Premagovanje izzivov hranjenja podatkov v verigi blokov

Mitja Gradišnik,[1] Daniel Copot,[2] Martin Domajnko,[1] Muhamed Turkanović[1]

[1] Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
mitja.gradisnik@um.si, martin.domajnko@student.um.si, muhamed.turkanovic@um.si
[2] ITC - Inovacijsko tehnološki grozd, Murska Sobota, Slovenija
daniel.copot@itc-cluster.com

Hiter razvoj na področju tehnologij veriženja blokov prinaša številne možnosti inovacij in vpeljave novih poslovnih modelov. Vpeljava hranjenja podatkov v verige blokov v poslovna okolja prinaša predvsem transparentnost podatkov, integriteto, boljšo dostopnost, varnost in možnost decentraliziranega upravljanje podatkov. Vpeljava hranjenja podatkov v verige blogov prinaša s seboj tudi številne inženirske izzive, ki jih je potrebno nasloviti v okviru razvojnega procesa tovrstnih rešitev. Namen prispevka je snovalcem tovrstnih programskih rešitev predstaviti nabor inženirskih pristopov, ki jih je smiselno vzeti v obzir pri analizi, načrtovanju, vrednotenju ali preoblikovanju na verigah blokov temelječih programskih rešitev. V prispevku povzamemo ključne inženirske izzive razvoja tovrstnih informacijskih rešitev ter predstavimo nekatere praktične rešitve za predstavljene izzive. V prispevku izpostavimo izzive in rešitve vpeljave verig blokov na performančne lastnosti in skalabilnost programskih rešitev. V primerjavi z dostopnimi časi podatkovnih baz se izvršitve transakcij in povpraševanj pri obdelavi podatkov zapisanih v verigah blokov soočajo tudi z višjimi latentnimi časi. Ti izhajajo iz razpršenosti podatkov med bloki, omejitve velikosti blokov in konstantnega preverjanje integritete zapisanih podatkov. Nenazadnje je pri arhitekturnem načrtovanju potrebno vzeti v obzir, da so v verige blokov zapisani podatki nespremenljivi, kar pogosto trči ob temeljno potrebo programske rešitve po njeni evoluciji.

Ključne besede:
tehnologije veriženja blokov,
arhitekturne taktike,
kratke oskrbovalne verige
programsko inženirstvo
prilagoditev razvojnih metod

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-894-9
DOI https://doi.org/10.18690/um.feri.4.2024.10

1 Hramba podatkov v poslovnih okoljih

Podatkovne baze, med katerimi gre v prvi vrsti izpostaviti predvsem relacijske baze, so bile desetletja hrbtenica hranjenja podatkov v poslovnih programskih rešitvah. Podatkovne baze se v osnovi zanašajo na centralizirano arhitekturo, pri čemer so podatki hranjeni v tabelaričnih strukturah s predhodno definiranimi medsebojnimi odvisnostmi [2]. Desetletja razvoja podatkovnih baz so pripeljala do rešitev, ki se ponašajo z nizkimi zakasnitvami, visoko prepustnostjo transakcij in visoko kapaciteto hranjenja podatkov [1]. Vzporedno s tradicionalnimi podatkovnimi bazami so se v zadnjih desetletjih bliskovito razvijale ne-relacijske podatkovne baze (t. i. NoSQL) ter v zadnjem obdobju tudi tehnologije veriženja blokov. Slednje zraven porazdeljenega vpeljejo tudi decentraliziran pristop hrambe podatkov in upravljanja podatkovne baze. Primerjano s tradicionalnimi podatkovnimi bazami tehnologije veriženja blokov ubirajo povsem različen in edinstven pristop k hranjenju podatkov [2]. Razumevanje razlik s tradicionalnimi podatkovnimi bazami je ključno za načrtovanje in vzdrževanje programskih rešitev, ki vpeljujejo uporabo tehnologijo veriženja blokov.

1.1. (Tradicionalne) podatkovne baze

Arhitektura tradicionalnih podatkovnih baz je zasnovana po pristopu odjemalec – strežnik. To velja tako za relacijske kot ne-relacijske podatkovne baze (t. i. NoSQL). Podatki so praviloma hranjeni na centraliziranem strežniku, na katerega odjemalci pošiljajo poizvedbe. Ključna značilnost tradicionalnih podatkovnih baz je sposobnost odjemalcev, da vstavljene podatke kasneje poljubno spreminjajo ali celo izbrišejo [3]. Odjemalci so neposredno različne programske rešitve ter posredno njihovi uporabniki. Upravljanje podatkovne baze ohranja vrhnja avtoriteta, ki je podatkovno bazo vzpostavila. Ta ves čas ohranjajo nadzor nad strukturo in obliko podatkov in odjemalcem podeljuje dostope do upravljanja podatkov (ne tudi strukture) v podatkovni bazi. Podatkovna baza je sicer lahko tudi porazdeljena med številne strežnike oz. vozlišča, vendar je kljub temu ena vrhnja entiteta, ki nadzira vsako posamezno vozlišče [1]. Tradicionalna podatkovna baza ima torej v praksi skoraj vedno skrbnika, ki nad njo ohranja nadzor, vključno z upravljanjem podatkov, spreminjanjem strukture in optimizacijo [4]. Prisotnost takšne vrhnje avtoritete pri upravljanju podatkovne baze tako zahteva zaupanje odjemalcev, da ta podatkov ne spreminja zlonamerno. Pomembna značilnost podatkovnih baze je njihova zaprtost znotraj okvirjev organizacij. Ni običajna praksa, da bi si deležniki podatkovne baze delili in tako soustvarjali podatke.

1.2. Hramba podatkov v verige blokov

Arhitekturna zasnova podatkovne shrambe, ki temelji na tehnologijah veriženja blokov, je poglavitno različna od prej predstavljene arhitekture tradicionalnih podatkovnih baz. Osrednja komponenta tehnologije je t. i. glavna knjiga (angl. ledger), ki predstavlja porazdeljeno podatkovno hrambo v katero se zapisujejo transakcije iz P2P omrežja medsebojno povezanih računalnikov [2]. V veliki večini je osnova za takšno hrambo ravno NoSQL podatkovna baza, kot npr. LevelDB [5]. Iz decentraliziranost in porazdeljenosti glavne knjige izhaja, da vsa vozlišča v omrežju hranijo sinhrone kopije vseh zapisanih podatkov.

Podatki se na vozliščih hranijo v skupkih transakcij imenovanih bloki, ki so enovite velikosti [4], pri čemer v blok zapisana zgoščevalna vrednost predhodnega bloka zagotavlja varnost podatkov pred zlonamernimi spremembami. Poglavitna sprememba v primerjavi s podatkovnim bazami predstavlja način dela s podatki. Verige blokov namreč dovoljujejo izključno vstavljanje in dodajanje podatkov, ne pa tudi njihovega spreminjanja ali brisanja. Podatki zapisani v verige blokov so torej v praksi nespremenljivi [6]. Iz navedene lastnosti izhaja možnost visoke stopnje zaupanja odjemalcev v zapisane podatke, saj je kasnejša manipulacija podatkov izjemno malo verjetna.

