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. Je možno tudi poslovno logiko prestaviti v decentralizirano okolje na način, da bo sodelujoči v omrežju ob klicu želene storitve vedno dobil odgovor, izvedla ga bo katerakoli 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. [13]

2.1 Arhitektura mikrostoritev

Gradnja aplikacij je do nedavnega potekala na način, da so razvijalci vse odvisnosti in logiko, potrebno za delovanje, zložili skupaj v veliko tvorbo - monolit. Tak način gradnje ima svoje prednosti in slabosti. Prednosti na

eni strani predstavljajo enostavna zgradba aplikacije, ker je vsa izvorna koda zbrana na enem mestu. Orodja za razvoj so prilagojena takemu načinu dela in razvijalcu ponujajo širok nabor funkcij, ki podpirajo celotno življenjko pot aplikacije, od razvoja, testiranja, namestitve v testna in produkcijska okolja ter vzdrževanje. Velikost projekta je na drugi strani ena od slabosti monolitov, majhne spremembe enega sestavnega dela potrebujejo ponovno namestitev celotne aplikacije. Skaliranje poteka vertikalno, le preko ustvarjanja novih instanc celotne aplikacije. Monolitna zasnova aplikacije razvijalce in vzdrževalce zaveže k dolgoročni uporabi tehnologij, ki so bile uporabljene na začetku. Kasnejše uveljavljanje novih tehnologij oziroma nadomeščanje obstoječih je časovno in finančno potratno, saj je potrebno celotno logiko aplikacije prepisovati. [13]

Arhitektura mikrostoritev se problema gradnje aplikacij loti drugače. Celotno aplikacijo se logično razbije na posamezne sestavne dele, ki se izvajajo samostojno in se med seboj povezujejo preko lahkih komunikacijskih protokolov. Vsak sestavni del aplikacije je samostojen v smislu skaliranja, življenjske dobe posamezne instance, razvoja in podpornih tehnologij. Tak način gradnje sledi tistemu, ki ga v fizičnem svetu poznamo že stoletja, to je sestavljanje vnaprej pripravljenih delov v celoto. Lep primer tega je avtomobilska industrija. Na tekočem traku se na tisoče sestavnih delov različnih proizvajalcev zloži v polno funkcionalno enoto - avtomobil. Podobno želimo doseči pri razvoju programske opreme, kar bi pohitrilo in pocenilo razvoj novih aplikacij, krepko pa bi omejili tudi nepotrebno podvajanje izvorne kode. [12, 9]

V povezavi z mikrostoritvami je tesno povezana tudi arhitektura „cloud-native“. Gre za novo paradigmo razvoja programske opreme, ki sledi načinom izdelave stvari v fizičnem svetu. Z namenom uveljavljanja in razvoja paradigme je bila ustanovljena „Cloud Native Computing Foundation“, ki bdi nad razvojem standardov in novih smernic. Oblačne sisteme sestavljajo [17]:

- Aplikacije in procesi se izvajajo znotraj vsebnikov, ki so neodvisne in izoloirane izvajalne enote
- Storitve so dinačmično upravljajo in nadzorujejo preko centralnega or-

kestracijskega procesa

- Sistem sestavljajo mikrostoritve, ki so med seboj šibko sklopljene

Računalništvo v oblaku je dostop in uporaba računskih virov (aplikacije, podatkovna skladišča, procesorski čas...) na zahtevo preko interneta. Plačilo se izvede skladno s količino porabljenih virov. Viri so elastični in zmožni hitrega in učinkovitega skaliranja ter prilagajanja trenutnim zahtevam. V grobem med seboj ločimo tri glavne komponente oblačnih sistemov: SaaS, PaaS in IaaS. SaaS (Software as a Service) - programska oprema kot storitev, je oblačna aplikacija, ki se izvaja na oddaljenih računalnikih, do katerih uporabnik storitve dostopa preko interneta. Prednosti teh aplikacij so dostopnost od koderkoli, za nemoteno delovanje aplikacije je odgovoren ponudnik in storitev je zmožna dinamičnega skaliranja, da zadovolji trenutnim potrebam. PaaS (Platform as a Service) - platforma kot storitev, uporabnikom ponuja programsko platformo, brez stroškov nakupa in kompleksnosti upravljanja podporne strojne in programske opreme. IaaS (Infrastructure as a Service) - infrastruktura kot storitev, ponuja dostop do računskih virov (strežniki, omrežna oprema, shramba...). Uporabnikom ni potrebno investirati v lastno strojno opremo, tako kot sestrske storitve (SaaS in PaaS), je tudi ta zmožna samodejnega skaliranja. [6]

