Prototipni IoT sistem s tehnologijo blokovnih verig Hyperledger Fabric

Gašper Pirnat[1], **doc. dr. Matevž Pustišek**[1]

[1] *Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, Ljubljana*
E-pošta: gp5302@student.uni-lj.si

Abstract

Abstract*.This paper presents a proof-of-concept IoT system based on the Hyperledger Fabric blockchain technology. As IoT systems governed by different entities are becoming ever more interconnected and complex, a need arises for trusted interoperability, transaction integrity and automation between such systems. In some cases, the use of blockchain technology can improve trust, device autonomy and ease automation and M2M communications. We created a proof-of-concept IoT system by adding low-cost Wi-Fi microchips ESP8266 to simple air quality sensors to give them Wi-Fi connectivity. These sensors then transmit their readings over an IP network to an edge gateway that can submit the data to the blockchain network, where it is then stored in the name of their respective organization. We conclude that such a system would be feasible and meaningful if it were deployed on a much larger scale with many more features, for example in a smart city.*

1 Uvod

Digitalizacija delovnih procesov v modernih časih s sabo prinaša željo po čim večji interoperabilnosti in avtomatiziranosti med digitalnimi sistemi. Zaradi te želje se je razvil sedaj že dobro poznan koncept interneta stvari. Ker postajajo sistemi interneta stvari, ki jih upravljajo različni subjekti vedno bolj medsebojno povezani in zapleteni, se pojavlja potreba po inherentno **zaupanja vredni** interoperabilnosti med takimi sistemi.

V nekaterih primerih lahko uporaba tehnologije veriženja blokov to omogoči, saj izboljša zaupanje in avtonomijo naprav ter poenostavi avtomatizacijo in komunikacijo stroj-stroj (M2M) [1]. Kot predstavitev ene izmed tehnologij za ustvarjanje omrežja ki uporablja veriženje blokov smo ustvarili konceptni sistem IoT tako, da smo našim senzorjem kakovosti zraka IKEA Vindriktning [2] dodali poceni mikročipe Wi-Fi ESP8266, da jim omogočimo Wi-Fi povezljivost. Ti senzorji nato prenesejo svoje odčitke prek IP protokola do robnega prehoda, ki jih v imenu svoje organizacije shrani v blokovno verigo.

Omrežje blokovnih verig je zgrajeno z tehnologijo Hyperledger Fabric, ki nam omogoča kontrolo nad tem kdo se lahko omrežju pridruži in tudi kaj lahko znotraj njega počne, kar nam da nekaj ključnih prednosti pred javnimi decentraliziranimi omrežji blokovnih verig, predvsem pa močno omili glavne slabosti decentraliziranih omrežij v kontekstu IoT uporabe, ohrani pa pomembnejše prednosti.

Tak sistem je zelo skalabilen in zato primeren za uporabo v industriji, pametnih mestih, logistiki oz. transportu ter podobnih področjih. V drugem poglavju je podrobnejša predstavitev tehnologije Hyperledger Fabric v primerjavi z bolj znanimi tehnologijami blokovnih verig, v tretjem je pa predstavljena izvedba IoT rešitve z Hyperledger Fabric tehnologijo.

2 Hyperledger Fabric

Hyperledger Fabric je tehnologija za vzpostavitev decentraliziranega konzorcijskega omrežja z omejenim dostopom[3]. Primarno je namenjeno uporabi, kjer si dve ali več organizacij želijo transparentno sodelovanje brez medsebojnega zaupanja. Podobno kot ostale tehnologije za decentralizirana omrežja omogoča hranjene za nazaj nespremenljivih porazdeljenih evidenc, ki so rezultat poljubno definiranih transakcij sredstev med entitetami različnih organizacij.

