# Primjena tehnologije raspodijeljenih glavnih knjiga u digitalnom novcu središnjih banaka

**Belušić, Bojan**

Sveučilište u Zagrebu

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Bojan Belušić

# PRIMJENA TEHNOLOGIJE RASPODIJELJENIH GLAVNIH KNJIGA U DIGITALNOM NOVCU SREDIŠNJIH BANAKA

SPECIJALISTIČKI RAD

Zagreb, 2022.

Završni specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva, na Zavodu za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Mentor: doc. dr. sc. Ante Đerek

Završni rad: 81 stranica

Završni rad br.:

Povjerenstvo za ocjenu u sastavu:

1. Prof. dr. sc. Marin Golub – predsjednik
2. Doc. dr. sc. Ante Đerek – mentor
3. Doc. dr. sc. Marcel Maretić – Sveučilište u Zagrebu Fakultet organizacije i informatike – član

Povjerenstvo za obranu u sastavu:

1. Prof. dr. sc. Marin Golub – predsjednik
2. Doc. dr. sc. Ante Đerek – mentor
3. Doc. dr. sc. Marcel Maretić – Sveučilište u Zagrebu Fakultet organizacije i informatike – član

Datum obrane: 31. siječnja 2022.

# Sadržaj


1. Uvod ... 1
2. Korištenje DLT-a u svrhu izdavanja CDBC-a ... 3
3. Istraživanja i projekti središnjih banaka u svrhu izdavanja CDBC-a ... 6
   3.1. Izdavanje veleprodajnog CDBC-a na DTL platformi ... 7
      3.1.1. Projekt Jasper središnje banke Kanade ... 9
      3.1.2. Istraživanje središnje banke Brazila ... 12
      3.1.3. Projekt Ubin Monetarnog autoriteta Singapura ... 16
      3.1.4. Projekt Stella Europske središnje banke i središnje banke Japana ... 29
      3.1.5. Projekt Khokha središnje banke Južnoafričke republike ... 38
   3.2. Izdavanje maloprodajnog CDBC-a na DLT platformi ... 40
      3.2.1. Projekt Bakong Narodne banke Kambodže ... 42
      3.2.2. Digitalni dolar Monetarne unije istočnih Kariba ... 44
      3.2.3. Pješčani dolar središnje banke Bahama ... 46
      3.2.4. E-kruna središnje banke Švedske ... 47
4. DLT platforme korištene u projektima i istraživanjima središnjih banaka ... 49
   4.1. Ethereum ... 51
   4.2. Quorum ... 53
   4.3. Hyperledger Fabric ... 57
   4.4. Corda ... 59
5. Sigurnosna razmatranja izdavanja CDBC-a na DLT platformi ... 63
6. Zaključak ... 71

Literatura ... 73

Skraćenice ... 77

Sažetak ... 78

Abstract ... 79

Životopis ... 80

Biography ... 81

# 1. Uvod

Središnje banke dužne su održavati stabilnost financijskog sustava države na kojoj djeluju, putem utvrđivanja i provođenja monetarne i devizne politike, držanja i upravljanja međunarodnim pričuvama te izdavanja gotovine, odnosno novčanica i kovanog novca što je u Hrvatskoj i propisano Zakonom o Hrvatskoj narodnoj banci. Smanjenje korištenja gotovine kao sredstva za plaćanje u svijetu, financijska inkluzija stanovništva koje živi na udaljenim mjestima, ovisnost o međunarodnim financijskim institucijama koje pružaju financijsko posredovanje i njihovo moguće grupiranje u kartele i monopole te njihove visoke provizije i moguća volatilnost tečaja natjerale su središnje banke da razmisle o izdavanju digitalnog novca središnjih banaka (engl. Central Bank Digital Currency, CBDC).

Sve veća popularnost kriptovaluta kao sredstva za plaćanje i ulaganje te najave uvođenja elektroničkih platnih sredstava baziranih na tehnologiji raspodijeljenih glavnih knjiga (engl. Distributed Ledger Technology, DLT) od strane društvenih mreža[1] još su samo neki od razloga zašto središnje banke sve više razmišljaju o implementaciji maloprodajnog CBDC-a za upotrebu među građanstvom. Navedeno još više dolazi do izražaja kad uzmemo u obzir da često ne postoji mogućnost da se transakcije na spomenutim platformama povežu sa stvarnim identitetima ili storniraju, te se samim time se ne mogu ni spriječiti pokušaji pranja novca i financiranja terorizma.

Središnje banke već koriste veleprodajni elektronički novac, drugu vrstu CBDC-a koja je dostupna za korištenje poslovnim bankama. Poslovne banke imaju otvorene račune kod lokalne središnje banke gdje pohranjuju svoje djelomične pričuve kao jamstvo koje im omogućuje da mogu iskoristiti ostatak novca svojih klijenata za zajmove i na taj način zarađivati. Navedeni računi poslovnih banaka koriste se i za elektroničko poravnanje u

[1] primjerice, južnokorejska korporacija Kakao, orijentirana na pružanje usluga preko Interneta, 2018. godine pokrenula je DLT platformu Klaytn te sljedeće godine krenula s izdavanjem kriptovalute Klay, dok je društvena mreža Facebook 2019. godine najavila izdavanje kriptovalute Diem koja za vrijeme pisanja ovog rada još uvijek nije bila u opticaju

sustavima bruto namire u realnom vremenu (engl. Real Time Gross Settlement, RTGS) putem kojih banke međusobno provode manji broj transakcija velike vrijednosti.

Brojne središnje banke u svijetu u posljednjih nekoliko godina počele su testirati mogućnost korištenja sustava baziranih na DLT-u u svrhu povođenja nacionalne i prekogranične bruto namire u realnom vremenu kako bi se bolje upoznale s prednostima i manama navedene tehnologije. Osim navedene primjene korištenja, središnje banke analiziraju mogućnost uvođenja maloprodajnog CDBC-a koji bi bio implementiran na DLT sustavu, u čemu je najdalje otišla Narodna banka Kambodže i dvije središnje banke iz karipskog područja koje su svoje pilote potpuno ili djelomično pustile u javnost, te švedska središnja banka Riksbank, koja je za vrijeme pisanja ovog rada još uvijek samo testirala pilot plaćanja svojim CBDC-om e-krunom.

Prema dostupnim informacijama Narodna banka Kine 2020. godine započela je s testiranjem vlastite digitalne valute koje građani Kine mogu osvojiti putem lutrija i potrošiti kod određenih elektroničkih trgovaca. Distribucija digitalnog juana planira se provoditi putem takozvanog dvorazinskog sustava, što znači da će Narodna banka Kine distribuirati digitalni juan poslovnim bankama koje će biti odgovorne za omogućavanje korištenja te valute krajnjim korisnicima. Međutim, za vrijeme pisanja ovog rada još uvijek nije bilo jasno kako će se taj CDBC koristiti, niti su objavljene informacije na kojoj se tehnologiji bazira sustav Narodne banke Kine [1]. Iz navedenih razloga ovaj rad se neće osvrtati na izdavanje CDBC-a Narodne banke Kine.

Ovim radom obradit će se najbolje dokumentirani projekti i istraživanja središnjih banaka kojima se željelo utvrditi mogu li se DLT platforme koristiti za izdavanje i platni promet digitalnog novca. Nakon toga rad ukratko objašnjava način rada DLT platformi koje su najčešće korištene u projektima i istraživanjima središnjih banaka u tu svrhu. Naposlijetku će se rad osvrnuti i na potencijalne kibernetičke rizike vezane uz DLT platforme te tehnike koje se mogu implementirati za smanjivanje navedenih rizika.

# 2. Korištenje DLT-a u svrhu izdavanja CDBC-a

Raspodijeljena glavna knjiga je baza podataka koja može biti dijeljena i replicirana putem mreže koja se sastoji od mnoštva čvorova ili institucija. Sigurnost, integritet i ispravnost podataka u takvoj bazi jamči se pomoću kriptografskih sažetaka (engl. hash), ključeva i digitalnih potpisa. Takve baze podataka su zapravo kriptografski lanci blokova kod kojih svaki element uz ostale proizvoljne podatke sadrži i sažetak pokazivač (engl. hash pointer) na prethodni element. Različiti korisnici i čvorovi, koji putem raspodijeljenog konsenzusa postižu dogovor o točnom stanju glavne knjige, mogu posjedovati jednake verzije baze podataka što omogućuje visoku razinu transparentnosti, dok se kriptografijom može osigurati kontrola identiteta i integritet podataka.

Korištenje DLT sustava u svrhu izdavanja CDBC-a omogućilo bi izbacivanje posrednika koji provode namire u transakcijama između dviju ili više strana. Sigurnost pohranjenih podataka i autorizacije korisnika može se jamčiti kriptografskim atributima sustava, a zbog raspodijeljenosti sustava koja omogućuje izbacivanje posrednika smanjuje se i potreba za pričuvnim sustavima ili visokom dostupnošću. Ugrađivanjem regulatornih zahtjeva u takav DLT sustav automatski bi se mogao zahtijevati dokaz identiteta i vršiti nadzor transakcija koji bi pod određenim uvjetima bile označene kao sumnjive u sklopu borbe protiv pranja novca i financiranja terorizma. Dodatno, korištenjem pametnih ugovora na DLT sustavima, središnje banke bi korisnicima CDBC-a automatski mogle naplaćivati porez ili isplaćivati preplaćeni porez te osigurati distribuciju državne pomoći i subvencija.

DLT sustavi prema tipu pristupa mogu biti javni, kod kojih bilo tko može čitati informacije iz lanca blokova, i privatni, kod kojih postoji centralni autoritet koji odlučuje tko može vidjeti koje informacije. Prema načinu pristupa i sudjelovanja DLT sustavi se dijele na one bez dozvola (engl. premissionless), kod kojih se bilo koji čvor može priključiti mreži ili je napustiti bez prethodnog traženja dozvole, te one s dozvolom (engl. premissioned), kod kojih centralni autoritet odlučuje tko se može pridružiti mreži i koja će prava na mreži imati. Izbor između ovih tipova DLT platformi ovisi o tome

kolika je razina povjerenja između sudionika u sustavu te može li se dozvoliti neprovjerenim sudionicima uvid u osjetljive podatke.

Prvi DLT sustav nazvan Bitcoin predložen je kao decentralizirani platni sustav bez centralnog autoriteta u kojem su svi sudionici jednaki. Kako bi se osiguralo povjerenje u takvom sustavu potrebno je bilo definirati mehanizam konsenzusa kojim će se omogućiti da sudionici dođu do kolektivnog dogovora koje će transakcije ući u novi blok. Na Bitcoin mreži je izabran *proof-of-work* mehanizam koji je, osim omogućavanja dogovora među čvorovima, sprječavao dvostruko trošenje istih vrijednosti i poticao sudionike da ostanu ispravni te poštuju pravila mreže. Takva vrsta konsenzusa osigurava da skupina sudionika s većinom računalne snage na mreži odlučuje koji će biti najduži, i stoga ispravan, lanac blokova. Osim te vrste mehanizma, mogu se koristiti i drugi, primjerice, *proof-of-stake* kod kojeg se vjerojatnost da će sudionik predložiti novi blok povećava s većim udjelom tog sudionika u ukupnoj imovini na mreži. Zatvorene privatne DLT mreže s dozvolom u kojima su poznati svi sudionici ili postoji autoritet u koji ostali sudionici imaju povjerenja mogu koristiti *proof-of-authority* mehanizme konsenzusa kod kojeg jedan sudionik ili grupa sudionika odlučuje kako će izgledati sljedeći blok transakcija.

Na DLT platformama poput Bitcoina svaka transakcija ima jedan ili više izlaza koji predstavljaju sumu Bitcoin valuta (BTC-a) koje je nakon te transakcije moguće potrošiti. Te nepotrošene sume nazivaju se nepotrošeni izlazi transakcije (engl. Unspent Transaction Outputs, UTXO) te ostaju u takvom stanju dok ih novi vlasnik ne odluči potrošiti. Svaki UTXO, osim svoje vrijednosti, predstavlja i lanac vlasništva u obliku lanca digitalnih potpisa kojima su platitelji potpisali transakcije kojima su prebacili vlasništvo nad svojim UTXO na javni ključ primatelja, koji predstavlja njegovu adresu. Taj lanac vlasništva, koji je pohranjen na svakom čvoru i ažurira se sa svakom novom transakcijom, služi za provjeru valjanosti transakcije kako bi se onemogućila dvostruka potrošnja. Na platformama koje koriste UTXO model, sudionici nemaju svoje račune ni stanja sredstava na tim računima, nego međusobno transferiraju vrijednost u UTXO jedinicama poput fizičkog novca.

UTXO model predstavlja jedan od modela sustava za izdavanje digitalne valute koji je baziran na vrijednosti ili tokenu (engl. value-based ili token-based) te bi u takvom sustavu CDBC bio izveden kao token specifične vrijednosti. Prebacivanje tokena između dviju strana ne zahtjeva usklađivanje dviju baza podataka, već predstavlja gotovo

trenutno prebacivanje vlasništva imovine slično pružanju novčanica gotovine. No s druge strane, sustavi za izdavanje digitalne valute mogu se izvesti i kao modeli bazirani na računima (engl. account-based) koji zahtijevaju održavanje računa korisnika od strane središnjih banaka [2]. Prema mišljenju središnje banke Švedske izvedba modela baziranog na računima je kompleksnija, no pruža više mogućnosti proširivanja modela u fazama i prilagodbe budućim zahtjevima. Prednosti modela baziranog na vrijednosti su veća dostupnost skupinama koje nisu u mogućnosti ili ne žele imati vlastite račune, a model se dodatno može razvijati kako bi se udovoljilo potrebama posebnih skupina za osnovnim uslugama plaćanja [3].

Digitalna virtualna valuta čija je vrijednost vezana uz vrijednost stvarne *fiat* valute ili druge vrste stabilne imovine naziva se *stablecoin*. Takve valute osmišljene su kako bi sudionicima omogućile anonimnost i sigurnost prijenosa sredstava koje donose javni DLT sustavi kao Bitcoin, bez bojazni od naglih padova ili rasta vrijednosti koje su s njima povezani. Istraživanje Banke za međunarodne namire (engl. Bank for International Settlements, BIS) provedeno 2019. godine otkrilo je da 58% ispitanih središnjih banaka analizira potencijalni utjecaj *stablecoin*-ova na monetarnu i financijsku stabilnost u njihovoj nadležnosti [4]. Korištenje CDBC-a za prijenos sredstava na privatnim DLT sustavima s dozvolom, koji bi središnjim bankama osigurali provedbu svojih politika, omogućilo bi sigurnu i dostupnu alternativu *stablecoin*-ovima.

# 3. Istraživanja i projekti središnjih banaka u svrhu izdavanja CDBC-a

Razmišljanja središnjih banaka o izdavanju digitalnog novca nisu toliko svježa koliko se na prvu može činiti. Već 2014. godine središnja banka Ekvadora objavila je da će započeti s izdavanjem elektroničkog novca, iako njihova izvedba nije koristila DLT. Korisnici navedenog CDBC-a su u periodu od 2015. do 2018. godine mogli držati otvoren račun u središnjoj banci Ekvadora te prebacivati sredstva putem aplikacije na mobilnom telefonu. Zbog nemogućnosti da privuče veći broj korisnika i ostvari značajne transakcijske volumene, u Ekvadoru je donesen zakon kojim se ukida taj prvi pokušaj CDBC-a u svijetu [5]. Ni eksperimentiranja središnjih banaka s tehnologijom raspodijeljenih glavnih knjiga nisu neka novost, primjerice, nizozemska središnja banka De Nederlandsche Bank već je 2016. godine kroz više prototipova testirala mogućnost rudarenja CDBC-a baziranog na Bitcoinu, no zaključak je bio da virtualne valute nisu najperspektivnija primjena DLT sustava [6].

Međutim, postotak središnjih banaka u svijetu koje na neki način istražuju mogućnost izdavanja CDBC-a je u značajnom porastu te je 2019. godine prema istraživanju Banke za međunarodne namire iznosio 80%. Kao motivaciju za navedena istraživanja vezana uz maloprodajni CDBC banke su na najviša mjesta po važnosti stavljale sigurnost i efikasnost plaćanja te financijsku inkluziju, odnosno dostupnost i jednake mogućnosti za pristup financijskim uslugama. Nadalje, neke središnje banke su važnim istaknule smanjivanje troškova upravljanja gotovinom te unaprjeđivanje procesa za prikupljanje informacija o klijentima (engl. Know Your Customer, KYC), sprječavanje pranja novca (engl. Anti-Money Laundering, AML) i financiranje terorizma, dok je za druge važna motivacija bila sve manji udio gotovine u platnom prometu [4].

Kao motivaciju za istraživanje upravljanja veleprodajnim CDBC-om, koji bi povezivao mogućnosti jamstvenih računa i međubankarskog platnog sustava te potencijalno koristio DLT, BIS navodi da središnje banke ističu efikasnost i sigurnost plaćanja, podjednako domaćeg i prekograničnog, te stabilnost financijskog sustava. Navedeno istraživanje možemo povezati s upitnikom o globalnim platnim sustavima Svjetske

Banke iz 2018. godine prema kojem 81% ispitanih financijskih regulatornih tijela planira ili već provodi reforme nacionalnog platnog sustava. Prema njihovom istraživanju najčešći faktori koji su utjecali na navedene reforme su povećanje efikasnosti platnog sustava, praćenje tehnoloških inovacija i potreba za povećanjem dostupnosti financijskih usluga među stanovništvom [7].

## 3.1. Izdavanje veleprodajnog CDBC-a na DTL platformi

Mogućnost pravovremene i konačne namire plaćanja, tj. bezuvjetnog i neopozivog prijenosa vrijednosti koju primatelj može koristiti bez rizika od storniranja, jedno je od glavnih pitanja o primjerenosti korištenja DLT-a u svrhu izdavanja veleprodajnog CDBC-a koje su središnje banke svojim istraživanjima pokušale odgovoriti. Osim toga, središnje banke su se željele uvjeriti mogu li sustavi bazirani na DLT-u podnijeti produkcijske količine dnevnih transakcija, primjerice, uz velike zahtjeve za računalnom snagom nekih algoritama konsenzusa ili uz čekanje da svi sudionici na mreži potvrde sve transakcije. Dodatna mogućnost ovakvih sustava koja se željela istražiti je interoperabilnost s različitim nacionalnim i međunarodnim financijskim tržištima te korištenje u svrhu razmjene različitih klasa imovine na istoj dijeljenoj bazi podataka [8].

Tijekom 2016. i 2017. godine cijeli je niz središnjih banaka u svijetu krenuo u istraživanje mogućnosti korištenja DLT sustava u svrhu izdavanja veleprodajnog CDBC-a. Središnja banka Kanade početkom 2016. godine krenula je u prvu fazu projekta Jasper kojemu je cilj bio istražiti korištenje digitalnih potvrda o položenim sredstvima izdanih u svrhu namire od strane središnje banke koristeći DLT platformu. Druga faza projekta Jasper nastavila se fokusirati na međubankarske namire, no za njene potrebe razvijena je nova DLT platforma [9], dok je u trećoj fazi DLT ekosistem proširen kako bi uključivao i namiru vrijednosnih papira uvrštenih na burzu u Torontu [10].

U rujnu 2016. godine središnja banka Brazila započela je prvu fazu vlastitog istraživanja kojem je cilj bio ocijeniti i analizirati DLT sustave te se bolje upoznati s primjenjivošću i nedostacima navedene tehnologije. U prvoj fazi odlučili su istražiti moguće primjere korištenja DLT-a unutar središnje banke Brazila, izabrati jedan od primjera korištenja i moguću platformu na kojoj bi ga proveli te kreirati minimalan dokaz koncepta. U drugoj fazi istraživanja zadatak je bio analizirati različite DLT platforme koristeći izabrani primjer iz prve faze kao mjerilo [11].

Krajem 2016. godine Monetarni autoritet Singapura pokrenuo je projekt Ubin čiji je cilj bio procijeniti implikacije tokeniziranog oblika singapurskog dolara na tehnologiji raspodijeljenih glavnih knjiga i njegove potencijalne koristi za financijski ekosustav Singapura. Prve dvije faze projekta bile su usredotočene na izgradnju tehnoloških mogućnosti u kontekstu domaće veleprodajne platne mreže, dok su se sljedeće dvije faze usredotočile na interoperabilnost mreže temeljene na lancu blokova za isporuke po plaćanju (engl. delivery-vs-payments, DvP) i prekogranično plaćanje po plaćanju (engl. payment-vs-payment). Završna peta faza projekta prebacila se s dokazivanja tehničkih koncepata na dokazivanje potencijalne vrijednosti, uključujući razumijevanje kako bi takvi modeli mogli poboljšati učinkovitost namire te koji bi bile koristi za širi ekosustav [12].

Otprilike s početkom projekta Ubin, središnja banka Japana i Europska središnja banka (ECB) objavile su da kreću u zajednički istraživački projekt nazvan Stella kako bi procijenili primjenjivost DLT rješenja u području infrastrukture financijskog tržišta. Analiza prve faze usredotočila se na aspekte učinkovitosti i sigurnosti platnog sustava u DLT okruženju, dok je druga faza projekta istraživala koncepte isporuke vrijednosnih papira po gotovini u DLT okruženju oslanjajući se na postojeće pristupe isporuke po plaćanju te inovativna rješenja DLT-a [13]. U trećoj fazi projekta istraživala su se inovativna rješenja za prekogranična plaćanja u različitim valutama [14], dok su u finalnoj četvrtoj fazi istraživanja obuhvaćala uravnoteživanje povjerljivosti i nadzora u DLT okruženju, odnosno, korištenje tehnika za unaprjeđenje privatnosti u svrhu osiguravanja povjerljivosti i učinkovitog nadzora transakcija na infrastrukturi financijskog tržišta [15].

Početkom 2018. godine Južnoafrička središnja banka započela je projekt Khokha čiji je cilj bio pružiti realističan test veleprodajnog platnog sustava temeljenog na DLT-u. Konkretnije, željelo se provjeriti može li takav sustav osigurati povjerljivost u produkcijskim opterećenjima i može li istodobno raditi s više vrsta čvorova koje bi konfigurirale različite banke sudionici. Projekt je dokazao da se za sedam različitih banaka, koje su uz središnju banku sudjelovale u projektu, na takvom sustavu može omogućiti normalan rad tipičnog dnevnog platnog prometa unutar Južnoafričke Republike koji uključuje osiguravanje povjerljivosti transakcija, konačnost namire te nadzor središnje banke [16].

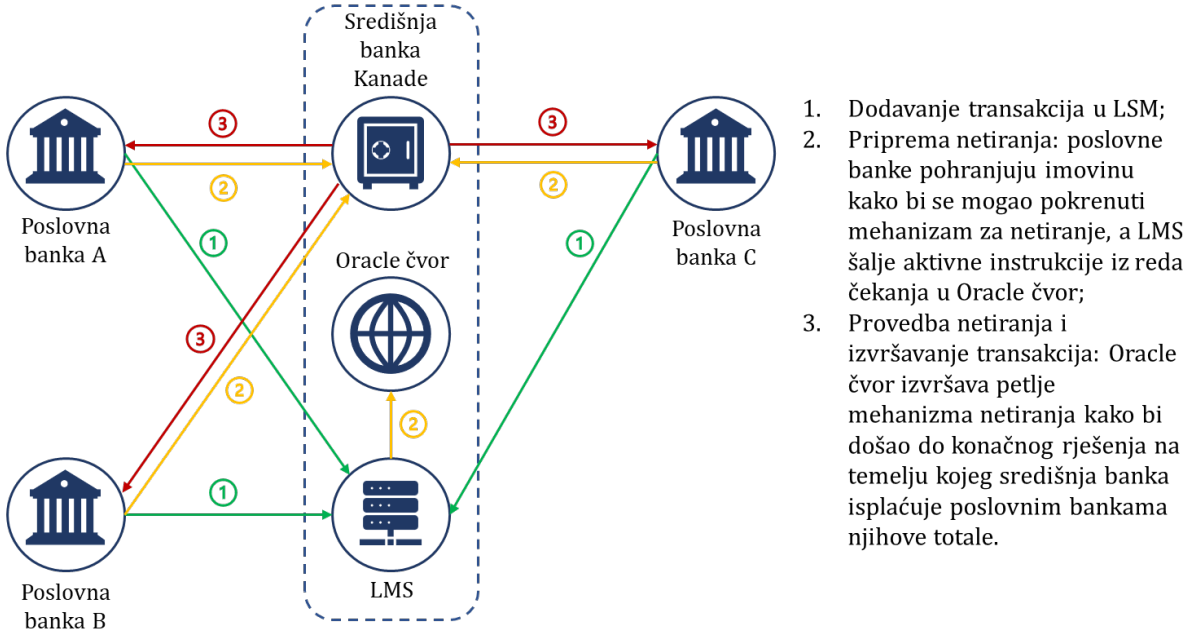
Osim navedenih središnjih banaka, istraživanja o mogućem korištenju DLT platformi u svrhe prijenosa vrijednosti provele su ili još uvijek provode i središnje banke Francuske, Australije, Engleske, Njemačke i Švicarske, no njihova istraživanja su provedena u mnogo manjem obimu od onih navedenih u ovom radu ili rezultati njihovih istraživanja nisu javno objavljeni u opsežnijem obliku.

### 3.1.1. Projekt Jasper središnje banke Kanade

Središnja banka Kanade je početkom 2016. godine, zajedno s organizacijom Payments Canada, operaterom kanadskog nacionalnog sustava za obračun i namiru, te tvrtkom R3 i nekoliko velikih poslovnih banaka u Kanadi pokrenula projekt Jasper s ciljem istraživanja upotrebe DLT-a za namiru međubankarskih plaćanja. U prvoj fazi projekta razvijen je sustav baziran na platformi Ethereum kojim se trebala omogućiti razmjena vrijednosti u obliku digitalne imovine za namiru koju je izdala središnja banka. Navedena imovina, nazvana digitalna depozitarna potvrda (engl. digital depository receipt, DDR), odražava potraživanje na depozite u kanadskim dolarima na računima u središnjoj banci Kanade te su poslovne banke u ovoj fazi morale založiti kanadske dolare u zamjenu za DDR-ove i obratno, otkupiti DDR-ove u zamjenu za dolare. Mehanizam konsenzusa *proof-of-work* koji je korišten u prvoj fazi zahtijevao je da svi članovi DLT sustava izvrše provjeru valjanosti transakcije kao uvjet da se transakcija evidentira u bazi podataka, no pokazalo se da navedeni mehanizam ne bi mogao osigurati dovoljan protok u slučaju većeg broja banaka i volumena transakcija. Nadalje, korištena izvedba omogućavala je svim čvorovima uvid u transakcije čime nije zadovoljen zahtjev za povjerljivošću podataka te ostvarenje konačnosti namire nije bilo izvjesno [8].

Za potrebe druge faze projekta sustav Jasper migriran je s platforme Etherum na platformu Corda tvrtke R3 koja uvodi koncept bilježničkog (engl. notary) čvora u jezgru mehanizma konsenzusa, uz čvorove sudionika i nadzornika. Konsenzus se na platformi Corda ostvaruje tako da čvorovi sudionika izvrše provjeru valjanosti transakcije, a zatim bilježnički čvorovi provjeravaju jedinstvenost transakcije, odnosno da korišteni DDR-ovi prethodno nisu već potrošeni. Kako bi se sačuvala povjerljivost podataka čvor sudionika pohranjuje samo vlastite transakcije, dok bilježnički i nadzorni čvorovi pohranjuju sve zapise o transakcijama. S obzirom da samo bilježnički i nadzorni čvorovi čuvaju potpunu bazu podataka, za razliku od sustava baziranog na platformi Ethereum u prvoj fazi,

potrebno je osigurati visoku dostupnost tih čvorova. Sustav je u drugoj fazi omogućavao različite modele namire, atomarnu (engl. atomic) opciju sličnu RTGS-u te opciju s mehanizmom čuvanja likvidnosti (engl. Liquidity-saving Mechanism, LSM) koja unaprjeđuje koordinaciju dolaznih i odlaznih plaćanja kako bi se onemogućila pojava zastoja. LSM omogućava korištenje centralnih redova i algoritama za uparivanje plaćanja slične vrijednosti kako bi se osigurala likvidnost i nesmetan tok transakcija [8].