2.2 Vzorci

2.2.1 Metrike

Posamezna storitev se lahko izvaja na različnih (fizičnih) lokacijah, na različni strojni opremi in v več instancah. Pojavi se potreba po spremljanju storitve in njenega obnašanja, kje in zakaj prihaja do izpadov oziroma morebitnih dolgih odzivnih časih. Vse želene metrike želimo shraniti na enem centraliziranem sistemu, jih po možnosti agregirati, in tako omogočiti odkrivanje napak in reševanje teh. V osnovi poznamo dva modela zbiranja metrik:

- mikrostoritev sama pošilja metrike centralni zbirki (push)

- centralna zbirka zahteva metrike od storitve (pull)

Zbiranje metrik ponuja dober vpogled v obnašanje posameznih storitev, s sabo pa prinese dodatno potrebno infrastrukturo in dodatne težave pri implementaciji.[10]

Ena izmed bolj znanih storitev za zbiranje aplikacijsih metrik je Prometheus, odprtokodna zbirka orodij za zbiranje in agregiranje metrik ter obveščanje. Projekt je bil, takoj za orkestracijskim okoljem Kubernetes, pridružen fundaciji CNCF. Prometheus zahteva metrike od storitve (način pull), jih agregira in proži morebitna opozorila. Skupaj z ogrodjem Grafana omogoča celovit grafičen vpogled v zbrane metrike. [15]

2.2.2 Preverjanje odzivnosti (Health Check)

Pogosto se zgodi, da se storitev še vedno odziva na posamezne zahteve, vendar so te neuspešne. V takšnih primerih je pričakovano obnašanje sistema, da nedelujočo storitev iz omrežja označi kot nedosegljivo in jo nadomesti z novo. Tu v igro vstopi koncept preverjanja odzivnosti storitev (ang. Health check), ki za vsako storitev pričakuje izpostavljeno dostopno točko, preko katere lahko sistem pridobi informacije o sposobnosti storitve, da odgovori na zahtevke. Vsaka storitev je odgovorna za preverjanje svojih zunanjih in notranjih virov in generiranja poročila o trenutnem statusu posamezne komponente. Tipični testi so preverjanje zmožnosti povezave na podatkovno bazo, dosegljivost ostalih odvisnih storitev, povezljivost z vrstami... Poleg zunanjih odvisnosti se preveri tudi stanje gostitelja: razpoložljiv prostor na disku, zasedenost CPE ipd. Nadzorna storitev periodično proži zahteve na vse registrirane storitve in preverja njihove odzive. Tipičen ukrep ob negativnem odzivu je zaustavitev in ponovni zagon nedelujoče storitve. [11]

2.2.3 Odkrivanje storitev (Service discovery)

Ko želimo od zunanje entitete pridobiti podatke oziroma prožiti določeno akcijo, potrebujemo njen omrežni naslov (kombinacija naslova IP in številke

vrat). Pri klasičnih aplikacijah, ki se izvajajo na fizični napravi, so naslovi relativno statični. Zelo malo je tudi klicev med posameznimi aplikacijami, saj se storitve med seboj kličejo preko programskih klicev. V arhitekturi mikrostoritev je omrežnih klicev bistveno več, ker je celotna programska logika aplikacije sestavljena iz več samostojnih storitev. Njihovo število se dinamično spreminja, skladno s tem tudi omrežni naslovi posameznih instanc. Posledično je potrebno za odjemalca vpeljati nov mehanizem, ki je zmožen dinamično odkriti naslove, na katerih se želena storitev nahaja.