Podatki hranjeni v verigah blokov za zapisani v več porazdeljenih vozliščih, pri čemer vsako izmed vozlišč aktivno sodeluje pri upravljanju podatkovne zbirke preko verifikacije vstavljanja novih podatkov. Slednje vozlišča izvedejo preko mehanizma doseganja porazdeljenega soglasja [3]. Ravno mehanizem doseganja soglasja, ki je nujen zaradi

decentraliziranosti omrežja, predstavlja steber varnosti omrežja, ki oteži neželene posege v podatke zlonamernih vozlišč. Ker so podatki podvojeno zapisani na več fizičnih lokacijah, zapisi ne pripadajo posamezni entiteti v omrežju temveč so last vseh deležnikov.

Izpostaviti je potrebno tudi ključno dejstvo, da koncept tehnologije veriženja blokov pade v vodo, če nimamo decentraliziranega omrežja, saj bi v nasprotnem primeru imeli zgolj porazdeljeno podatkovno bazo, katere vozlišča so pod nadzorom ene vrhnje avtoritete. Četudi nesmiselna se takšna omrežja verig blokov v literaturi imenujejo zasebna omrežja. Takšna omrežja ohranjajo vso kompleksnost tehnologije veriženja blokov, ki stremi k zagotavljanju varnosti, transparentnosti in nespremenljivosti, pri čemer pa se vse to lahko preprosto zaobide s strani vrhnje avtoritete. Ne glede na to pa obstajajo t. i. zasebna omrežja verig blokov, kjer pa vozlišča niso pod nadzorom ene vrhnje avtoritete, temveč več različnih. V tem primeru imamo decentralizirano omrežje, ki pa ni javno dostopno, temveč je pod nadzorom peščice entitet, katere same vzdržujejo omrežje in definirajo pravila igre ter s tem tudi način doseganja porazdeljenega soglasja. Takšna omrežja imenujemo konzorcijska in se največkrat pojavijo v informacijskih rešitvah. Primarni tip omrežij verig blokov pa so t. i. javna omrežja brez dovoljenja (angl. permissionless), ki predstavljajo omrežja v katero so lahko pridruži kdor koli in s tem postane del številnih decentraliziranih vozlišč, ki skupaj vzdržujejo omrežje ter skupaj dosegajo porazdeljeno soglasje glede vsebine glavne knjige.

Avtonomnost verig blokov naredi korak naprej z vpeljavo pametnih pogodb, ki na podlagi soglasja med vozlišči in vnaprej kodirane poslovne logike avtonomno izvedejo vstavljanje zapisov v verige blokov [7]. Slednje daje dodatne možnosti za inovativne programske rešitve. Vpeljava tehnologij veriženja blokov v informacijske rešitve torej vpelje podatkovno shrambo, ki je robustna iz vidika centralne točke odpovedi in prav tako relativno dobro odporna na zlonamerno spreminjanje zapisanih podatkov [4], [7].

Hramba podatkov v verige blokov se od hrambe v podatkovne baze loči po štirih ključnih parametrih. In sicer dosežena stopnja podatkovne integritete, izvajanje transakcij, učinkovitost povpraševanj in strukture. Od navedenih razlik je odvisno, kdaj je kateri izmed primerjanih pristopov primernejši za integracijo v informacijsko rešitev. Razlike med primerjanima pristopoma hrambe podatkov prikazuje Slika [8]. Pri podatkovni integriteti pa je potrebno izpostaviti še dejstvo, da se v verigah blokov vsaka posamezna transakcija pred procesiranjem digitalno podpiše s strani končnih uporabnikov informacijskih rešitev, za razliko od tradicionalnih podatkovnih baz, kjer tega nismo vajeni, saj so odjemalci tisti, ki na zahtevo svojih uporabnikov podatke pripravijo in posredujejo do strežnika podatkovne baze. S tega vidika lahko izpostavimo tudi, da so v primeru verig blokov odjemalci praviloma digitalne denarnice končnih uporabnikov, ki lahko digitalno podpisane transakcije prožijo neposredno na katerokoli vozlišče omrežja verig blokov.

Slika 1: Primerjava verig blokov in podatkovnih baz.

1.3. Lastnosti tehnologij veriženja blokov

Prepoznane prednosti in lastnosti tehnologij veriženja bloka so gonilo potrebe po njihovi integraciji v sodobne informacijske rešitve. Čeprav gre v osnovi za podatkovne shrambe, so lastnosti verig blokov takšne, da jim dajejo edinstvenost in nezamenljivost z drugimi pristopi hrambe podatkov. V praksi to pomeni, da bi s tradicionalnimi podatkovnimi bazami izredno težko, če ne že nemogoče, realizirali številne poslovne scenarije, ki jih tehnologije veriženja blokov omogočajo. Poglavitne lastnosti verig blokov so nespremenljivost zapisov, transparentnost podatkov, decentraliziranost, nadzor deležnikov nad lastnimi zapisi in varnost zapisanih podatkov [9].

1.3.1. Nespremenljivost zapisov

Verige blokov omogočajo izključno vstavljanje oz. pripenjanje novih podatkov. Ker manipulacija že zapisanih podatkov ni podprta, bi vsak poskus spreminjanja ob sprejetih varnostnih mehanizmih izredno težko izpeljali. Za slednje poskrbijo zapisane zgoščevalne vrednosti posameznega bloka, ki poskrbijo za integriteto in nespremenljivost zapisov celotne podatkovne zbirke in mehanizmi sprejemanja soglasja pri zapisovanju blokov. Nepremenljivost zapisanih podatkov postavlja temelj zaupanju deležnikov v zapise, saj je enkrat zapisane podatke na nivoju verig blokov nemogoče manipulirati ali kasneje zanikati njihov obstoj. Prav tako lahko vsak deležnik v vsakem trenutku preveri integriteto zapisanih podatkov.

1.3.2. Transparentnost podatkov

Za razliko od centraliziranih podatkovnih baz poseduje pri verigah blokov vsako izmed vozlišč omrežja popolno kopijo celotne podatkovne zbirke. Te podatkovne zbirke prav tako niso zamejene znotraj organizacij, temveč so med deležniki deljene. Slednje daje kateremukoli soudeležencu v omrežju vpogled v zapise vseh udeležencev v omrežju, kar omogoča učinkovito soustvarjanje zapisov med deležniki. Interakcijo med udeleženci je torej neposredna, prav tako omogoča hitro razreševanje nejasnosti povezanih s transakcijami v omrežju [10]. Možnost soustvarjanja podatkov odpira dodatne možnosti postavitve temeljev za nova medorganizacijska sodelovanja ter vzpostavitve skupnosti deležnikov, ki delajo na skupnih podatkih.

1.3.3. Decentraliziranost

Decentraliziranost predstavlja eno izmed ključnih lastnosti podatkovnih zbirk, ki temeljijo na tehnologijah veriženja blokov. V praksi decentraliziranost pomeni odsotnost vrhnje avtoritete, ki bi upravljala podatkovno zbirko. Nadzor nad podatkovnimi zbirkami zapisanih v verige blokov je tako porazdeljena med vsa vozlišča omrežja in se uveljavlja preko izbranega mehanizma soglasja. Odsotnost osredne avtoritete nadzora omogoča dinamičnost pri dodajanju in odstranjevanju vozlišč v omrežju, ki sodelujejo pri soustvarjanju zapisov brez potrebe po centralizirani administraciji. Navedena lastnost je temelj ustvarjanju skupnosti akterjev, ki sodelujejo v skupnih procesih, brez potrebe, da bi si ti med seboj zaupali.