Sl. 1 Koraci mehanizma čuvanja likvidnosti

Platforma Jasper, razvijena za potrebe ovog projekta, obuhvaća distribuiranu bazu podataka koja se sastoji od međusobno dogovorene i ovjerene evidencije o transakcijskoj aktivnosti između različitih sudionika platforme. Distribuirana baza podataka omogućava svakoj strani u transakciji da održava uobičajenu kopiju zapisa na vlastitim glavnim knjigama, kao i sinkronizirano emitiranje promjena u glavnoj knjizi u realnom vremenu svake stranke koja je za to ovlaštena. Da bi pokrenuo razmjenu DDR-a i izvršio transakciju s drugim članovima, sudionik mora kreirati tzv. DDR objekt koji sadrži sve bitne podatke o transakciji te se mora ostvariti konsenzus o legitimitetu transakcije između više strana da bi se objekt zapisao u bazu podataka. Nakon što se DDR objekt zapiše u bazu, mijenja stanje iz "nepotrošenog" u "potrošen", a saldo nepotrošenih DDR-ova platitelja odražavat će smanjeno stanje. Sudionici platforme putem elektroničkog novčanika, baziranog na Corda UTXO modelu, provode razmjenu i otkup DDR-ova te upravljaju poretkom transakcija. I u prvoj i u drugoj fazi projekta

sudionici su sve DDR-ove morali povratiti na kraju dana kako bi se izbjegla potreba isplate kamata na DDR-ove umjesto na gotovinske depozite sudionika [8].

Zaključak na kraju druge faze projekta bio je da će se korištenjem DLT platforme značajni napredak u učinkovitosti ostvariti jedino ako se na platformi mogu izvršavati namire različite vrste imovine. Na temelju tog zaključka pokrenuta je treća faza projekta Jasper u kojoj je cilj bio realizirati dokaz koncepta (engl. proof-of-concept) kod kojeg će se DLT platformu istodobno koristiti za trgovanje i namiru tokenizirane gotovine i dionica. Omogućavanje trenutne konačnosti namire rezultiralo je mogućnošću da se tokenizirana imovina odmah ponovo iskoristi čime se podržava učinkovitost likvidnosti. U navedenom dokazu koncepta uvedeni su novi tipovi čvorova s različitim ulogama, pa su tako uz čvor središnje banke Kanade, koji je odgovoran za tokeniziranje gotovine, čvora organizacije Payments Canada, koji je odgovoran za nadzor transakcija, bilježničkog čvora za provjeru jedinstvenosti transakcija i čvorova dosadašnjih sudionika, dodani čvorovi brokera te čvor Kanadskog depozitara za vrijednosne papire čija je odgovornost tokeniziranje dionica i namira transakcija. Tokeniziranje dionica slijedilo je model DDR-a kao sigurnih digitalnih potraživanja izdanih od strane Kanadskog depozitara za vrijednosne papire kao temeljnog kapitala koji se čuva kod navedene institucije [10].

Namira pojedinačnih neto pozicija u trećoj fazi projekta provodila se kao atomarna transakcija koja kao ulazne vrijednosti uzima poziciju koja se namiruje te tokene gotovine i dionica potrebne da se namira izvrši. Ako je transakcija uspješna sve ulazne vrijednosti se označavaju kao potrošene te se stvaraju novi tokeni koje je definirala pozicija, a ako se transakcija ne izvrši sve ulazne vrijednosti ostaju valjane i ne generiraju se nove izlazne vrijednosti. Posljedično, transakcijom se postiže isporuka po plaćanju, tj. trenutna i konačna razmjena dionica i novca za danu poziciju. Proces namire pokušava odraditi sve otvorene pozicije poredane prema Međunarodnom identifikacijski broju vrijednosnih papira (ISIN) i prema padajućoj vrijednosti te preskače one pozicije kod kojih druga strana nema dostatnu vrijednost tokena bilo u gotovini ili dionicama. Čitav proces se ponavlja dok ne postoje pozicije koje se mogu namiriti [10].

Labavo povezivanje uvjeta za obradu i provjera valjanosti za različite vrste imovine koje dopušta platforma Corda omogućava da promjene u dioničkim ugovorima,

transakcijama ili tokovima ne utječu na životni vijek gotovinskih tokena. Navedeno osigurava potpunu kontrolu nadzornih tijela nad imovinom koju izdaju na DLT sustav. Iako se dokazom koncepta uspješno demonstriralo da se DLT platforma može istodobno koristiti za namiru platnih transakcija i transakcija vrijednosnih papira, naposlijetku je zaključeno da opseg dokaza koncepta u trećoj fazi projekta nije bio dovoljno širok da bi se utvrdilo može li DLT platforma omogućiti značajno smanjenje troškova i povećanje učinkovitosti [10].

### 3.1.2. Istraživanje središnje banke Brazila

Potencijalne prednosti i dosadašnje primjene DLT tehnologije ponukale su središnju banku Brazila da pokrene istraživačku grupu kojoj je bio zadatak procijeniti i analizirati trenutno dostupne DLT platforme kako bi se bolje upoznala primjenjivost tehnologije i njene prateće mogućnosti. Cilj te istraživačke grupe bio je ustanoviti potencijalne probleme u postojećim sustavima u kojima bi DLT platforma mogla biti rješenje za situacije koje traže decentralizaciju i visoku otpornost na pojedinačne greške te identificiranje ograničenja navedene platforme koja su trenutno prisutna [11].

U prvoj fazi istraživanja, u kojoj je skupina unutar središnje banke Brazila tražila potencijalne kandidate za primjenu DLT platforme, odabrana su četiri interna sustava za daljnje istraživanje:

- sustav za upravljanje identitetom,
- sustav za plaćanje u lokalnoj valuti (SML),
- sustav za podršku sporazumu o uzajamnim plaćanjima i kreditima (CCR),
- alternativni sustav za namiru transakcija (SALT).

Koncept alternativnog sustava za namiru transakcija (SALT) koji bi bio alternativa za RTGS sustav središnje banke Brazila odabran je kao idealni kandidat za istraživanje kojim se htjelo provjeriti može li DLT podržati minimalni rad sustava namire u realnom vremenu u slučaju da katastrofa zaustavi rad RTGS sustava. Zahtjevi ovog dokaza koncepta bili su da se kreira DLT sustav s dozvolom u kojem će u trenutku pokretanja središnja banka izdati konačnu količinu novca na glavnoj knjizi te se novi novac neće moći generirati. Za svakog sudionika kreirao bi se elektronički novčanik te bi mu se sigurnim putem distribuirali ključevi, a središnja banka bi dodijelila stanja sudionicima

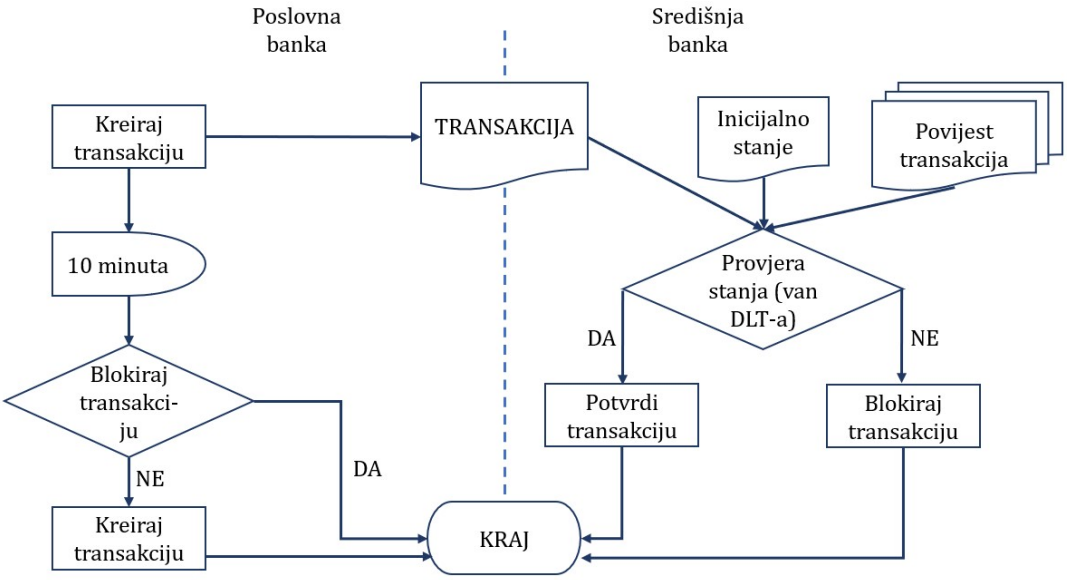
te bi sudionici putem vlastitih čvorova ili čvorova trećih strana mogli slati i primati novac. Središnja banka bila bi u mogućnosti nadzirati transakcije i stanja računa u bilo kojem trenutku, a sustav bi nakon pokretanja trebao moći funkcionirati i bez čvora središnje banke [11].

Kao DLT platforma za potrebe prve faze testiranja izabran je Ethereum koji omogućuje korištenje pametnih ugovora čime se ostavila opcija nadogradnje sustava u budućnosti, a sustav je razvijen na razvojnoj platformi BlockApps. Navedeni sustav omogućuje svim sudionicima uvid u transakcijske podatke, što onemogućuje željene zahtjeve za povjerljivošću podataka, što se pokušalo ispraviti enkripcijom početnih stanja računa javnim ključevima sudionika raspodijeljenih od strane središnje banke. Osim navedenog, središnja banka je generirala i svim sudionicima raspodijelila različite simetrične transakcijske ključeve kojima bi se onemogućilo uvid u transakcijske podatke drugih sudionika [11].

Kada sudionik želi poslati novac drugom sudioniku treba pročitati njegov transakcijski ključ korištenjem svog privatnog ključa te kriptirati transakciju pomoću navedenog transakcijskog ključa i pohraniti je na lanac blokova. Središnja banka može u svakom trenutku doći do transakcijskih ključeva i dekriptirati bilo koju transakciju, dok sudionici mogu pregledavati samo transakcije u kojima su i sami sudjelovali. Takvo spremanje kriptiranih transakcijskih podataka na lanac blokova uzrokuje dvije neželjene posljedice, nemogućnost da pametni ugovori dohvaćaju transakcijske podatke i mogućnost da se kompromitacijom ključeva omogući neovlaštenim stranama otkrivanje povijesti transakcija sudionika [11].

Na kreiranom sustavu transakcije se registriraju na lanac blokova u nepotvrđenom stanju kao prijedlozi i ne prikazuju se odmah kao promjene na stanjima računa. Prijedlog transakcije otvara vremenski interval za provjeru transakcije u kojem središnja banka mora promijeniti stanje transakcije u 'potvrđena' ili 'blokirana', ovisno o stanju računa, nakon čega pošiljatelj potvrđuje transakciju ako je središnja banka promijenila stanje transakcije u 'potvrđena'. Na taj način sprječavaju se prekoračenja kad je čvor središnje banke spojen na mrežu, no onemogućuju se sve transakcije u slučaju nedostupnosti navedenog čvora. Bez obzira što navedeno rješenje nije bilo idealno, središnja banka Brazila smatrala je da su rezultati prve faze pozitivni jer su

istraživači uspješno utvrdili potencijalne primjere korištenja te razvili uspješan prototip za odabrani slučaj [11].




Sl. 2 Dijagram toka izvođenja transakcije na sustavu izvedenom u prvoj fazi testiranja

Druga faza istraživanja fokusirala se na analiziranje drugih DLT platformi u kontekstu primjera alternativnog sustava za namiru transakcija osmišljenog u prvoj fazi. DLT platforme koje su izabrane za ovu fazu istraživanja su Hyperledger Fabric, platforma tvrtke IBM, Quorum, platforma bazirana na Ethereumu koju razvija tvrtka ConsenSys te prethodno spomenuta platforma Corda tvrtke R3.

Testiranje platforme Hyperledger Fabric provedeno je na verziji 0.6 navedene platforme na kojoj postoje 2 tipa čvorova, oni koji provode provjeru valjanosti i odgovorni su za izvršavanje pametnih ugovora i postizanje konsenzusa te oni koji ne provode provjeru valjanosti već samo čuvaju kopiju lanca blokova. Platforma je implementirana u smanjenoj razini privatnosti kod koje korisnici mogu pristupiti samo svojim podacima, no administratori čvorova mogu pristupiti svim podacima na lancu blokova. Za postizanje konsenzusa na ovoj platformi koristio se praktični algoritam tolerantan na bizantske greške (engl. practical byzantine fault tolerance, PBFT), a za potrebe istraživanja su pametni ugovori izvedeni programskim jezikom Go[2], dok je za ostatak koda korišten JavaScript[3]. Rezultat korištenja platforme Hyperledger Fabric bio je

[2] proceduralni programski jezik otvorenog koda

[3] objektno orijentirani programski jezik osmišljen za korištenje u mrežnim aplikacijama

zadovoljavajući u smislu da je koncept realiziran, no ostala su ista ograničenja vezana uz postizanje potpune privatnosti podataka kao i kod platforme Ethereum [11].

Platforma Quorum koja je također testirana u drugoj fazi istraživanja nadograđuje izvorni Ethereum protokol s mogućnostima za čuvanje tajnosti podataka, omogućuje korištenje različitih mehanizama konsenzusa i upravljanje dozvolama sudionika. Quorum dodatno proširuje dizajn platforme Ethereum uvodeći privatne kriptirane transakcije za sigurnu razmjenu podataka između čvorova, a čvorovi koji nisu dio privatnih transakcija primaju samo kriptografske sažetke podataka iz privatnih transakcija. Za osiguravanje konsenzusa korišten je QuorumChain algoritam s vremenskim ograničenjem koji definira tri moguće uloge čvora; tvorac, glasač ili promatrač. Tvorac generira blokove u ograničenom slučajnom vremenskom intervalu te ih predaje mreži gdje glasači analiziraju predložene transakcije i uspoređuju rezultirajući korijen sažetaka javnih stanja s novim blokom. Privatne transakcije potvrđuju i izglasavaju samo uključene strane, dok ostali čvorovi samo uspoređuju listu sažetaka privatnih transakcija [11].

Prototip izveden na platformi Quorum koristio je dva pametna ugovora kako bi se postigla funkcionalnost RTGS sustava. Prvi pametni ugovor, koji je sprječavao lažno predstavljanje, prijevare i mogućnost prekoračenja, sadržavao je podatke o privatnim transakcijama i stanju sredstava čvorova te je trebao biti implementiran na svakom čvoru. Drugi pametni ugovor čuvao je sažetke privatnih transakcija i informacije institucija koje su sudjelovale u njima. Navedene informacije pohranjivale su se najprije u nepotvrđenom stanju do trenutka potvrđivanja od strane regulatora i platitelja, kao u algoritmu korištenom u prvoj fazi. Takva izvedba prototipa osiguravala je zahtijevanu tajnost podataka no nije osiguravala prevenciju dvostruke potrošnje bez oslanjanja na čvor regulatora. Uz navedeno, korišteni algoritam konsenzusa nije osiguravao izvjesnost konačnosti namire kao i kod korištenja platforme Ethereum u prvoj fazi projekta Jasper [11].

Na platformi Corda naposlijetku nije realiziran koncept jer je procijenjeno da platforma u to vrijeme nije bila dovoljno zrela te su jako često mijenjane verzije izvornog koda platforme. Nadalje, prema procjeni istraživača, navedenoj platformi nedostajale su neke od njima važnih funkcionalnosti. Primjerice, čvorovi na platformi Corda moraju imati omogućen sustav oporavka od katastrofe s obzirom da su kod njih pohranjene samo

transakcije u kojima su sudjelovali. Nadalje, u ranijim verzijama ove platforme bilježnički čvorovi mogli su biti izvedeni kao oni koji provode provjeru valjanosti ili oni koji je ne provode, što nije zadovoljavalo inicijalne zahtjeve za nadzorom i dostupnošću. Naposljetku, nije potpuno bilo moguće zadovoljiti ni zahtjev za tajnošću povijesti transakcija jer je platforma tada bila izvedena da omogućava djelomičan uvid u transakcijske podatke bilježničkim čvorovima koji ne provode provjeru valjanosti i proročkim čvorovima koji se koriste za unos vanjskih podataka na platformu, a mogu biti u vlasništvu trećih strana [11].

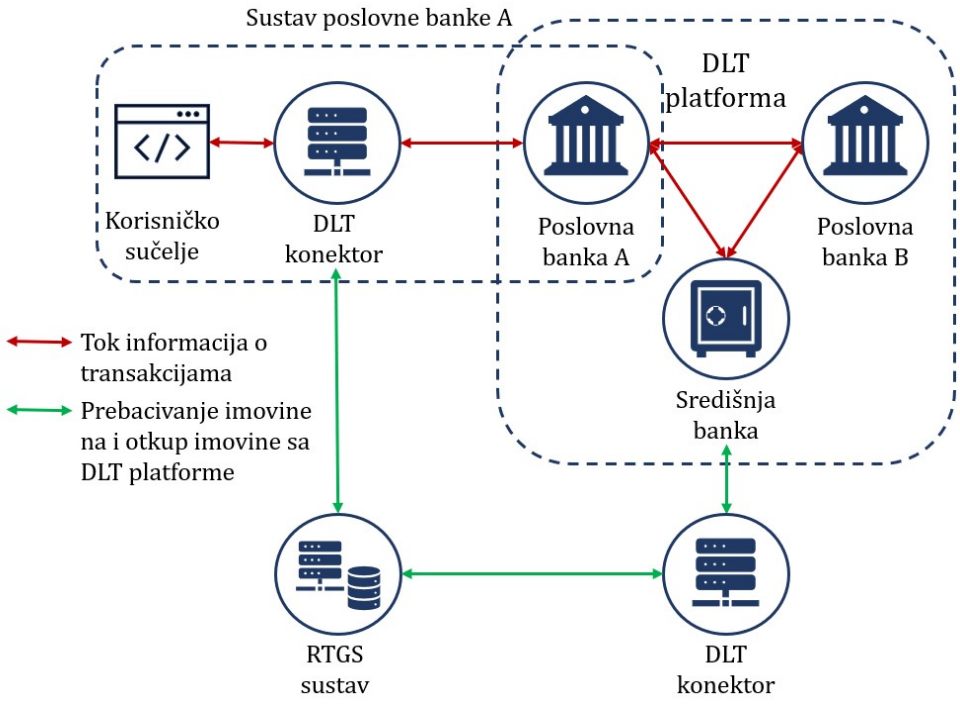
### 3.1.3. Projekt Ubin Monetarnog autoriteta Singapura

Krajem 2016. godine Monetarni autoritet Singapura (MAS) objavio je da zajedno s tvrtkom R3 i nekim od najvećih svjetskih financijskih institucija započinje rad na dokazu koncepta provođenja međubankarskih transakcija baziranog na DLT sustavu. Za projekt Ubin naposlijetku će se ispostaviti je vjerojatno najopsežnije istraživanje korištenja DLT platformi jedne središnje banke u svrhu izdavanja i razmjene veleprodajnog digitalnog novca. U prvoj fazi projekta iskoristio se MEPS+ sustav za provedbu neopozivih prijenosa sredstava i državnih vrijednosnih papira, kako bi se omogućilo prijenos sredstava i namira u realnom vremenu koristeći DLT. Osmišljen je prototip povezan sa MEPS+ i sustavom tekućih računa čime se omogućilo automatizirano upravljanje kolateralom koji je podržavao tok singapurskih dolara na DLT sustavu. Zahtjevi prototipa su bili da se na lancu blokova čuvaju stanja sredstava sudionika, da se u stvarnom vremenu stvaraju, prebacuju i uništavaju sredstva, da se omogući besprekidna provedba transakcija i da se navedeni prototip može integrirati u postojeći sustav za namire [17].

Za realizaciju prototipa izabran je sustav baziran na platformi Ethereum na kojem su banke mogle razmjenjivati novčane kolaterale na MEPS+ računima za digitalne depozitarne potvrde (DR) na DLT sustavu. Prototip se sastojao od dva čvora MAS-a na kojima se nalaze Ethereum i IBM Websphere Message Queue klijenti (WS MQ) od kojih jedan kreira izvorni blok (engl. genesis block) te osam čvorova banaka na kojima se nalaze Ethereum, WS MQ klijent i platni pristupnik (engl. payment gateway). Kontrolna ploča koja se nalazila na poslužiteljima MAS-a i bila povezana s MAS-ovim čvorovima služila je uvidu u stanje računa te pregled transakcija na lancu blokova. DLT mreža bila

je povezana s MEPS+ sustavom koristeći simulator SWIFT[4] poruka kako bi se automatizirali i sinkronizirali računi sa stanjima DR-a između ta dva sustava [17].

Svaki sudionik imao je otvorena dva računa na MEPS+ sustavu, RTGS račun i gotovinski račun za čuvanje DR kolaterala. Banke u radno vrijeme MEPS+ sustava mogu založiti gotovinske kolaterale tako što zadaju zahtjeve za prijenosom sredstava s RTGS računa na račun za čuvanje DR kolaterala čime se stvara ekvivalentno stanje na DR računu na DLT sustavu. Banke sudionici mogu u bilo kojem trenutku inicirati prijenos sredstava ili plaćanje na DLT sustavu te isto tako pokrenuti otkup sa svojih DR računa na DLT-u, što bi prebacilo sva sredstva na njihov račun za čuvanje DR kolaterala. Kamate za držanje sredstava se na DLT sustavu nisu isplaćivale jer su na taj način izvedeni i tekući računi na MEPS+ sustavu [17].




Sl. 3 Funkcionalna arhitektura prve faze projekta Ubin

Zaključci i naučene lekcije iz prve faze projekta bile su da bi ovakva izvedba Ethereum sustava generirala likvidnosni i kreditni rizik u slučaju da bi se poštovali regulatorni zahtjevi te ako bi ovakav sustav u stvarnom okruženju egzistirao usporedno s MEPS+

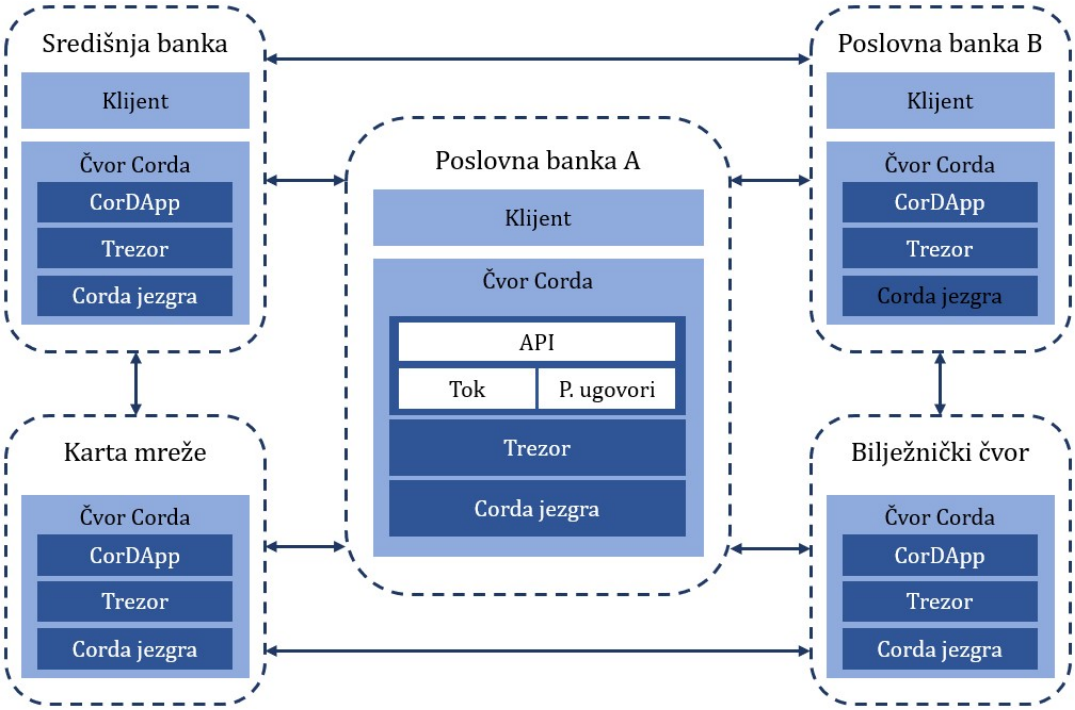
[4] engl. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) – organizacija koja povezuje više od 11000 financijskih institucija u 200 država kako bi koordinirala razmjenu i prijenos platnih poruka.

sustavom. Osim toga kod ovakve izvedbe postoji potreba za enkripcijom podataka u blokovima kako bi se osigurala tajnost podataka [17].

Cilj druge faze projekta Ubin bio je na tri različite DLT platforme razviti tri različita prototipa sa specifičnim funkcionalnostima RTGS sustava. Izabrane platforme bile su Corda, Hyperledger Fabric i Quorum koje bi za potrebe projekta bile podignute na Microsoft Azure infrastrukturi u oblaku. Ključni zahtjev koji su sustavi trebali ispuniti bilo je izvršiti prijenos sredstava na DLT-u sustavu koji omogućuje decentralizaciju te digitalizacija plaćanja uz korištenje mehanizma čuvanja likvidnosti (LSM) i bez ugrožavanja tajnosti podataka [18].

Prototip je za potrebe druge faze projekta na platformi Corda razvijen na verziji 1.0 te platforme koristeći Kotlin[5] kao glavni razvojni programski jezik. Sudionici su mogli provoditi transakcije u obliku *gotovine* kad bi platitelj imao dovoljno sredstava na raspolaganju, te u obliku *obveza* koje bi se uvrštavale u redni mehanizam ako platitelj u trenutku pokretanja transakcije nije imao dovoljno sredstava za namiru. Svaki čvor imao je trezor za pohranu stanja *gotovine* i *obveza* na UTXO modelu, a za potrebe svake nove transakcije stvarao se jedinstveni par javnih ključeva i certifikata za razmjenu među sudionicima transakcije kako bi se osigurala anonimnost. Uz trezor i Corda jezgru, svaki čvor sadržavao je i Corda distribuiranu aplikaciju (CorDApp) koja upravlja poslovnom logikom a sastoji se od namjenskog programskog sučelja, *tokova*, *ugovora* i *stanja*. Izvedeni sustav sastojao se i od bilježničkog čvora te servisa za mapiranje mreže koji upravlja i distribuira poznate javne ključeve i povezane fizičke IP adrese kako bi se omogućila identifikacija čvorova [18].

[5] objektno orijentirani programski jezik opće namjene



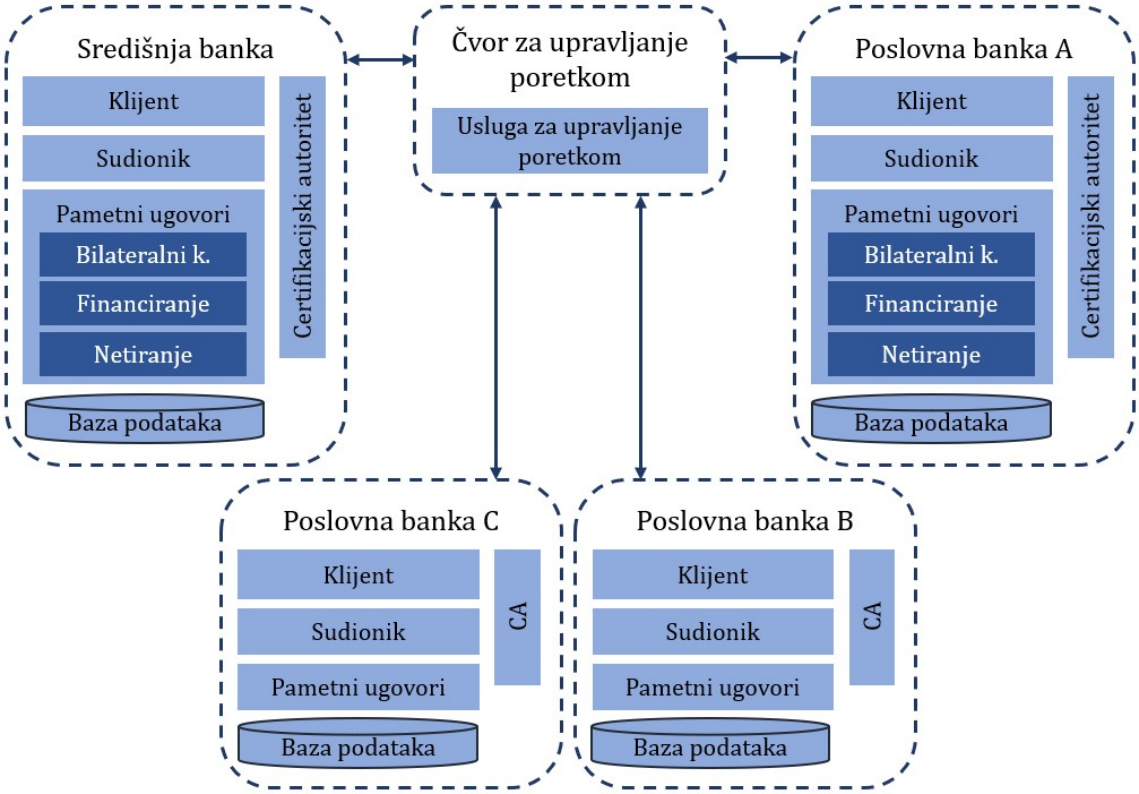

Sl. 4 Komponente arhitekture mreže na platformi Corda u sklopu druge faze projekta

Za realizaciju sustava na platformi Hyperledger Fabric korištena je inačica 1.0.1. te platforme i programski jezici Go, za razvoj pametnih ugovora nazvanih *chaincode* kojima se definira poslovna logika, te Node.js[6], za razvoj aplikacijskog sloja. Svaki sudionik na ovom sustavu imao je otvoreno više kanala kojima se omogućava uvid u samo one transakcije za koje postoji odgovarajuća dozvola. Bilateralni kanali otvoreni su za svaki različiti par banaka sudionika, za čije potrebe su banke morale održavati odvojene račune za svaki kanal što omogućava fleksibilnost dodjeljivanja različitih fiksnih iznosa likvidnosti za različite ugovorne strane. Uz to, sudionici su morali sudjelovati u dva multilateralna kanala, jedan za omogućavanje rješavanja zastoja nazvan kanal za netiranje (engl. netting) te drugi, nazvan kanal za financiranje, koji služi za provedbu prijenosa sredstava preko računa na razini bilateralnih kanala [18].