Tipično za oblačne arhitekture je, da se odkrivanje storitev realizira s pomočjo centralnega registra. Storitve se ob pričetku izvajanja registrirajo. Odjemalska aplikacija ob potrebi po dostopu do zunanje storitve na register naslovi poizvedbo za lokacijo instanc želene mikrostoritve. Zakasnitev pri omrežnih klicih je bistveno večja kot pri programskih klicih znotraj aplikacije, zato želimo visoko učinkovitost poizvedb. [14, 18]

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 [3]. Osrednja komponenta sistema je glavna knjiga (ang. ledger), ki beleži vse akcije (transakcije), izvedene na omrežju. [5] Entiteta, ki transakcijo izvede, jo podpiše s svojim privatnim ključem. Skupek transakcij tvori podatkovni blok, bloki pa se med seboj povezujejo v podatkovno verigo. Posamezne člene verige med seboj povezuje zgoščevalna funkcija, na vhod katere postavimo zgoščeno vrednost trenutnega in prejšnjega bloka. Podatkovno verigo je moč vedno le podaljševati, trenutno veljavno in resnično stanje omrežja je trenutno najdaljša serija blokov. Celotna veriga blokov je replicirana na vsaki izmed sodelujočih entiteti.

Kombinacija teh pristopov omogoča, da nobena izmed sodelujočih entitet ne more spreminjati že zapisanih blokov. Napad na omrežje je možen le s pridobitvijo več kot polovice vseh sodelujočih entitet v omrežju, ki bi potrjevale resničnost ponarejenih transakcij in sčasoma sestavile daljšo podatkovno verigo, ki bi obveljala kot trenutna resnica. 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". [5] To je del programske kode, ki se lahko odziva na dogodke v omrežju, izvede zapisano poslovno logiko ter ustvarja nove transakcije.

3.1 Razlaga osnovnih konceptov

3.1.1 Glavna knjiga

3.1.2 Pametne pogodbe

3.1.3 Soglasje

3.1.4 Izvajalna okolja glede na zaupanje med udeleženci

V grobem lahko, glede na stopnjo zaupanja, ločimo dva tipa izvajalnih okolij, 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 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). [5]

3.1.5 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. [5]

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. [3] 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. [4]

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, deterministčnem 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

Decentralizirano izvajanje

4.1 Registracija in odkrivanje storitev v decentraliziranem okolju

Izvajanje storitev se danes seli v oblak, kjer se posamezne instance storitve replicira glede na trenutne potrebe.

Izvajanje storitev želimo decentralizirati - vsaka sodelujoča entiteta v omrežju lahko, pod določenimi pogoji, izvaja katerokoli izmed nabora razpoložljivih storitev. Prednost, ki jo prinaša decentralizirano izvajanje poslovne logike je praktično nemogoč napad zavrnitev storitve (DOS) in porazdeljen napad zavrnitve storitve (DDOS). Napadalec je zmožen posamezno sodelujočo entiteto v omrežju obremeniti do te mere, da le ta preneha z izvajanjem določene storitve. Decentraliziran sistem bi v primeru prenehanja izvajanja storitve na eni entiteti izvajanje dodelil drugi. Postopek bi moral biti za končnega uporabnika storitve transparenten.

Dodatno se vsak klic storitve opremi s finančnimi podatki in ob uspešno izvedenem klicu je izvajalec za svoje delo nagrajen.

4.2 Odkrivanje storitev v decentraliziranem okolju

Predlagana rešitev registracije in odkrivanja storitve v decentraliziranem okolju je sestavljna iz naštetih komponent:

- Registracija nove storitve 4.2.1
- Registracija izvajalcev 4.2.2
- Registracija izvajanja 4.2.3
- Odkrivanje storitev 4.2.4

4.2.1 Registracija nove storitve

Vsak izmed sodelujočih ima možnost v omrežje javno objaviti novo storitev, za katero navede pogoje uporabe. Izvorna koda oziroma izvršljiva datoteka storitve se shrani shrani v decentralizirano shrambo, temu pa sledi zapis podatkov o storivti v glavno knjigo. Ob uspešni registraciji se v omrežju sproži dogodek, na katerega se sodelujoče entitete odzovejo. Glede na lastne določene omejitve in trenutno aktivna naročila v omrežju, lahko poljuben člen omrežja prične z izvajanjem storitev.

