra
- podatki (opcijsko)
- STARTGAS največje dovoljeno število izvedenih računskih operacij
- GASPRICE cena posamezne računske operacije

Sporočila so namenjena interni komunikaciji med pametnimi pogodbami. So le navidezni objekti, obstajajo izključno v izvajalnem okolju. Sestavlja jih:

- pošiljatelj
- prejemnik
- količina prenesenega ethra
- STARTGAS

[1]

3.2.2 Navidezni stroj Ethereum

Navidezni stroj je glavna abstrakcija celotnega omrežja. Je izvajalno okolje za pametne pogodbe v Ethereum omrežju in služi kot „peskovnik“ za izvajanje kode. Celotni navidezni stroj lahko predstavimo s terko **(stanje blokov, transakcija, sporočilo, koda, spomin, sklad, programski števec,**

plin). *Stanje blokov* je predstavitev vseh računov s trenutnim stanjem ethra in shrambe. Vsaka izvedena operacija zmanjša vrednost preostale količine plina, glede na uteženost posamezne operacije. Transakcija se zaključi ob izvedbi zadnje operacije v programu oziroma s prekinitvijo, ko porabljena količina plina preseže največjo dovoljeno.

Potrjevanje in kreiranje blokov

Vsak blok v Ethereum verigi vsebuje kopijo vseh transakcij in zadnjega stanja omrežja. Poleg tega sta v bloku zapisani tudi zaporedna številka bloka in zahtevnost. Postopek validacije bloka poteka sledeče:

1. Preveri, če predhodni blok obstaja in je veljaven
2. Preveri časovni žig bloka - večji od prejšnejga bloka, vendar ne več kot 15 v prihodnosti
3. Preveri številko bloka, zahtevnost, izvor transakcije, izvor štrica"in omejitev količine plina
4. Preveri veljavnost „Proof of Work“
5. Naj bo S[0] stanje na koncu predhodnega bloka
6. Naj bo TX seznam transakcij v bloku. Za vsak $\{i \mid 0, 1, \ldots, n-1\}$ je naslednje stanje $S[i+1] = APPLY(S[i], TX[i])$. V primeru napake ali presežene omejitve količine plina na blok (GASLIMIT), vrni napako.
7. Naj $S_FINAL = S[n]$. Nagrada za najden blok se izplača samo najditelju.
8. Preveri, da je vrhnje vozlišče Merklovega drevesa **CITAT!!!** stanja S_FINAL enaka končnemu stanju v bloku. V tem primeru je blok veljaven.

Koda je izvedena s strani vseh sodelujočih entitet v omrežju. [1]

3.3 Hyperledger

Hyperledger je družina odprtokodnih projektov, namenjenih razvoju tehnologije veriženja podatkovnih blokov. Projekt deluje pod okriljem organizacije The Linux Foundation, v sodelovanju s skupnostjo. Med prvimi in najbolj znamimi izmed Hyperledger projektov je Hyperledger Fabric, prvotno razvit v podjetju IBM in Digital Asset. Pod okrilje projekta Hyperledger spadajo še Sawtooth, Iroha, Burrow ter Indy. Vsak izmed projektov na svoj način rešuje izzive s področja podatkovnih verig ali pa naslavlja ozko problemsko domeno, za primer: projekt Indy se ukvarja s problematiko spletne identitete uporabnika. [2] Trenutno najbolj znana in razširjena platforma je Fabric, trenutno v različici 1.1. Od ostalih podobnih projektov se loči predvsem v konceptu privatnih omrežjih, pri katerih je sodelovanje omejeno s sistemom dovoljenj. Omogoča modularno izbiro načina soglasja in ga je moč prilagajati zahtevam poslovnih uporabnikov. [3]

3.3.1 Fabric

Hyperledger Fabric je v sami zasnovi namenjen poslovni uporabi. Omogoča modularno in prilagodljivo arhitekturo, podobno kot ostale implementacije tehnologije veriženja blokov pozna tudi pametne pogodbe, tu imenovane „chain code“. Pametne pogodbe se tu izvajajo znotraj vsebnikov Docker in omogočajo implementacijo v poljubnem splošnonamenskem programskem jeziku. Drugačen je tudi postopek izvedbe transakcije.