1.3.4. Zapisi nadzorovani s strani lastnikov

Ker verige blokov ne poznajo administracije podatkovne zbirke in upravljanja dostopov do nje, je upravljanje zapisov prepuščeno lastnikom zapisov samim. V praksi to pomeni, da niti upravljalcem vozlišč posegi v podatke na vozlišču niso dovoljeni. Lastništvo v celoti pripada zapisovalcem, ki pa lahko lastništvo prenese na katerega izmed preostalih deležnikov v omrežju. Navedena lastnost daje temelje ustvarjanju digitalnih sredstev (ang. asset), ki jih je mogoče prosto prenašati med deležniki. Pojem digitalnih sredstev je v tem kontekstu razumljen kot digitalna reprezentacija bodisi realnih bodisi virtualnih dobrih, lastništvo katerih je med akterji prenosljivo. Primeri takšnih dobrin so digitalni denar, kmetijski pridelki ali zdravila. Seveda imajo možnost prenosov sredstev zgolj njihovi lastniki, ki lastništvo izkažejo z ustreznim naborom privatnih ključev.

1.3.5. Varnost in zasebnost podatkov

Uporaba ustreznih kriptografskih algoritmov poskrbi, da so podatkovne zbirke na visokem nivoju zaščitene pred nepooblaščenimi dostopi ali celo nepooblaščenimi spremembami. Navedene lastnost dela podatkovne zbirke zapisane v verige blokov primerne tudi za programske rešitve, ki terjajo visoko stopnjo varnosti. Čeprav so verige blokov v veliki večini primerov javne oz. dostopne širšemu krogu deležnikov, je mogoče z ustreznimi kriptografskimi metodami doseči popolno zasebnost zapisov.

2 Vpliv tehnologij veriženja blokov na inovacije

Lastnosti informacijskih rešitev, ki temeljijo na tehnologijah veriženja blokov, odpirajo številne možnosti za inovacije in nove poslovne modele, ki izkoriščajo nespremenljivost in preverljivost zapisanih podatkov v skupni podatkovni shrambi. Vpeljava tehnologij veriženja blokov v organizacije tako ustvarja okolja, v katerih je različnim deležnikom omogočeno varno soustvarjanje skupnih podatkov, brez potrebe po revizijah in avtorizacijah s strani tretjih oseb [11]. Tehnologije veriženja blokov morda primarno povezujemo s finančnim sektorjem, ki na tem področju ponuja rešitve za P2P plačilne sisteme, P2P posojila in sisteme za prenos premoženja [12]. Ob boku finančnega sektorja so tehnologij veriženja blokov dosegle pomembno uveljavitev na področjih zavarovalništva, zdravstvenega varstva, izobraževanja, upravljanja, upravljanja z intelektualno lastnino in oskrbovalnih verig [1], [10]. Tehnologije veriženja blokov so pomemben katalizator inovacij v domenah, ki so sposobne v svojih poslovnih procesih izkoristiti prednosti nespremenljivosti, sledljivosti, transparentnosti, varnosti in robustnosti skupnih podatkov [11].

2.1. Oskrbovalne verige

Pomembna domena, na katerega so tehnologije veriženja blokov naredile v zadnjih letih pomemben vpliv, je domena oskrbovalnih verig. Na področju oskrbovalnih verig je potrebno izpostaviti predvsem vpeljavo rešitev za sledenje zdravil v oskrbovalnih verigah, sledenje produktom z višjo vrednostjo in sledenju živilskih izdelkom tekom prehranske verige [1], [13], [14], [15]. Sledenje produktov v oskrbovalnih veriga običajno poteka od proizvodnje, preko distributerjev in posrednikov, do končnih kupcev. Neglede na vrsto produktov, ki se prenašajo po oskrbovalni verigi, npr. zdravila, izdelki z višjo vrednostjo ali prehranski izdelki, je vsem rešitvam skupno to, da izkoriščajo možnost necentraliziranega sodelovanja različnih deležnikov oskrbovalnih verig, da ustvarijo transparentne, sledljive, varne in preverljive zapise o stanju produktov v posameznem členu oskrbovalne verige. V praksi to pomeni, da deležniki v oskrbovalnih verigah ustvarijo skupnost, znotraj katere soustvarjajo zapise o kakovosti produktov z namenom ustvarjanja zaupanja končnih potrošnikov v deklarirano kakovost produkta. Z inovacijami v programskih rešitvah, podprtimi s tehnologijami veriženja blokov, se cilja na zmanjševanje poneverbe, zavajanj in drugih zlorab zaupanja povezanih s kakovostjo produkta povezanih trditev.

2.2. Predstavitev prototipa

Kot primer vzamemo prototip sledenja lokalnim pridelkom v kratkih oskrbovalni verigah. Prototip programske rešitve se imenuje BlockIS in se razvija v partnerstvu Zelene točke, ITC Murska sobota in Blockchain Lab:UM. Rešitev je prilagojena specifičnim zahtevam pridelovalcev oskrbe z lokalnim sadjem in zelenjavo. Rešitev povezuje različne akterje v oskrbovalne verige, pri čemer so v ospredju pridelovalci lokalnega sadja in zelenjave, posredniki s svojim prodajnim mestom in potrošnikov pridelkov. Osnovni namen rešitve je, da pridelovalci s sledenjem in sprotnim beleženjem procesa pridelave pridelkov kupcu na transparenten in preverljiv način ponudijo dokaz o trditvah poveznih z lokalnostjo in načinom pridelave ponujenih pridelkov. Kupcu so tako na voljo vsi podatki o natančni lokaciji pridelave, metodah pridelave ter času, ki je minil med pobiranjem pridelkov in časom nakupa. Vse od navedenega ima znaten vpliv na kakovost pridelkov. Temeljni namen sledenje je, kljub dodatnem delu in

povišanim stroškom, krepitev zaupanja potrošnikov v ponujene izdelke. Potrošniki do zapisov o izbranem pridelku dostopajo s preprostim odčitavanjem QR kode postavljenim ob pridelku na prodajnem mestu posrednika pridelkov. Predstavljen prototip rešitve za podporo prehranskim oskrbovalnim verigam grajen s tehnologijami veriženja blokov, je trenutno v aktivni uporabi na območju Prekmurja. Prototipna rešitev ima torej aktivne pridelovalce, ki sledijo pridelavi svoje zelenjave in posrednika, ki na prodajnem mestu omogoča dostop do zapisov o pridelkih preko generiranih QR kod. Prototip temelji na rešitvi Hyperledger Besu [16], ki transakcije izvršuje v konzorcijskem omrežju verig blokov DIH AGRIFOOD-a.