4.2.2 Registracija izvajalcev

Vsaka digitalna identiteta lahko upravlja z več izvajalnimi enotami. Ta pristop omogoča enemu uporabniškemu računu pripis vseh nagrad, ki jih posamezni izvajalec prisluži. Podatki, ki se o posameznem izvajalcu zabeležijo so: lastnik (account), unikatna številka izvajalca (id) in naslov, preko katerega je izvajalec dosegljiv. Posameznemu izvajalcu se lokalno konfigurira omejitve glede porabe sistemskih virov, ki jih lastnik nameni decentraliziranemu izvajanju storitev.

4.2.3 Registracija izvajanja storitve

Izvorno kodo oz. izvršljivo datoteko storitve se najprej pridobi iz omrežja. Nadzorni proces nato storitev zažene, storitev sama pa ob inicializaciji sama izcede postopek registracije. V glavno knjigo se zabeleži izvajalca in storitev, ki se izvaja.

4.2.4 Odkrivanje storitve

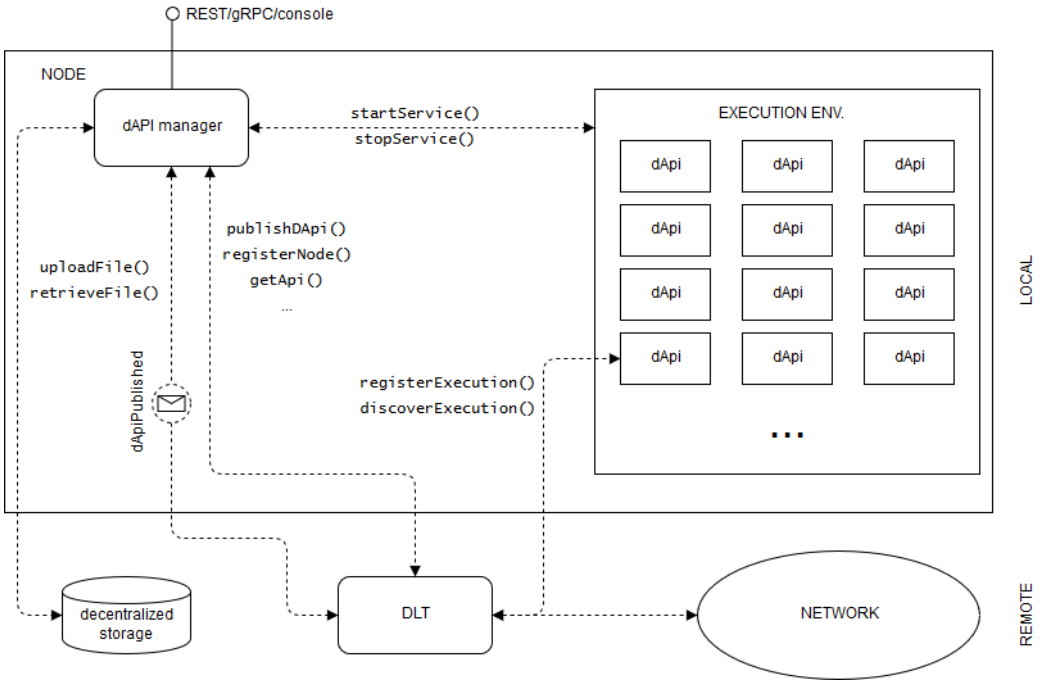
Storitve, ki se trenutno izvajajo v omrežju, pridobimo z enostavnim vpogledom v glavno knjigo. Med razpoložljivimi storitvami odjemalec izbere eno, pridobi podatke o lokaciji izvajanja in izvede klic po izbranem protokolu. Od tu naprej komunikacija med storitvami poteka preko trenutnih protokolov (REST, gRPC, Event-driven).