Dvostruka potrošnja sprječava se tako da sudionici moraju potvrditi da su transakcije u skladu s politikom odobravanja kako bi se osigurala ispravna dodjela i autentificiranje potpisa. Politika odobravanja različita je za svaki *chaincode* te definira koji je broj odobrenja i potpisa dovoljan za pojedinu transakciju. Za sve bilateralne transakcije politika odobrenja je definirana tako da zahtjeva odobrenje od obje banke koje sudjeluju

[6] izvršno okruženje otvorenog koda za pokretanje programa napisanih u JavaScript programskom jeziku

u tom kanalu. Čvor za upravljanje poretkom prima odobrene transakcije koje pakira u blokove i odašilje svim sudionicima na kanalu koji zatim provjeravaju valjanost transakcija prije nego što se bilježe u glavnu knjigu. Jedan ili više čvorova za upravljanje poretkom čine uslugu za upravljanje poretkom koja pruža zajednički komunikacijski kanal prema klijentima i sudionicima. Regulatorni čvor MAS-a sudionik je u svim bilateralnim i multilateralnim kanalima kako bi se omogućio nadzor nad transakcijama. Uz bazu podataka, klijent i *chaincode*, svaki čvor sudionik sadrži i svoj certifikacijski autoritet za upravljanje registracijom identiteta i certifikatom, te sudionik (Fabric Peer) koji prima ažurirana poredana stanja u blokovima od usluge slaganja te održava stanje glavne knjige [18].




Sl. 5 Komponente arhitekture mreže na platformi HL Fabric u sklopu druge faze projekta

Kod dizajna sustava na platformi Quorum MAS je koristio verziju 1.5 navedene platforme te mehanizam konsenzusa Raft, poznat po tome što se koristi za replikaciju kod distribuiranih baza podataka etcd[7], koji omogućuje brzo generiranje blokova i

[7] sustav za pohranu podataka visoke dostupnosti baziran na distribuiranim ključevima

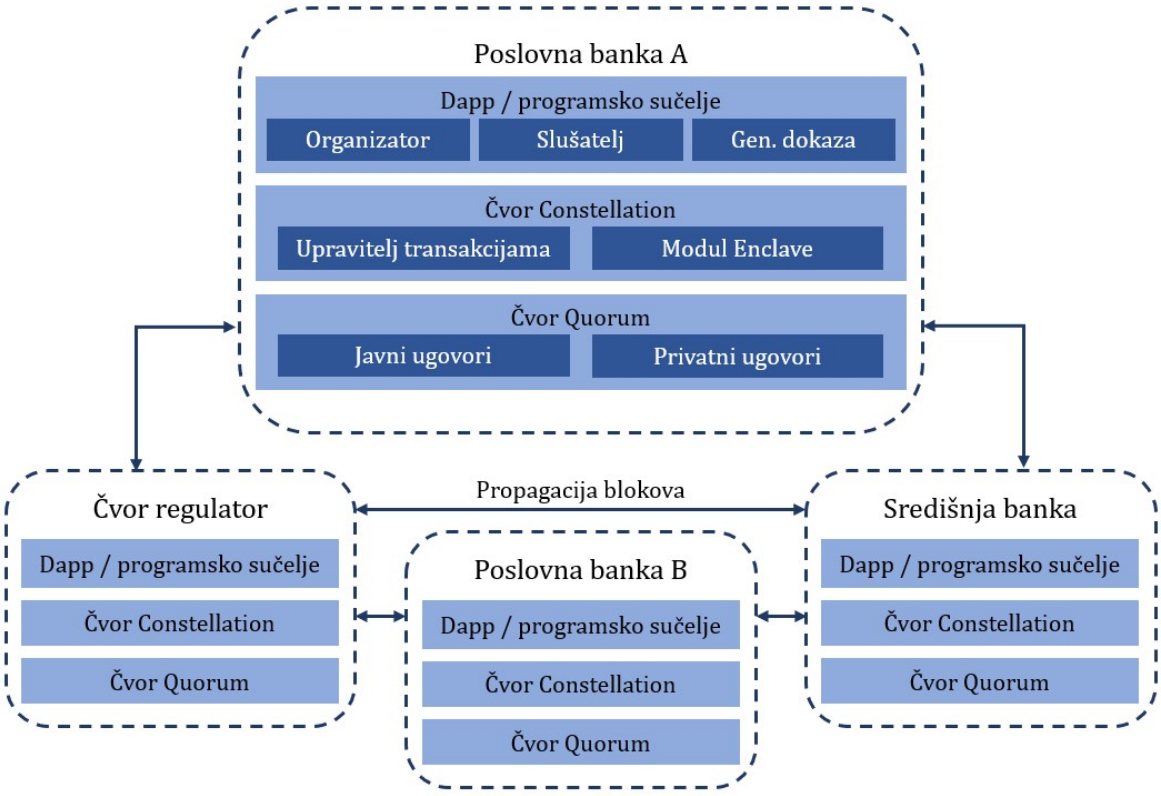
konačnost transakcija. Mehanizam Constellation[8] korišten je za osiguravanje tajnosti kriptiranjem potvrđenih i nepotvrđenih transakcija, dok je Zero Knowledge Security Layer (ZSL) protokol korišten za prebacivanje sredstava na DLT bez otkrivanja informacija o sudionicima i iznosima. Za pisanje pametnih ugovora korišten je programski jezik Solidity[9], a za potrebe razvoja aplikacijskog sloja korišten je Node.js [18].

Decentralizirana aplikacija Quorum (DApp), koja obavlja funkcije REST[10] sučelja te osluškuje događaje pametnih ugovora, odgovorna je za organiziranje različitih funkcionalnosti za provedbu plaćanja u pametnim ugovorima i generiranje dokaza bez znanja (engl. zero-knowledge proofs, ZKP). ZKP je ključna značajka uvedena u drugoj fazi projekta kako bi se očuvala tajnost podataka u odsutnosti centralnog autoriteta koja dokazuje da banka ima dovoljno sredstava kako bi provela javno plaćanje bez otkrivanja točnog stanja cijeloj mreži. Navedeni dokazi generiraju se izvan lanca blokova kao sažeci inicijalnih stanja, iznosa transakcija i finalnih stanja te se zatim šalju na lanac za provedbu provjere valjanosti. Kad ostali čvorovi potvrde dokaze oba sudionika transakcije, transakcija se potvrđuje ažuriranjem stanja računa [18].

[8] mehanizam za razmjenu kriptiranih privatnih poruka

[9] objektno orijentirani programski jezik namijenjen pisanju pametnih ugovora

[10] arhitekturni razvojni stil za razvoj programskih sučelja za mrežne servise

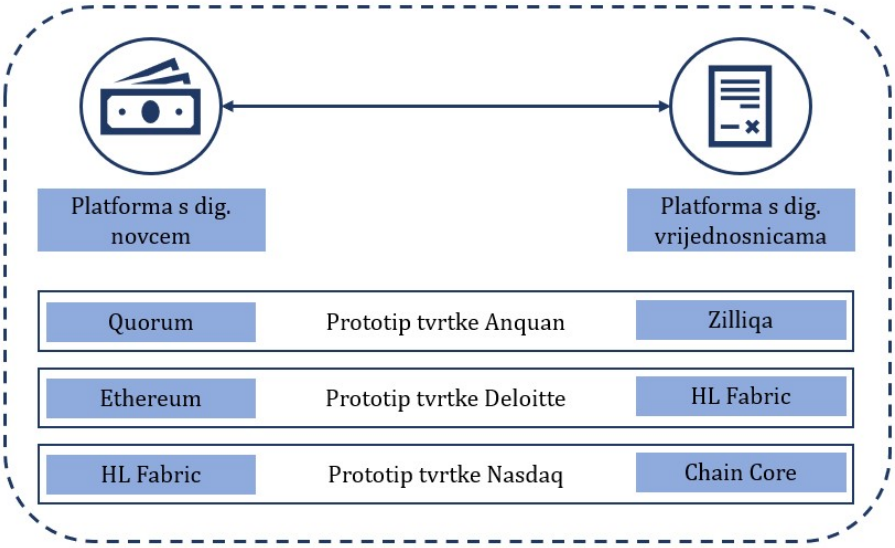



Sl. 6 Komponente arhitekture mreže na platformi Quorum u sklopu druge faze projekta

Sve tri izvedbe omogućavale su upravljanje redom čekanja transakcija uključujući izmjenu prioriteta i otkazivanje transakcija, te stavljanje na čekanje i reaktivaciju. Na platformi Corda ako platitelj nije imao dovoljno sredstava transakcija bi se generirala u obliku obveze, dok bi se nenamirene transakcije na platformi Hyperledger Fabric generirale kao nova transakcija u redu na bilateralnom kanalu. Kod platforme Quorum svaka banka održava svoj privatni red čekanja na kojem je popis nenamirenih transakcija, dok se globalni zastojni red koristi za nadzor svih transakcija na čekanju. Zaključak druge faze projekta bio je da su svi ciljevi uspješno dosegnuti; na sve tri platforme moglo se provoditi transakcije, izvoditi reprioritizaciju transakcija u redu čekanja te rješavati zastoje na decentralizirani način uz osiguravanje tajnosti podataka [18].

Trećom fazom projekta željelo se kreirati sustav koji podržava isporuke po plaćanju (DvP) dvije tokenizirane imovine, vrijednosnica vlade Singapura (engl. Singapore Government Securities, SGS) i digitalnog singapurskog dolara, između različitih DLT platformi. Za potrebe ove faze tri tehnološka partnera realiziralo je tri različita prototipa:

- tvrtka Anquan povezala je vlastiti verziju platforme Zilliqa s dozvolom i platformu Quorum,
- tvrtka Deloitte povezala je platforme Hyperledger Fabric i Ethereum,
- tvrtka Nasdaq povezala je platforme Chain Core i Hyperledger Fabric.




Sl. 7 Funkcionalna arhitektura treće faze projekta Ubin

Prototip tvrtke Anquan koristio je PBFT protokol za postizanje konsenzusa među čvorovima vlastite DLT platforme, dok je za razvoj pametnih ugovora korišten programski jezik Scilla[11]. Za zaštitu tajnosti podataka korištena je Intelova platforma Software Guard Extensions na kojoj su se nalazili svi čvorovi u mreži, a koja je osiguravala da svaki čvor može provjeriti valjanost svih transakcija otkrivajući autoriziranim sudionicima samo nekriptirane podatke. Iako je prototip omogućavao atomarne razmjene sredstava bez centraliziranog arbitra, njegova uloga bila je ključna jer može zaobići mehanizam vremenskog zaključavanja u slučaju neuspješnih razmjena i tako riješiti potencijalne likvidnosne rizike. Dodatno, pametni ugovor koji je omogućavao atomarnu razmjenu nije bio kompatibilan sa ZKP značajkom za očuvanje tajnosti platforme Quorum [19].

Rješenje koje je razvila tvrtka Deloitte koristilo je platformu Hyperledger Fabric kao glavnu knjigu za vrijednosnice te platformu Ethereum kao glavnu knjigu za digitalnu gotovinu. Povjerljivost podataka na DLT platformi za vrijednosnice osiguravala se

[11] programski jezik srednje razine za pisanje pametnih ugovora razvijen za potrebe platforme Zilliqa

prethodno spomenutim kanalima, a autorizirana treća strana korištena je za upravljanje ključevima. Atomarnost transakcija i DvP logika ugrađena je u pametne ugovore, dok je arbitar korišten kao pouzdana treća strana s uvidom u obje platforme za razrješavanje sporova. Kako bi se osigurala tajnost informacija sudionika tijekom provedbe razmjene sredstava, transakcije i namire mogu se izvršiti tek kad ovlašteni sudionik potpiše i odobri razmjenu sigurnom tajnom koju su izdali pružatelji usluga poput MAS-a ili Singapurske burze [19].

Iako je tvrtka Nasdaq koristila platformu Chain Core za izdavanje i namiru vrijednosnica, a platformu Hyperledger Fabric za digitalnu gotovinu, svoje rješenje za potrebe treće faze napravila je da bude neovisno o DLT platformama na kojima je bazirana digitalna imovina koja se među njima razmjenjuje. To se postiglo jedinstvenim programskim sučeljem koje može upravljati različitim DLT platformama i inicijacijom pametnih ugovora putem programskog alata koji je jednako tako nezavisan o DLT platformama. Iako je uspostavljen centralni arbitar kako bi se povećalo povjerenje u sustav, transakcije niže vrijednosti mogle bi se automatizirati kako bi se povećala učinkovitost i realizirala trenutna DvP namira. Sigurnost i tajnost na Chain Core DLT platformi osigurana je konfiguracijom s više ključeva i korištenjem HSM-a, dok se povjerljivost i anonimnost transakcija dodatno može osigurati korištenjem odvojenih kanala između sudionika transakcija kao i kod platforme Hyperledger Fabric [19].

Zaključak treće faze projekta Ubin bio je da se dokazala mogućnost korištenja pametnih ugovora u svrhu programiranja konvencionalnih uvjeta prema definiranim pravilima. Navedeno bi moglo rezultirati provođenjem regulatornih zahtjeva središnjih banaka nad sudionicima u različitim jurisdikcijama koji su sukladno tome podvrgnuti različitim stupnjevima nadzora i standardima usklađenosti. Također je zaključeno da je uloga arbitra neophodna za procjenu okolnosti spornih razmjena prije donošenja odluke o mogućem djelovanju, bilo da se radi o povratu sredstava platitelju ili nastavljanju transakcije i prijenosom sredstava na primatelja. Uloga arbitra također se može urediti pomoću pametnih ugovora koji su definirani na početku ciklusa namire ili nakon isteka gotovinskih ugovora [19].

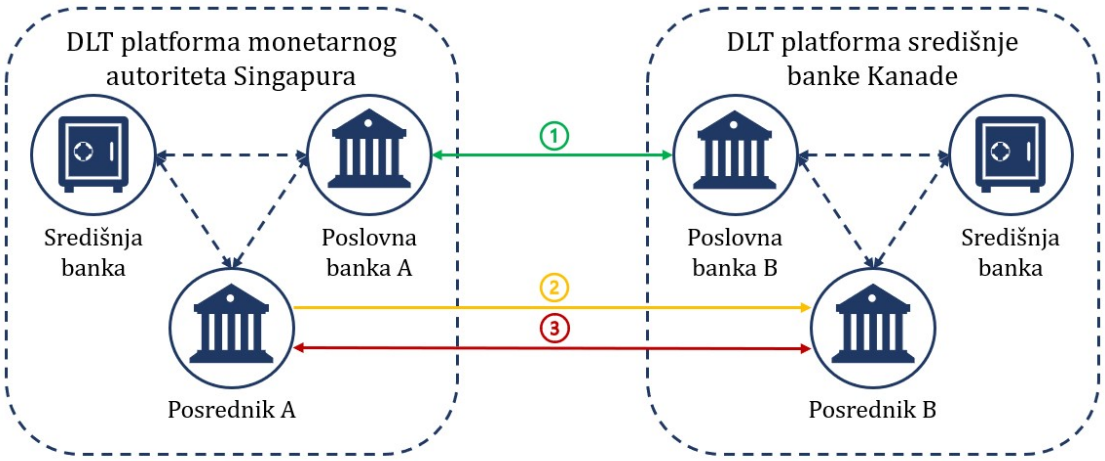
U četvrtoj fazi projekta Ubin MAS-u se priključila središnja banka Kanade kako bi zajedno utvrdili mogu li se korištenjem tehnoloških inovacija provesti sigurna prekogranična plaćanja i ostvariti druge pogodnosti u okruženju heterogenih DLT

platformi. Prekogranična plaćanja se uobičajeno izvode preko nekoliko povezanih transfera na različitim glavnim knjigama koristeći niz posredničkih transakcija između različitih povezanih financijskih institucija. Takva plaćanja često uključuju razmjenu valuta (engl. foreign exchange, FX) s obzirom da platitelj sredstva čuva u vlastitoj domaćoj valuti (eng. local currency, LCY), dok bi primatelj htio primiti sredstva u njegovoj domaćoj valuti, označenoj kao strana valuta u transakciji (engl. foreign currency, FCY). U tom slučaju transakcija će se realizirati u nekoliko logičnih koraka. Platitelj će prebaciti sredstva FX posredniku u domaćoj valuti, zatim će FX posrednik prebaciti sredstva u stranoj valuti direktno primatelju ili najprije platitelju, nakon čega će platitelj primatelju prebaciti navedena sredstva u stranoj valuti. U svakom slučaju takve transakcije sudionike u njima izlaže riziku treće strane [20].

Za smanjenje rizika namire korištenjem posrednika i osiguravanje atomarnosti transakcija predloženo je korištenje sažetih vremenski zaključanih ugovora (engl. Hashed Time-Locked Contracts, HTLC) koji se koriste za razmjenu sredstava između različitih DLT platformi. HTLC protokol ne zahtjeva korištenje FX posrednika već se koriste založni (engl. escrow) računi kojima autonomno upravljaju pametni ugovori prema definiranim pravilima koji mogu koristiti druge sudionike ili centralne operatere kao posrednike. U prvom slučaju kad bi banke koristile druge sudionike kao posrednike morali bi postojati sudionici koji posluju i na domaćoj i na stranoj mreži, dok bi u drugom slučaju i domaća i strana mreža morale podržavati račune i transakcije u različitim valutama [20].

Transakcije se putem HTLC protokola izvrše tako da platitelj od primatelja zatraži sažetak H(S) koji je generirao koristeći svoju tajnu S, nakon čega platitelj kreira pametni ugovor s informacijom o primatelju, iznosu i sažetku te pohrani iznos u založni račun na domaćoj mreži. Domaća mreža tada otvara vremenski period u kojem se transakcija mora izvršiti te platitelj posredniku šalje informacije o transakciji. Posrednik na domaćoj mreži tada zatraži informacije o pametnom ugovoru te šalje informacije o transakciji posredniku na stranoj mreži koji prema njima kreira drugi pametni ugovor i otvara vremenski period za izvršavanje koji mora biti kraći od onog otvorenog na domaćoj mreži. Posrednik na stranoj mreži tada polaže sredstva na založni račun i zaključava ga te obavještava primatelja o tome i šalje mu informaciju o njegovom sažetku H(S). Primatelj tada koristi svoju tajnu S da bi otključao pametni ugovor i oslobodio sredstva

na založnom računu te šalje tajnu posredniku na stranoj mreži koji je zatim prosljeđuje posredniku na domaćoj mreži. Posrednik na domaćoj mreži tada koristi tajnu S za otključavanje pametnog ugovora na domaćoj mreži ne bi li preuzeo sredstva sa založnog računa na domaćoj mreži [20].




1. Razmjena sažetka H(S) nakon čega posl. banka A pokreće izvršavanje HTLC ugovora;
2. Slanje informacija o transakciji nakon provjere HTLC ugovora od strane posrednika A;
3. Razmjena tajne S i kompletiranje HTLC ugovora.

Sl. 8 Koraci izvršavanja HTCL razmjene između različitih DLT platformi

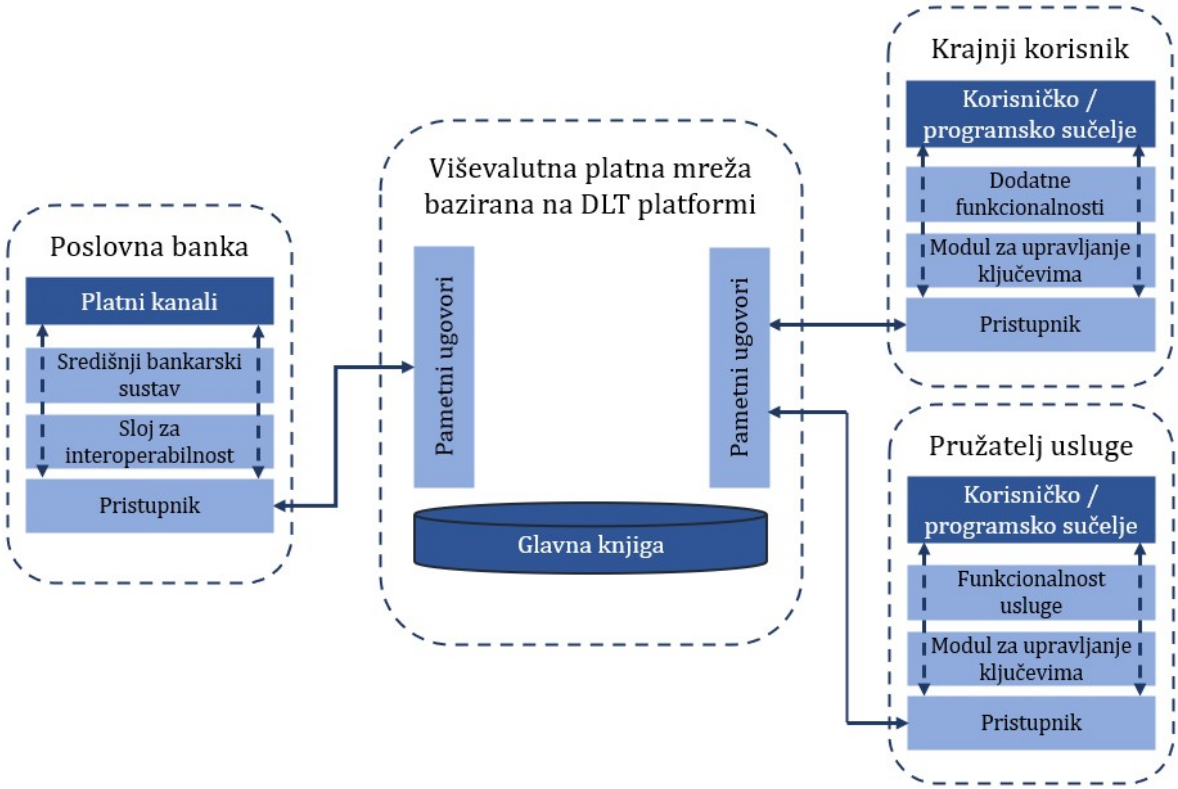
Za ostvarivanje dokaza koncepta MAS i središnja banka Kanade ipak su zbog jednostavnosti koristili pristup s posrednikom kako bi dokazali mogućnost atomarne transakcije između dva različita DLT sustava. Prvi DLT sustav u nadležnosti MAS-a bio je baziran na platformi Quorum, dok je drugi, onaj u nadležnosti središnje banke Kanade, bio baziran na platformi Corda. Posrednik je bio sudionik na oba sustava i imao je čvorove na obje mreže, a transakcije su izvršene koristeći HTLC protokol. Zaključak četvrte faze bio je da je moguće uspješno prebaciti sredstva u različitim valutama između različitih DLT sustava. Osim uspješnih transakcija, testirano je i nekoliko scenarija s neuspjelim transakcijama te je utvrđeno da je HTLC protokol dovoljno robustan za upravljanje takvim situacijama. No, da bi se navedeni protokol mogao implementirati, platforma mora omogućavati zaključavanje sredstava, zaštićeni prijenos informacija putem redundantnih komunikacijskih kanala i vremensko ograničavanje transakcija [20].

Posljednja peta faza projekta Ubin, koja je završena 2020. godine, za cilj je imala razviti prototip platnog sustava baziranog na DLT platformi koji podržava plaćanje različitim valutama. Navedeni sustav trebao je omogućiti povezivanje različitim sustavima

baziranim na drugim DLT platformama putem sučelja kako bi se lagano mogli povezati i integrirati. Osim toga, ovom fazom projekta željelo se istražiti i poslovnu vrijednost plaćanja baziranog na DLT sustavima omogućavanjem poslovnih prilika koje bi mogle imati koristi ili bi bile održive zahvaljujući ekonomičnosti DLT sustava u usporedbi sa postojećim sustavima. U sklopu tog toka ove faze pokrenuto je 40 radionica s različitim partnerima koje su iznjedrile 124 projekata od kojih je 16 odabrano za daljnje istraživanje te pretočeno u primjere korištenja [12].

U tehničkom toku pete faze MAS-ov partner tvrtka J.P.Morgan iskoristila je DLT platformu Quorum, vlastiti servis za rješavanje zastoja u plaćanjima Interbank Information Network (IIN)[12] te JPM Coin, svoju aplikaciju za izdavanje *stablecoin*-ova i prijenos sredstava, za razvoj platne mreže spremne za produkcijsko korištenje. Razvijena platna mreža nazvana Ubin V osmišljena je da omogući jednostavan pristup svim sudionicima, primjerice, izdavateljima digitalnog novca, drugim platformama i krajnjim korisnicima. Funkciju izdavatelja mogu provoditi središnje banke, koje bi izdavale CDBC, ili poslovne banke, koje mogu izdavati vlastiti digitalni novac koji bi funkcionirao poput kliringa stranih valuta u inozemstvu. Sudionici mogu direktno međusobno provoditi transakcije u različitim valutama koristeći namiru plaćanja po plaćanju (engl. payment-versus-payment, PvP) na taj način smanjujući rizik od namire u stranoj valuti [12].

[12] platforma IIN je krajem 2020. godine preimenovana u Liink




Sl. 9 Funkcionalni dijagram infrastrukture platne mreže Ubin V

Osim osnovnih funkcionalnosti provođenja plaćanja i pregleda statusa transakcija, Ubin V omogućava namiru isporuke po plaćanju, založna te uvjetovana plaćanja koristeći pametne ugovore, dok uvjete i kontrole za ta plaćanja definiraju financijske institucije na mreži. Pristup mreži omogućen je korištenjem različitih elektroničkih novčanika putem izloženog sučelja, kako bi se omogućilo korisnicima da putem jednog novčanika pristupaju različitim sustavima kao što je Ubin V. Platna mreža je razvijena da omogućava međubankarska i poslovna plaćanja, a testirana je korištenjem dviju različitih valuta, singapurskih dolara i američkih dolara, te s namjerom da druge središnje banke i poslovne banke ponude vlastite valute. Komunikacija na mreži zaštićena je korištenjem dva seta ključeva, jednih za razmjenu poruka koji kriptiraju i dekriptiraju transakcijske podatke te ključeva kojima se potpisuju transakcije predane DLT sustavu. Pohrana ključeva za potpisivanje transakcija omogućena je pomoću tri modela čuvanja, korištenjem usluge novčanika treće strane, korištenjem banke posrednika ili samostalnu pohranu ključeva krajnjeg korisnika [12].

Završna faza projekta Ubin također se željela fokusirati i na iskorištavanje efikasnosti DLT sustava za ekonomiju te je u tu svrhu identificirano 124 mogućih projekata s primjerima korištenja koji bi mogli iskoristiti tokeniziranu imovinu na ovakvoj DLT

platformi. Od tih 124 projekata 16 je izabrano za daljnje istraživanje, a četiri su razvijena u prototipove te testirana i predstavljena u sklopu FinTech Festivala u Singapuru u studenom 2019. godine. Prototip privatne burze 1exchange omogućavao je trgovanje dionicama privatnim poduzećima, dok je fintech tvrtka STACS u sklopu svog prototipa razvila platformu za trgovanje i namiru koja omogućava izdavanje i upravljanje životnim vijekom vrijednosnih papira. Osim navedenih prototipova, tvrtka Digital Ventures razvila je platformu Procure-to-Pay za razmjenu dokumentacije o nabavi s automatiziranom provjerom dokumenata i obradom plaćanja, a tvrtka Digital Asset osmislila je platformu za upravljanje životnim vijekom potraživanja iz domene zdravstvenog osiguranja [12].