3 Arhitekturni izzivi in z njimi povezani pristopi

Čeprav gre v osnovi za podatkovne shrambe, se po svoji zasnovi, načinu uporabe in vplivu na atribute kakovosti programskih rešitev ločijo od v industriji dodobra uveljavljenih podatkovnih baz ali datotečnih sistemov. Posledično so pri izgradnji informacijskih rešitev, ki vključujejo tehnologije veriženja blokov, potrebni prilagojeni inženirski pristopi. K izgradnji tovrstnih programskih rešitev je potrebno torej pristopiti premišljeni ob razumevanju konceptov tehnologij veriženja blokov ter njihovega vpliva na atribute kakovosti programske rešitve. Večdesetletni razvoj podatkovni baz je rezultiral v programske komponente, ki jih odlikuje visoka prepustnost, nizke zakasnitve in učinkovitost povpraševanja po podatkih. Podatkovne baze tako v programskih rešitvah nudijo hiter in učinkoviti mehanizem hranjenja podatkov, s katerim je mogoče graditi hitre, skalabilne in visoko propustne programske rešitve [1], ki jih je mogoče uporabiti praktično v vseh scenarijih poslovnih programskih rešitev. Hranjenje podatkov v verige blokov je zaradi znatno drugačnega pristopa k zapisovanju podatkov, drugačno od zapisovanja v podatkovnih baz. Pri vpeljavi podatkovnih shramb, ki temeljijo na tehnologijah blokov v poslovne informacijske rešitev, je tako potrebno biti pozoren na nekatere značilnosti, ki jih tovrstne podatkovne shrambe izkazujejo. Ključne značilnosti na verigah blokov temelječih podatkovnih shramb v poslovnih okoljih so predstavljene v nadaljevanju, pri čemer za vsako podamo tudi praktično rešitev. Izpostavljamo tudi, da so navedene rešitve omejene na spekter in zmožnosti razvijalca informacijskih rešitev, ki zgolj uporablja tehnologijo veriženja blokov.

3.1. Skalabilnost in zmogljivost

Skalabilnost se tesno navezuje na metriko, ki meri število transakcij, ki jih lahko omrežje obdela v eni sekundi. Skalabilne poslovne programske rešitve so se čez čas uporabe rešitve zmožne učinkovito prilagajati vedno večji frekvenci transakcij, brez da bi prepustnost obdelovanja transakcij postalo ozko grlo. Primerjave iz domene plačilnega prometa s kripto valutami kažejo [17], da je skalabilnost omrežij verig blokov prepoznana kot resna omejitev, ki jo je pri načrtovanju na verigah blokov temelječih programskih rešitev potrebno nasloviti z ustreznimi arhitekturnimi rešitvami. Količina izvršenih transakcij na sekundo je pri zapisovanje v verige blokov nekajkrat nižja kot pri zapisovanju v podatkovne baze. Povečevanje števila transakcij bi lahko tako pripeljalo do ozkega grla.

3.1.1. Rešitev

Zaradi omejitev pri prepustnosti transakcij je pri zapisovanju podatkov v verige blokov potreben tehten premislek, katere funkcionalnosti programske rešitve bodo hranile podatke v verige blokov ter katere v klasične podatkovne baze [10]. V praksi se izkaže, da vsi podatki, ki jih programska rešitev obdeluje, niso vedno relevantni za ostale deležnike vpletene v poslovne procese in zadevajo zgolj organizacijo samo. Verige blokov torej nikakor ne nadomeščajo obstoječih ERP sistemov in drugih internih podatkovnih baz organizacije, temveč jih zgolj dopolnjujejo. V verige blokov torej sodijo le podatki, ki jih želi organizacija deliti zunanjimi deležniki in so zanje relevantni.

Kot morebitna rešitev za večjo skalabilnost omrežja verig blokov je uporaba konzorcijskega omrežja, ki uporablja preprostejši mehanizem soglasja (npr. dokaz o avtoriteti – PoA). V takšnih omrežij se prepustnost transakcij

izredno poveča, vendar je splošna varnost nižja, saj imamo znatno manjše število vozlišč, ki so posledično lahko hitreje okno napada na celotno omrežje. Uporaba takšnega omrežja pa je seveda pogojena tudi s tem, da za poslovno rešitev niso ključna javno dostopna digitalna sredstva oz. kriptovalute ali kriptožetoni.
V primerih, ko smo odvisni od uporabe javnih omrežij verig blokov, kot so BitCoin, Ethereum in podobni, pa je seveda smotrn razmislek o tem, katero izmed teh omrežij je za naš poslovni primer smiselno uporabiti, saj ima vsako od teh omrežij svoje prednosti in slabosti ter tudi različne prepustnosti. Glede na izbiro omrežja se nam nato ponujajo tudi njihove specifične rešitve drugega sloja (angl. Layer-2), kot so kanali stanja (angl. state channels), stranske verige (angl. side-channels) itn.

3.2. Velikost zapisanih podatkov

Pri podatkovnih bazah je povsem običajno, da je vanje mogoče dokaj enostavno hraniti tudi zapise večjega formata, kot so obsežnejši dokumenti, slike in videoposnetki. Verige blokov imajo omejeno kapaciteto hranjenja podatkov [10]. Slednje izhaja iz dejstva, da vsi deležniki posedujejo zgodovino vseh transakcij vseh deležnikov v omrežju. Pri zapisovanju podatkov v verige blokov so omejitve povezane s količino zapisanih podatkov posledično bolj stroge. Prva omejitev izvira iz velikosti samega bloka v verigi, ki je velikostno omejen iz zamejuje možnosti hranjenja podatkov. Druga omejitev je posredna in izhaja iz stroškov zapisovanja velike količine podatkov, v primeru, da se za hrambo podatkov uporabi javno omrežje.

3.2.1. Rešitev

Omejitev glede velikosti podatkov, ki jih je mogoče zapisati v verigo blokov, je mogoče zaobiti z vpeljavo ločene shrambe dosegljive ostalim akterjem v omrežju. V teh primerih se praviloma uporabi porazdeljena shramba datotek (angl. distributed file storage system). Za vse podatke zapisane v ločeni shrambi se izračunajo zgoščevalne vrednosti, ki se namesto podatkov samih zapišejo v verigo blokov. Ker je takšna porazdeljena shramba praviloma javna, je drugim deležnikom v omrežju tako omogočeno, da lahko za vse zapise preverijo, ali so bili po zapisu morda spremenjeni. Takšno arhitekturno rešitev je mogoče doseči z vpeljavo IPFS omrežij [18], na katere se hranijo datoteke, slike, videoposnetki in ostali zapisi, ki presegajo velikostne omejitve blokov. Osnovna prednost IPFS omrežja, je da ohranja decentralizirano naravo tehnologij veriženja blokov, saj ne vpeljuje potrebe po centralizirani administraciji zapisov. Dodatna prednost IPFS omrežja je tudi to, da so hranjene datoteke preko zgoščevalne vrednosti tudi naslovljive.
Poleg uporabe IPFS (InterPlanetary File System) za shranjevanje velikih datotek, slik in videoposnetkov zunaj verige blokov, obstaja še nekaj drugih rešitev za obvladovanje omejitev velikosti zapisanih podatkov v verigah blokov. Podobno kot pri IPFS, je mogoče uporabiti različne decentralizirane ali centralizirane rešitve za shranjevanje velikih podatkov zunaj verige blokov, medtem ko se v verigi zapišejo samo zgoščevalne vrednosti (hashi). Tako lahko uporabite obstoječe storitve v oblaku, kot so Amazon S3, Google Cloud Storage, ali decentralizirane rešitve, kot so Swarm, Storj, Filecoin itn. Razen tega pa so nam na voljo še drugi kompleksnejši pristopi, kot je uporaba tehnik kompresije, uporaba ZK-SNARKs, plazemske tehnike, Merklovih dreves itn.
Vsaka od teh rešitev ponuja različne prednosti in omejitve glede na specifične potrebe poslovnih procesov in naravo podatkov, ki jih je potrebno shranjevati. Pomembno je, da se izbere ustrezna kombinacija teh pristopov glede na zahteve sistema in obstoječo infrastrukturo.