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 predlagane rešitve



Slika 5.1: Arhitekturna shema rešitve

Na sliki 5 je prikazana shema predlagane rešitve. Osrednji del omrežja je

nadzorni proces - dApi manager, ki dostopa do glavne knjige, decentralizirane shrambe in upravlja s storitvami, ki jih gostitelj izvaja. Gostiteljski sistem v trenutni različici podpira upravljanje z vsebniki Docker. Storitve, ki so na voljo za izvajanje so shranjene na datotečni shrambi IPFS, podatkovna veriga je osnovana na Ethereum verigi. Posamezne komponente sistema so podrobneje opisane v nadaljevanju.

5.1 Nadzorni proces

Nadzorni proces za izvajanje dApijev skrbi za:

- registracijo novih storitev v omrežje,
- prenos izvršljivih datotek v in iz omrežja,
- zagon, zaustavitev in upravljanje storitev

Komunikacija z nadzornim procesom trenutno poteka preko REST aplikacijskega vmesnika, v načrtu pa je implementacija vmesnikov za konzolni nadzor ter podpora novejšim komunikacijsim protokolom kot so gRPC, Apache Trift in podobni.

Za registracijo nove storitve nadzornemu procesu podamo pot do slike vsebnika Docker. Sistem poskrbi za distribucijo slike v omrežje IPFS in podatke o storitvi doda v shrambo pogodbe na Ethereum omrežju. Ob uspešni registraciji se proži dogodek, ki sodelujoče entitete obvesti o novi storitvi, pripravljeni na izvajanje. Te se lahko na dogodek lahko odzovejo z zahtevo za izvajanje storitve. Trenutno je izvajanje nove storitve potrebno prožiti ročno, ko bo pripravljen modul za razporejanje opravil, bo postopek v celoti avtomatiziran. Pred pričetkom izvajanje se želeno storitev pridobi iz omrežja (IPFS), sliko vsebnika naloži v izvajalno okolje Docker in proži izvajanje. Storitev nato sama poskrbi za registracijo in odkrivanje ostalih storitev v omrežju.

Razširitev obstoječe KumuluzEE konfiguracijske datoteke:

```
dapi-manager:
  storage:
    remote:
      type: ipfs
      location: /ip4/127.0.0.1/tcp/5001
    local:
      downloadFolder: download
      execution:
  managers:
  - type: docker
    connection: tcp://192.168.99.100:2376
    tls: true
    certificate-path: /path/to/certificate
    instance-limit: 10
  blockchain:
    provider: ethereum
    host: http://127.0.0.1:8545
    account: /path/to/wallet
    password: password
```

5.2 Decentralizirana shramba

Izvršljive datoteke oziroma slike vsebnikov storitve je potrebno shraniti na način in lokacijo, kjer bodo dostopne vsem sodelujočim entitetam v omrežju. Podobno, kot želimo izvajanje storitev decentralizirati, moramo poskrbeti tudi za decentralizirano shrambo. V svoji implementaciji sem uporabil decentralizirano shrambo IPFS. Gre za projekt, osnovan na omrežju Ethereum, namen projekta pa je shranjevanje datotek v porazdeljeni shrambi, dostop do njih pa preko omrežji P2P, podobno kot deluje protokol BitTorrent, po katerem se projekt tudi zgleduje. Vsako datoteko, ki jo želimo shraniti v omrežje, odjemalec razbije na podatkovne bloke, izračuna zgoščeno vrednost

posameznega bloka, te vrednosti pa nato sestavi v strukturo imenovano Merkle Tree. Datoteko pridobimo enostavno preko zgoščene vrednosti v korenu drevesa. Omrežje je sposobno poiskati posamezne koščke prvotne datoteke, vsebino posameznega pa hitro preveri z izračunom zgoščene vrednosti. V kolikor nam kdo želi podtakniti napačne bloke posamezne datoteke, sistem to prepozna in neveljavne bloke preprosto zavrže, ko od ostalih sodelujočih entitet prejme iste dele datoteke. Datoteka je veljavna, če sistem uspe sestaviti podatkovno strukturo Merkle Tree, katerega zgoščena vrednost v korenu drevesa je identična zahtevani. [8]

