UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

IZZIVI UPORABE TEHNOLOGIJE RAZPRŠENE EVIDENCE PRI PLAČILIH, OBRAČUNIH IN PORAVNAVAH V BANČNIŠTVU

Ljubljana, september 2024 DANIEL VALENTINE

IZJAVA O AVTORSTVU

Podpisani Daniel Valentine, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Izzivi uporabe tehnologije razpršene evidence pri plačilih, obračunih in poravnavah v bančništvu, pripravljenega v sodelovanju s svetovalcem izr. prof. dr. Antonom Manfredo

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi;

11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 11. 9. 2024

Podpis študenta: Daniel Valentine

Digitally signed by Daniel Valentine
DN: C=SI, O=state authorities, OU=mid/ID card/basic, G=Daniel + SN=Valentine + SERIALNUMBER=1238290914019 + CN=Daniel Valentine
Reason: I am the author of this document
Location:
Date: 2024-09-25 12:55:40

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
ABS – (angl. Association of Banks in Singapore); Združenje bank v Singapurju
AML – (angl. Anti-Money Laundering); predpis proti pranju denarja
API – (angl. Application Programming Interface); programski vmesnik
ASIC – (angl. specializirano integrirano vezje); Application-Specific Integrated Circuit
BDP – bruto domači proizvod
BFT – (angl. Byzantine Fault Tolerance); toleranca napake, konsenzni mehanizem
BIS – (angl. Bank for International Settlements); Banka za mednarodne poravnave
BoA – (angl. Bank of America); Bank of America, poslovna banka
BoC – (angl. Bank of Canada); centralna banka Kanade
BoE – (angl. Bank of England); centralna banka Anglije
BoJ – (angl. Bank of Japan); centralna banka Japonske
BTC – (angl. bitcoin); bitcoin, kriptovaluta
CARICOM – (angl. Caribbean Community); Svetovalno-delovna skupina za finančno tehnologijo v Karibski skupnosti

CB – (angl. Central Bank); centralna banka
CBDC – (angl. Central Bank Digital Currency); digitalna valuta centralne banke
CDD – (angl. Customer Due Diligence); skrbni pregled stranke
CFT – (angl. Combating the Financing of Terrorism); boj proti financiranju terorizma
CPMI – (angl. Committee on Payments and Market Infrastructures); Odbor za plačila in tržno infrastrukturo
CPU – (angl. Central Processing Unit); centralno procesna enota
CSD – (angl. Central Securities Depository); centralno depotna družba
DAG – (angl. Directed Acyclic Graph); usmerjeni aciklični graf, struktura podatkov
DAO – (angl. Decentralized Autonomous Organization); decentralizirana avtonomna organizacija
DApps – (angl. Decentralised Applications); decentralizirane aplikacije
DDoS – (angl. Distributed Denial-of-Service); porazdeljeni napad zavrnitve storitve
DDR – (angl. Digital Depository Receipt); digitalno potrdilo o prejemu
DeFi – (angl. Decentralized Finance); decentralizirane finance
DLT – (angl. Distributed Ledger Technology); tehnologija razpršene evidence
DvP – (angl. Delivery versus Payment); dostava proti plačilu
ECB – (angl. European Central Bank); Evropska centralna banka
EK – Evropska komisija
EU – (angl. European Union); Evropska unija
FED – (angl. Federal Reserve); Zvezne rezerve, centralna banka Amerike
FI – (angl. Financial Institution); finančna institucija
FinTeh – finančna tehnologija
FSB – (angl. Financial Stability Board); Odbor za finančno stabilnost
GBN – (angl. Global Banking News); globalne bančne novice, publikacija
GPU – (angl. Graphics Processing Unit); grafični procesor
H/s – (angl. Hash/second); heš/sekundo
HTLC – (angl. Hash Time Locked Contracts); zgoščena časovno zaklenjena (pametna) pogodba
IBRD – (angl. International Bank for Reconstruction and Development); Mednarodna banka za obnovo in razvoj
ING – (angl. Internationale Nederlanden Groep); nizozemska finančna institucija
IT – (angl. Information Technology); informacijska tehnologija
KDPW – (polj. Krajowy Depozyt Papierów Wartościowych); centralno depotna družba vrednostnih papirjev
KIR – (polj. Krajowa Izba Rozliczeniowa); klirinška hiša
KYC – (angl. Know Your Client); zahteva poznavanja svoje stranke
LSM – (angl. Liquidity-Saving Mechanism); mehanizem za varčevanje z likvidnostjo
LVTS – (angl. Large Value Transfer System); sistem velikih plačil
M2M – (angl. Machine-to-Machine); med napravami
MAS – (angl. Monetary Authority of Singapore); Monetarni organ Singapurja, centralna banka