Zaključci finalne faze projekta Ubin bili su da je povezivost bolja korištenjem zajedničke platforme, a čvršća integracija platformi poboljšava vidljivost i sigurnost transakcija te smanjuje potrebu za namirom na različitim platformama. Bolja povezivost i čvršća integracija omogućavaju automatizaciju plaćanja i procesa, no potrebno je voditi računa o razinama dozvola trećih strana koje upravljaju ključevima kako im se ne bi omogućila potpuna kontrola korisničkih računa [12]. Platna mreža Ubin V i dalje je dostupna središnjim bankama i financijskim institucijama kao testna mreža za omogućavanje i olakšavanje suradnje na području infrastrukture prekograničnih plaćanja sljedeće generacije, a tehničke specifikacije mreže javno su dostupne kako bi potaknule daljnji razvoj industrije [21].

### 3.1.4. Projekt Stella Europske središnje banke i središnje banke Japana

U prosincu 2016. godine ECB i središnja banka Japana objavile su da započinju sa zajedničkim istraživačkim projektom Stella s namjerom da doprinesu široj raspravi o upotrebljivosti DLT sustava u sklopu infrastrukture financijskog tržišta te istraže mogu li inovacije omogućiti sigurnije, brže i jeftinije financijske transakcije. U prvoj fazi projekta željelo se analizirati mogu li se određene funkcije postojećih platnih sustava,

posebice mehanizmi čuvanja likvidnosti (LSM) sustava BOJ-NET[13] i TARGET2[14], sigurno i učinkovito prebaciti u DLT okruženje [22].

Za potrebe analize u prvoj fazi projekta korištena je platforma Hyperledger Fabric, verzije 0.6.1, na kojoj su svi sudionici pohranjivali informacije o svim provedenim transakcijama koje su kontinuirano usklađivane koristeći algoritam konsenzusa PBFT. Za potrebe razvoja poslovne logike osmišljena su dva pametna ugovora, jedan jednostavan za obradu plaćanja bez mogućnosti čekanja transakcija u redu i prebijanja transakcija, te drugi koji je uključivao LSM logiku temeljenu na redovima čekanja i bilateralnim mehanizmima za prebijanje sustava TARGET2 i BOJ-NET. Kako bi usporedili rezultate testiranja, logika pametnih ugovora najprije je testirana izvan DLT sustava, pa samo na jednom čvoru bez mehanizma konsenzusa te zatim na distribuiranom DLT sustavu [22].

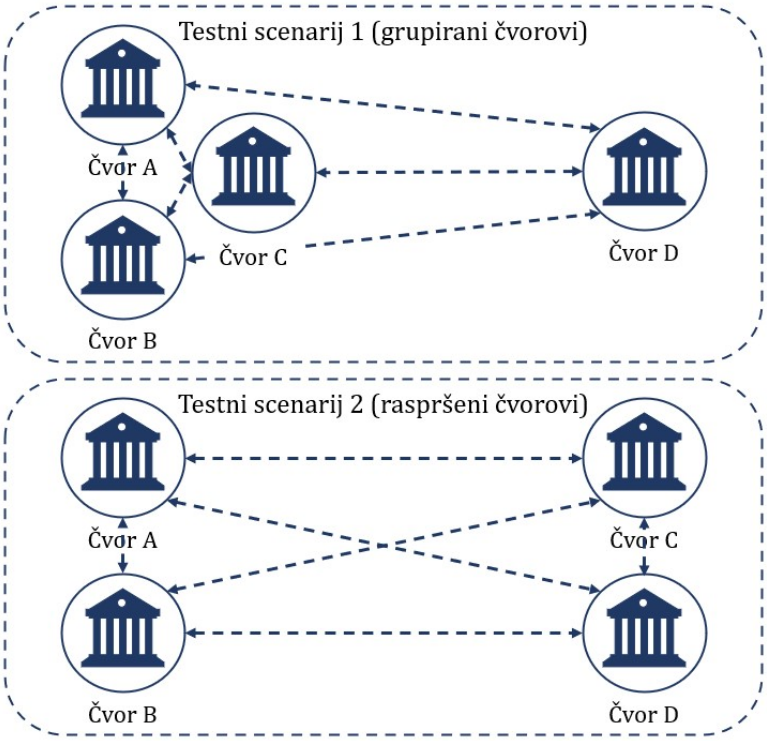
Testiranja su provedena zasebno od strane ECB-a i središnje banke Japana na odvojenim testnim okruženjima koristeći simulirane podatke koji su, ovisno o vrsti testa, unošeni u konstantnim intervalima ili replicirajući stvarne uzorke transakcija tijekom dana. Mjerena je latencija sustava kao vrijeme od trenutka u kojem je transakcija poslana do trenutka u kojem je zapisana u blok na svim čvorovima pod opterećenjima od prosječne dnevne količine prometa do maksimuma od 250 transakcija u sekundi. Fokus testiranja otpornosti bio je na tri specifična scenarija funkcioniranja sustava. U prvom scenariju je privremeno bio nedostupan jedan od čvorova koji sudjeluje u potvrdi valjanosti transakcija, u drugom je privremeno bio nedostupan čvor koji se koristi za certifikaciju sudionika i transakcijskih zahtjeva, dok je kod trećeg scenarija dio zadanih transakcija koristio neprimjerene formate podataka [22].

---

[13] RTGS sustav u vlasništvu središnje banke Japana za namiru plaćanja koja proizlaze iz transakcija na novčanom tržištu, transakcija vrijednosnim papirima, plaćanja klijenata, operacija monetarne politike i transakcija koje proizlaze iz neto platnih sustava privatnog sektora i druge infrastrukture financijskog tržišta

[14] RTGS sustav u vlasništvu Eurosystem-a za namiru plaćanja koja se odnose na operacije monetarne politike, međubankarska plaćanja i plaćanja klijenata, te plaćanja koja se odnose na poslovanje svih sustava neto namire velike vrijednosti i druge infrastrukture financijskog tržišta koja služi upravljanje Eurom

Oba zasebno provedena testiranja došla su do istih rezultata. U prvoj simulaciji s jednostavnim pametnim ugovorom potvrđena je veza između latencije i broja čvorova na sustavu. Prosječna latencija u testiranju sustava s brojem čvorova između 4 i 65 bila je 0.6 sekundi, a najveća vrijednost dosezala je 1.6 sekundi kod sustava s 65 različitih čvorova. U drugoj simulaciji, koristeći pametni ugovor s LSM-om, transakcije su trajale 0.01-0.02 sekundi duže nego u prethodnom testu što je dovelo do zaključka da korištenje takvog mehanizma ne utječe značajno na sustav. Testiranje utjecaja udaljenosti među čvorovima provedeno je na četiri čvora s time da je u prvom scenariju jedan čvor bio udaljen do ostatka čvorova dok su kod drugog scenarija dva čvora bila udaljena od druga dva čvora. Udaljenost je simulirana vremenom povratka od 12 milisekundi, procijenjeno vrijeme povratka poruke između Rima i Frankfurta ili Osake i Tokija, te 228 milisekundi što je procijenjeno vrijeme povratka poruke između Frankfurta i Tokija [22].




Sl. 10 Testni scenariji za testiranje utjecaja udaljenosti među čvorovima

Testovi otpornosti i mogućeg utjecaja DLT sustava na sigurnost također su provođeni koristeći sustav sa četiri čvora. Testiranje kod kojeg je privremeno bio nedostupan jedan od čvorova koji sudjeluje u potvrdi valjanosti transakcija pokazalo je da dostupnost cjelokupnog sustava nije ugrožena sve dok je broj operativnih čvorova veći ili jednak onome koji je potreban za konsenzus. U slučaju nedostupnosti certifikacijskog

autoriteta, koji na platformi Hyperledger Fabric registrira i autentificira sudionike i transakcije, transakcije se odbijaju i šalju se obavijesti o nedostupnosti sustava. Pomoću mehanizma za otkrivanje grešaka ugrađenog u pametne ugovore provelo se testiranje sa slanjem transakcija neprimjerenih formata podataka. Testovi s velikim brojem poruka neprimjerenog formata pokazali su da sustav nema poteškoća s obradom transakcija u ispravnom formatu bez obzira na postotak pogrešno formatiranih poruka [22].

Zaključak prve faze projekta bio je da rješenja bazirana na DLT-u mogu zadovoljiti performansne zahtjeve RTGS sustava te da performanse takvog sustava ovise o broju čvorova i udaljenosti između čvorova. Naime, analiza testiranja pokazala je da DLT sustav može bez problema obraditi prosječne volumene prometa centraliziranih RTGS sustava u Japanu ili unutar eurozone. Osim toga testiranja su dokazala izvedivost implementacije logike za LSM u DLT sustavu te je potvrđeno da povećanje broja čvorova na sustavu dovodi do povećanja vremena potrebnog za izvršavanje transakcija. Analiza je također pokazala da udaljeniji čvorovi mogu utjecati na brzinu donošenja konsenzusa, no utjecaj udaljenosti među čvorovima je minimalan sve dok je dovoljan broj čvorova potreban da se donese konsenzus na relativno maloj udaljenosti. Dodatno, jedan od zaključaka ove faze bio je i da DLT sustavi imaju potencijal da podignu razinu otpornosti i pouzdanosti infrastrukture financijskog tržišta [22].

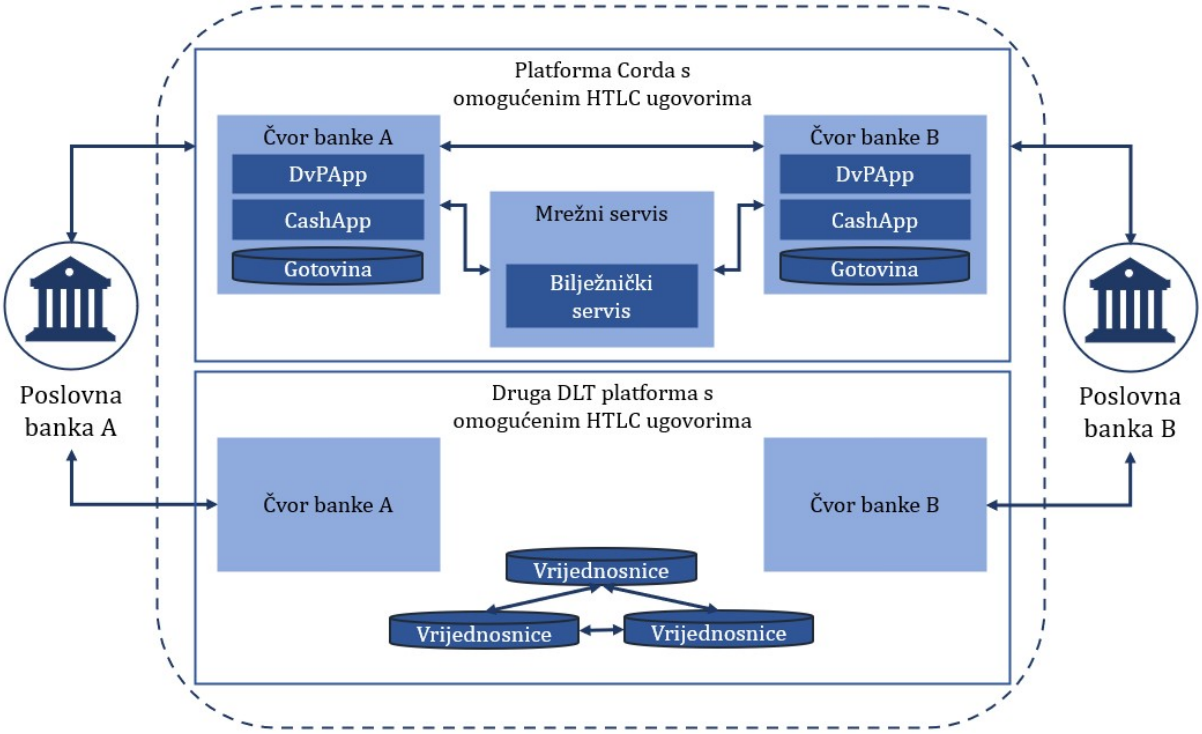
Druga faza projekta istraživala je načine na koje se može konceptualno osmisliti i tehnički ostvariti isporuke po plaćanju (DvP) u DLT okruženju na temelju dosadašnjih iskustava s DvP modelima i inovativnim rješenjima koje omogućuju DLT platforme. Za potrebe navedenog istraživanja razvijeni su prototipovi rješenja na platformama Corda verzije 2, Elements verzije 2.14.1.1, te Hyperledger Fabric verzije 1.1.0-alpha. Analiza je provedena na jednostavnom scenariju gdje dvije strane razmjenjuju vrijednosnice za novac u dvije različite izvedbe okruženja. U prvoj su vrijednosnice i novac zabilježeni na istom DLT sustavu, dok se u drugoj situaciji nalaze na različitim sustavima u sklopu koje se moraju implementirati mehanizmi koji će povezati transfere navedene imovine. Izvedbu s dva različita DLT sustava dodatno možemo razložiti na dva tipa; jedan koji koristi direktnu ili indirektnu vezu između dva sustava koji dodatno može zahtijevati korištenje posrednika koji će koordinirati sudionike na različitim sustavima, te drugi u kojem ne postoji veza između sustava [23].

Analiza druge faze projekta usredotočila se na testiranje izvedbe s jednim DLT sustavom te dva nepovezana sustava na koji oba sudionika transakcije imaju pristup te koji za ostvarivanje isporuka po plaćanju (DvP) koristi HTLC protokol. Kod izvedbe s jednim DLT sustavom razmjena se provede kao jedna transakcija kad se sudionici dogovore oko imovine koju će razmijeniti. Jedan sudionik kreira instrukciju za potrošnju vrijednosnica te je šalje drugom koji prethodno kreira instrukciju za potrošnju gotovine. Drugi sudionik tada provjerava podatke u instrukciji s vrijednosnicama, potpisuje vlastitu instrukciju s gotovinom te kombinira dvije instrukcije u krajnji set instrukcija koje šalje prvom sudioniku. Prvi sudionik zatim provjerava krajnji set instrukcija, potpisuje svoju instrukciju s vrijednosnicama te objavljuje krajnji set s obje potpisane instrukcije za potvrdu valjanosti [23].

U izvedbi s dva nepovezana DLT sustava, nakon što se sudionici dogovore o iznosima, tipu imovine, vremenu zaključavanja i funkciji sažimanja koja će se koristiti u HTLC protokolu, prvi sudionik generira tajnu S. Sažetak tajne H(S) zatim šalje drugom sudioniku te generira instrukciju s vrijednosnicama s uvjetom da će drugi sudionik dobiti vrijednosnice ako dostavi tajnu S' za koju vrijedi H(S)=H(S') ili će prvi sudionik vrijednosnice dobiti natrag nakon što istekne vrijeme zaključavanja. Nakon toga prvi sudionik potpisuje svoju instrukciju i objavljuje je na DLT sustav s vrijednosnicama, te se ona upisuje na glavnu knjigu nakon postizanja konsenzusa. Drugi sudionik nakon potvrde valjanosti instrukcije s vrijednosnicama generira svoju instrukciju s gotovinom s uvjetom da će prvi sudionik dobiti gotovinu ako dostavi tajnu S' koja zadovoljava H(S')=H(S) ili će drugi sudionik gotovinu dobiti natrag nakon što istekne vrijeme zaključavanja koje mora biti kraće nego ono u prvoj instrukciji. Drugi sudionik zatim potpisuje svoju instrukciju i objavljuje je na DLT sustav s gotovinom te se ona upisuje na glavnu knjigu nakon postizanja konsenzusa. Prvi sudionik provjerava valjanost prve instrukcije s gotovinom te generira instrukciju za preuzimanje gotovine u koju uključi i tajnu S, potpisuje navedenu instrukciju i šalje je na DLT sustav s gotovinom. Drugi sudionik tada dolazi do tajne S te generira instrukciju za preuzimanje vrijednosnica s uključenom tajnom S, potpisuje navedenu instrukciju i šalje je na DLT sustav s vrijednosnicama na provjeru valjanosti [23].

Na platformi Corda svaki čvor može pokretati više različitih aplikacija (CordApp) koje mogu upravljati različitim klasama imovine. Za potrebe testiranja s jednim DLT

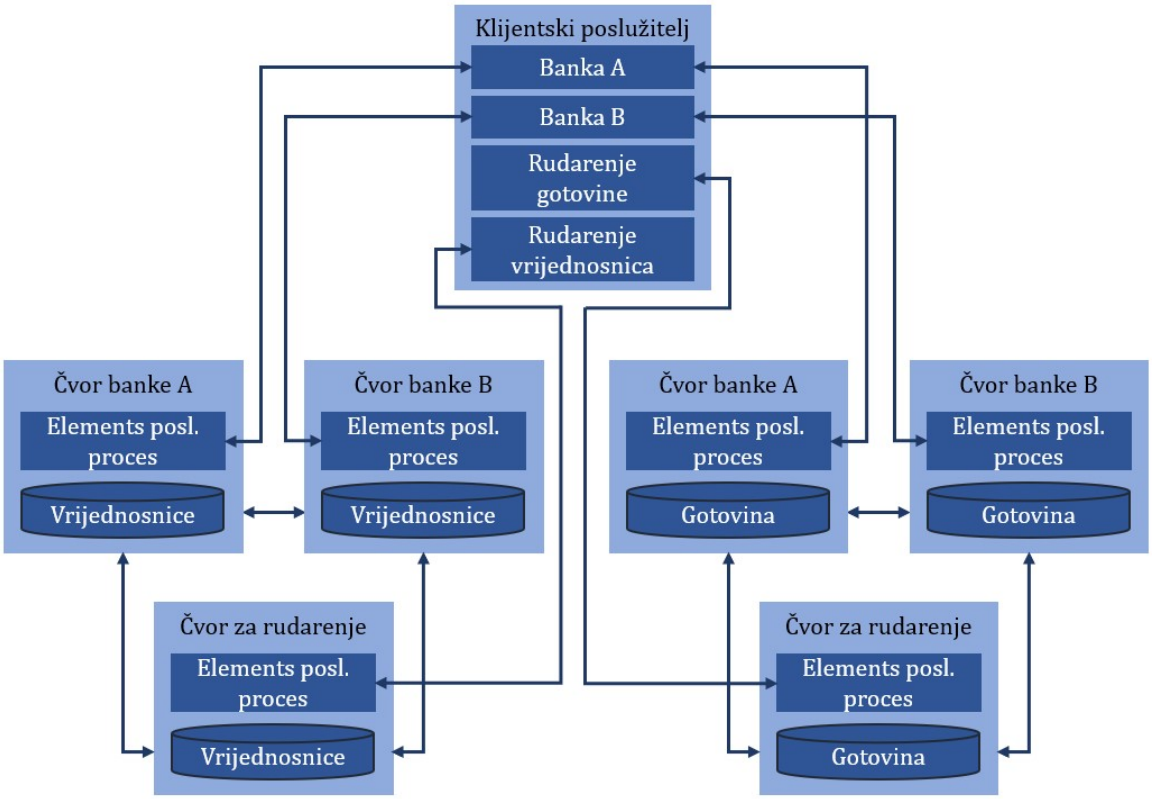
sustavom na platformi Corda svaka banka imala je dva čvora, jedan za upravljanje vrijednosnicama i jedan za upravljanje gotovinom, a zaseban čvor imao je funkciju bilježničkog čvora koji provjerava valjanost transakcija. Čvorovi banaka imali su instalirane aplikacije za razmjenu različitih klasa imovine te aplikaciju za omogućavanje DvP razmjene. U izvedbi s dva nepovezana sustava, bilježnički čvor bio je odgovoran za zaključavanje stanja u prvoj fazi razmjene imovine te oslobađanje imovine u drugoj fazi nakon što provjeri valjanost transakcija, vremena zaključavanja, tajne S' te potpisa sudionika. Platforma Corda omogućava direktnu komunikaciju između čvorova što omogućuje da sudionici razmjenjuju samo one informacije koje trebaju te svi sudionici imaju samo dio svih zapisa. Navedeno onemogućava da jedan sudionik ima potpuni uvid u sve zapise osim ako je sustav osmišljen da određenom sudioniku omogući uvid u sve zapise glavne knjige [23].




Sl. 11 DLT mreža s dva nepovezana sustava za trgovanje gotovinom i vrijednosnicma

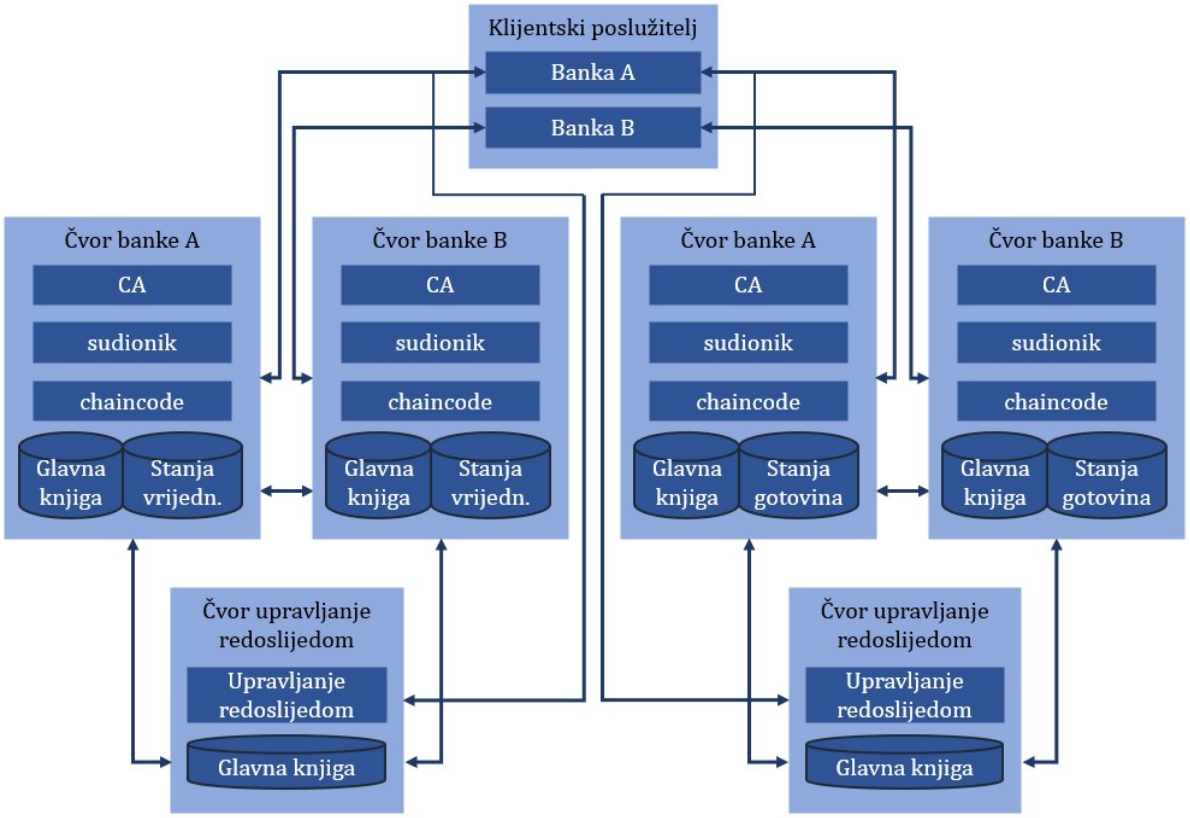
Deterministička konačnost rezultata na platformi Elements nije garantirana za korišteni *proof-of-work* algoritam konsenzusa te da bi se ostvarila rudarenje se mora ograničiti na samo jedan čvor. Stoga je testiranje realizirano tako da na jednom klijentskom poslužitelju imamo dva procesa od kojih svaki predstavlja jednu banku. Izvedba s jednim DLT sustavom, osim čvorova banaka, imala je jedan čvor za rudarenje koji je rudario i gotovinu i vrijednosnice, dok je u izvedbi s dva nepovezana sustava klijent

imao dva čvora za rudarenje, jednog za vrijednosnice i jednog za gotovinu. Komunikacija između klijenata i čvorova, kao i kod izvedbe na platformi Corda, obavljala se putem poziva udaljene procedure (RPC). Tajnost podataka na ovoj platformi mora se osiguravati dodatnim kriptografskim tehnikama s obzirom da se u potpunosti oslanja na globalno objavljivanje podataka verificiranih od strane čvora za rudarenje, a glavna knjiga je raspodijeljena između svih sudionika. Ova platforma, slično kao i platforma Corda, koristi UXTO model za pohranu podataka u glavnu knjigu [23].




Sl. 12 DLT mreža s dva nepovezana sustava bazirana na platformi Elements

U testnoj izvedbi na platformi Hyperledger Fabric također su dva procesa na jednom klijentskom poslužitelju predstavljale banke. Kod izvedbe s dva nepovezana sustava, svaki sustav imao je jedan čvor za upravljanje poretkom i dva čvora banaka, koji su imali svoj certifikacijski autoritet i pametne ugovore *chaincode*. Platforma Hyperledger Fabric omogućava direktnu komunikaciju putem otvorenih kanala kojima se može osigurati povjerljivost podataka, dok sudionici dijele glavnu knjigu ovisno o tome u kojim kanalima sudjeluju [23].




Sl. 13 DLT mreža s dva nepovezana sustava bazirana na platformi Hyperledger Fabric

Osnovni nalazi proizašli iz druge faze projekta Stella su da se isporuke po plaćanju (DvP) mogu uspješno provesti na jednom DLT sustavu ili dva različita DLT sustava koji ne moraju biti povezani, što može pomoći u osiguravanju interoperabilnosti između različitih DLT platformi. No kompleksnost tih transakcija i različiti koraci koje svaki sudionik na različitim platformama mora poduzeti utječu na brzinu njihove provedbe te mogu dovesti do privremene blokade likvidnosti, a samim time jedna platforma nenamjerno može utjecati na operativnost druge. Dodatno, nemogućnost potpune sinkronizacije koraka u procesu DvP transakcije sudionike također mogu izložiti riziku smanjenja glavnice (engl. principal risk) ako jedna od dviju ugovornih strana ne izvrši potrebne korake procesa [23].

U trećoj fazi projekta ECB i središnja banka Japana željele su istražiti inovativna rješenja za prekogranična plaćanja između područja različitih valuta te mogu li navedena rješenja unaprijediti sigurnost i efikasnost takvih transakcija. Analiza globalne interoperabilnosti u ovoj fazi projekta usredotočila se na mogućnost implementiranja jedinstvenog protokola za plaćanja između centraliziranog sustava i DLT sustava, različitih DLT sustava i različitih centraliziranih sustava. Istraživanja su provedena

koristeći Interledger protokol verzije 3 (ILPv3) konzorcija W3C za provedbu plaćanja, DLT platformu Hyperledger Fabric u izvedbi iz prethodne faze projekta te centralizirane sustave Five Bells Ledger[15]. U testiranju se koristilo nekoliko različitih metoda plaćanja:

- *trustline*, kod koje platitelj obećava izvršavanje plaćanja ukoliko primatelj ispuni predefinirane uvjete,
- plaćanje sa založnim računom u sklopu glavne knjige koristeći HTLC protokol,
- plaćanje sa založnim računom kod pouzdane treće strane,
- plaćanje jednostavnim platnim kanalom koristeći zajednička založena sredstva,
- plaćanje uvjetnim platnim kanalom koristeći HTLC protokol [14].

Zaključci ove faze bili su da plaćanja sa založnim računom i plaćanja uvjetnim platnim kanalom osiguravaju sigurnost plaćanja zato što navedene metode koriste mehanizme utjerivanja (engl. enforcement) kojima se može osigurati da sve strane u potpunosti ispune svoje odgovornosti. Što se tiče efikasnosti likvidnosti *trustline* metoda se pokazala najefikasnijom, s obzirom da se radi o jedinom načinu plaćanja s naknadnim financiranjem. Dodatno, metode plaćanja sa založnim računom pokazale su se boljim za likvidnost od onih s platnim kanalima. Nadalje, iz tehničke perspektive, zaključeno je da se sigurnost prekograničnih plaćanja može unaprijediti korištenjem platnih metoda koje sinkroniziraju plaćanja i zaključavanje sredstava koja se koriste u plaćanjima [14]. Istraživanje treće faze projekta ovaj rad neće detaljnije obrađivati jer ono nije proširilo do tada ustanovljena rješenja za izdavanje digitalnog novca niti je mijenjalo do tada korištenu tehnologiju DLT sustava.