Hyperledger Fabric se razlikuje od večine drugih tehnologij blokovnih verig v tem da je omrežje ki ga z njim postavimo javnosti nedostopno, v njem lahko sodelujejo samo tisti ki so del konzorcija organizacij, ki so omrežje vzpostavile. Še več, vsak udeleženec ima tudi natančno predpisano vlogo v omrežju, ki omejuje kaj lahko sploh počne. S tem je odpravljena zahteva za protokole, kot je dokaz o delu (ang. proof-of-work) za potrditev transakcij, saj se člani takega omrežja včlanijo prek zaupanja vrednega ponudnika storitev članstva (ang. membership service provider, MSP), njihova identiteta je znana, morebitno škodoželjno delovanje pa je tako lahko kaznovano z izključitvijo iz omrežja in legalnimi posledicami.

Znotraj Hyperledger Fabric omrežja definiramo kanale, ki jih uporabljamo za logično ločitev procesov v omrežju. V omrežju imamo lahko poljubno število kanalov. So ključni za delovanje omrežja, saj se porazdeljena evidenca ustvari znotraj kanala in je tako vidna samo udeležencem kanala. To je posebej pomembno za omrežja, v katerih imamo konkurente, ki si ne želijo, da bi bila vsaka njihova transakcija znana vsem v omrežju. Prednost take strukture je tudi povečana varnost.

2.1 Hyperledger Fabric elementi

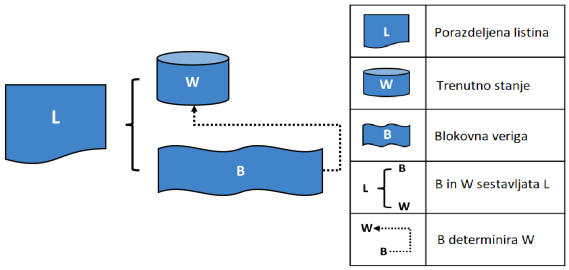
Naslednje sekcije predstavljajo ključne komponente za sestavo in delovanje Hyperledger Fabric omrežja.

2.1.1 Sredstva

Sredstva, s katerimi poslujemo, so lahko opredmetena (premičnine in nepremičnine) ali neopredmetena (intelektualna lastnina, pogodbe, ipd.). Hyperledger Fabric omogoča spreminjanje lastnikov ali pa lastnosti sredstev z uporabo pametnih pogodb. Sredstva so v Hyperledger Fabric predstavljena kot zbirka parov ključ-vrednost v binarni obliki ali obliki JSON, spremembe stanja pa so zabeležene kot transakcije v blokovni verigi.

2.1.2 Porazdeljene evidence

V porazdeljeni evidenci je zaporedni zapis vseh prehodov stanj oziroma transakcij, ki je odporen proti spreminjanju za nazaj. Prehodi med stanji so rezultat klicev pametnih pogodb. Rezultat vsakega klica je niz parov ključ-vrednost, ki se vnese v evidenco kot ustvaritev, posodobitev ali izbris nekega sredstva.



Slika 1: Diagram porazdeljene evidence: [4]

Porazdeljeno evidenco sestavlja blokovna veriga v katero shranjujemo transakcije ter podatkovna zbirka v obliki relacijske baze, ki odraža trenutno stanje sredstev, kot posledico vseh preteklih transakcij. Podatkovna zbirka nam omogoča, da na hiter in enostaven način pridobimo vpogled v trenutno stanje nekega sredstva brez da bi morali po blokovni verigi iskati zadnjo transakcijo, ki vključuje to sredstvo. Na kanal je ena porazdeljena evidenca, vsak sodelujoč pa vzdržuje kopijo za vsak kanal, katerega član je.

2.1.3 Pametne pogodbe

Pametne pogodbe so programska oprema, ki opredeljujejo navodila transakcij za branje, spreminjanje ali ustvarjanje sredstev. Omogočajo deterministično izvedbo poslovne logike, ki se hkrati zapiše tudi v blokovno verigo. Verižna koda uveljavlja pravila za branje ali spreminjanje parov ključ-vrednost ali drugih informacij v podatkovni zbirki stanja. Pametne pogodbe se izvajajo proti trenutnemu stanju porazdeljenih evidenc in se sprožijo s predlogom transakcije. Rezultat izvajanja je niz zapisov ključ-vrednost, ki se pošlje v omrežje in zapiše v porazdeljeno evidenco.