5.3 Odjemalec za Ethereum omrežje

Sistem za delovanje potrebuje odjemalca, ki se zna povezati v Ethereum omrežje. V moji testni postavitvi je mesto odjemalca prevzel program Geth, implementacija Ethereum protokola v programskem jeziku Go. [2] Nadzorni proces se preko JSON RPC povezuje na lokalno instanco odjemalca Geth, decentralizirane storitve v izvajalnem okolju Docker pa se povezujejo na proces, dostopen preko mreže Infura. Infura nam omogoča enostaven dostop do Ethereum omrežja, brez potrebe po lokalnem izvajanju Ehtereum protokola. Za sodelovanje v decentraliziranem svetu nam lokalno ni potrebno namestiti ničesar, prav tako nam ni potrebno hraniti celotne zgodovine - podatkovne verige. Na spletni strani se enostavno registriramo, s tem pridobimo unikaten ključ, ki nam omogoča dostop do oddaljenega izvajalca. [7]

5.4 Implementacija pametne pogodbe

5.5 Razširitev KumuluzEE platforme za podporo decentraliziranim aplikacijam

5.5.1 Priprava aplikacije

V standardno KumuluzEE aplikacijo je potrebno vključiti razširitev *kumuluzdapi*. Razširitev ponuja nabor anotacij, s katerimi storitev bodisi registriramo v omrežje, bodisi določeno storitev poiščemo. Potrebna je še dopolnitev konfiguracijske datoteke, v kateri podamo dodatne informacije o naši storitvi. Ob zagonu storitve se preko anotacij poišče in registrira v omrežje. V glavno knjigo se zapišejo podatki o izvajani storitvi, izvajalcu ter naslov, na katerem je storitev dostopna.

Za odkrivanje storitev poskrbi razširitev, ki v glavni knjigi poišče izvajalce storitve, med njimi pa na podlagi izbranega algoritma za razporejanje bremena, izbere enega izmed izvajalcev in pridobi naslov, na katerem se storitev trenutno izvaja.

Razširitev obstoječe KumuluzEE konfiguracijske datoteke:

```
dapi:
  blockchain:
    host: naslov izvajalca
    account: /pot/do/datoteke
    password: geslo
  type: docker
  storage: ipfs
  api: rest
```

V konfiguraciji so predvidene tudi trenutno neuporabljene nastavitve za tip izvršljive datoteke, v kateri shrambi se storitev nahaja in tip aplikacijskega vmesnika. Trenutno sistem podpira le vsebnike Docker, ki jih je moč pridobiti preko omrežja IPFS, aplikacijski vmesnik pa je REST.

Poglavje 6

Delovanje in evalvacija

6.1 Demo aplikacija

Za namene demonstracije delovanja sistema sem implementiral dve preprosti REST storitvi. Prva se ob zagonu registrira kot izvajalec, druga ob zagonu poišče prvo in nam ob klicu storitve le posreduje podatke, ki jih pridobi od prve. Storitev ki se registrira v omrežje ima le eno izpostavljeno točko - seznam vseh uporabnikov. Podobno velja za drugo, ki prvo storitev kliče in nam podatke samo posreduje naprej.

6.2 Pomankljivosti trenutnega sistema in izboljšave v prihodnosti

Prva različica sistema ponuja kar nekaj možnosti za izboljšave. Prva izmed pomankljivosti je sama cena registracije in deregistracije storitev in njihovih izvajalcev. Vsaka registracija novega izvajalca pomeni nov zapis na podatkovno verigo, kar v dinamičnem sistemu in ob trenutnih cenah transakcije na Ethereum omrežju predstavlja potencialno veliko finančno breme za izvajalca. Zahtevnejša od prve je druga pomankljivost sistema in sicer deregistracija izvajalca. Brisanje podatkov iz podatkovne verige je nemogoče zaradi same zasnove tehnologije - nespremenljivost. S transakcijo je možno le navi-

dezno brisati - razveljaviti preteklo transakcijo, zapis pa na podatkovni verigi ostane. Brisanje je prav tako razmeroma draga operacija, posebno velik problem predstavlja brisanje izvajalca in s tem posledično še deregistracijo vseh storitev, ki jih je ta izvajalec v trenutku prekinitve izvajanja izvajal.