3.3. Stroški transakcij

Naslednja posebnosti vredna upoštevanja pri načrtovanju tovrstnih programskih rešitev in je neposredno povezana s količino zapisanih podatkov, so stroški zapisovanja podatkov. Javna omrežja verig blokov veljajo za prostorsko in energetsko potratne. Slednje ima neposredni vpliv na stroške zapisovanja in hrambe podatkov. Slednje velja predvsem, kadar je za hrambo podatkov izbrano javno omrežje. Gre torej za iskanje ravnotežja zaupanjem, varnostjo in transparentnostjo, ki jih nudi zapisovanje podatkov v javno omrežje, in stroški, ki jih zapisovanje podatkov v javna omrežja prinaša.

3.3.1. Rešitev

Zaupanje, transparentnost in varnost zapisanih podatkov pogosto ne odtehta stroškov, ki jih s seboj prinese uporaba javnih omrežij. Javna omrežja zaradi velikosti omrežja veljajo za bolj varna, saj je za izvedbo uspešnega napad nanje potrebnih ogromno virov. V mnogih poslovnih primerih tako visoka stopnja zaupanja in varnosti ni prioriteta. V takšnem primeru gre za razmisliti o uporabi konzorcijskih omrežij, pri katerih deležniki vzpostavijo lastno infrastrukturo verig blokov. Ker so pri konzorcijskih omrežjih vozlišča porazdeljena med deležnike, ki prav tako posedujejo kopijo vseh zapisanih podatkov ter morajo pri zapisovanju v bloke doseči konsenz, veljajo tovrstne konfiguracije prav tako za varne in zaupanja vredne, pri čemer so običajno stroški transakcij občutno nižji.
Podobno kot pri rešitvah za obvladovanje velikosti, se tudi za obvladovanje stroškov ponujajo rešitve v uporabi drugega sloja (Layer-2). Layer 2 rešitve omogočajo izvajanje transakcij zunaj glavne verige blokov. To zmanjšuje število transakcij, ki se morajo zapisati na verigo, kar posledično znižuje stroške transakcij. Prav tako je možno združevati transakcije brez uporabe rešitev drugega sloja. Z združevanjem več transakcij v eno samo se zmanjša število potrebnih zapisov na verigi blokov. S tem pristopom se lahko optimizirajo stroški, saj en zapis na verigi predstavlja več transakcij, kar znižuje stroške na posamezno transakcijo. Transakcije lahko tudi stiskamo pred izvedbo. Stiskanje podatkov pred zapisovanjem v verigo blokov lahko zmanjša velikost transakcij, kar posledično zniža stroške, saj so stroški zapisovanja pogosto odvisni od količine podatkov, ki se zapisujejo. Ker je večina poslovnih rešitev povezanih s tehnologijo veriženja blokov odvisna od pametnih pogodb, je tudi te smotrno optimizirati. Optimizacija kode pametnih pogodb, da je bolj učinkovita in zahteva manjšo porabo računalniških virov, lahko zmanjša stroške transakcij. To vključuje zmanjšanje števila nepotrebnih operacij in uporabo bolj učinkovitih algoritmov.
Z uporabo zgoraj omenjenih rešitev lahko podjetja in organizacije zmanjšajo stroške zapisovanja podatkov v verige blokov, hkrati pa ohranijo ustrezno raven varnosti, zaupanja in transparentnosti. Vsekakor pa vsaka od predstavljenih rešitev doprinese k že tako visoki kompleksnosti uporabe tehnologije veriženja blokov. Ključno je najti pravo ravnovesje med stroški in zahtevanimi lastnostmi sistema glede na specifične poslovne potrebe.

3.4. Učinkovitost povpraševanja po podatkih

V primerjavi s podatkovnimi bazami, po katerih je zaradi dobre strukturiranosti podatkov mogoče izjemno učinkovito in hitro povpraševati, je pri verigah blokov povpraševanje občutno bolj zamudno. Slednje izhaja iz dveh lastnosti verig blokov, slabše strukturiranosti zapisovanja podatkov ter mehanizmov varnosti, ki sproti preverjajo integriteto zapisanih podatkov v blokih preko preverjanja zgoščevalnih vrednosti blokov. Varnost zapisanih podatkov pred manipulacijami ima torej tudi svojo ceno, ki jo je potrebno ustrezno nasloviti. Učinkovitost povpraševanja ovira tudi sama struktura zapisov, pri kateri so zapisani podatki razpršeni po različnih blokih v verigah in naslovljivi izključno preko naslovov. Pomembna pomanjkljivost verig blokov je tudi odsotnost standardiziranih povpraševalnih jezikov, kot je na primer pri relacijskih bazah SQL.

3.4.1. Rešitev

Ker imajo deležniki nadzor le nad podatki znotraj lastne organizacije, je razpršenost zapisanih podatkov po verigi blokov je mogoče premostiti z indeksiranjem zapisov v verigah blokov. Indeks zapisov deluje kot predpomnilnik, ki združuje zapise vseh deležnikov v omrežju. S tem lahko pridemo do dobro strukturiranih podatkov, po katerih je mogoče hitro in učinkovito poizvedovati. Platforme, kot so Apollo GraphQL [19] vzpostavijo infrastrukturo, ki omogoča integriran pogled in enostavni dostop z možnostjo poganjanja kompleksnih poizvedb nad integriranimi podatki. GraphQL dodatno vpelje poenoteno povpraševanje po podatkih s pomočjo poizvedovalnih nizov.
Do zapisov v verigah blokov pogosto dostopamo preko proženja pametnih pogodb. Da bi zamejili kompleksnost proženja pametnih pogodb, je vmesnike dostopa do pametnih pogodb smiselno zagraditi v namensko mikrostoritev, ki dostop do podatkov izpostavlja preko končnih točk, s katerimi si je mogoče podatke izmenjevati preko sporočil v JSON formatu.
Prav tako zapisovanje pomembnih dogodkov in sprememb v podatkih v dnevniške zapise (logs) omogoča hitrejši dostop do ključnih informacij brez potrebe po celovitem iskanju po verigi blokov. Dnevniški zapisi omogočajo hitro povpraševanje po specifičnih dogodkih ali spremembah. Uporaba predpomnilnika (cache) na nivoju aplikacije ali omrežja za pogosto dostopane podatke lahko znatno izboljša hitrost povpraševanja. Predpomnjenje omogoča hitrejši dostop do podatkov brez potrebe po ponovnem iskanju ali preverjanju celovitosti zapisov v verigi blokov.