2.1.4 Kanali in zasebnost

Kot že omenjeno, Hyperledger Fabric uporablja porazdeljene evidence po posameznih kanalih. Če imamo v omrežju samo en kanal, to pomeni da se porazdeljena evidenca efektivno deli po celotnem omrežju.

Kanal je v nekem omrežju ustvarjen tako, da se več organizacij med seboj domeni o konfiguraciji kanala. Konfiguracija kanala določa katere organizacije so članice kanala, kdo so vozlišča in kaj bo njihova vloga, pravila za dodajanje in izvajanje pametnih pogodb pa tudi pogoje za spremembe nastavitev kanala. Vsaka organizacija to konfiguracijo digitalno podpiše, nato pa se shrani v prvi blok verige. Če posodobitev kanala odobri zadostno število organizacij, oziroma če je zadoščeno pogojem za spremembo konfiguracije, se nova konfiguracija doda v nov blok v verigi in od takrat naprej velja ta konfiguracija kanala. Upošteva se torej konfiguracijo, ki je bila dodana zadnja v verigo.

2.1.5 Konsenz in vozlišča

Do sedaj so bile predstavljene funkcionalnosti Hyperledger Fabric omrežja, niso pa bili še predstavljeni mehanizmi in strukture za doseganje teh funkcionalnosti. Za obstoj porazdeljenih evidenc moramo seveda imeti neke osebke katerim te evidence sploh porazdelimo, prav tako potrebujemo osebke, ki bodo izvajali pametne pogodbe. Tej osebki pa morejo tudi nujno imeti nek mehanizem za doseganje konsenza o posodobitvah porazdeljene listine z transakcijami in v kakšnem vrstnem redu se bodo transakcije oz. spremembe zapisovale.

Za dosego teh ciljev se uporabljajo dve vrsti vozlišč. Na splošno so vozlišča entitete, ki imajo pooblastilo svojih organizacij, da v njihovem imenu sprejemajo konsenz za posodobitev porazdeljenih listin, izvajajo pametne pogodbe ter določajo vrstni red posodobitev.

Odgovornost za sprejem konsenza za posodobitev listin in izvajanje pametnih pogodb prevzamejo vrstniška vozlišča. Da lahko opravlja to delo mora hraniti kopijo porazdeljene listine ter kodo pametnih pogodb. Ker pa je gostitelj teh storitev morajo vse aplikacije in skrbniki omrežja za dejansko interakcijo z omrežjem uporabljati vrstniška vozlišča.

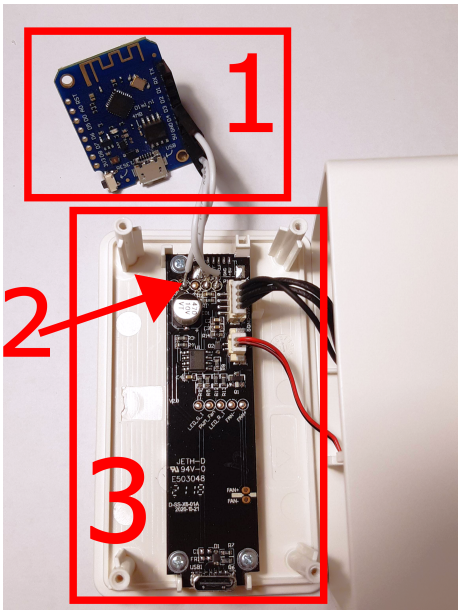
Druga vrsta vozlišč so urejevalna vozlišče. Naloga teh vozlišč je, da sprejemajo v obdelavo transakcije, ki jih prejemajo od udeležencev v omrežju. Preveriti morajo ali imajo zadostno število podpisov vrstniških vozlišč ter določiti v kakšnem vrstnem redu bodo zapisane v blokovno verigo. Nato več obdelanih transakcij zapiše v blok, ki ga porazdeli med vsa vrstniška vozlišča v omrežju. Tako imajo vsa vrstniška vozlišča v svojih porazdeljenih listinah zapisane ne le vse transakcije, vendar so tudi v enakem vrstnem redu.