Dodatni mehanizmi, ki jih poznajo obstoječi sistemi za odkrivanje storitev, so še samodejna deregistracija storitve ob vnaprej določenem pretečenem času neaktivnosti. Trenutna implementacija tega mehanizma še ne pozna, problem predstavlja predvsem decentralizacija. V tem sistemu ne poznamo centralne storitve, ki bi ob določenem času iz registra preprosto brisala vse neaktivne storitve. Sistem potrebuje nov mehanizem, ki bo znal med storitvami poiskati neaktivne in jih odstraniti iz registra. Kakšen bo mehanizem in princip delovanja sta v tem trenutku neznanka.

Sistem potrebuje tudi način prerazporejanja zahtev po omrežju. Kdo izmed trenutno registriranih izvajalcev bo lahko najhitreje odgovoril? Hiter odgovor je pogojen s fizično oddaljenostjo gostitelja od izvajalca, omrežnimi zakasnitvami, hitrost samega izvajalca. Reševanje teh izzivov je naslednja v vrsti, ki jih predstavlja celostna postavitev, v praksi uporabnega, sistema.

Vsakega izvajalca storitve želimo za uspešno izveden klic ustrezno finančno nagraditi. Tu se poraja več vrst odprtih vprašanj, izstopa predvsem vprašanje finančne vrednosti posameznega klica in način preverjanja pravilnosti izvedbe klica. Je izvajalec dejansko pravilno izvedel zahtevano dejanje, tako kot je predvidel razvijalec in naročnik? Potreben je mehanizem, ki ga zaenkrat imenujmo „Proof of Execution“. Podobno kot trenutni mehanizmi „Proof of Work“, „Proof of Stake“ ter sorodni, ki jih uporabjajo decentralizirane podatkovne verige, potrebujemo mehanizem, preko katerega se bodo sodelujoče entitete v omrežju sposobne odločiti, ali je določen izvajalec pravilno izvedel zahtevano dejanje. S tem področjem se trenutno aktivno ukvarjajo tudi pri startupu SONM, ki objublja računsko moč na zahtevo v decentraliziranem okolju. Iz oblačnega računalništva želijo preiti na t.i. „računalniške storitve v megli“ (fog computing). [16]

Poglavje 7

Zaključek

Proof of Execution, Scheduling, naročila izvajanja in potek avkcij **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] Go ethereum. https://geth.ethereum.org/. Dostopano: 28. 06. 2018.

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

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

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

[6] IBM. What is cloud computing? Dosegljivo: https://www.ibm.com/cloud/learn/what-is-cloud-computing. Dostopano: 11. 07. 2018.

[7] Infura. https://infura.io/. Dostopano: 28. 06. 2018.

[8] Ipfs. https://ipfs.io/. Dostopano: 28. 06. 2018.

[9] Microservices: a definition of this new architectural term. Dosegljivo: https://martinfowler.com/articles/microservices.html. Dostopano: 11. 07. 2018.

[10] Pattern: Application metrics. http://microservices.io/patterns/observability/application-metrics.html. Dostopano: 28. 06. 2018.

[11] Pattern: Health check. Dosegljivo: http://microservices.io/patterns/observability/health-check-api.html. Dostopano: 04. 07. 2018.

[12] Pattern: Microservice Architevture. Dosegljivo: http://microservices.io/patterns/microservices.html. Dostopano: 11. 07. 2018.

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

[14] Pattern: Service discovery. Dosegljivo: https://www.nginx.com/blog/service-discovery-in-a-microservices-architecture/. Dostopano: 04. 07. 2018.

[15] Prometheus overview. https://prometheus.io/docs/introduction/overview/. Dostopano: 28. 06. 2018.

[16] Sonm. https://sonm.com/. Dostopano: 28. 06. 2018.

[17] The Linux Foundation. Cloud native computing foundation („cncf“) charter. Dosegljivo: https://www.cncf.io/about/charter/. Dostopano: 11. 07. 2018.

[18] Urban Malc. Zasnova in razvoj rešitve za dinamično odkrivanje mikrostoritev v oblačnih arhitekturah. Diplomska naloga, Fakulteta za in računalništvo in informatiko, Univerza v Ljubljani, 2017.