Projekt Stella je u četvrtoj, posljednjoj, fazi bio usredotočen na istraživanje koncepta i praktično testiranje usklađivanja potreba za povjerljivošću podataka i mogućnošću nadzora kako bi se osigurala odgovornost sudionika slična onoj kod centraliziranih sustava. Točnije, željelo se ocijeniti način na koji bi tehnike za unaprjeđenje povjerljivosti (engl. privacy-enhancing tehniques, PET) mogle osigurati povjerljivost te mogućnost nadzora i revizije transakcija na infrastrukturi financijskog tržišta baziranoj

[15] originalno interno ime Ripple-ovog protokola ILP koji se može koristiti za povezivanje različitih tipova glavnih knjiga

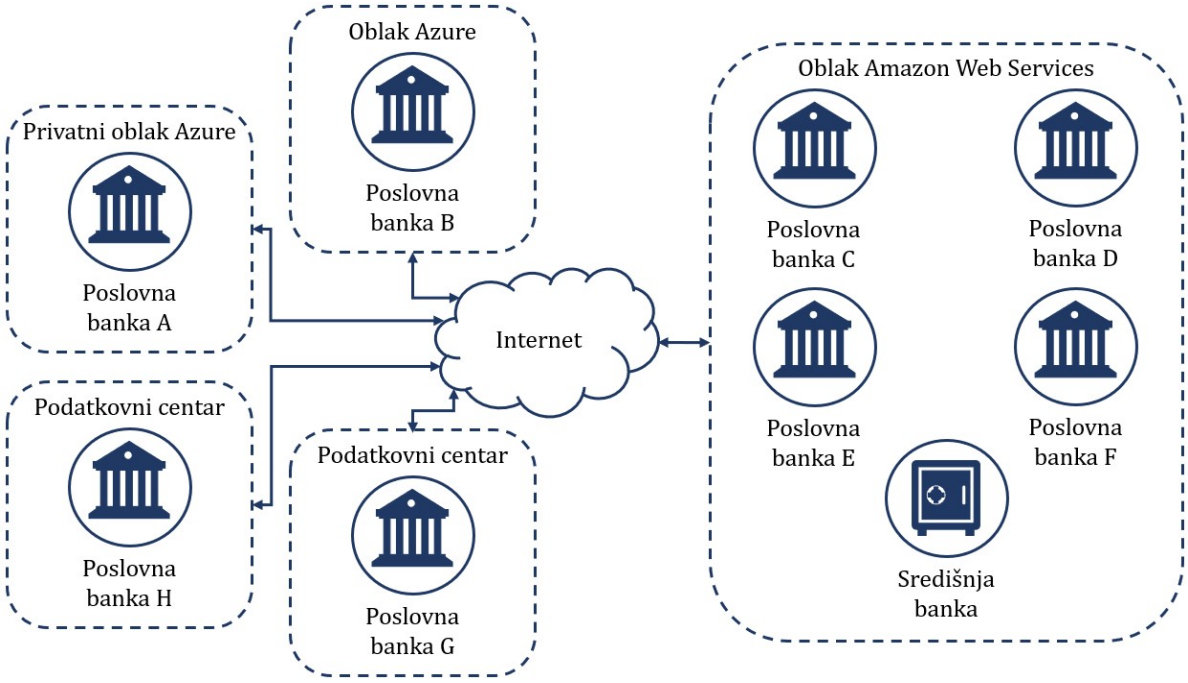
na DLT-u. Za potrebe istraživanja navedene tehnike podijeljene su u tri kategorije; segregirajuće tehnike koje osiguravaju da svaki sudionik ima uvid samo u podskup svih provedenih transakcija, sakrivajuće tehnike koje korištenjem kriptografskih algoritama sprječavaju treće strane da vide detalje transakcija, te nevezujuće (engl. unlinking) tehnike koje otežavaju mogućnost određivanja odnosa u provedenim transakcijama iz informacija pohranjenih na glavnoj knjizi. U istraživanju je također pseudonimizacija podataka bila pretpostavljena [15].

Mogućnost nadzora i revizije transakcija procjenjivana je prema dostupnosti potrebnih podataka, pouzdanosti dobivenih informacija i učinkovitosti procesa nadzora i revizije. Dostupnost podataka odnosi se na mogućnost revizora da pristupi podacima koji su mu potrebni za provođenje revizije te se može osigurati dobivanjem informacija od povjerljivih izvora ili sudionika koje je moguće identificirati. Pouzdanost podataka pokazuje može li revizor biti siguran da se izvorni transakcijski podaci mogu dobiti iz prikupljenih informacija te se ista može osigurati ako revizor informacije dobije od povjerljivih izvora ili ako može iskoristiti podatke pohranjene na DLT sustavu. Nadalje, učinkovitost postupka revizije se može mjeriti potrošnjom potrebnih resursa koji utječu na izvedivost procesa dobivanja pouzdanih podataka [15]. Rezultati istraživanja dobiveni u ovoj fazi bit će predstavljeni u poglavlju 5 u kojem će se obraditi sigurnosni aspekti izdavanja CDBC-a na DLT sustavima.

### 3.1.5. Projekt Khokha središnje banke Južnoafričke republike

Cilj projekta Khokha bio je doprinijeti globalnim inicijativama analize implementacija DLT platforme te pružiti realističan test veleprodajnog platnog sustava baziranog na DLT-u. Točnije, htjelo se istražiti može li se osigurati povjerljivost podataka na sustavu koji podržava realne produkcijske volumene transakcija s čvorovima pojedinih banaka sudionika izvedenih na različitoj infrastrukturi. Sustav za potrebe projekta razvijen je na platformi Quorum, koristeći istanbulski algoritam tolerantan na bizantske greške, Pedersenove obveze te protokol za dokaz raspona (engl. range proof), podvrstu dokaza bez znanja (ZKP), kako bi se omogućila skalabilnost i otpornost sustava te povjerljivost i konačnost transakcija. Sedam banaka sudionika bilo je odgovorno za konfiguriranje vlastitih čvorova, dok je središnja banka imala uvid u sve transakcije kako bi se omogućio regulatorni nadzor [16].

Zahtjevi projekta bili su da osmišljeni sustav može obraditi prosječan promet RTGS sustava središnje banke JAR-a od 70.000 transakcija dnevno s mogućnošću povećanja na 200.000 kako bi se predvidio budući rast tržišta, te 70.000 transakcija unutar dva sata kako bi se osigurao ubrzani povrat dnevnog prometa u slučaju gubitka podataka. Također se projektom željelo omogućiti da se s 95-postotnom sigurnošću može očekivati propagacija blokova po cijeloj mreži unutar jedne sekunde i s 99-postotnom sigurnošću propagacija blokova po cijeloj mreži unutar dvije sekunde. Nadalje, zahtjevi su bili da transakcije budu povjerljive, odnosno da informacije unutar transakcija budu jasne samo njenim sudionicima. Osim toga, željelo se zadovoljiti tri principa[16] infrastrukture financijskih tržišta koji zahtijevaju konačnost namire, izvršavanje namire u novcu izdanom od središnje banke te identifikaciju izvora operativnih rizika [16].




Sl. 14 Arhitektura čvorova banaka na DLT platformi korištenoj u sklopu projekta Khokha

Projekt je proveden kroz nekoliko iteracija te je u prvoj od tih iteracija omogućeno čvoru središnje banke da izdaje digitalni novac dok je dvjema bankama omogućeno da naprave transfer sredstava. U drugoj iteraciji mreža je radila poput RTGS sustava, a čvor središnje banke je odobravao transakcije čiji su podaci bili vidljivi svima. Pedersenove

[16] engl. Principles for Financial Market Infrastructures (PFMIs) – međunarodni standardi za platne sustave te sustave za obračun i namiru koje zajedno objavljuju Banka za međunarodne namire (BIS) i Međunarodna organizacija komisija za vrijednosne papire (IOSCO)

obveze dodane su u trećoj iteraciji kako bi se onemogućio uvid u iznos transakcije čvorovima koji ne sudjeluju u transakciji, s time da je središnja banka mogla otvoriti obveze kako bi odobrila transakcije. Uz to, u trećoj iteraciji omogućen je i kriptirani *peer-to-peer* kanal (engl. whisper channel) kako bi sudionici mogli razmjenjivati ključeve. U završnoj iteraciji povećana je otpornost sustava omogućavanjem korištenja dokaza raspona koji omogućuje sudionicima da potvrde da su i iznos transakcije i stanje računa platitelja nakon transakcije oboje pozitivni bez da se zapravo prikažu točni iznos i stanje računa. Iako je u završnom obliku čvor središnje banke i dalje imao uvid u iznose transakcija, korištenjem dokaza raspona omogućen je konsenzus sudionika korištenjem istanbulskog algoritma tolerantnog na bizantske greške čime je nestala potreba za verifikacijom od strane središnje banke [16].

Testiranja su pokazala da platforma Quorum može osigurati i nadmašiti zahtijevane performanse, te je uz osigurane povjerljivost podataka i konačnost namire omogućena 99-postotna propagacija blokova unutar jedne sekunde te 100-postotna unutar 1,25 sekundi. Završna iteracija dozvoljavala je procesiranje 12,86 transakcija u sekundi što je značajno više od 9,72 transakcije koje bi se trebalo odraditi u jednoj sekundi da bi se dosegao cilj od 70.000 transakcija dnevno. Operativna konačnost namire, prvi od tri principa infrastrukture financijskih tržišta, ostvaren je korištenjem algoritma konsenzusa, dok je drugi ostvaren tako što je središnja banka financirala stanja računa banaka sudionika u obliku tokeniziranih randa koji su predstavljali direktno potraživanje središnje banke. No, identifikacija izvora operativnih rizika, odnosno posljednji princip infrastrukture financijskih tržišta koji se htjelo ispoštovati, naposlijetku nije u potpunosti zadovoljen. Zaključeno je da bi bilo potrebno proširiti projekt na daljnja istraživanja cjelokupnog dizajna i arhitekture sustava koji bi obuhvatili integritet, sigurnost i dostupnost mreže kako bi se razumjelo sve rizike koje bi mogli utjecati na sustav [16].

## 3.2. Izdavanje maloprodajnog CDBC-a na DLT platformi

S obzirom da su središnje banke u svijetu kao glavnu motivaciju za izdavanje maloprodajnog CDBC-a isticale financijsku inkluziju te želje da nacionalni platni sustav bude efikasniji i nediskriminirajući, možda nije ni čudno da je Narodna banka Kambodže među prvima, još 2016. godine, pokrenula radnu skupinu za istraživanje mogućeg

korištenja lanaca blokova i DLT-a u svrhu izdavanja CDBC-a. Želja Narodne banke Kambodže bila je da se navedeni sustav koristi podjednako za provedbu maloprodajnih plaćanja građana i za veleprodajne međubankarske transakcije. Već u prvoj polovici 2019. godine pokrenut je pilot koji je uključivao četiri institucije i njihove klijente u sklopu kojeg su se mogle provoditi transakcije koristeći digitalni inačice kambodžanskog rijala i američkog dolara. Krajem 2020. godine projekt Bakong, podržan od strane 18 financijskih institucija, službeno je pušten u produkciju u cijeloj Kambodži [24].

Nakon toga, druga dva pilota maloprodajnog CDBC-a baziranog na DLT-u predstavljena su od strane karipskih središnjih banaka. Naime, središnja banka istočnih Kariba (engl. Eastern Caribbean Central Bank, ECCB) pokrenula je u ožujku 2019. godine suradnju s fintech tvrtkom Bitt vezanu uz provođenje pilota izdavanja CDBC-a baziranog na DLT-u unutar Monetarne unije istočnih Kariba[17] (engl. Eastern Caribbean Currency Union, ECCU). Digitalni EC dolar nazvan DCash distribuiraju i koriste licencirane financijske institucije i nebankarske financijske institucije u ECCU-u, a može se koristiti za financijske transakcije između potrošača i trgovaca te *peer-to-peer* transakcije koristeći pametne uređaje [25].

Krajem 2019. godine središnja banka Bahama predstavila je digitalnu verziju Bahamskog dolara, nazvavši navedenu digitalnu valutu pješčani dolar (engl. sand dollar). Središnja banka Bahama kao razloge izdavanja navela je financijsku inkluziju zajednica izvan ekonomičnog dosega usluga fizičkog bankarstva, potaknuti smanjivanjem mreže podružnica banaka uslijed rezanja troškova. Do kraja 2020. godine šest pružatelja usluga elektroničkog novčanika dobilo je odobrenje za distribuiranje pješčanih dolara [26], a središnja banka Bahama početkom 2021. godine izašla je s prijedlogom izmjene zakonskih odredbi kojima će se regulirati pružanje i korištenje njihovog CDBC-a, interoperabilnost, zaštita korisnika, financijska inkluzija i ovlaštenja središnje banke nad pružateljima usluga elektroničkog novčanika [27].

Švedska središnja banka Riksbank još je u proljeće 2017. godine započela projekt putem kojeg ispituje mogućnosti za izdavanje vlastite digitalne valute nazvane e-kruna. Riksbank očekuje da bi e-kruna široj javnosti omogućila pristup digitalnoj zamjeni za

[17] monetarna unija Organizacije istočnokaripskih država koju čine otočne države Angvila, Antigva i Barbuda, Dominika, Grenada, Montserrat, Sv. Kristofor i Nevis, Sv. Lucija te Sv. Vincent i Grenadini

gotovinu, pri čemu bi država jamčila vrijednost navedenog elektroničkog novca. Iako švedska središnja banka putem sustava RIX poslovnim bankama i drugim financijskim institucijama već nudi veleprodajni CDBC za provođenje velikih plaćanja među sobom, ovim projektom želi testirati korištenje maloprodajnog CDBC-a te promovirati siguran i učinkovit sustav plaćanja, zadatak koji će možda u budućnosti biti još i važniji s obzirom da upotreba novčanica i kovanica u Švedskoj opada [28]. Odabrano tehničko rješenje za testiranje izdavanja maloprodajnog CDBC-a bazirano na DLT-u omogućava korisnicima čuvanje e-krune u elektroničkom novčaniku u obliku mobilne aplikacije putem koje je moguće vršiti pologe i prijenose, kao i vršiti i primati uplate [29]. Riksbank je, prema posljednjim vijestima za vrijeme pisanja ovog rada, produžila testiranje u sklopu pilota do kraja veljače 2022. godine te još uvijek nije donijela konačnu odluku o izdavanju e-krune, njenoj izvedbi i korištenoj tehnologiji [30].

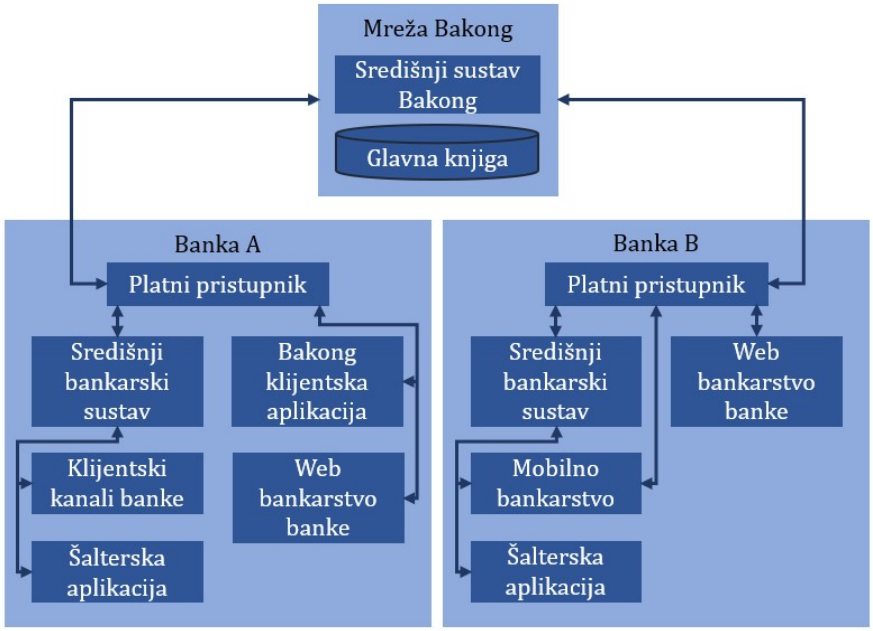
### 3.2.1. Projekt Bakong Narodne banke Kambodže

Narodna banka Kambodže je u proteklom desetljeću započela nekoliko inicijativa s ciljem unaprjeđivanja sigurnosti i efikasnosti plaćanja od kojih je posljednja, projekt Bakong, pokrenuta da istraži upotrebu alternativne tehnološke platforme za unaprjeđenje platnog sustava te promovira korištenje lokalne valute. Navedenim projektom pokušalo se riješiti probleme kao što su loša povezivost i interoperabilnost trenutnih sustava te povećati efikasnost plaćanja smanjivanjem cijena, povećanjem brzine i unaprjeđivanjem sigurnosti. Platforma Bakong omogućava korisnicima da besplatno prebacuju sredstva sa svojih računa u poslovnim bankama, omogućava *peer-to-peer* transakcije u realnom vremenu bez potrebe za poravnanjem, a centralizirana platforma koja je povezana s bankama uklanja probleme s povezivanjem i interoperabilnošću te povećava sigurnost provedbe transakcija [31].

Platforma Bakong osmišljena je kao platni sustav baziran na DLT-u u kojem su čvorovi smješteni u privatnom lancu blokova na zatvorenoj infrastrukturi Narodne banke Kambodže kojoj sudionici mogu pristupati putem sučelja. Samo registrirani sudionici mogu provoditi plaćanja a konsenzus o ispravnim transakcijama bazira se na odluci 2N+1 od 3N+1 čvorova u algoritmu tolerantnom na bizantske greške. Korisnici putem mobilne aplikacije mogu provoditi transakcije korištenjem QR kodova, unosom brojeva telefona ili odabirom kontakata u imeniku pametnog telefona. Registracija korisnika vrši

se putem vjerodajnica banaka u kojim imaju otvoren račun, koje su također odgovorne za provođenje KYC i AML procedura te čuvanje informacija o klijentima. Banke sudionici pri Narodnoj banci moraju imati otvoren račun za namire te se na kraju dana stanje računa krajnjih korisnika mora prikazati i na računima za namire banaka sudionika. Svaki korisnik na sustavu Bakong ima dva odvojena računa, jedan u lokalnoj valuti i drugi u američkim dolarima, no Narodna banka i sustav Bakong ne omogućuju konverziju valuta već navedenu opciju prepuštaju bankama sudionicima [31].

Kao partner na projektu izabrana je fintech tvrtka Soramitsu koja je na zahtjev Narodne banke Kambodže osmislila sustav privatnog lanca blokova s dozvolom baziranog na DLT platformi Hyperledger Iroha. Navedeni sustav dizajniran je tako da iskoristi postojeću infrastrukturu lokalnog maloprodajnog platnog sustava FAST tako da se za povezivanje koriste postojeća grafička i aplikacijska sučelja, autentifikacijski zahtjevi i poslovni procesi kako bi se financijskim institucijama omogućilo što jednostavnije priključivanje u sustav. Korištenjem DLT platforme u mreži čvorova kojima upravlja Narodna banka Kambodže osigurava se konačnost i transparentnost transakcija te zaštita privatnosti jer se trećim stranama ne otkriva identitet pojedinaca uključenih u transakciju. Algoritam konsenzusa osigurava konzistentnost transakcija u cijeloj mreži te otpornost na cenzuru transakcija i DDoS napade istodobno izbjegavajući dvostruku potrošnju i rizik druge ugovorne strane (engl. counterparty risk) u zamjeni digitalne imovine [31].



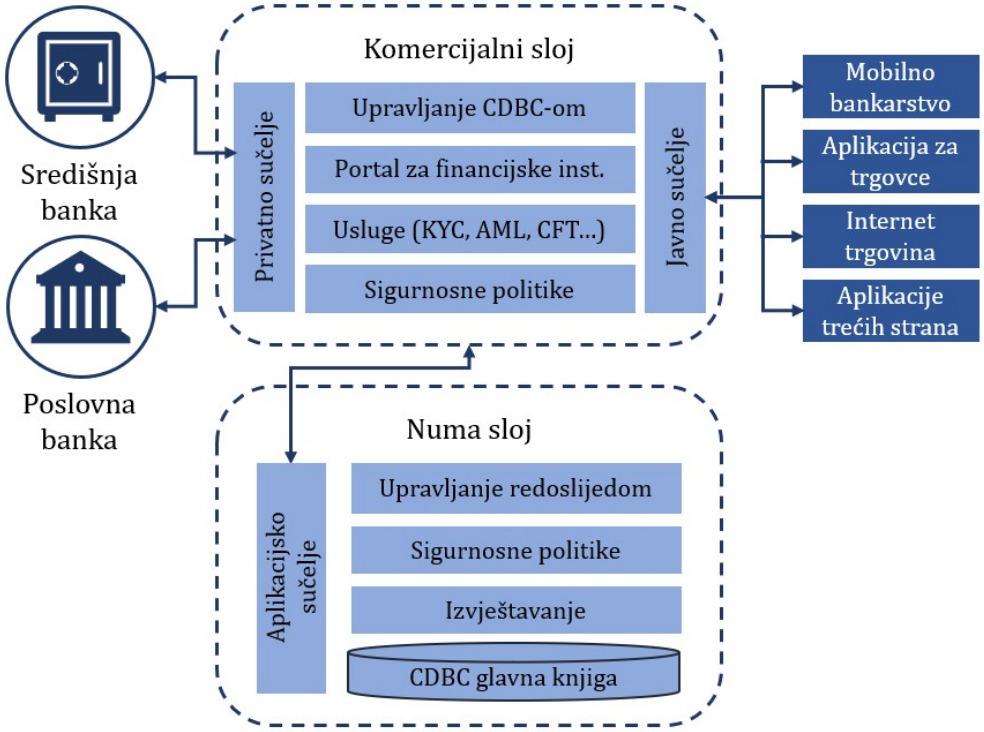

Sl. 15 Funkcionalni prikaz različitih opcija pristupa banaka mreži Bakong

Platni pristupnik svake financijske institucije koja pristupa mreži Bakong čini zasebnu domenu na središnjem sustavu Bakong na kojem korisnici mogu otvarati račune. Pomoću platnih pristupnika financijske institucije također mogu nadzirati transakcije provedene na njihovoj domeni te upravljati KYC operacijama i ograničenjima prometa. Krajnji korisnici mogu računima na mreži Bakong pristupati putem desktop i mobilne aplikacije Narodne banke Kambodže ili aplikacija poslovnih banaka koje se mogu spajati na mrežu Bakong putem aplikacijskog sučelja te izravno provoditi transakcije s drugim korisnicima na različitim domenama unutar mreže Bakong [31].

### 3.2.2. Digitalni dolar Monetarne unije istočnih Kariba

Glavni cilj DXCD-a, digitalnog dolara Monetarne unije istočnih Kariba, je ljudima koji nemaju kreditne kartice omogućiti maloprodajno plaćanje i e-trgovinu te provođenje doznaka bez dodatnih provizija. Dovoljno je preuzeti aplikaciju na pametni telefon da bi počeli koristiti elektroničke novčanike bazirane na računima ili one bazirane na vrijednosti (tokenima). Usluge upravljanja novčanicima baziranim na računima pružaju poslovne banke za vlasnike računa koji su ispunili KYC, AML i druge uvjete. Elektronički novčanici bazirani na vrijednosti namijenjeni su osobama bez redovnih bankovnih računa, a navedene omogućuju i održavaju odabrane državne agencije uz minimalne zahtjeve, no s mjesečnim ograničenjima prometa [32].

Javno predstavljanje pilota započelo je u ožujku 2021. godine u četiri članice ECCB-a dok je implementacija za ostale četiri članice planirana za kraj iste godine. Osmišljeni sustav trenutno provodi plaćanja putem skeniranja QR kodova s informacijama o trgovcima i iznosu transakcije, no ne omogućuje provedbu transakcija ako platitelj nije povezan na Internet [33]. Što se sigurnosti tiče, ECCB i njihov partner Bitt jamče da je aplikacija razvijena vodeći računa o minimiziranju rizika vezanih uz najčešće sigurnosne ranjivosti mobilnih i web aplikacija. Financijske institucije spojene na sustav moraju koristiti dvofaktorsku autentifikaciju, dok pametni uređaji za pristup aplikaciji koriste ugrađene sigurnosne hardverske elemente. Pozadinski sustav rasprostranjen je u nekoliko podatkovnih centara, a sustav za izdavanje elektroničkog novca se nalazi na sigurnoj lokaciji u izvanmrežnom načinu rada [34].




Sl. 16 Arhitektura za upravljanje CDBC-om Monetarne unije istočnih Kariba

Fintech tvrtka Bitt kao rješenje za razvoj DXCD-a izabrala je DLT platformu Hyperledger Fabric kako bi kreirala privatni lanac blokova s dozvolom [35]. Arhitektura sustava podijeljena je na komercijalni sloj, na koji se povezuju banke, trgovci, korisnici i treće strane, te Numa sloj, na kojem se nalazi raspodijeljena glavna knjiga, koji nema izravnu vezu s komercijalnim slojem. Sve interakcije s Numa slojem odvijaju se putem zaštićenog aplikacijskog sučelja. Komercijalni sloj ima privatno sučelje za središnje banke i financijske institucije te javno sučelje za korisnike, trgovce i treće strane. Pristup sustavu zaštićen je višefaktorskom autentifikacijom, dok je upravljanje identitetom i pohrana korisničkih podataka prepuštena bankama i državnim agencijama. Sustavi financijskih institucija su decentralizirani i koriste postojeću naslijeđenu infrastrukturu integriranu s komercijalnim slojem. Aplikacijsko sučelje na sloju Numa labavo je povezano (engl. loosely coupled) s raspodijeljenom glavnom knjigom kako bi se omogućila jednostavna zamjena vrste ili verzije DLT-a. Korištenjem labavo povezane arhitekture omogućuje se daljnji razvoj sustava koji bi mogao podržavati više različitih valuta ili druge imovine te naposlijetku omogućiti transformaciju u sustav baziran na tokenima (engl. token-based) s promjenom naglaska na dokazivanje vlasništva imovine, a ne dokazivanje identiteta [36].

### 3.2.3. Pješčani dolar središnje banke Bahama

Središnja banka Bahama odradila je rigorozan postupak odabira izvođača tehnološkog rješenja za implementaciju pješčanog dolara, naglasivši potrebu za robusnim rješenjem koje će uzeti u obzir infrastrukturne izazove brojnosti i udaljenosti otočja te ispuniti međunarodne regulatorne standarde. Fintech tvrtka NZIA Limited izabrana je za izvođača na temelju predloženog rješenja koje će omogućiti interoperabilnost s postojećim kanalima za platni promet, podržavati izvanmrežnu funkcionalnost koja bi pamtila i provodila plaćanja nakon ponovne uspostave mrežne komunikacije, gotovo trenutnu validaciju transakcija te obradu transakcija u stvarnom vremenu. Kao ostali aspekti predloženog rješenja navedeni su podrška trgovcima, bilježenje transakcijskih zapisa koji omogućuju rekonstrukciju događaja, nadzor prijevarnih transakcija, multifaktorska autentifikacija, omogućavanje digitalne identifikacije te ograničavanje korištenja samo za domaću upotrebu [37].

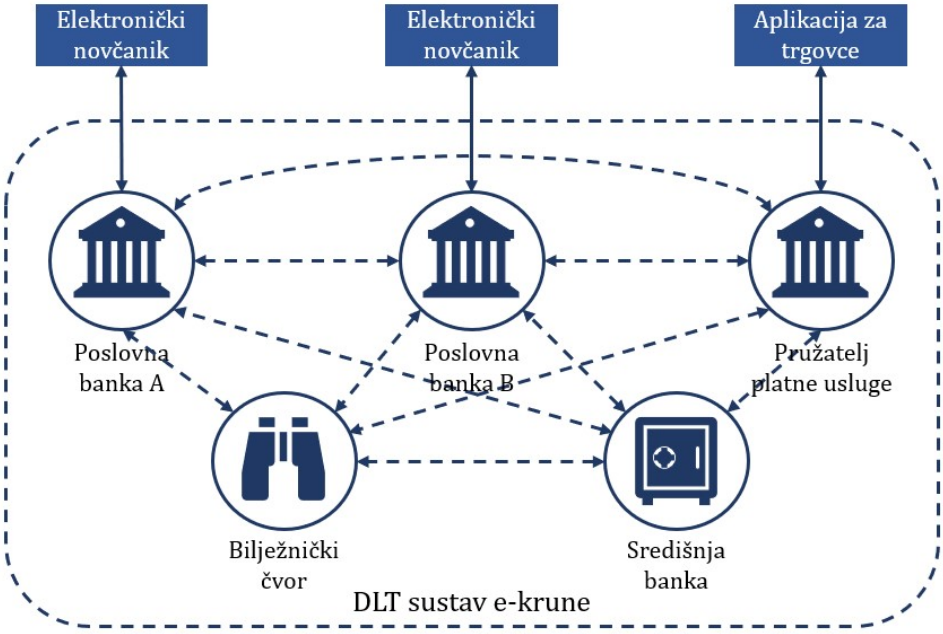
Uz maloprodajnu upotrebu koja omogućuje stanovništvu provedbu digitalnih plaćanja, osmišljeno rješenje omogućuje upotrebu pješčanog dolara i u veleprodajne svrhe provedbe međubankarskih namira. Da bi se spriječila mogućnost prevelikog utjecaja na bankarski sustav elektronički novčanici u vlasništvu tvrtki moraju biti vezani uz račune otvorene u poslovnim bankama, kamate se neće obračunavati na posjedovanje pješčanog dolara te su postavljena ograničenja na maksimalne iznose u elektroničkim novčanicima. Nadalje, s obzirom da je krajnji cilj izdavanja pješčanog dolara financijska inkluzija, omogućeno je posjedovanje elektroničkog novčanika koji nije povezan s bankovnim računom, no takva opcija nudi manje mogućnosti i provedbu transakcija ograničene vrijednosti, a centraliziranu infrastrukturu za upravljanje identitetom omogućuje središnja banka Bahama za razliku od implementacije DXCD-a gdje je navedeno prepušteno poslovnim bankama [37].