Poleg številnih preverjanj veljavnosti transakcij ki se izvajajo, se v vseh smereh toka transakcij izvajajo tudi stalna preverjanja identitete. Vsako vozlišče ki prejme neko transakcijo v pregled za odobritev preveri identitete vseh ostalih vozlišč ki so transakcijo že odobrile.

2.1.6 *Identifikacija in preverjanje istovetnosti*

Za varno delovanje vseh do sedaj opisanih elementov moramo nujno imeti mehanizme, ki omogočajo identifikacijo akterjev v omrežju in preverjanje njihove istovetnosti. V nasprotnem primeru bi lahko prišlo do nelegitimnih dogodkov v omrežju kot so ponarejanje identitete, onemogočanje storitev, sprejemanja lažnih podatkov in podobno.

Ker je Hyperledger Fabric po naravi zaprt sistem in je anonimnost nezaželena za razliko od javnih decentraliziranih tehnologij, je ta problematika rešena na preprost način z uporabo organov za overjanje certifikatov (ang. certificate authority, CA). Vsaka organizacija ima svojo identiteto registrirano pri izbranem organu za overjanje. Z uporabo te identitete lahko potem izdaja dodatne identitete osebkom, ki v omrežju delujejo v imenu organizacije. Pomembno je omeniti tudi, da je v sklopu identitete ki je izdana osebkom določena tudi vloga, ki jo bo osebek imel v omrežju. Te vloge so zapisane v konfiguracijskem bloku kanala in natančno določajo kaj lahko osebek v omrežju počne.



Slika 2: 1: Wemos D1 mini, 2: Testna točka, 3: Vezje izdelka

3 Prototipni IoT sistem

Prototipni IoT sistem je bil sestavljen z namenom preizkusa Hyperledger Fabric tehnologije. Ključno je bilo, da koristi večino funkcionalnosti Hyperledger Fabric tehnologije, saj lahko le tako naredimo sistem, ki je reprezentativen produkcijski uporabi. V ta namen smo vzpostavili omrežje v katerem sodeluje več organizacij, vsaka s svojimi IoT napravami. Tako smo lahko preizkusili postavljanje omrežja, ustvarjanje kanalov in določanje vlog, izvajanje pametnih pogodb, doseganje konsenza ter posodabljanje porazdeljene listine.

V ta namen smo predelali več komercialnih izdelkov za merjenje kvalitete zraka IKEA Vindriktning tako, da smo jim dodali mikročip, ki omogoča brezžično povezljivost. Vsak senzor pripada eni izmed organizacij in je vir informacij, ki se zapisujejo v porazdeljeno listino.

3.1 Izdelava IoT naprav

Uporabljen izdelek s senzorjem za kvaliteto zraka je IKEA Vindriktning. Sestavljen je iz Cubic PM1006 senzorja za trde delce PM2.5, ventilatorja in mikrokontrolerja Eastsoft ES7P001FGS, ki kontrolira ventilator in odčitava vrednosti s senzorja.

Na sliki 2 lahko vidimo označeno vezje izdelka, ki omogoča direktno branje senzorskih odčitkov preko testne točke. Na to točko smo povezali Wemos D1 mini mikročip, prav tako smo ga povezali na GND in 5V priključke, da smo omogočili napajanje in prenos podatkov. Na Wemos D1 mini smo naložili preprosto kodo, ki bere senzorske podatke ter jih preko lokalnega Wi-Fi omrežja preko UDP protokola dostavi na robni prehod, ki je povezan v Hyperledger fabric omrežje.

3.2 Vzpostavitev IoT sistema s Hyperledger Fabric tehnologijo/orodji

Za vzpostavitev sistema nam Hyperledger Fabric nudi na voljo binarne programe, ki izvajajo vlogo vozlišč, na voljo pa so tudi binarni programi, ki ob izvajanju lahko delujejo kot organi za izdajanje identitet. Priporočeno je, da jih izvajamo v Docker zabojnikih, saj nam to omogoči, da jih na preprost način konfiguriramo in vzpostavimo povezave le teh preko različnih gostiteljev in omrežij. Takšnega pristopa smo se poslužili tudi mi, saj nam je omogočil preprosto testiranje komunikacije med vozlišči ki so delovala v različnih omrežjih in na različnih računalnikih.