3.5. Evolucija programskih rešitev

Elementarna lastnost programskih rešitev je, da se s tokom časa pojavljale potrebe po njenih spremembah. Potreba po spremembah izhaja iz različnih dejavnikov, na primer spremembe v zahtevah uporabnikov ali poslovnem okolju. Po drugi strani je temeljna prednost tehnologij veriženja blokov, nespremenljivost zapisanih podatkov, saj je nove podatke na najnižjem nivoju dovoljeno le pripenjati ne pa tudi spreminjati ali celo brisati. Če je pri relacijskih bazah spreminjanje tabel in transformacija podatkov samoumevna, pri zapisih v verige blokov te operacije preprosto niso na voljo. Iz nespremenljivosti podatkov neposredno izhaja zaupanje v zapisane podatke, kot ena izmed temeljnih prednosti pristopa. Dejstvi, da bo tekom življenjskega cikla aplikacije neizbežno prišlo do zahtev po njenih spremembah in da zapisanih podatkov v verigah blokov ni mogoče enostavno spreminjati terja veliko pozornosti pri načrtovanju tovrstnih rešitev. Evolucija programske rešitve mora biti načrtovana vnaprej ob upoštevanju omejitev zaradi nezmožnosti spreminjanja podatkov oz. cene, ki jo prinese nameščanje nove različice programske rešitve.

3.5.1. Rešitev

Razvijalci so ustvarili koncept nadgradljivih pametnih pogodb (angl. upgradable smart contracts) kot odgovor na izzive, ki jih prinaša nespremenljivost tradicionalnih pametnih pogodb. Ta pristop temelji na ločevanju poslovne logike od shranjevanja podatkov. Sistem je sestavljen iz dveh ključnih delov: posredniške pogodbe (angl. proxy contract) in izvedbene pogodbe (angl. logic contract). Posredniška pogodba služi kot stalna točka interakcije za uporabnike. Njena naloga je shranjevanje podatkov in posredovanje klicev funkcij. Izvedbena pogodba pa vsebuje dejansko poslovno logiko in jo je mogoče posodobiti. Ob potrebi po nadgradnji se uvede nova izvedbena pogodba, posredniška pogodba pa se preusmeri nanjo. Ta mehanizem omogoča odpravljanje napak, dodajanje novih funkcionalnosti in prilagajanje spremembam brez motenja naslova pogodbe ali izgube podatkov. Pomembno je omeniti, da so spremembe v shranjevanju podatkov mogoče, vendar zahtevajo previdnost. Skrbno načrtovanje je ključnega pomena, da se izognemo trkom pri shranjevanju ali izgubi podatkov. Razvijalci morajo biti pozorni na strukturo shranjevanja pri vsaki nadgradnji, da zagotovijo združljivost in ohranijo celovitost obstoječih podatkov. Kljub temu, da ta rešitev prinaša določeno mero kompleksnosti in potencialnih varnostnih izzivov, predstavlja kompromis med potrebo po nespremenljivosti v tehnologiji veriženja blokov in praktičnimi zahtevami razvoja programske opreme. Omogoča posodabljanje pametnih pogodb ob ohranjanju podatkov in stalnosti naslova pogodbe, s čimer ponuja bolj fleksibilen in vzdržljiv pristop k razvoju na platformah veriženja blokov [20].

3.6. Drugi izzivi in potencialne rešitve

Poleg že omenjenih izzivov obstajajo še drugi pomembni izzivi, ki jih je treba upoštevati. Eden izmed ključnih izzivov je **pravna in regulativna skladnost**. Tehnologija veriženja blokov pogosto deluje v globalnem okolju, kjer je treba spoštovati različne zakone in regulative, ki se razlikujejo od države do države. Pravne zahteve glede zasebnosti podatkov, varstva potrošnikov in drugih regulativnih področij so lahko zelo zapletene in težko uskladljive z naravo tehnologije. Za rešitev tega izziva je nujno, da pravni strokovnjaki in tehnologi tesno sodelujejo pri razvoju rešitev, ki bodo skladne z zakonodajo. Prav tako je pomembno razviti prilagodljive arhitekture, ki omogočajo skladnost z različnimi regulativnimi zahtevami v različnih jurisdikcijah.
Naslednji izziv je **interoperabilnost med različnimi omrežji verig blokov**. Obstaja veliko različnih omrežij verig blokov, ki pogosto niso združljiva med seboj, kar otežuje izmenjavo podatkov in interoperabilnost med različnimi poslovnimi rešitvami. Rešitev tega izziva je razvoj standardov za interoperabilnost med omrežji, kot so protokoli za prenos podatkov med verigami (angl. cross-chain communication protocols), ki lahko pomagajo pri reševanju tega problema.
Zasebnost podatkov je še en pomemben izziv, saj so v javnih omrežjih verig blokov vsi podatki načeloma dostopni vsem udeležencem, kar predstavlja izziv glede zasebnosti. V poslovnih okoljih, kjer so pogosto potrebne visoke ravni zasebnosti, to lahko predstavlja pomembno oviro. Uporaba omrežij z nadzorovanim dostopom do podatkov (angl. permissioned blockchains), kjer je dostop do podatkov omejen na določene udeležence, in tehnologije, kot so ničelno spoznavni dokazi (angl. Zero-Knowledge Proofs), ki omogočajo preverjanje informacij brez razkritja dejanskih podatkov, lahko pripomorejo k izboljšanju zasebnosti.
Sprejemanje tehnologije in uporabniška izkušnja sta prav tako izziva, saj je tehnologija veriženja blokov za mnoge uporabnike še vedno nova in kompleksna. Pomanjkanje znanja in zavedanja o prednostih in slabostih tehnologije lahko upočasni sprejemanje le te. Rešitev tega izziva vključuje izobraževanje in usposabljanje uporabnikov ter razvoj uporabniku prijaznih vmesnikov (UX/UI), ki poenostavijo interakcijo s tehnologijo.
Izguba ključa in posledice tega dogodka predstavljajo še en izziv. Tehnologija veriženja blokov temelji na kriptografskih ključih za dostop do sredstev in podatkov, izguba zasebnega ključa pa pomeni izgubo dostopa, kar je v primeru poslovnih rešitev lahko katastrofalno. Implementacija varnih sistemov za upravljanje ključev, vključno z večpodpisnimi shemami (angl. multi-signature schemes) in varnostnimi kopijami, lahko pomaga preprečiti izgubo dostopa.