Nažalost, do kraja pisanja ovog rada nije bilo moguće doći do nikakvih tehničkih detalja o načinu korištenju izvedenog rješenja za podršku izdavanja i provedbe plaćanja pješčanim dolarima te su jedine dostupne informacije da je tvrtka NZIA koristila svoju DLT platformu NZIA Cortex u suradnji s tvrtkama IBM i Zynesis [38].

### 3.2.4. E-kruna središnje banke Švedske

Glavni razlog zašto je tema e-krune u Švedskoj postala toliko važna je naglo smanjenje korištenja gotovine tijekom posljednjeg desetljeća. Digitalni razvoj koji je omogućio jednostavne i prikladne načine plaćanja doveo je do toga da trenutno u Švedskoj na mnogim mjestima postaje nemoguće platiti gotovinom. Iako ne postoji CDBC dostupan široj javnosti, postoji digitalni novac i načini plaćanja koje pružaju poslovne financijske institucije i pružatelji platnih sustava. Omogućavanjem korištenja maloprodajnog CDBC-a dostupnog svima smanjio bi se rizik slabljenja položaja krune u odnosu na konkurentske alternative privatnoj digitalnoj imovini. Prema Riksbanku, izdavanje e-krune bi također pridonijelo razvoju i inovacijama na tržištu plaćanja, povećanju zaštite integriteta podataka o transakcijama te bi društvo učinilo manje ranjivim u slučaju problema s postojećim sustavima plaćanja [39].

Tehničko rješenje temelji se na e-kruni koja je distribuirana među sudionicima u mreži e-krune, kao što su banke, te nudi robusnu infrastrukturu koja funkcionira paralelno postojećem platnom sustavu. E-krune su zapravo digitalni tokeni koji su prijenosni i ne mogu se krivotvoriti ili kopirati tako da ne može doći do dvostrukog trošenja jednog tokena, te omogućuju trenutna *peer-to-peer* plaćanja. Kao tehnologija za sinkronizaciju baza podataka koje održavaju različiti sudionici koristi se DLT platforma koja osigurava evidentiranje samo ispravnih transakcija. Svaki sudionik u mreži e-krune sastoji se od jednog ili više čvorova koji pohranjuju e-krune te primaju, potvrđuju i prosljeđuju transakcije [39].




Sl. 17 Arhitektura mreže e-krune za vrijeme pilota projekta

Testno okruženje za pilot strukturirano je u dvije razine, na prvoj razini Riksbank izdaje e-krune sudionicima u mreži dok na drugoj sudionici distribuiraju e-krune krajnjim korisnicima. Sudionici e-krune mogu dobiti na raspolaganje terećenjem svojih rezervi i dobivanjem kredita na temelju rezervi u sustavu za namire središnje banke RIX ili kao predstavnici neizravnih sudionika uplaćujući rezerve u RIX. Korisnici i trgovci mogu kontrolirati stanje i plaćanje e-krunama putem elektroničkog novčanika u mobilnoj aplikaciji ili aplikaciji kase, a u pilotu će se raditi i na mogućnošću plaćanja pametnim satovima i karticama [39].

Kao platforma za izdavanje e-krune izabrana je DLT platforma Corda koja je izvedena kao privatna mreža dostupna samo onim sudionicima koje odobri Riksbank. Robusnost i skalabilnost mreže trebalo bi se osigurati sudjelovanjem malih brojem čvorova zajedno s bilježničkim čvorom koji bi sprječavao dvostruko trošenje tokena. Regulatorni zahtjevi osiguravali bi se tehničkim i zakonskim pravilima zadanim kroz Corda distribuiranu aplikaciju (CordApp) koja će definirati, primjerice, tko može distribuirati e-krunu, kako će transakcije teći kroz mrežu te kako će se potpisivati i pohranjivati transakcije. Arhitektura korištena u pilotu biti će realizirana tako da bude fleksibilna i u budućnosti omogući proširenja i dodatne usluge koje bi mogli razviti sudionici u mreži kao što su automatski polozi ili prijenosi sredstava [39].

# 4. DLT platforme korištene u projektima i istraživanjima središnjih banaka

Korištenjem DLT platforme omogućuje se da nijedan sudionik mreže ne može potrošiti sredstva koja ne posjeduje, nijedan sudionik se ne može lažno predstavljati te nijedan nečastan sudionik mreže ne može krivotvoriti transakcije. Navedeno je omogućeno korištenjem asimetrične kriptografije, ulančavanjem transakcija i mehanizmom konsenzusa na DLT platformi prve generacije nazvanoj Bitcoin, koja je zamišljena kao *peer-to-peer* verzija elektroničke gotovine koja bi omogućavala direktna online plaćanja između dva sudionika bez potrebe uključivanja financijske institucije [63]. Ethereumom, drugom generacijom DLT platformi, omogućeno je korištenje rekurzivnog programskog jezika ugrađenog u platformu koji se može koristiti za programiranje proizvoljnih funkcija prijelaza stanja. Te funkcije, koje još nazivamo i pametni ugovori, omogućuju korisnicima osmišljavanje različitih vrsta imovine na DLT sustavima te upravljanje tom imovinom na različite načine [40].

Upravo je Ethereum bio početna točka istraživanja središnjih banaka Kanade i Brazila te Monetarnog autoriteta Singapura. No iako su verzijom platforme 2.0 na Ethereumu uvedena mnoga unaprjeđenja, i dalje postoje zabrinutosti vezane uz sigurnost i skalabilnost zbog kojih mnogi smatraju da platforma nije prilagođena korištenju u poslovne svrhe. DLT platformu Quorum, koja je zapravo privatna platforma bazirana na implementaciji Ethereuma u programskom jeziku Go, razvila je banka JP Morgan kako bi se zadovoljili poslovni zahtjevi za financijske transakcijske sustave. Stoga je logično da su istraživanja na platformi Quorum nastavile središnja banka Brazila i Monetarni autoritet Singapura, a na navedenoj platformi svoje istraživanje provela je i središnja banka JAR-a.

Kao DLT platforme kojima će se moći zadovoljiti poslovne potrebe razvijene su i platforme Hyperledger Fabric, koju su u svojim istraživanjima koristile središnje banke Brazila, istočnih Kariba i Japana (zajedno s ECB-om) te Monetarni autoritet Singapura, Hyperledger Iroha, koju je za potrebe razvoja platnog sustava Bakong iskoristila središnja banka Kambodže, te Corda, na kojoj su za potrebe svojih projekata razvijale

središnje banke Kanade, Brazila, Švedske i Japana (zajedno s ECB-om) te Monetarni autoritet Singapura. Osim navedenih platformi, u projektima obrađenim ovim radom korištene su i manje raširene DLT platforme Zilliqa, Chain Core, Elements i NZIA Cortex.

Tablica 1 Korištene platforme u projektima i istraživanjima pojedinih regulatora

| **Regulator / DLT** | **Ether-eum** | **Quor-um** | **HL Fabric** | **Corda** | **HL Iroha** | **Zilliqa** | **Chain Core** | **NZIA Cortex** | **Elem-ents** |
|---|---|---|---|---|---|---|---|---|---|
| S.B. Kanade | X | | | X | | | | | |
| S.B. Brazila | X | X | X | X | | | | | |
| M.A. Singapura | X | X | X | X | | X | | | |
| ECB i S.B. Japana | | | X | X | | | | | X |
| S.B. JAR-a | | X | | | | | | | |
| S.B. Kambodže | | | | | X | | | | |
| M.U. ist. Kariba | | | X | | | | | | |
| S.B. Bahama | | | | | | | | X | |
| S.B. Švedske | | | | X | | | | | |

Ovaj rad u nastavku će detaljnije opisati DLT platforme koje su se najčešće koristile u obrađenim istraživanjima i projektima središnjih banaka. S obzirom na relativno kratku povijest tehnologije raspodijeljenih glavnih knjiga, u trenucima istraživanja središnjih banaka obrađenih u ovom radu neke od navedenih DLT platformi još uvijek su bile u procesu dinamičkog razvoja te su testiranja provedena na beta verzijama platformi. U skladu s time, za očekivati je da aktualne verzije platformi mogu biti različite od onih korištenih na projektima ili da je trenutno moguće koristiti opcije koje tada nisu bile raspoložive.

## 4.1. Ethereum

Namjera Ethereuma bila je stvoriti alternativni protokol za izgradnju decentraliziranih aplikacija koji će ispraviti ograničenja[18] platforme Bitcoin, koristeći opcije koje omogućuju razvoj decentraliziranih aplikacija, s naglaskom na brzi razvoj, sigurnost i sposobnost različitih aplikacija da učinkovito komuniciraju. Na Ethereumu sudionici ili pametni ugovori mogu kontrolirati račune koji služe za provođenje transakcija i čuvanje stanja sredstava a definirani su *nonce-om* (jednokratnom vrijednošću), stanjem računa, kodom ugovora, u slučaju da se radi o računu pametnog ugovora, te korijenom spremnika. Svi računi i njihova stanja dio su virtualnog izvršnog okruženja Ethereum (engl. Ethereum Virtual Machine, EVM) koji je pohranjen na svim čvorovima u Ethereum mreži te se o njegovom stanju moraju usuglasiti svi sudionici mreže [40].

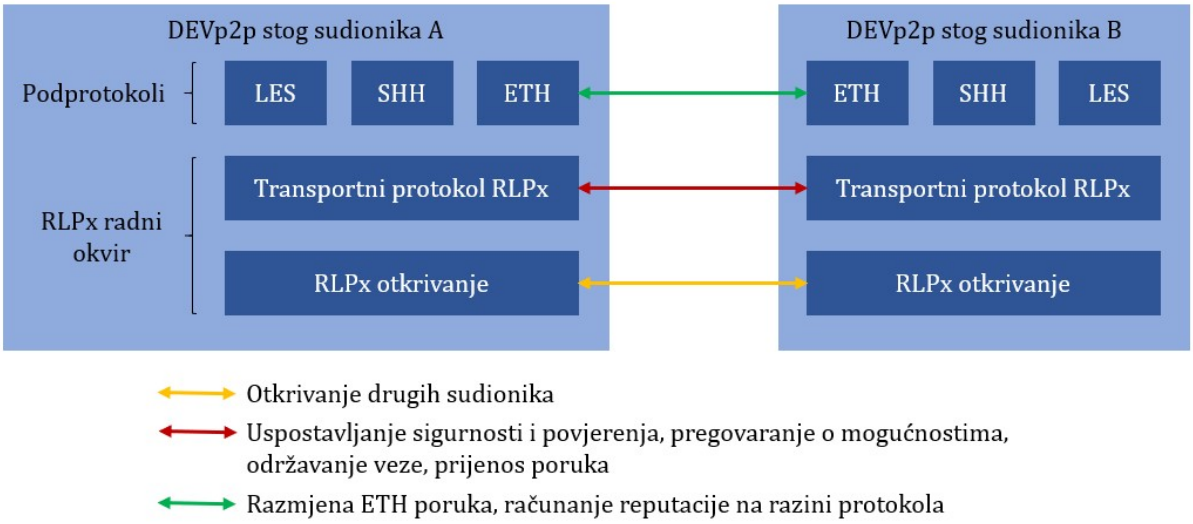
Svaki sudionik može odaslati transakcijski zahtjev na mrežu koji ostali sudionici moraju potvrditi, izvršiti i zapisati. Ispunjeni transakcijski zahtjev postaje transakcija koja mijenja stanje EVM-a i koja se odašilje svim čvorovima na mreži. Podaci zapisani u transakciji su adresa primatelja, potpis platitelja, iznos transakcije, opcionalni dodatni podaci te najveća vrijednost *gas*-a koja se može utrošiti na navedenu transakciju i naknada koju pošiljatelj plaća po jedinici *gas*-a. *Gas* na platformi Ethereum predstavlja jedinicu za količinu računalnih resursa potrebnih za izvršavanje određenih operacija na mreži, a osmišljen je kako bi se spriječilo slučajno ili namjerno uzaludno trošenje računalnih resursa, primjerice, beskonačnim petljama [41].

Mehanizam konsenzusa koji koristi platforma Ethereum je *proof-of-work* te se čvorovi koji rudare natječu u kreiranju blokova transakcija za koje dobivaju navedenu proviziju u protuvrijednosti *gas*-a. Čvorovi sudionika na Ethereum mreži koji ne rudare mogu pohranjivati podatke u lancu blokova na različite načina. Puni čvorovi čuvaju cijeli lanac blokova, lagani čvorovi pohranjuju samo zaglavlje lanca, dok arhivski čvorovi čuvaju potpuni lanac blokova zajedno s arhivom povijesnih stanja koja se može koristit za pretraživanje stanja računa u svim blokovima. Ethereum mreže mogu biti javne i dostupne svima, u kojem slučaju svatko može čitati, stvarati i potvrđivati transakcije

[18] kao što su nemogućnost korištenja *Turing-complete* programskih jezika, nerazlikovanje vrijednosti vezanih uz stanje te nepostojanje prijelaznih stanja UTXO

koje se izvršavaju, ili privatne, pri čemu se time ne jamči sigurnost već samo izoliranost od javnosti [41].

Međutim, platforma Ethereum decentraliziranim aplikacijama omogućuje tajnu *peer-to-peer* asinkronu komunikaciju putem sustava za slanje poruka Whisper koji se koristi kao podprotokol SHH protokola DEVp2p (ĐΞVp2p Protocol). DEVp2p protokol koristi RLPx okvir za pretraživanje mreže i uspostavljanje komunikacije između čvorova. Sve Whisper poruke šalju se svakom čvoru s omogućenom Whisper komunikacijom, a kako bi se onemogućilo bespotrebno slanje poruka i DDoS napadi, slanje poruka zahtjeva dokaz o odrađenom poslu kako bi se poruka zaštitila. Takav svojevrsni *proof-of-work* sastoji se od traženja najmanjeg broja unutar određenog vremenskog okvira pomoću algoritma SHA3, a davanje algoritmu više vremena rezultirat će manjim brojem čime će se omogućiti veći prioritet poruke u mreži. Whisper poruke kriptirane su protokolom DEVp2p, koji može koristiti AES enkripciju različitih dužina ključeva, dok podprotokol SHH, koji može koristiti i simetričnu i asimetričnu enkripciju, kriptira ovojnicu poruke s tajnim sadržajem. Svaki čvor može imati više ključeva kojima će pokušati dekriptirati ovojnicu, no samo čvorovi kojima je namijenjena moći će je otključati [42].




Sl. 18 Shematski prikaz DEVp2p mrežnog stoga Ethereum klijenata [43]

Pametni ugovori na platformi Ethereum imaju svoj račun te stanje računa i mogu slati transakcije na mrežu, no ne mogu ih kontrolirati sudionici u mreži već su implementirani na mreži kako bi ih se pokretalo kao programe. Sudionici mogu komunicirati s pametnim ugovorom na način da mu predaju transakcije koje izvršavaju funkciju definiranu pametnim ugovorom. Programski jezici razvijeni za platformu

Ethereum s najaktivnijom zajednicom korisnika te koji se najredovitije održavaju su Solidity, objektno orijentirani jezik razvijen po uzoru na C++, i Vyper, razvijen na bazi jezika Python. Aplikacije koje kombiniraju pametne ugovore s korisničkim sučeljem na platformi Ethereum nazivaju se decentralizirane aplikacije (dapps) [41].

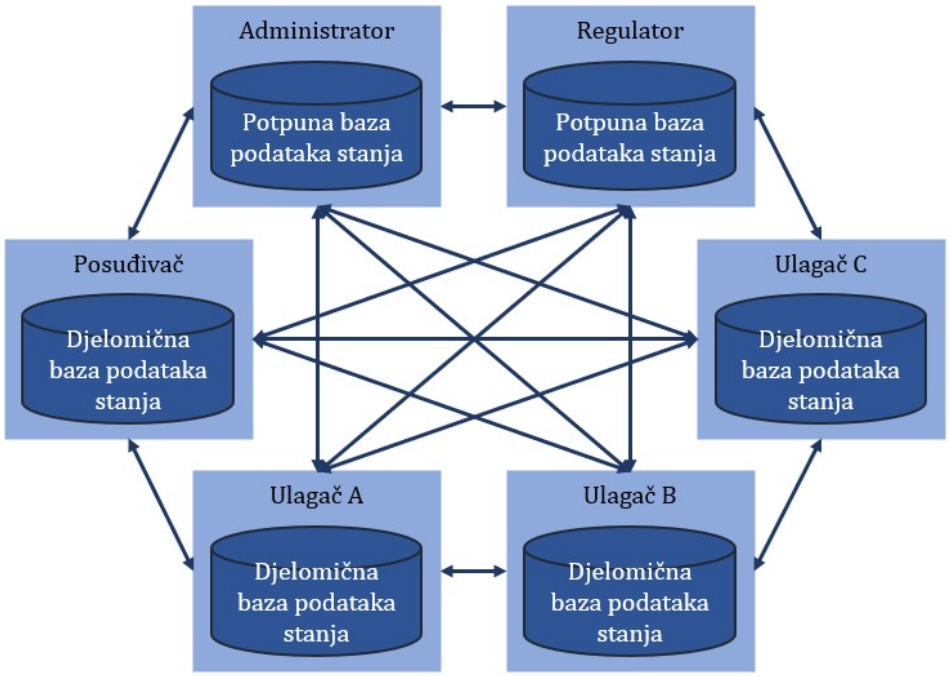
Tijekom pisanja ovog rada platforma Ethereum bila je u postupku značajne nadogradnje nazvane Ethereum 2.0 koja se izvodi u nekoliko faza. Najznačajnija svrha nadogradnje je povećanje protoka transakcija s trenutnih oko 15 u sekundi na desetke tisuća u sekundi. Navedeno se planira postići dijeljenjem radnog opterećenja na mnogo lanaca blokova koji će se usporedno izvoditi te uvođenjem zajedničkog mehanizma konsenzusa za sve lance blokova koji će se bazirati na principu *proof-of-stake*. Navedene promjene će zahtijevati od napadača da će, ukoliko pokuša izmijeniti podatke na jednom lancu, morati utjecati na zajednički mehanizam konsenzusa svih lanaca blokova [44].

## 4.2. Quorum

Quorum je privatna DLT platforma s odobrenjem bazirana na službenoj implementaciji protokola Ethereum u programskom jeziku Go, jednoj od tri službene implementacije uz one u programskim jezicima C++ i Python. Modifikacije od standardne implementacije protokola Ethereum, osmišljene za potrebe kreiranja platforme Quorum, napravljene su kako bi se zadovoljili zahtjevi koje bi mogle imati tvrtke koje u poslovanju koriste DLT platforme. Jedan od ciljeva dizajna Quoruma bio je što više iskoristiti postojeću tehnologiju i minimizirati promjene u platformi Go-Ethereum kako bi se smanjio trud potreban za usklađivanjem s budućim verzijama koda službene implementacije Ethereuma [45].

Osnovna ideja Quoruma bila je iskoristiti kriptografske postavke kako bi se svima koji nisu sudionici u transakciji onemogućilo uvid u povjerljive podatke. Postupak provjere valjanosti blokova modificiran je na način da čvorovi provjeravaju valjanost svih javnih transakcija te onih privatnih transakcija čiji su sudionici izvršenjem ugovornog koda povezanog s transakcijama, dok za tuđe privatne transakcije čvor jednostavno preskoči proces izvršenja ugovornog koda. Takav način provjere valjanosti dovodi do segmentacije baze podataka stanja na javnu bazu, koja je jednaka za sve, i privatnu bazu, koja se razlikuje kod pojedinih čvorova. Iako baza podataka na klijentskom čvoru više ne pohranjuje stanje cijele globalne baze podataka, stvarni distribuirani lanac blokova i sve

transakcije u njemu u potpunosti su replicirani na svim čvorovima i kriptografski osigurani kako bi jamčili nepromjenjivost [45].




Sl. 19 Prikaz Quorum DLT sustava sa zajedničkim javnim stanjem i zasebnim privatnim stanjima

Kao osnovni mehanizam konsenzusa na platformi Quorum trenutno se koristi Raft, mehanizam otporan na ispade. Osim toga, platforma omogućava i korištenje istanbulskog algoritma tolerantnog na bizantske greške (IBFT), te algoritma baziranog na dokazu autoriteta Clique, kod kojeg je dovoljna jednostavna većina da bi se postigao konsenzus [46]. Implementacija platforme koja koristi mehanizam Raft predlaže se kod zatvorenog konzorcija sudionika kod kojih algoritam tolerantan na bizantske greške nije uvjet, odnosno tamo gdje postoji model vođa - sljedbenik te nije dozvoljeno račvanje lanaca. Kod takve izvedbe mreže postoji jedan vođa, kojeg se naziva i kovač (engl. minter), koji zapisuje sve unose u lanac blokova te nema potrebe za *proof-of-work* dokazima. Vođa se izabire glasanjem tijekom kojeg svi čvorovi preuzimaju ulogu kandidata, a nakon što čvor koji je pobijedio na izborima preuzme ulogu vođe, ostali čvorovi preuzimaju ulogu sljedbenika. Kada vođa kreira novi blok transakcija, taj blok se postavlja kao nova glava lanca tek nakon što većina čvorova koji su sudjelovali u glasanju potvrdi novi blok, koji tada svi čvorovi zapisuju u lanac [45].

Raft je mehanizam konsenzusa otporan na ispade (engl. Crash Fault Tolerant, CFT) u kojem se pretpostavlja da će se vođa uvijek ponašati ispravno. Svi sljedbenici slijepo repliciraju unose koje je predložio vođa bez postavljanja pitanja. Ako vođa prestane s

radom, ostatak mreže automatski će izabrati novog vođu nakon isteka određenog vremena i mreža će nastaviti raditi, a kad se srušeni čvor oporavi, postat će sljedbenik i počet će replicirati blokove koje je propustio dok je bio u izvanmrežnom radu. Prednost ovog mehanizma je brže slaganje blokova u odnosu na ostale mehanizme, s obzirom da ih slaže samo vođa, a propagacija blokova kroz mrežu i prikupljanje većine prihvaćanja je nezahtjevan i brz proces [47].

Istanbulski algoritam tolerantan na bizantske greške izvodi se u tri faze; predpripremnoj, pripremnoj i obvezujućoj (engl. commit). Validirajući čvorovi odabiru čvor predlagatelj koji predlaže novi blok i odašilje ga na mrežu ga zajedno s predpripremnom porukom. Po primanju navedene poruke, validirajući čvorovi ulaze u stanje pripreme i zatim odašilju pripremnu poruku, što osigurava da svi validirajući čvorovi rade na istom lancu i istom krugu definiranja bloka. Nakon primanja pripremne poruke od dvije trećine čvorova, čvor predlagatelj ulazi u pripremno stanje, a zatim u mrežu odašilje obvezujuću poruku kojom obavještava sudionike da prihvaća predloženi blok i da se isti dodaje u lanac. Posljednja faza završava kada dvije trećine validirajućih čvorova dobije obvezujuću poruku i spreme navedeni blok u svoj lanac [45].

Za razliku od mehanizma Raft kod kojeg sljedbenici slijepo vjeruju vođi, kod mehanizma IBFT svaki blok zahtijeva više krugova glasovanja validirajućih čvorova da bi se postigao međusobni konsenzus, što se bilježi kao zbirka potpisa u sadržaju bloka. Validirajući čvor nikada ne pretpostavlja da je vođa ili predlagač blokova ispravan, već provjerava predloženi blok baš kao i drugi konsenzusni mehanizmi koji rade u nepouzdanom okruženju, primjerice, *proof-of-work* mehanizmi. Mehanizam konsenzusa IBFT, kao i svi ostali tipovi mehanizma PBFT kojih je i on varijanta, može tolerirati do N nepoštenih (neispravnih) čvorova u mreži od 3N+1 čvorova da bi se osigurala konačnost transakcija [47].

Mehanizam konsenzusa Clique oslanja se na skup pouzdanih čvorova koji se nazivaju autoriteti te koji koriste pojednostavljeni algoritam za slanje poruka kako bi postigli bolje performanse od standardnih algoritama tipa PBFT. Razmjena poruka kod ovakvog *proof-of-authority* mehanizma zahtjeva samo jednu fazu, za razliku od tri faze kod prethodno spomenutog mehanizma IBFT. Mreže koje koriste mehanizme konsenzusa bazirane na dokazu autoriteta mogu normalno raditi kad je jednostavna većina od N/2+1 čvorova autoriteta ispravna. Više čvorova autoriteta može predlagati blokove s

transakcijama, a mehanizam se oslanja na algoritam GHOST[19] da spriječi račvanje lanaca koje se može dogoditi kad više različitih autoriteta predlaže različite blokove u isto vrijeme. Ovakav mehanizam, kod kojeg samo autoritet koji je predložio blok mora isti potpisati kako bi ga zatvorio i na taj način osigurao nepromjenjivosti podataka, može kreirati blokove u vremenskom intervalu koji se može konfigurirati [47].

Zaštita podataka na platformi Quorum postiže se enkripcijom transakcija i segmentacijom pristupa na lokalnim bazama stanja na pojedinim čvorovima. Samo čvorovi koji sudjeluju u privatnim transakcijama mogu izvršiti kod povezanog privatnog ugovora, nakon čega se ažuriraju podaci privatnog ugovora u lokalnoj bazi stanja. Rezultat toga je da je lokalna baza stanja svakog čvora popunjena samo javnim i privatnim podacima iz transakcija u kojima je taj čvor sudjelovao. Privatne transakcije na javnoj bazi sadrže samo 256-bitni sažetak podataka, a stanja povezanog privatnog ugovora definirani su zasebnim Merkle Patricia stablom odvojenim od stabla s javnim stanjima. Standardna provjera bloka na platformi Ethereum uključuje korak kojim se potvrđuje da se globalno stanje svih ugovora podudara sa sažetkom globalnog stanja koji je uključen u zaglavlje bloka, što predstavlja kriptografski dokaz da svaki čvor u mreži ima potpuno istu bazu podataka stanja. Na platformi Quorum takva se provjera radi samo za javna stanja, a za potrebe kriptografskog dokaza o konsenzusu stanja sudionika u privatnom ugovoru, distribuirana aplikacija može dohvatiti sažetak stanja privatnog ugovora za određeni blok sa zasebnog stabla i podijeliti tu vrijednost sa sudionicima [45].

Nakon početnog razvoja platforme Quorum[20] od strane tvrtke JP Morgan, daljnji razvoj preuzela je tvrtka ConsenSys. Iako je prvotno upravljanje privatnim transakcija bilo omogućeno putem modula Constellation i Tessera, ConsenSys je odustao od razvoja Constellationa te održava samo modul Tessera [48]. Tessera se koristi za pohranu i pristup kriptiranim podacima o transakcijama te razmjenu kriptiranih podataka s drugim čvorovima, bez da ima pristup privatnim ključevima. Većina zadataka vezana uz enkripciju, uključujući generiranje simetričnih ključeva te kriptiranje i dektriptiranje,

[19] *proof-of-work* mehanizam koji prati put podstabla s kombiniranim dokazom koji je najteže ostvariti

[20] aktualna verzija platforme Quorum je 21.1.0 objavljena 9.3.2021.

delegirana je modulu Enclave kako bi se razdvojili zadaci i omogućilo poboljšanje rada određenih operacija vezanih uz enkripciju [49].