Prvi korak pri vzpostavljanju delujočega sistema je bil generiranje identitet za vsako od organizacij in njenih predstavnikov, ki bodo delovali v sistemu. To smo storili z orodjem Cryptogen, ki je priloženo v nabor Hyperledger Fabric orodij in je namenjeno za uporabo v testnih okoljih. Omogoča nam generiranje asimetričnih parov ključev, ki jih lahko uporabimo za identiteto osebkov ali pa za enkripcijo medsebojne komunikacije preko TLS protokola. V našem primeru smo ustvarili tri organizacije, od tega sta dve v omrežje dodajali podatke iz IoT senzorjev, vsaka preko svojega vrstniškega vozlišča, tretja pa je prevzela odgovornost za urejevalno vozlišče, ki je koordiniralo konsenz med prvima dvema. Za organizaciji, ki v omrežje dodajata podatke smo ustvarili identiteti katerim smo pripisali vlogo vrstniških vozlišč. Prav tako smo ustvarili še identiteto z vlogo urejevalnega vozlišča, ki je pripadalo tretji organizaciji.

V logičnem smislu sedaj obstajajo vsi potrebni akterji za vzpostavitev sistema, med seboj se lahko tudi zanesljivo identificirajo, saj organizacije izmenjajo javne ključe svojih identitet izven sistema, ki ga želijo vzpostavit, prav tako pa je komunikacija v sistemu šifrirana z uporabo TLS protokola.

Naslednji korak je bil zagon vozlišč v Docker zabojnikih, ki bodo izvajala naloge svojih organizacij v omrežju. Vsakemu smo morali podati primerne certifikate s katerimi se je lahko v omrežju identificiral in overjal identitete ostalih vozlišč.V produkcijskih sistemih ta pristop ne

bi bil primeren, saj zmanjšuje varnost in otežuje razveljavljanje identitet. V takih sistemih bi morali obvezno uporabiti organe za certificiranje identitet, katere bi vozlišča uporabljala za periodično preverjanje identitet osebkov s katerimi komunicira. Dodajamo še, da Hyperledger Fabric ponuja orodje za ustvarjanje organov za certificiranje identitet, lahko pa bi uporabljali tudi komercialne rešitve.

Ko smo postavili vozlišča in je komunikacija med njimi bila zavarovana in verificirana smo lahko pričeli z genezo decentraliziranega omrežja za naš sistem. Pri tem je prvi korak bil ustvarjanje konfiguracijske datoteke, ki je določila vloge in pravila delovanja na kanalu. O vsebini te datoteke se organizacije pomenijo preden sploh pride do tehnološke izvedbe, zato jo načeloma lahko ima vsako vozlišče že ob sami vzpostavitvi. Vsako vozlišče je to datoteko digitalno podpisalo, za dodajanje v porazdeljeno listino pa je poskrbelo urejevalno vozlišče, ki je z uporabo RAFT protokola[5] zapisalo konfiguracijo v blokovno verigo in poskrbelo, da je vsem porazdeljena enaka verzija. V tem trenutku je bil kanal logično ustvarjen, prav tako porazdeljena evidenca saj so imeli vsi enako konfiguracijsko datoteko iz katere so lahko ustvarili prvi blok v blokovni verigi.

3.3 Uvedba IoT naprav v omrežje preko pametnih pogodb

Za uvedbo IoT naprav v omrežje smo morali najprej namestiti našo pametno pogodbo na vsa vrstniška vozlišča, saj smo tako določili v konfiguraciji kanala. Lahko bi se tudi odločili za pristop kjer je potrebno da ima pametno pogodbo samo polovica vozlišč, v našem primeru bi to bilo samo 1 vozlišče, vendar bi to pomenilo da za sprejem transakcij ne bi potrebovali potrditev še drugega vozlišča. V pametni pogodbi so bile funkcije, ki so določale kako se bo izpis iz senzorjev zapisoval v porazdeljeno listino. Zapisovale so se identifikacijske številke IoT naprav skupaj s trenutnim odčitkom vrednosti na senzorju v obliki ključ-vrednost.