Celotno omrežje je zasnovano na predpostavki (delnega) zaupanja med sodelujočimi entitetami, za razliko od javnih omrežij. Enostavna je menjava implementacije protokola za doseganje konsenza, bodisi na osnovi reševanja napak ob odpovedi (Crash Fault Tolerant – CFT) ali ??? (Byzantine Fault Tolerance – BFT). Za samo delovanje ne potrebuje kriptovalute, potrjevanje transakcij in blokov pa ni nujno izvedeno s strani vseh sodelujočih, ampak le določene podmnožice, kar v teoriji omogoča paralelizacijo in posledično višjo zmogljivost.

Modularnost

Omrežje sestoji iz šestih osnovnih komponent, ki jih je moč poljubno menjati:

1. urejevalnik (ordering service)
2. upravitelj članstva (membership service) - povezuje zunanje entitete z njihovimi kriptografskimi predstavitvami
3. P2P gossip protocol - opcijski
4. Pametne pogodbe (chaincode) - procesno izolacijo zagotavlja izvajanje znotraj vsebnikov Docker. Onemogočen je neposreden dostop do glavne knjige
5. SUPB (DBMS)
6. zamenljiva politika potrjevanja in validiranja

Pametne pogodbe

Pametne pogodbe so delčki programske kode, ki se izvajajo kot distribuirane aplikacije. Tri glavne značilnosti teh aplikacij so: veliko število sočasno izvajanih pametnih pogodb, dinamično dodajanje v omrežje in nevredne zaupanja. Obstoječi načini izvajanja pogodb so umeščene v arhitekturo **uredi-izvedi**. Za njih je značilno, da transakcije validirajo in sekvečno uredijo, temu pa sledi propagacija potrjenih blokov po omrežju. Vsaka sodelujoča entitea nato transakcije izvede v tem vrstem redu. Za enoličen način sekvenčnega izvajanja tu nastane potreba po novem, determinističnem programskem jeziku. En izmed predstavnikov je programski jezik za programiranje pogodb v omrežju Ethereum, Solidity. Ker je vsaka izmed transakcij izvedena s strani vsake entitete, to predstavlja veliko porabo razpoložljivih virov ter omejuje skaliranje ter performase.

Fabric pametne pogodbe izvaja po arhitekturi **izvedi-uredi-validiraj**. Vsaka transakcija je najprej izvedena s čimer se preveri njeno pravilnost.

Nato je urejena, glede na protokol za doseganje konseza. Nazadnje je transakcija validirana s strani za to pooblaščenih zunanjih entitet. Tu v igro vstopi domensko specifična politika potrjevanja. Slednje prinaša potencialno velike performančne prihranke.

TODO: dopolni s podrobnostmi

Poglavje 4

Koncepti registracije in odkrivanja storitev v decentraliziranem svetu

TODO: Opis predlaganega koncepta za registracijo in odkrivanje storitev s pametnimi pogodbami.

Predvidoma do sredine junija, ko bo predvidoma znana končna zasnova.

Poglavje 5

Implementacija in validacija rešitve

TODO: Implementacija predlaganih konceptov (Proof of concept). Pravilnost delovanja, dosežki, pregled in uteževanje rezultatov.

Predvidoma do konca junija. Trenutno v fazi koncepta in prototipiranja.

Poglavje 6

Zaključek

TODO: Glavne ugotovitve, povzetek narejenega. Kratka evalvacija. Napisan ob zaključku dela.

Literatura

[1] Ethereum whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper#ethereum. Dostopano: 22. 05. 2018.

[2] Hyperledger. https://www.hyperledger.org. Dostopano: 22. 05. 2018.

[3] Hyperledger - open source blockchain for business. https://www.ibm.com/blockchain/hyperledger.html. Dostopano: 22. 05. 2018.

[4] Hyperledger Fabric documentation. https://hyperledger-fabric.readthedocs.io. Dostopano: 22. 05. 2018.

[5] Pattern: Monolithic Architecture. http://microservices.io/patterns/monolithic.html. Dostopano: 22. 05. 2018.