## 4.3. Hyperledger Fabric

Projekt Hyperledger pokrenut je 2016. godine od strane zaklade Linux s namjerom da se ostvari suradnja bazirana na otvorenom kodu koja će se fokusirati na razvoj niza stabilnih radnih okvira, alata i knjižnica za implementaciju DLT sustava sposobnih da podrže poslovne zahtjeve. Inicijalno je tehnički upravljački odbor projekta odobrio dva radna okvira za poslovne DLT sustave; platformu Fabric, koja kombinira rad tvrtki Digital Asset, Blockstream i IBM, te platformu Sawtooth, koju je razvio inkubator predvođen tvrtkom Intel. U međuvremenu je u sklopu projekta razvijeno sveukupno 6 radnih okvira za poslovne DLT sustave, od kojih je u ovom radu već spomenuta platforma Iroha korištena na projektu Bakong, koja se fokusira na upotrebu u mobilnim uređajima i Internetu stvari [50].

Platforma Fabric osmišljena je kao distribuirani operativni sustav za DLT sustave s dozvolom koji može pokretati aplikacije napisane u programskim jezicima opće namjene, kao što su Go, Java i Node.js. Kako bi eliminirala ograničenja dotadašnjih DLT sustava koji prate arhitekturu *poredaj-izvrši* (engl. order-execute), kao što su sekvencijalno izvršavanje, nedeterministički kod i povjerljivost izvršavanja, platforma Fabric uvodi arhitekturu koja prati tri koraka *izvrši-poredaj-potvrdi*. Pametni ugovori nazvani *chaincode*, koji su središnji dio distribuirane aplikacije platforme, implementiraju logiku koja se pokreće tijekom koraka *izvrši*. Osim njih osnovni dio distribuirane aplikacije čini i politika odobravanja transakcija koja se provjerava u koraku *potvrdi* koju, za razliku od pametnih ugovora, mogu modificirati samo pouzdani administratori mreže. Tipična politika odobravanja omogućuje *chaincode*-u da definira sudionike koji su potrebni za odobravanje, no prilagođene politike mogu implementirati proizvoljnu transakcijsku logiku [51].

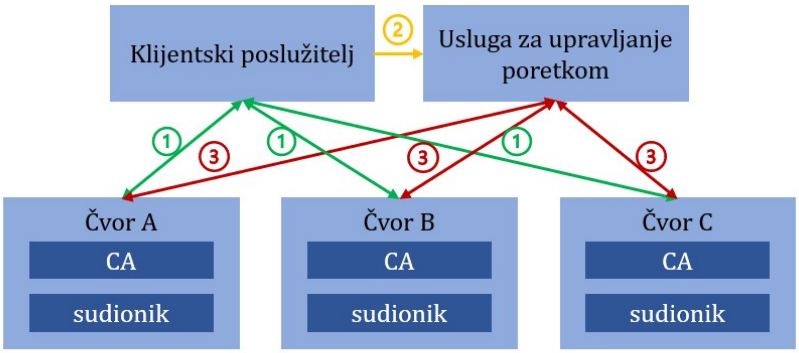
Klijent šalje transakcije specificirane politikom odobravanja drugim sudionicima u mreži te svaku transakciju izvršavaju određeni sudionici. Nakon izvršavanja, odobrene transakcije se u koraku *poredaj* formiraju u potpuno uređeni slijed u lancu blokova pomoću proizvoljnog mehanizma konsenzusa te se takve transakcije odašilju svim sudionicima. Na platformi Fabric transakcije se slažu prema transakcijskim izlazima i

ovisnostima stanja koja su izračunata tijekom koraka *izvrši* te svi sudionici potvrđuju transakcije istim slijedom, a potvrda transakcija je deterministička. Takvim slijedom replikacije transakcija uvodi se hibridna paradigma bizantskog modela kojim se kombinira pasivna replikacija, kod računanja novih stanja prije konsenzusa, te aktivna replikacija, kod potvrde rezultata izvršavanja i promjena stanja nakon konsenzusa [51].

Modularni pružatelj usluge članstva (engl. membership service provider, MSP) upravlja identitetom svih čvorova koji se mogu podijeliti u tri uloge:

- klijenti, koji predlažu transakcije za izvršavanje, pomažu koordinirati korak *izvrši* te odašilju transakcije za slaganje u red;
- sudionici, koji izvršavaju predložene te potvrđuju izvršene transakcije. Osim toga oni održavaju povijest transakcija i trenutno stanje glavne knjige;
- čvorovi za upravljanje poretkom (engl. ordering service nodes, OSN).

Mreža na platformi Fabric može imati različite lance blokova, takozvane kanale, koji koriste istu uslugu za upravljanje redom transakcija. Kanali se mogu koristiti za particioniranje stanja DLT mreže, no konsenzus između kanala nije koordiniran i konačni poredak transakcija u svakom kanalu je različit za različite kanale [51].




1. Slanje transakcije, izvršavanje pametnih ugovora i prikupljanje potvrda;
2. Emitiranje poretka;
3. Dostavljanje poretka, izvršavanje potvrda i pohrana transakcije u blok.

Sl. 20 Prikaz tijeka transakcije na platformi Hyperledger Fabric

Platforma Fabric omogućuje fleksibilne pretpostavke o povjerenju i pogreškama. Svi klijenti se generalno smatraju potencijalno zlonamjernima, a sudionici su grupirani u organizacije koje čine domene povjerenja u kojima sudionici međusobno imaju povjerenja u druge članove organizacije ali ne i sudionike izvan nje. Preporučeno je da svaka organizacija ima vlastiti certifikacijski autoritet. Čvorovi za upravljanje poretkom

sve sudionike i klijente smatraju potencijalno zlonamjernima [51]. Od verzije platforme 2.0 tvorci platforme preporučaju korištenje mehanizma Raft za upravljanje poretkom, dok se implementacije mehanizama Kafka[21] i Solo smatraju zastarjelima. Mehanizam Solo koristi samo jedan čvor za upravljanje poretkom i eventualno se može koristiti za potrebe testiranja [52].

Osim spomenutih politika odobravanja koje se nalaze u pametnim ugovorima, postoje politike za upravljanje kanalima i politike za upravljanje životnim vijekom pametnih ugovora. Popisi kontrola pristupa (engl. Access Control Lists) pružaju mogućnost konfiguriranja pristupa resursima kanala povezivanjem tih resursa s postojećim politikama. Komunikacija između čvorova zaštićena je TLS protokolom, a sudionici i čvorovi za upravljanje poretkom sadrže HTTP poslužitelj koji koristi RESTful programsko sučelje za komunikaciju s aplikacijom Fabric vlasnika čvorova. Preporuča se da se aplikacije Fabric smjeste na zaštićenu infrastrukturu vlasnika čvorova, koji će onda samostalno upravljati korisnicima koji putem aplikacije mogu predlagati i pretraživati transakcije. Za upravljanje kriptografskim operacijama i čuvanje privatnih ključeva može se koristiti HSM[22] [53].

## 4.4. Corda

U osmišljavanju platforme Corda vodilo se računa o potrebama reguliranih financijskih institucija i o tome da se ne koriste funkcionalnosti standardnih DLT platformi koje čine te platforme neprikladnim za izvršavanje stvarnih poslovnih transakcija. Corda poput Bitcoina koristi UTXO model definiranja vrijednosti, a transakcije imaju ulaze, izlaze i potpise poput onih na platformi Bitcoin, no za razliku od Bitcoina, retci u bazama podataka platforme Corda mogu sadržavati proizvoljne podatke. Temeljni objekt u konceptu platforme Corda je objekt stanja, koji predstavlja digitalni dokument koji bilježi postojanje, sadržaj i trenutno stanje ugovora između dvije ili više stranaka, a glavna knjiga definirana je kao niz nepromjenjivih objekata stanja [54].

[21] platforma za upravljanje tokom podataka otvorenog koda

[22] engl. Hardware Security Module – računalo za upravljanje kriptografskim ključevima i enkripcijom

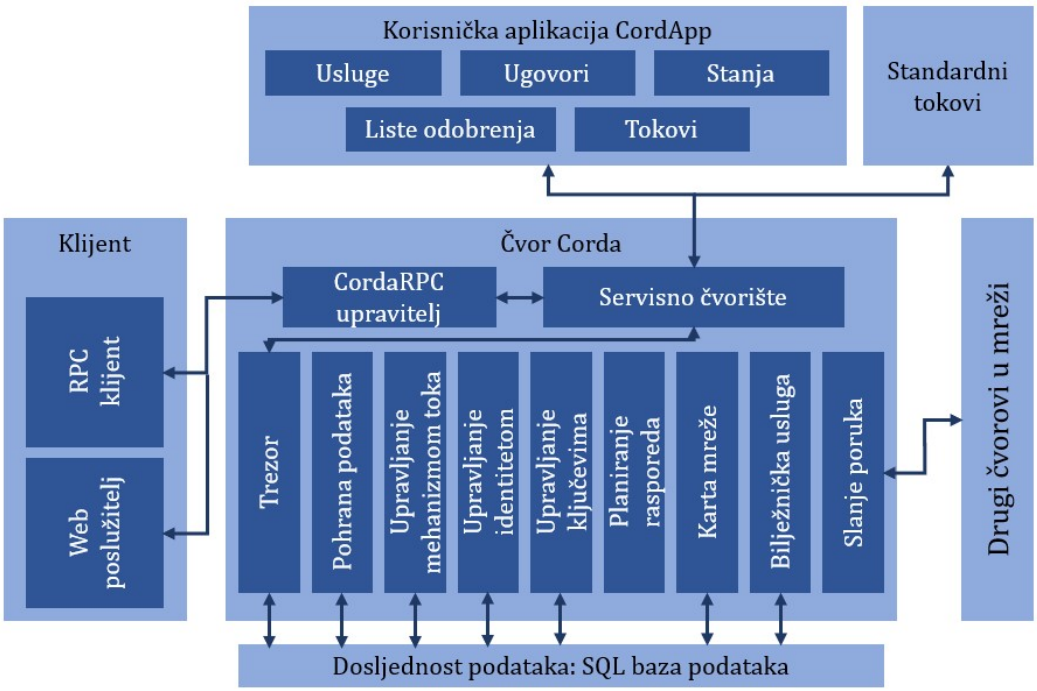
Ažuriranje glavne knjige provodi se transakcijama koje iskorištavaju postojeće objekte stanja i stvaraju nove te se na taj način bilježi lanac podrijetla imovine. No u modelu pohrane podataka platforme Corda sve transakcije nisu vidljive svima, tj. transakcije su vidljive samo njihovim sudionicima te čvorovima čiji uvid u glavnu knjigu može ovisiti o provjeri valjanosti transakcije. Sudionici u transakcijama međusobno se dogovore o valjanosti transakcije tako da neovisno jedan o drugome pokreću kod ugovora i validacijsku logiku. Međutim, jedinstvenost transakcije, kojom se jamči da je ta transakcija jedina koja iskorištava ulazna stanja transakcije, provjeravaju bilježnički čvorovi kao predodređeni neovisni promatrači. Usluga određivanja jedinstvenosti transakcije može biti raspodijeljena između jedinstvenog tijela koje upravlja svim bilježničkim čvorovima ili nekoliko međusobno nepovjerljivih čvorova koji se koordiniraju koristeći proizvoljne mehanizme konsenzusa, primjerice, Raft ili BFT [54].

Poštivanje poslovne logike se na platformi Corda osigurava primjenom pametnih ugovora koji mogu biti pisani u programskim jezicima Kotlin i Java. Svaki objekt stanja definira funkciju koja mora biti izvršena transakcijom kojom se želi potrošiti ili kreirati takav tip stanja, stoga je transakcija valjana samo ako je kod ugovora povezan sa svim stanjima sadržanim u transakciji zadovoljen. Provjera transakcija mora biti deterministička stoga bi ugovor trebao ili uvijek prihvatiti ili uvijek odbiti transakciju. Ako provjera transakcije ovisi o podacima koji nisu definirani unutar transakcije, potrebno je koristiti nezavisne Oracle čvorove koji će navedene informacije prikupljati izvan DLT platforme i biti jedinstveno mjesto za provjeru podataka od strane svih sudionika u transakciji. Osim ugovornih obaveza definiranih samim pametnim ugovorom, svaki se pametni ugovor poziva i na pravni dokument koji definira pravila koja uređuju razvoj stanja tijekom vremena te se ugovorne strane na ovaj se dokument mogu osloniti u slučaju pravnih sporova [55].

Corda mreža ne podržava globalno emitiranje poruka, već se poruke šalju od čvora do čvora, što znači da sudionici moraju točno odrediti koje podatke treba poslati, kojim ugovornim stranama i kojim redoslijedom ako žele da se ažuriranja glavne knjige provedu koordinirano. Navedeni postupak automatiziran je pomoću tokova koji predstavljaju slijed koraka koji čvoru govore kako da postigne određeno ažuriranje glavne knjige, kao što je izdavanje imovine ili namiru transakcije. Jednom kada je zadani poslovni proces definiran u toku i instaliran na čvor kao dio distribuirane aplikacije

CorDapp, vlasnik čvora može naložiti čvoru da pokrene taj proces u bilo kojem trenutku pomoću poziva udaljene procedure. Radni okvir za tokove omogućava čvorovima da imaju više aktivnih tokova u istom trenu, što je omogućeno serializiranjem tokova kad uđu u blokirajuće stanje i pokretanjem sljedećih zakazanih tokova. Na taj način omogućeno je sudionicima u transakcijama koordiniranje aktivnosti bez potrebe za centralnim upravljanjem [56].

Čvorovi u mreži Corda izvršna su okruženja koja koriste Java Virtual Machine s jedinstvenim mrežnim identitetom koji pokreću Corda servise i distribuirane aplikacije CorDapp. Svaki čvor ima dva sučelja kojima komunicira s vanjskim svijetom; mrežni sloj, kojim komunicira s drugim čvorovima, te poziv udaljene procedure (RPC), kojim čvor komunicira sa svojim vlasnikom. Osim njih, temeljni elementi arhitekture svakog čvora su; sloj dosljednosti, koji služi pohrani podataka, servisno čvorište, koje omogućava tokovima čvora da poziva ostale usluge, te sučelje za instalaciju distribuiranih aplikacija [57]. Sloj dosljednosti, uz sustav za pohranu podataka, čini i trezor koji sadrži podatke izvučene iz glavne knjige koji se smatraju relevantnima za vlasnika čvora, a pohranjene su u relacijskom modelu koji se lako može pretraživati. Trezor, slično kao i standardni novčanici kriptovaluta, čuva informacije o nepotrošenim i potrošenim stanjima te može generirati transakcije za prijenos stanja drugim sudionicima [58].




Sl. 21 Interna arhitektura čvora na DLT platformi Corda

Svaka Corda mreža može imati grozdove bilježničkih čvorova koji sudjeluju ili ne sudjeluju u provjeri transakcija što omogućuje sudionicima da izabiru preferirani grozd bilježničkih čvorova ovisno o transakciji [59]. Navedeno omogućava da svi čvorovi nemaju potrebu vidjeti sve transakcijske podatke, primjerice, nevalidirajući bilježnički čvorovi ili čvorovi Oracle. Iz tog razloga platforma Corda koristi koncept filtriranih transakcija kod kojih predlagatelj transakcije koristi ugnježđeno Merkleovo stablo kako bi sakrio dijelove transakcije koje ne želi podijeliti. Merkleovo stablo sastoji se od transakcija koje su razdijeljene u listove, gdje svaki listi sadrži ulaz, izlaz, naredbu ili prilog. Konačna struktura ugnježđenog stabla sadrži ostala polja transakcije, kao što su vremenski interval, bilježnički čvor i potrebni potpisnici. Sakrivanje podataka i pružanje dokaza da su ti podaci činili dio transakcije vrši se konstrukcijom grana Merkleovog stabla. Merkleova grana je skup sažetaka, koji se s obzirom na podatke listova koristi za izračunavanje korijenskog sažetka, koji se zatim uspoređuje sa sažetkom cijele transakcije te nam njihovo podudaranje jamči da su podaci istovjetni onima u transakciji [60].

# 5. Sigurnosna razmatranja izdavanja CDBC-a na DLT platformi

Uobičajena praksa informacijske sigurnosti usredotočena je na implementaciju načela povjerljivosti, integriteta i dostupnosti, takozvanog sigurnosnog CIA[23] trokuta. Integritet podataka na DLT platformama trebao bi biti zajamčen samom kriptografskom izvedbom blokova transakcija u raspodijeljenoj glavnoj knjizi s obzirom da svaki novi blok sadrži sažetak koji pokazuje na prethodni blok transakcija. Na vrijednost spomenutog sažetka utječe cijeli prethodni blok transakcija uključujući i njegov sažetak pokazivač. To znači da su takve glavne knjige nepromjenjive te ako se pokuša promijeniti podatke u nekim od prethodnih blokova ni jedan sažetak pokazivač u sljedećim blokovima neće biti ispravan. Dostupnost podataka na DLT sustavu trebala bi biti osigurana konfiguracijom, bilo da je glavna knjiga raspodijeljena između svih sudionika u sustavu, bilo da svaki sudionik čuva samo podatke o transakcijama u kojim je on sudjelovao ili da je zagarantirana korištenjem nekoliko čvorova centralnog autoriteta koji čuvaju sve podatke s mreže.

Za potrebe osiguravanja povjerljivosti na DLT sustavima razvijena su različita rješenja koja nazivamo tehnike za unaprjeđenje povjerljivosti (PET) koje su već spomenute u poglavlju 3.1.4. Međutim, kako bi se omogućilo korištenje DLT platformi za potrebe infrastrukture financijskog tržišta, potrebno je osigurati i odgovornost sudionika na način da se omogući njihov nadzor i revizija od strane centralnog autoriteta. U tu svrhu centralni autoritet trebao bi imati uvid i mogućnost razumijevanja informacija u blokovima transakcija bez obzira na implementirane tehnike za unaprjeđenje povjerljivosti. Ovaj rad iskoristit će istraživanje ECB-a i središnje banke Japana iz četvrte faze projekta Stella, u kojem su navedene tehnike podijeljene su u tri kategorije; segregirajuće, sakrivajuće i nevezujuće. Međutim, implementiranje tehnika za unaprjeđenje povjerljivosti transakcija na DLT sustavima može otežati centralnom autoritetu mogućnost nadzora i revizije podataka o transakcijama. Analiza navedenih

[23] engl. confidentiality, integrity and availability

tehnika provedena u četvrtoj fazi projekta Stella procijenila je prihvatljivu razinu dostupnosti potrebnih podataka, pouzdanosti dobivenih informacija i učinkovitosti procesa nadzora i revizije [15].

Povjerljivost na DLT sustavu mogla bi se osigurati izvedbom mreže na način da su transakcijski podaci segregirani između sudionika koji imaju pristup informacijama sukladno dozvolama (engl. need-to-know basis). Kad se koristi segregirajuća tehnika ne postoji dijeljena glavna knjiga koja je dostupna svim sudionicima, već svaki sudionik ima samo podskup zapisa svih transakcija. Jedan od primjera segregirajuće tehnike je izvedba DLT platforme Corda kod koje se informacije o transakciji razmjenjuju samo između sudionika transakcije i validirajućih bilježničkih čvorova. S obzirom da validirajući bilježnički čvorovi primaju i čuvaju informacije u razumljivom obliku, centralno tijelo prikupljanjem njihovih podataka može očekivati zadovoljavajuću razinu dostupnosti i pouzdanosti podataka te učinkovitosti procesa nadzora. Prikupljanjem podataka od nevalidirajućih čvorova, koji transakcijske podatke primaju u zaštićenom obliku, dok podatke o platiteljima čuvaju u razumljivom obliku, centralni autoritet bi do podataka o transakcijama mogao doći jedino suradnjom sa sudionicima. Na taj način smanjila bi se učinkovitost procesa nadzora i revizije, no navedenom problemu moglo bi se doskočiti uključivanjem čvorova promatrača u mrežu te konfiguriranjem čvorova sudionika da njima šalju sve transakcijske podatke [15].

Kod DLT platforme Hyperledger Fabric segregirajuća tehnika se provodi na način da se mreža dijeli na podmreže nazvane kanali koje imaju svoje podskupe glavne knjige, dok čvorovi koji čine uslugu za upravljanje poretkom sadrže podatke o svim transakcijama. Ako se centralnom autoritetu omogući pristup podacima usluge za upravljanje poretkom zadovoljava se razina dostupnosti i pouzdanosti podataka te učinkovitosti procesa nadzora. Još jedan od primjera segregirajuće tehnike su i izvanmrežni (engl. off-ledger) platni kanali kod kojih sudionici mogu provoditi proizvoljne transakcije putem tih kanala dok će se na glavnoj knjizi zabilježiti samo pseudonimi sudionika te sveukupni neto iznos razmjene na tom kanalu. Mreža Raiden koja funkcionira uz platformu Ethereum primjer je takvog izvanmrežnog platnog kanala. S obzirom da transakcije provedene na izvanmrežnim platnim kanalima pohranjuju informacije o sudionicima na dijeljenoj glavnoj knjizi osigurana je dostupnost podataka. Međutim, da bi dobio informacije o pojedinoj transakciji centralni autoritet ovisi o suradnji s platnim kanalom,

te bi pouzdanost podataka i učinkovitost procesa nadzora bile zadovoljavajuće jedino u slučaju da se platni kanala proglasi pouzdanom trećom stranom [15].

Sakrivajuće tehnike za unaprjeđenje povjerljivosti koriste se u slučaju kad svi sudionici dijele glavnu knjigu koja sadrži podatke o svim provedenim transakcijama. Navedene tehnike koriste različite kriptografske metode kako bi spriječile neautorizirane treće strane da interpretiraju detalje transakcija. Jedna od takvih tehnika koristi se na platformi Quorum kod provedbe prethodno spomenutih privatnih transakcija kod kojih čvorovi koji nisu sudjelovali u transakciji pohranjuju samo 256-bitni sažetak transakcijskih podataka te informacije o platitelju. Centralni autoritet tada može interpretirati podatke o platitelju, no potrebna je suradnja s platiteljem da bi dobio uvid u transakcijske podatke, te je u tom slučaju osigurana dostupnost i pouzdanost podataka no uz smanjenu učinkovitost procesa nadzora. No platforma Quorum, kao i platforma Corda, nudi opciju uključivanja čvorova promatrača u mrežu koji bi ispravnim konfiguriranjem ostalih čvorova sudionika imali pristup svim transakcijskim informacijama čime bi se zadovoljila sva tri aspekta revizije i nadzora [15].

Pedersenova obveza je također vrsta sakrivajuće tehnike koja omogućuje platitelju da stvori obvezu na iznos te za potrebe provjere valjanosti podijeli obvezu umjesto samog iznosa transakcije. Obveza se kreira sukladno definiranim parametrima mreže, a osigurava da treće strane mogu provjeriti valjanost ulaznih i izlaznih vrijednosti transakcije bez da mogu interpretirati točan iznos transakcije, dok informacije o platitelju i primatelju ostaju javno dostupne. S obzirom na to centralnom autoritetu koji provodi nadzor omogućena je zadovoljavajuća razina dostupnosti, dok se pouzdanost podataka i učinkovitost procesa mogu osigurati ako centralni autoritet dobije informacije o iznosu transakcije i zasljepljujućem faktoru. Tada bi centralni autoritet mogao izračunati obvezu iz dobivenih informacija te ju usporediti s onom zapisanoj na dijeljenoj glavnoj knjizi [15].

Još jedna vrsta sakrivajuće kriptografske metode su i dokazi bez znanja (ZKP) koji dozvoljavaju sudioniku da dokaže posjedovanje informacija bez otkrivanja točnih podataka te na taj način omogući provjeru valjanosti povjerljivih transakcija. Primjeri protokola koji koriste dokaze bez znanja, a ne zahtijevaju interakciju između platitelja i

čvorova koji provjeravaju valjanost transakcije su zk-SNARK[24] i zk-STARK[25]. U slučaju da su ovom tehnikom sakriveni podaci o platitelju i primatelju transakcije, centralni autoritet ne može doći do tih podataka čime se ne osigurava ni dostupnost podataka za nadzor i reviziju. Ako bi se ovom tehnikom sakrivali samo podaci o transakciji, dobivanjem ključeva za pregled transakcija centralni autoritet osigurao bi sva tri uvjeta za provođenje nadzora i revizije [15].

Tehnike koje mogu ukloniti poveznicu između stvarnih podataka o transakciji i informacija o platitelju i primatelju vidljivih na dijeljenoj glavnoj knjizi nazivaju se nevezujuće tehnike za unaprjeđenje povjerljivosti. Navedeno se može ostvariti na način da se ukloni poveznica o identitetu platitelja i/ili primatelja pomoću definiranog pseudonima ili da se ukloni poveznica o transakcijskom odnosu između platitelja i primatelja. Na taj način neovlaštene treće strane mogu vidjeti transakcijske podatke i interpretirati iznose ali ne mogu odrediti koji su transakcijski odnosi. Jedna od takvih tehnika je korištenje različitih pseudonima ili adresa za svaku transakciju (engl. one-time address). Kako bi se olakšala upotreba ove tehnike koja može zahtijevati čuvanje velikog broja adresa i povezanih privatnih ključeva, koriste se deterministički novčanici koji generiraju ključeve koristeći uvijek isto sjeme te na taj način smanjuju složenost upravljanja različitim adresama. Provedba nadzora i revizije uz implementaciju ove tehnike potpuno ovisi o tome hoće li sudionici pružiti centralnom autoritetu informacije o adresama korištenim u svakoj transakciji te u skladu s time nije zadovoljen uvjet o dostupnosti podataka za reviziju [15].

Miješanje je nevezujuća tehnika koja omogućuje različitim sudionicima premetanje više transakcija tako da treće strane ne mogu povezati transakcijske odnose. Takva izmiješana transakcija koja se pohranjuje na dijeljenoj glavnoj knjizi omogućuje veću razinu povjerljivosti što je više strana uključeno u provedbu transakcija. Međutim, kod korištenja tehnike miješanja problem predstavlja traženje sudionika za sudjelovanje u takvim transakcijama te nemogućnost ostvarivanja potpune povjerljivosti ukoliko u izmiješanoj transakciji postoji transakcija s jedinstvenim iznosom. U slučaju da miješanje transakcija provodi centralizirana usluga, proces nadzora i revizije

[24] engl. zero-knowledge succinct non-interactive argument of knowledge

[25] engl. zero-knowledge scalable and transparent argument of knowledge

zadovoljavao bi dostupnost i pouzdanost podataka te učinkovitost procesa ukoliko bi navedenu usluga miješanja provodila pouzdana treća strana. Ako bi se proces miješanja provodio direktno između sudionika transakcije, centralizirani autoritet imao bi uvid u sudionike, no prikupljanje informacija o transakcijskim odnosima i iznosima ovisilo bi o suradnji sa sudionicima. Navedeno dovodi do zaključka da je provođenjem tehnike miješanja direktno između sudionika osiguran jedino uvjet dostupnosti podataka za reviziju, no ne i pouzdanost u te podatke [15].

Korištenje prstena potpisa još je jedna vrsta nevezujuće tehnike kod koje se može dokazati da je potpisnik dio grupe potpisnika bez da se otkrije stvarni potpisnik. Ova tehnika omogućava platitelju da prikupi više javnih ključeva različitih sudionika članova prstena koje iskoristi za potpisivanje transakcije zajedno s vlastitim privatnim ključem. Time se onemogućava trećim stranama da točno utvrde tko od članova je zapravo platitelj, dok se istodobno jamči da potpisnik dolazi iz grupe potpisnika. Bez obzira što bi centralni autoritet imao uvid u transakcijske podatke na dijeljenoj glavnoj knjizi, ne bi mogao izdvojiti stvarnog platitelja od svih potpisnika transakcije. Primjenom ove tehnike za unaprjeđenje povjerljivosti ne bi se zadovoljila prihvatljiva razina dostupnosti podataka potrebnih za nadzor i reviziju [15].

Uz prethodno spomenutu problematiku vezanu uz povjerljivost, DLT platforme mogu imati ranjivosti vezane uz odabrani mehanizam konsenzusa ili loše izvedene pametne ugovore. Najčešći napadi vezani uz mehanizam konsenzusa su napadi preuzimanjem kontrole mehanizma (51%[26] ili 34%[27] napad), generiranje novog najdužeg lanca blokova, napadi podmićivanjem[28] i Ballance[29] napadi. Navedeni napadi mogu se ostvariti ako sudionik ili grupa sudionika preuzmu kontrolu nad dovoljnim brojem resursa kojim mogu kontrolirati mehanizam konsenzusa i na taj način odlučivati koje će transakcije ući u blokove, reverzirati transakcije te dvaput trošiti istu imovinu. Takvi napadi lakše će se

[26] u slučaju mehanizama *proof-of-work* i *proof-of-stake*

[27] u slučaju mehanizama baziranih na algoritmu BFT

[28] engl. bribery attacks, poznati i pod nazivom P+epsilon napadi, kojim se podmićivanjem drugih sudionika povećava vjerojatnost dvostruke potrošnje

[29] napadi kod kojih napadač kombinira računalnu snagu i usporavanje komunikacije kako bi se natjeralo druge sudionike da omoguće dvostruku potrošnju

provesti na javnim DLT sustavima bez dozvole te se mogu spriječiti korištenjem privatnog sustava s primjerenom kontrolom pristupa, primjerenom konfiguracijom sustava koja zabranjuje račvanje lanaca te primjerenim odabirom mehanizma konsenzusa koji ovisi o centralnom autoritetu.