Nato smo v JavaScript-u napisali še aplikacijo, ki je delovala kot posrednik med IoT senzorjem in vrstniškim vozliščem. Aplikaciji smo morali ustvariti identiteto, ki je pripadala eni izmed organizacij, saj je to pogoj, da vozlišča sprejmejo predloge transakcij v obdelavo. Na omrežju kjer je delovala IoT naprava je poslušala za UDP promet na določenih vratih nato pa je iz vsebine sporočil ustvarjala predloge transakcij, ki jih je poslala v podpis obema vrstniškima vozliščema nato pa še urejevalnemu vozlišču, ki je poskrbel da se je transakcija zapisala v porazdeljeno listino.

Sistem je v tej točki bil vzpostavljen in delujoč. Podatke ki so prihajali s senzorjev je sistem obdeloval in zapisoval v porazdeljene listine, pri tem pa uporabljal vse mehanizme, ki bi se uporabljali v produkcijskem sistemu.

4 Zaključek

Pri vzpostavitvi IoT sistema s Hyperledger Fabric tehnologijo smo preverili sestavne dele in njihovo učinkovitost. Ugotovili smo, da je sistem v smislu obdelovanja transakcij zelo učinkovit, saj za doseganje konsenza uporablja v osnovi digitalno podpisovanje transakcij, za distribucijo podatkov pa etcd[6], ki uporablja učinkovit RAFT algoritem. Sam sistem ne doda računskega bremena na IoT naprave, razen če se za to odločimo, zato je primeren za uporabo tudi v primeru nizko zmogljivih baterijskih IoT naprav. Sama postavitev omrežja je odvisna od želene uporabe in je zelo prilagodljiva. Celotno omrežje je lahko postavljeno in deluje v megli (ang. fog computing) na nizkocenovnih napravah kot so Raspberry Pi, kar nam omogoča lokalizirane sisteme, ki ne zahtevajo komunikacije z oddaljenimi strežniki v oblaku.

Mehanizmi, ki sistemu postavljenim s Hyperledger Fabric tehnologijo dajejo prednosti pa istočasno povzročajo tudi slabosti. Tak sistem ni zelo odporen na zlonamerno delovanje udeležencev, saj mehanizmi sistema tega ne omogočajo. Škodoželjen udeleženec lahko zavira sprejemanje konsenza, ustvarja neveljavne transakcije in onemogoča storitve. Ob takih primerih morajo ostali udeleženci identificirati in izločiti take udeležence iz sistema. Ker pa je namenjena uporaba Hyperledger Fabric tehnologije v sistemih, kjer imamo možnost in ponavadi tudi zahtevamo, da se vsak udeleženec pravno identificira, njegova identiteta pa je vezana na njegovo delovanje v sistemu to pomeni da za razliko od javnih decentraliziranih omrežij lahko take udeležence veliko enostavneje pravno kaznujemo.

Literatura

[1] Andrej Kos, Natasa Zivic, Matevz Pustisek: Blockchain: Technology and Applications for Industry 4.0, Smart Energy, and Smart Cities

[2] IKEA Vindriktning, https://www.ikea.com/si/sl/p/vindriktning-senzor-kakovosti-zraka-80515910/

[3] Androulaki, Elli and Barger, Artem and Bortnikov, Vita and Cachin, Christian and Christidis, Konstantinos and De Caro, Angelo and Enyeart, David and Ferris, Christopher and Laventman, Gennady and Manevich, Yacov and Muralidharan, Srinivasan and Murthy, Chet and Nguyen, Binh and Sethi, Manish and Singh, Gari and Smith, Keith and Sorniotti, Alessandro and Stathakopoulou, Chrysoula and Vukolić, Marko and Cocco, Sharon Weed and Yellick, Jason:Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, 2018, Association for Computing Machinery

[4] https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

[5] RAFT, https://raft.github.io/

[6] etcd, https://etcd.io/