4 Opis arhitekturna rešitev

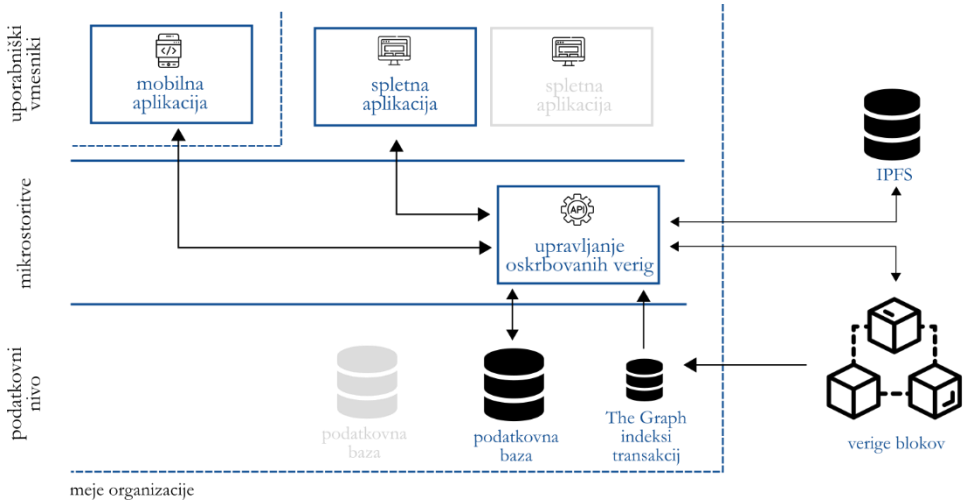
V tem poglavju na kratko predstavimo lastno arhitekturno rešitev, ki se je spopadala s premagovanjem izzivov uporabe tehnologije veriženja blokov v poslovnem scenariju. Rešitev temelji na prototipu poslovne rešitve predstavljene v poglavju 2.2.

Da bi se pri implementacije zastavljene rešitve čim bolje spopadli s v predhodnem poglavju navedenimi izzivi, smo rešitev zasnovali na temeljih programske rešitev Hyperledger Besu. Za potrebe projekta smo uporabili lastno konzorcijsko omrežje, ki temelji na mehanizmu soglasja Proof-of-Authority (PoA). Takšen pristop nam je omogočil učinkovito reševanje težav s skalabilnostjo in zmogljivostjo programske rešitve, saj ohranjamo nadzor nad zmogljivostjo vozlišč. Predstavljen pristop dodatno odpravi problem visokih transakcijskih stroškov, saj teh v konzorcijskem omrežju ne zaračunavamo. Seveda je potrebno poudariti, da v konzorcijskem omrežju partnerji zagotavljajo ustrezno strojno infrastrukturo, na katerih tečejo vozlišča omrežja. Slednje pa je seveda spet povezano z dodatnimi stroški.
Sama zasnova prototipne rešitve sledi pravilom trinivojske arhitekture, pri kateri so odgovornosti posameznega nivoja jasno razmejene. Osrednjo komponento rešitve predstavlja mikrostoritev, namenjena upravljanju zapisov o stanju pridelkov v oskrbovalni verigi v verigah blokov. Mikostoritev zajema vse funkcionalnosti povezane s upravljanjem stanj pridelkov in zapis stanja v verige blokov. Ker mikrostoritev na takšen način torej ovije vse

potrebne klice pametnih pogodb, posledično močno zmanjšamo kompleksnost same informacijske rešitve. V nasprotnem primeru bi bili klici pametnih pogodb razpršeni po preostalih mikrostoritvah informacijske rešitve. Mikrostoritev za upravljanje zapisov o stanju pridelkov v oskrbovalni verigi izpostavlja funkcionalnosti preko nabora REST končnih točk, katere je mogoče prožiti preko izmenjave JSON sporočil.

Mikrostoritev uporablja dva primarna podatkovna vira, v katera zapisuje podatke in iz katerega kasneje podatke tudi črpa. Prvi notranji podatkovni vir je podatkovna baza MongoDB, v kateri so hranjeni vsi podatki za organizacijo interne narave, in so potrebni za izvajanje poslovnih procesov znotraj organizacije. Drugi podatkov vir predstavljajo verige blokov, ki predstavlja zunanji podatkovni vir. V verige blokov se hranijo zgolj tisti nujni podatki o stanju pridelkov, ki so relevantni za ostale deležnike v prehranski oskrbovalni verigi in pripomorejo k krepljenju zaupanja deležnikov v pridelke znotraj oskrbovalne verige. Mikrostoritev zapisuje in bere podatke iz verig blokov preko proženja pametnih pogodb. Pri implementaciji pametnih pogodb smo uporabili koncept nadgradljivih pametnih pogodb, kar nam je omogočilo ohranitev podatkov, ustvarjenih v testni fazi prototipa, ter hkrati omogočilo izvajanje sprememb in nadgradenj za izboljšanje programske rešitve.

Ker zna biti proženje pametnih pogodb zamudno, hkrati pa vrača neagregirane podatke, torej le elementarne zapise iz blokov, je ob bok zunanjemu podatkovnemu viru verig blokov postavljena tudi rešitev za indeksiranje relevantnih zapisov iz verige blokov in izvajanje performančno učinkovitih povpraševanj po podatkih. Učinkovitost poizvedb po v verige blokov zapisane podatke smo tako optimizirali z uporabo protokola za indeksiranje The Graph. Ta protokol omogoča transformacijo in prenos izbranih dogodkov iz verige blokov v lokalno PostgreSQL podatkovno bazo, nad katero je na voljo GraphQL API. Preko programskega vmesnika za aplikacije je tako mogoče izvajati povpraševanja preko poenotenih in strukturiranih povpraševanj. Z uporabo rešitve The Graph smo bistveno povečali hitrost in učinkovitost poizvedb po zapisanih podatkih.
Izziv shranjevanja obsežnejših podatkov, ki presegajo velikostne omejitve osnovnih podatkovnih tipov, smo rešili s vzpostavitvijo instanc IPFS podatkovnih baz. V kategorijo obsežnejših podatkov uvrščamo vse dokumente, slike, videoposnetke in ostale datoteke večjega formata, ki so bili uporabljeni v rešitvi. V večini primerov te datoteke vsebujejo raznovrstne priloge zapisom o pridelkih v oskrbovalni verigi, kot so priloženi certifikati, izjave ter slike in videoposnetke stanja pridelkov v neki časovni točki. Takšna rešitev obravnave obsežnejših zapisov, ki jih ni smiselno zapisovati v verige blokov, nam je opravila velikostno omejitev zapisov, hkrati pa ohranila zaupanje v priložene dokumente, saj je preko zapisov zgoščevalnih vrednosti datotek v verigo blokov njihovo naknadno spreminjanje ali zanikanje nemogoče. IPFS podatkovna baza je bila vzpostavljena na nivoju konzorcijskega omrežja, pri čemer vsako izmed vozlišč omrežja ponuja tudi instanco IPFS podatkovne baze. Do naloženih vsebin lahko prosto dostopajo vsi uporabniki medmrežja z delujočo povezavo do zapisane datoteke. S takšno zasnovo obravnave dokumentov smo omogočili uporabnikom, ki bi želeli dostopati do vsebin povezanih s produktu v prehranski verigi, nemoten dostop do zapisov.



Slika 2: Arhitektura informacijske rešitve.

Pomembno komponento informacijske rešitve predstavlja tudi nivo uporabniških vmesnikov. Ta ponuja več komponent namenjeni interakciji z uporabniki. Komponente uporabniškega nivoja črpajo z zapisi o stanju pridelkov iz mikrostoritve za upravljanje oskrbovalnih verig in jih vizualno predstavijo uporabnikom informacijske rešitve. Uporabnikom so tako na voljo mobilne in spletne rešitev, ki omogočajo uporabnikom upravljanje prenosa pridelkov po prehranski oskrbovani verigi. Shemo arhitekture informacijske rešitve prestavi Slika .