Ranjivosti i programske greške ostavljene u pametnim ugovorima na javnim DLT sustavima otkrivaju se i iskorištavaju svakih nekoliko mjeseci te mogu dovesti do gubitaka koji se mjere u milijunima američkih dolara. Primjerice, iskorištavanje kombinacije ranjivosti u pametnom ugovoru decentralizirane autonomne organizacije DAO na mreži Ethereum rezultiralo je krađom tokena u tadašnjoj protuvrijednosti od gotovo 60 milijuna dolara te naposlijetku i prestankom rada navedene organizacije [61]. Platforma Ethereum, kao jedna od najstarijih i najkorištenijih DLT platformi koja podržava pametne ugovore, zasigurno je i najviše testirana u praksi te je na njoj pronađeno najviše ranjivosti. Stoga će se ovaj rad pozabaviti najčešćim ranjivostima vezanim uz pametne ugovore platforme Ethereum, iako svaka platforma zbog načina na koji je izvedena može imati vlastite specifične ranjivosti.

Pametni ugovori na platformi Ethereum imaju mogućnost pozivanja drugih računa na mreži, što se može koristiti za pozivanje funkcije na drugom pametnom ugovoru ili za prijenos vrijednosti. Pozivi iz pametnih ugovora nazivaju se interne transakcije te ne stvaraju transakcijske zapise koji se bilježe u lancima blokova. Pametni ugovor može odrediti količinu *gas*-a koju pozvana strana smije iskoristiti kad poziva drugi račun, a ako je taj račun drugi pametni ugovor on će biti izvršen i moći će iskoristiti predviđeni proračun *gas*-a. Ako je taj drugi pametni ugovor zlonamjeran, a proračun *gas*-a dovoljno visok, on može pokušati pozvati ugovor koji je njega pozvao. Ako ugovor koji je prvi pozivatelj ne ažurira interno stanje računa, napadač može iskoristiti navedenu ranjivost kako bi iscrpio sredstva na navedenom računu. Ova ranjivost, koja se naziva i mogućnost ponovnog ulaska (engl. re-entrancy), korištena je u već spomenutom napadu na DAO [62].

Neke operacije niže razine programskog jezika Solidity, primjerice, *send* koja se koristi za prebacivanje vrijednosti, ne vraćaju iznimke u slučaju neizvršavanja već izvještavaju o statusu vraćanjem logičke vrijednosti. Ako povratna vrijednost nije provjerena, ugovor koji je pozvao operaciju nastavlja s izvršenjem čak i ako plaćanje nije uspjelo što može

dovesti do nedosljednosti. Navedena ranjivost naziva se i neriješena iznimka (engl. unhandled exception) [62].

Pametni ugovori na platformi Ethereum, kao i svi ostali računi, mogu primiti sredstva, no postoji nekoliko razloga koji mogu rezultirati trajnim zaključavanjem navedenih sredstava. Jedan od tih razloga može biti taj što navedeni ugovor ovisi o drugome ugovoru koji se uništio instrukcijom *SELFDESTRUCT*, čime je njegov programski kod izbrisan i sredstva prebačena. Navedena ranjivost, koja se naziva zaključani Ether (engl. locked Ether), će rezultirati trajnim zaključavanjem sredstva ako je to jedini način na koji izvorni pametni ugovor može prebacivati sredstva [62].

Na platformi Ethereum jedan blok se sastoji od mnogo transakcija, što znači da se stanje sredstava pametnog ugovora može više puta mijenjati unutar jednog bloka. Ako poredak transakcija koje pozivaju pametni ugovor može promijeniti krajnji ishod, napadač bi mogao iskoristiti navedenu ranjivost koju nazivamo ovisnost poretka transakcija (engl. transaction order dependency). Navedeno se, primjerice, može iskoristiti ako vlasnik ugovora, koji sudioniku daje nagradu ako sudionik dostavi rješenje slagalice, smanji iznos nagrade kad se transakcija objavi u mrežu [62].

Preljev cjelobrojne varijable (engl. integer overflow) čest je tip programske greške u različitim programskim jezicima, no u kontekstu platforme Ethereum može imati ozbiljne posljedice. Ako bi se, primjerice, prelio brojač petlji te na taj način stvorio beskonačnu petlju, sredstva vezana uz ugovor mogla bi se zamrznuti. Postoji li način da se poveća broj ponavljanja petlje, navedenu ranjivost napadač može iskoristiti, na primjer, registracijom dovoljnog broja korisnika da dođe do preljeva [62].

Pametni ugovori mogu izvršavati autorizacije provjeravajući pošiljatelja poruke kako bi se moglo ograničiti koliko puta sudionik može poduzeti neku aktivnost. Uništavanje pametnih ugovora ili zadavanje novih vlasnika ugovora tipično bi trebalo biti omogućeno samo vlasniku. Ako programer pametnog ugovora zaboravi ugraditi kritične provjere ili ako napadač ima mogućnost izvršavanja proizvoljnog programskog koda, primjerice, na način da može kontrolirati adresu delegiranog poziva, ostavlja se mogućnost iskorištavanja ranjivosti neograničene aktivnosti (engl. unrestricted action) [62].

U posljednje vrijeme ulaže se mnogo resursa kako bi se spriječili napadi na pametne ugovore te kako bi se pametni ugovori općenito učinili sigurnijima. U tu svrhu koriste se

alati za statičku i dinamičku analizu koda. Alati za statičku analizu koda većinom rade analizu strojnog koda ili koda više razine pametnih ugovora kako bi pronašli poznate ranjive uzorke, dok su alati za dinamičku analizu napravljeni kako bi otkrili ranjivosti ugovora koje se mogu iskoristiti. Unatoč tome što na platformi Ethereum evidentirano mnogo pametnih ugovora s ranjivostima, istraživanje objavljeno 2019. godine utvrdilo je da se samo mali broj evidentiranih ranjivih ugovora može iskoristiti, odnosno da su rezultati o ranjivostima lažno pozitivni ili su ranjivosti u ugovorima neiskoristive u praksi [62].

# 6. Zaključak

Postojeći sustavi za platni promet uobičajeno uključuju velike informacijske sustave čija se infrastruktura nalazi u nadležnosti jedne institucije, a uz njih nužno je imati i različite mrežne sustave te sustave za razmjenu poruka. Održavanje takvih sustava je kompleksno te zahtjeva visoka početna ulaganja, a rezultat toga je centralizirani sustav koji predstavlja jedinstvenu točku prekida rada podložnu kibernetičkim napadima. Banke moraju uložiti mnogo resursa da bi svojim klijentima omogućile korištenje digitalnog novca ili ovisiti o uslugama dobavljača, čime se izlažu visokim regulatornim, reputacijskim i financijskim rizicima. Osim toga banke su primorane surađivati s nekolicinom međunarodnih mreža kako bi njihovi klijenti mogli plaćati u inozemstvu ili razmjenjivati sredstva s računima u inozemstvu. Pružanje usluge izdavanja maloprodajnog digitalnog novca od strane središnjih banaka na DLT infrastrukturi smanjilo bi troškove, povećalo povjerenje u korištenje digitalnog novca i naposlijetku raširilo njegovo korištenje.

Infrastruktura financijskog tržišta koja je trenutno na raspolaganju neučinkovita je za financijsko posredovanje, troškovi prekograničnih transakcija su visoki, upravljanje životnim ciklusom vrijednosnica je neučinkovito te su takvi sustavi podložni tržišnim manipulacijama. Korištenje DLT sustava u svrhu izdavanja veleprodajnog digitalnog novca središnjih banaka smanjilo bi troškove i povećalo operativnu otpornost takvih sustava. Dodatno, raspolaganje različitim vrstama imovine čini DLT sustave efikasnijima od standardnih. Sljedeći koraci u razvoju takvog sustava, primjerice, omogućavanje upravljanja sindiciranim zajmovima ili podrška financiranju trgovanja korištenjem pametnih ugovora, donijeli bi značajne koristi za cijeli financijski sektor i gospodarstvo u cjelini. Prekogranično povezivanje različitih sustava središnjih banaka i globalna koordinacija značajno bi olakšala monetarnu politiku i drugu prekograničnu fiskalnu koordinaciju središnjih banaka.

Primjereno konfigurirani DLT sustavi imaju ograničeni broj vektora kibernetičkih napada, a takve napade trebalo bi provoditi simultano na više različitih mjesta s obzirom da se podaci nalaze u posjedu više različitih čvorova. Konačnost transakcija na DLT sustavima dodatan su faktor koji odvraća moguće pokušaje prijevara. Ovakvi sustavi

otporniji su na neautorizirane i zlonamjerne promjene, jer će svi sudionici mreže istodobno uočiti promjene u dijeljenoj glavnoj knjizi. Prekid rada pojedinog čvora u takvom sustavu isključit će samo taj čvor iz sudjelovanja u mreži, no neće zaustaviti rad ostatka mreže, a uklanjanje posrednika dodatno čini mreže manje podložnim određenim vrstama kibernetičkih napada.

Ključni aspekti u osmišljavanju i održavanju DLT sustava koji bi se koristili za izdavanje i trgovanje digitalnim novcem središnjih banaka trebali bi biti upravljanje kriptografskim postavkama i ključevima, upravljanje pravima pristupa i tajnosti podataka te upravljanje kodom pametnih ugovora. Naposlijetku, treba voditi računa i o tome da takav sustav bude skalabilan, interoperabilan i konfigurabilan kako, primjerice, uslijed promjene načina enkripcije zbog zastarjelosti ne bi bilo potrebno ponovno učitavati sve povijesne podatke.

Iako je na primjerima središnjih banaka Kambodže i karipskih država moguće vidjeti da su DLT sustavi koji su prvi put korišteni u ove svrhe u stvarnom produkcijskom okruženju bili namijenjeni građanstvu, vjerujem da će ova tehnologija širu primjenu imati u veleprodajnom obliku izdavanja i trgovanja digitalnom imovinom. Navedeno se daje zaključiti na temelju smjera zanimanja većine središnjih banaka za DLT sustave te njihove spremnosti na suradnju, javnu diskusiju i objavu vlastitih iskustava i istraživanja.

Isto je tako izvjesno da središnje banke DLT kao tehnologiju još uvijek smatraju nedovoljno zrelom, što nije ni čudno s obzirom da se nove tehnike koje bi učinile DLT platforme spremnijima zadovoljiti njihove poslovne potrebe još uvijek dinamično razvijaju. Osim toga, relacijske baze podataka, koje su u bankarstvo ušle krajem sedamdesetih godina prošlog stoljeća, još uvijek posao koji im je namijenjen odrađuju savršeno dobro, a ljudski resursi koji ih održavaju imaju neusporedivo više iskustva na raspolaganju.

# Literatura


[1] Kharpal, A., “China has given away millions in its digital yuan trials. This is how it works“, dostupno na: https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html (10. lipanj 2021.)

[2] Bouchaud, M. et al, “Central banks and the future of digital money“, ConsenSys AG, siječanj 2020.

[3] "The Riksbank’s e-krona project, Report 1", Sveriges Riksbank, rujan 2017.

[4] Boar, C., Holden, H., Wadsworth, A., "BIS Papers No 107; Impending arrival – a sequel to the survey on central bank digital currency", Bank for International Settlements, siječanj 2021.

[5] White, L., "The World's First Central Bank Electronic Money Has Come – And Gone: Ecuador, 2014-2018", dostupno na: https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/ (8. ožujak 2021.)

[6] Econotimes, "Dutch central bank reveals results on DNBcoin experiments", dostupno na: https://www.econotimes.com/Dutch-central-bank-reveals-results-on-DNBcoin-experiments-226565 (9. ožujak 2021.)

[7] "Payment Systems Worldwide: A Snapshot", The International Bank for Reconstruction and Development/The World Bank Group, lipanj 2020.

[8] McCormack, A. et al, "Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement", Payments Canada, Bank of Canada and R3, rujan 2017.

[9] "Project Jasper Primer: Introduction to Project Jasper", Payments Canada, Bank of Canada, R3 Lab and Research Centre, siječanj 2017.

[10] Hendry, S. et al, "Jasper Phase III: Securities Settlement using Distributed Ledger Technology", Bank of Canada, TMX Group, Payments Canada, Accenture and R3, listopad 2018.

[11] Burgos, A. et al, "Distributed ledger technical research in Central Bank of Brazil", Banco Central do Brasil, kolovoz 2017.

[12] "Project Ubin Phase 5: Enabling Broad Ecosystem Opportunities", Monetary Authority of Singapore, Temasek, J.P. Morgan and Accenture, srpanj 2020.

[13] "Stella; BOJ/ECB joint research project on distributed ledger technology", European Central Bank and Bank of Japan, ožujak 2018.

[14] "Stella – joint research project of the European Central Bank and the Bank of Japan; Synchronised cross-border payments", European Central Bank and Bank of Japan, lipanj 2019.

[15] "Stella – joint research project of the European Central Bank and the Bank of Japan; Balancing confidentiality and auditability in a distributed ledger environment", European Central Bank and Bank of Japan, veljača 2020.

[16] "Project Khokha; Exploring the use of distributed ledger technology for interbank payments settlement in South Africa", South African Reserve Bank, lipanj 2018.

[17] Dalal, D., Young, S., Lewis, A., "Project Ubin: SGD on Distributed Ledger", Deloitte and Monetary Authority of Singapore, 2017.

[18] "Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies", Monetary Authority of Singapore, The Association of Banks in Singapore, and Accenture, studeni 2017.

[19] "Delivery versus Payment on Distributed Ledger Technologies, Project Ubin", Deloitte, Monetary Authority of Singapore, and Singapore Exchange, 2018.

[20] "Jasper – Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies", Accenture, Bank of Canada, and Monetary Authority of Singapore, 2019.

[21] Monetary Authority of Singapore, "Project Ubin: Central Bank Digital Money using Distributed Ledger Technology", dostupno na: https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin (6. svibanj 2021.)

[22] "Stella – joint research project of the European Central Bank and the Bank of Japan; Payment systems: liquidity saving mechanisms in a distributed ledger environment", European Central Bank and Bank of Japan, rujan 2017.

[23] "Stella – joint research project of the European Central Bank and the Bank of Japan; Securities settlement systems: delivery-versus-payment in a distributed ledger environment", European Central Bank and Bank of Japan, ožujak 2018.

[24] "Kingdom of Cambodia Launches Central Bank Digital Currency, Co-Developed with Fintech Company SORAMITSU", Soramitsu, listopad 2020

[25] Eastern Caribbean Central Bank, "ECCB to Issue World's First Blockchain-based Digital Currency", dostupno na https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency (9. ožujak 2021.)

[26] Sand Dollar, "Public Update - The Bahamas Digital Currency Rollout", dostupno na https://www.sanddollar.bs/publicupdates/public-update-the-bahamas-digital-currency-rollout (10. ožujak 2021.)

[27] "CONSULTATION PAPER: Proposed Legislation for the Regulation of the provision and use of Central Bank issued Electronic Bahamian Dollars", Central Bank of The Bahamas, veljača 2021.

[28] Sveriges Riksbank, "E-krona", dostupno na https://www.riksbank.se/en-gb/payments--cash/e-krona/ (14. ožujak 2021.)

[29] Sveriges Riksbank, "The e-krona pilot – test of technical solution for the e-krona", dostupno na: https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/ (14. ožujak 2021.)

[30] Sveriges Riksbank, "Riksbank extends test of technical solution for the e-krona", dostupno na: https://www.riksbank.se/en-gb/press-and-published/notices-and-

press-releases/notices/2021/riksbank-extends-test-of-technical-solution-for-the-e-krona/ (14. ožujak 2021.)

[31] "Project Bakong; Next Generation Payment System", National Bank of Cambodia, lipanj 2020.

[32] Antoine, T. N. J., "The ECCB's Digital Currency (DCash) is a Critical Step in the Buildout of a Digital Economy in the ECCU", dostupno na: https://eccb-centralbank.org/blog/view/the-eccbas-digital-currency-dcash-is-a-critical-step-in-the-buildout-of-a-digital-economy-in-the-eccu (13. ožujak 2021.)

[33] Eastern Caribbean Central Bank, "ECCB Digital EC Currency Pilot; What You Should Know", dostupno na: https://www.eccb-centralbank.org/p/what-you-should-know-1 (13. ožujak 2021.)

[34] Eastern Caribbean Central Bank, "ECCB Digital EC Currency Pilot; Security", dostupno na: https://www.eccb-centralbank.org/p/security (13. ožujak 2021.)

[35] "DXCD Times; Towards a digital economy", Eastern Caribbean Central Bank, listopad 2019.

[36] Bharathan, V., "DXCD, The Eastern Caribbean Central Bank Digital Money Is Being Readied For Production", dostupno na: https://www.forbes.com/sites/vipinbharathan/2021/01/30/dxcd-the-eastern-caribbean-central-bank-money-is-being-readied-for-production/?sh=1d1f07d7178d (9. ožujak 2021.)

[37] "Project Sand Dollar: A Bahamas Payments System Modernisation Initiative", Central Bank of The Bahamas, prosinac 2019.

[38] NZIA, "NZIA Limited Identified as Preferred Technology Solutions Provider by the Central Bank of The Bahamas for Digital Currency Project", dostupno na: https://nzia.io/pr/central-bank-of-the-bahamas/ (10. ožujak 2021.)

[39] "The Riksbank's e-krona pilot", Sveriges Riksbank, veljača 2020.

[40] ethereum.org, "Ethereum Whitepaper", dostupno na: https://ethereum.org/en/whitepaper/, (30. svibanj 2021.)

[41] Wackerow, P. et al, "Ethereum development documentation", dostupno na: https://ethereum.org/en/developers/docs/ (1. lipanj 2021.)

[42] The go-ethereum Authors, "Whisper Oweerview", dostupno na https://geth.ethereum.org/docs/whisper/whisper-overview (3. lipanj 2021.)

[43] Kripalani, P., "Releasing Wireshark dissectors for Ethereum ÐΞVp2p protocols", dostupno na: https://media.consensys.net/releasing-wireshark-dissectors-for-ethereum-%C3%B0%CE%BEvp2p-protocols-215c9656dd9c (3. lipanj 2021.)

[44] Wikipedia contributors, "Ethereum", dostupno na: https://en.wikipedia.org/wiki/Ethereum#Ethereum_2.0 (1. lipanj 2021.)

[45] "Quorum Whitepaper", dostupno na: https://github.com/ConsenSys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf (3. lipanj 2021.)

[46] ConsenSys, "GoQuorum Enterprise Ethereum Client", dostupno na: https://docs.goquorum.consensys.net/en/stable/ (4. lipanj 2021.)

[47] Zhang, J., "Consensus Algorithms: PoA, IBFT or Raft?", dostupno na: https://www.kaleido.io/blockchain-blog/consensus-algorithms-poa-ibft-or-raft (4. lipanj 2021.)

[48] Adarme, N., "Tessera: The Privacy Manager of Choice for ConsenSys Quorum Networks", dostupno na: https://consensys.net/blog/quorum/tessera-the-privacy-manager-of-choice-for-consensys-quorum-networks/ (3. lipanj 2021.)

[49] ConsenSys, "GoQuorum; Privacy", dostupno na: https://docs.goquorum.consensys.net/en/stable/Concepts/Privacy/Privacy/ (3. lipanj 2021.)

[50] The Linux Foundation, "About Hyperledger", dostupno na: https://www.hyperledger.org/about (7. lipanj 2021.)

[51] Androulaki, E. et al, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", travanj 2018.

[52] Hyperledger, "The Ordering Service", dostupno na: https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html (9. lipanj 2021.)

[53] Hyperledger, "Security Model", dostupno na: https://hyperledger-fabric.readthedocs.io/en/release-2.2/security_model.html (9. lipanj 2021.)

[54] Brown, R., G., "The Corda Platform: An Introduction", svibanj 2018.

[55] R3, "Corda Documentation; Contracts", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-contracts.html (4. lipanj 2021.)

[56] R3, "Corda Documentation; Flows", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-flows.html (4. lipanj 2021.)

[57] R3, "Corda Documentation; Nodes ", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-node.html (7. lipanj 2021.)

[58] R3, "Corda Documentation; Vault", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-vault.html (7. lipanj 2021.)

[59] R3, "Corda Documentation; Notaries", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-notaries.html (7. lipanj 2021.)

[60] R3, "Corda Documentation; Transaction tear-offs", dostupno na: https://docs.corda.net/docs/corda-os/4.8/key-concepts-tearoffs.html (7. lipanj 2021.)

[61] Cryptopedia Staff, "What Was The DAO?", dostupno na: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao (16. lipanj 2021.)

[62] Perez, D., Livshits, B., "Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited", listopad 2020.

[63] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", listopad 2008.

# Skraćenice

CBDC - digitalni novac središnje banke (engl. central bank digital currency)

DLT – Raspodijeljena glavna knjiga (engl. distributed ledger technology)

RTGS - sustav bruto namire u realnom vremenu (engl. real time gross settlement system)

UTXO - nepotrošeni izlazi transakcije (engl. unspent transaction outputs)

KYC - prikupljanje informacija o klijentima (engl. know your customer)

AML – sprječavanje pranja novca (engl. anti-money laundering)

BIS - Banka za međunarodne namire (engl. Bank for International Settlements)

DvP - isporuke po plaćanju (engl. delivery-vs-payments)

PvP - plaćanje po plaćanju (engl. payment-vs-payment)

ECB - Europska središnja banka (engl. European Central Bank)

DDR ili DR - digitalna depozitarna potvrda (engl. digital depository receipt)

LSM - mehanizam čuvanja likvidnosti (engl. liquidity-saving mechanism)

BFT - algoritam tolerantan na bizantske greške (engl. byzantine fault tolerance)

MAS - Monetarni autoritet Singapura

ZKP - sakrivajuća kriptografska metoda dokaz bez znanja (engl. zero-knowledge proofs)

FX - razmjena valuta (engl. foreign exchange)

HTLC - sažeti vremenski zaključani ugovori (engl. hashed time-locked contracts)

RPC - poziva udaljene procedure (engl. remote procedure call)

ECCB - središnja banka istočnih Kariba (engl. Eastern Caribbean Central Bank)

EVM - virtualno izvršno okruženje Ethereum (engl. Ethereum Virtual Machine)

# Sažetak

**Naslov:** Primjena tehnologije raspodijeljenih glavnih knjiga u digitalnom novcu središnjih banaka

Potreba izdavanja maloprodajnog digitalnog novca od strane središnjih banaka za građanstvo sve se češće spominje kao nužnost, ponajprije zbog financijske inkluzije i smanjenja korištenja gotovine u proteklih nekoliko godina. Osim toga, središnje banke razmatraju korištenje tehnologije raspodijeljenih glavnih knjiga zbog ubrzavanja veleprodajnog plaćanja i trgovanja imovinom te izbjegavanja korištenja pružatelja usluga u tu svrhu. S tim u vidu niz središnjih banaka u svijetu u posljednjih nekoliko godina pokrenuo je projekte i pilote za testiranje DLT sustava u svrhu izdavanja, trgovanja i plaćanja CDBC-om. Ovaj rad donosi načine provedbe i zaključke iz najznačajnijih te najbolje dokumentiranih istraživanja i pilota provedenih u tu svrhu. Nakon toga, rad ukratko prolazi kroz specifičnosti najčešće korištenih DLT platformi u navedenim istraživanjima i pilotima. Naposljetku se rad bavi sigurnosnim aspektima izdavanja CDBC-a na DLT platformi, uključujući tehnike za unaprjeđenje povjerljivosti te moguće ranjivosti i programske greške pametnih ugovora, te najboljim praksama koje bi trebalo slijediti kako bi se osigurala sigurnost takvih sustava.

**Ključne riječi:** raspodijeljena glavna knjiga, kriptovalute, digitalni novac, središnja banka, lanac blokova, sigurnosna razmatranja, tehnike za unaprjeđenje povjerljivosti, veleprodajni CDBC, maloprodajni CDBC

# Abstract

**Title:** Application of distributed ledger technology in central bank digital currencies

The need for central banks to issue retail digital currency is increasingly mentioned as a necessity, primarily due to financial inclusion and reduced use of cash in the past few years. In addition, central banks are considering the use of distributed general ledger technology to accelerate wholesale payments and asset trading, and to avoid using third party providers for this purpose. A number of central banks around the world in recent years have launched projects and pilots to test DLT systems for the purpose of issuing, trading and paying with CDBC. This paper reviews implementations and conclusions from the most significant and best documented research and pilots conducted for this purpose. After that, the paper briefly goes through the specifics of the most commonly used DLT platforms in the mentioned research and pilots. Finally, the paper addresses the security aspects of issuing CDBC on DLT platform, including privacy enhancing techniques, possible vulnerabilities and bugs of smart contracts, and best practices that should be applied to ensure the security of such systems.

**Keywords:** Distributed Ledger Technology (DLT), cryptocurrency, digital currency, central bank, blockchain, security considerations, privacy enhancing techniques, wholesale CDBC, retail CDBC

# Životopis

Bojan Belušić rođen je 13. svibnja 1984. godine u Puli. U Labinu, nakon osnovne, završava Srednju školu Mate Blažine u kojoj stječe zvanje elektrotehničara. Nakon srednje škole, 2002. godine upisuje Fakultet elektrotehnike i računarstva u Zagrebu. Tijekom i nakon studija član je Kluba studenata elektrotehnike te udruge za promicanje audiovizalnih umjetnosti Demode, u sklopu kojih volontira i organizira razne glazbene programe, koncerte i festivale. Diplomirani inženjer elektrotehnike postaje 2010. godine na smjeru radiokomunikacije i profesionalna elektronika, nakon obrane diplomskog rada "Optimizacija sustava ozvučenja" kod mentora prof. dr. sc. Hrvoja Domitrovića. Poslije završenog fakulteta zapošljava se u Intesa Sanpaolo Cardu, gdje od 2011. do 2018. godine radi kao specijalist i arhitekt autorizacijskih sustava. Na navedenim radnim mjestima skupio je široko iskustvo iz platnih i financijskih informacijskih sustava, te se upoznaje s informacijskom sigurnošću, kriptografijom i upravljanjem kontinuitetom poslovanja obavljajući zadatke skrbnika ključeva te koordinirajući redovite godišnje vježbe za oporavak od katastrofe. Godine 2018. zapošljava se u Privrednoj banci Zagreb na mjestu glavnog revizora u Reviziji informacijske i komunikacijske tehnologije, te 2019. stječe certifikat "Certified Information Security Auditor" organizacije ISACA. Kao glavni revizor redovito vodi timove u tehničkim i poslovnim revizijama koje uključuju područja kao što su upravljanje informacijskim sustavima, upravljanje kibernetičkom sigurnošću, upravljanje promjenama u IT-u ili vođenje IT projekata. Osim toga, u sklopu svojih zadataka u Internoj reviziji, provodi analize rizika i savjetovanja o usklađenosti sa zakonima, regulativom (GDPR, PSD2, NIS) i najboljim praksama (COBIT, NIST, ITIL, ISO27001).

# Biography

Bojan Belušić was born on May 13, 1984, in Pula, Croatia. In Labin, after finishing primary school, he graduated from Mate Blažina High School, where he acquired the title of electrical technician. After high school, he enrolled at the Faculty of Electrical Engineering and Computing in Zagreb in 2002. During and after his time at university, he was a member of the Electrical Engineering Students' Club (KSET) and Demode Association for Promotion of Audio-visual Arts, within which he volunteers and organizes various music programs, concerts and festivals. In 2010, he became Master of Engineering in electrical engineering in the field of radiocommunications and professional electronics, after defending his diploma thesis "Optimization of Public Audio systems" with the mentor prof. dr. sc. Hrvoje Domitrović. After graduating from university, he was employed by Intesa Sanpaolo Card, where from 2011 to 2018 he worked as a specialist and architect of authorization systems. There he gathered extensive experience in payment and financial information systems, and became acquainted with information security, cryptography, and business continuity management by performing key custodian tasks and coordinating regular annual disaster recovery exercises. In 2018, he was employed by Privredna banka Zagreb as Chief Auditor in ICT Audit, and in 2019 he obtained the "Certified Information Security Auditor" certificate given by ISACA organization. As Chief Auditor, he is regularly leading technical and business audit teams in areas such as information systems management, cyber security management, IT change management, or project management. In addition, as part of his tasks in Internal Audit, he is conducting risk analysis and provides consultation on compliance with laws, regulations (GDPR, PSD2, NIS) and best practices (COBIT, NIST, ITIL, ISO27001).