5 Zaključek

Tehnologija veriženja blokov prinaša številna prednosti, ki jih je mogoče s pridom izkoristiti pri razvoju informacijskih rešitev. Ključne prednosti tehnologij so zanesljivost, transparentnost in visoka stopanja varnosti podatkov. Tehnologije veriženja blokov tako omogočajo gradnjo decentraliziranih aplikacij, pri katerih so podatki porazdeljeni in deljeni med deležniki v omrežju, kar zmanjšuje tveganja z njihovo manipulacijo. S tovrstnimi tehnologijami je mogoče vzpostaviti soustvarjanje podatkov med deležniki, ki si med seboj ne rabijo zaupati. Dodano vrednost dodajo tudi pametne pogodbe, ki omogočajo povsem avtomatizirano izvajanje poslovnih procesov z doslednih izvrševanjem vnaprej kodirani pravil, takoj ko so pogoji za njihovo izvršitev izpolnjeni.
Pri vpeljavi tehnologij veriženja blokov v informacijske rešitve potrebno upoštevati, da se hramba podatkov v verige blokov nekoliko razlikuje od pristopov hranjenja podatkov v podatkovne baze. Razlike v obeh pristopih je potrebno ustrezno nasloviti in upoštevati tako v fazi načrtovanja kot kasneje vzdrževanja programskih rešitev. V Primerjavi s podatkovnimi bazami se ključni inženirski izzivi pojavijo skalabilnosti rešitev, učinkovitostjo izvrševanja povpraševanj in stroški hrambe zapisanih podatkov. Zaradi nespremenljivosti podatkov in pametnih pogodb, predstavlja pomemben inženirski izziv tudi načrtovanje dolgoročnega vzdrževanja informacijskih rešitev. Na tem mestu je potrebno še enkrat poudariti, da hramba podatkov v verige blokov v nobenem ne nadomešča podatkovnih baz znotraj organizacije, temveč te zgolj nadgrajuje z dodatnimi pristopi hrambe. Pri tem se v verige blokov hranijo izključno za poslovni scenarij nujni podatki, ki zadevajo tudi ostale deležnike v poslovnem procesu. Tehnologije veriženja blokov ponujajo številne nove možnosti v procesu razvoja informacijskih rešitev, ki podpirajo inovativne poslovne procese. Kljub nekaterim prepoznanim omejitvam tehnologij veriženja blokov pri integraciji v informacijske rešitve, imamo na voljo vrsto inženirskih pristopov, s katerimi je mogoče učinkovito premostiti prepoznane izzive. S pravilnim razumevanjem tehnologije in izbiro ustreznih inženirskih pristopov imajo tehnologije veriženja blokov potencial, da postanejo pomembna komponenta sodobnih informacijskih rešitev, seveda v poslovnih primerih, ki so sposobni njihove prednosti pred alternativnimi pristopi hrambe podatkov s pridom izkoristiti.

Literatura

[1] "BigchainDB 2.0 The Blockchain Database," Berlin, Germany, 2018. Accessed: Jun. 06, 2024. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

[2] Empiric Infotech LLP, "Blockchain vs. Traditional Databases: A Comparative Analysis." Accessed: Jul. 17, 2024. [Online]. Available: https://www.linkedin.com/pulse/blockchain-vs-traditional-databases-comparative-analysis/

[3] R. Shaan, "Blockchains versus Traditional Databases." Accessed: Jul. 17, 2024. [Online]. Available: https://towardsdatascience.com/blockchains-versus-traditional-databases-e496d8584dc

[4] S. Sukhpreet, "Blockchain Does not Replace Traditional Databases," 2022. Accessed: Jul. 18, 2024. [Online]. Available: https://www.linkedin.com/pulse/blockchain-does-replace-traditional-databases-sukhpreet-singh/

[5] B. Podgorelec, M. Turkanović, and M. Šestak, "A Brief Review of Database Solutions Used within Blockchain Platforms," *Advances in Intelligent Systems and Computing*, vol. 1238 AISC, pp. 121–130, 2020, doi: 10.1007/978-3-030-52535-4_13.

[6] "What Will Blockchain Mean for Data Storage?" Accessed: Jul. 17, 2024. [Online]. Available: https://blog.purestorage.com/perspectives/what-will-blockchain-mean-for-data-storage/

[7] IBM, "What's the difference between a blockchain and a database?"

[8] S. Sukhpreet, "Blockchain Does not Replace Traditional Databases," 2022. Accessed: Jul. 18, 2024. [Online]. Available: https://www.linkedin.com/pulse/blockchain-does-replace-traditional-databases-sukhpreet-singh/

[9] L. Anndy, "Basic Principles of the Blockchain Database Concept | Turkey." Accessed: Jul. 17, 2024. [Online]. Available: https://www.linkedin.com/pulse/basic-principles-blockchain-database-concept-turkey-anndy-lian/

[10] A. Carolina Ordonez-Guerrero, J. David Munoz-Garzon, E. Roberto Dulce Villarreal, A. Bandi, and J. Ariel Hurtado, "Blockchain Architectural Concerns: A Systematic Mapping Study," *2022 IEEE 19th International Conference on Software Architecture Companion, ICSA-C 2022*, pp. 183–192, 2022, doi: 10.1109/ICSA-C54293.2022.00043.

[11] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain: Research and Applications*, vol. 2, no. 4, p. 100027, Dec. 2021, doi: 10.1016/J.BCRA.2021.100027.

[12] M. Dashtizadeh, F. Meskaran, and D. Tan, "A Secure Blockchain-based Pharmaceutical Supply Chain Management System: Traceability and Detection of Counterfeit Covid-19 Vaccines," *MysuruCon 2022 - 2022 IEEE 2nd Mysore Sub Section International Conference*, 2022, doi: 10.1109/MYSURUCON55714.2022.9972646.

[13] M. Dashtizadeh, F. Meskaran, and D. Tan, "A Secure Blockchain-based Pharmaceutical Supply Chain Management System: Traceability and Detection of Counterfeit Covid-19 Vaccines," *MysuruCon 2022 - 2022 IEEE 2nd Mysore Sub Section International Conference*, 2022, doi: 10.1109/MYSURUCON55714.2022.9972646.

[14] J. Ktari, T. Frikha, F. Chaabane, M. Hamdi, and H. Hamam, "Agricultural Lightweight Embedded Blockchain System: A Case Study in Olive Oil," *Electronics 2022, Vol. 11, Page 3394*, vol. 11, no. 20, p. 3394, Oct. 2022, doi: 10.3390/ELECTRONICS11203394.

[15] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[16] "Hyperledger Besu – Hyperledger Foundation." [Online]. Available: https://www.hyperledger.org/use/besu

[17] "A Deep Dive Into Blockchain Scalability." Accessed: Jul. 23, 2024. [Online]. Available: https://crypto.com/university/blockchain-scalability

[18] "An open system to manage data without a central server | IPFS." Accessed: Jul. 24, 2024. [Online]. Available: https://ipfs.tech/

[19] "Apollo GraphQL." Accessed: Jul. 24, 2024. [Online]. Available: https://www.apollographql.com/

[20] "Proxy Upgrade Pattern - OpenZeppelin Docs." Accessed: Jul. 31, 2024. [Online]. Available: https://docs.openzeppelin.com/upgrades-plugins/1.x/proxies