MB – (angl. Megabyte); megabajt
NARA – (angl. National Archives and Records Administration); vladna agencija za arhiviranje
NBP – (polj. Narodowy Bank Polski); centralna banka Poljske
OMFIF – (angl. Official Monetary and Financial Institutions Forum); Uradni forum denarnih in finančnih institucij
P2P – (angl. peer-to-peer); vrstniško (omrežje)
PB – poslovna banka
pBFT – (angl. practical Byzantine Fault Tolerance); praktična toleranca bizantinske napake
PC – (angl. Payments Canada); upravljalec plačilnih sistemov in infrastrukture v Kanadi
PCS – (angl. Payments, Clearing and Settlements); plačila, obračuni in poravnave
POS – (angl. Point of Sale); prodajno mesto (na plačilnih terminalih)
PoW – (angl. Proof of Work); dokaz o delu
PSD2 – (angl. Payment Services Directive 2); direktiva o plačilnih storitvah
PSP – (angl. Payment Service Provider); ponudnik plačilnih storitev
PvP – (angl. Payment versus Payment); plačilo proti plačilu
RTGS – (angl. Real Time Gross Settlement); bruto poravnava v realnem času
SEPA – (angl. Single Euro Payments Area); enotno območje plačil v evrih
SGD – (angl. Singapore Dollar); singapurski dolar
SGX – (angl. Singapore Exchange); singapurska borza
SNB – (nemš. Schweizerische Nationalbank); centralna banka Švice
SWIFT – (angl. Society for Worldwide Interbank Financial Telecommunication); Združenje za svetovno medbančno finančno telekomunikacijo
T2S – (angl. TARGET2-securities); evropski sistem za centralizirano kliring in poravnavo vrednostnih papirjev
TARGET – (angl. Trans European Automated Real-time Gross Settlement Express Transfer System); transevropski sistem bruto poravnav v realnem času
TARGET2 – (angl. Trans European Automated Real–time Gross Settlement Express Transfer System 2); transevropski sistem bruto poravnav v realnem času 2
TIPS – (angl. Target Instant Payment Settlement); sistem takojšnjih plačil
tns – transakcij na sekundo
USD – (angl. United States Dollar); ameriški dolar
UST – (angl. Terra USD); kriptovaluta
VP – vrednostni papir
WEF – (angl. World Economic Forum); Svetovni ekonomski forum

1 UVOD

Izume in inovacije četrte industrijske revolucije zaznamujejo napredki na področju umetne inteligence, robotike, interneta stvari, avtonomnih vozil, 3D-tiskanja, nanotehnologije, biotehnologije, novih materialov, učinkovitejšega shranjevanja energije in kvantnega računalništva (Schwab, 2016). Ena izmed tehnologij, v zadnjem času deležna večje pozornosti, je veriga podatkovnih blokov (angl. blockchain) in z njo povezana decentralizacija digitalnega sistema na distribuiranem omrežju (Fintech, brez datuma). Transakcije na verigi blokov potekajo s posredovanjem bloka vsem udeležencem v omrežju, da potrdijo veljavnost transakcije in je blok lahko dodan k verigi, ki predstavlja neizbrisen in transparenten dokaz o transakciji (Nakamoto, 2008).

Prvo desetletje razvoja tehnologije razpršene evidence (angl. Digital Ledger Technology, v nadaljevanju DLT) je kot edino zaznamovala veriga podatkovnih blokov kot hitro razvijajoči se pristop k beleženju in razdelitvi podatkov po številnih hranilcih oziroma knjigah. Ta tehnologija omogoča beleženje, porazdelitev ter usklajenost transakcij in podatkov prek distribuiranega omrežja različnih udeležencev. Kriptovalute so zgolj ena od možnosti uporabe tega sistema, potencial ima tudi pri mednarodnih plačilih, infrastrukturi finančnih trgov, deviznih trgih in registru zavarovanj (International Bank for Reconstruction and Development, 2017; v nadaljevanju IBRD). Denarni in plačilni sistemi so neločljivo povezani, saj so se razvijali skupaj, kar je razvidno iz pristojnosti centralnih bank pri zagotavljanju stabilnosti valute in plačilnih sistemov za nemoteno delovanje gospodarstva (Ali in drugi, 2014).

Na podlagi poročila Svetovnega ekonomskega foruma iz leta 2016 je bilo v treh letih pred tem namenjenih več kot 1,4 milijarde ameriških dolarjev za raziskovanje in vpeljavo DLT v industrijo finančnih storitev (Workie in Jain, 2017). Kljub povečanemu zanimanju za DLT je verjetna pot uvedbe postopna in ne takojšnja zamenjava obstoječe infrastrukture (Meaning in drugi, 2018). Dandanes zakonsko regulirana finančna institucija zagotavlja istovetnost uporabnika in posreduje pri transakcijah, ki morajo biti avtentične, enkratne, preverljive in nepovratne, če se ne izkažejo za goljufive. Delovanje distribuirane kriptovalute je neodvisno od institucij, razlog za to je avtonomnost DLT, na kateri temelji (Conte de Leon in drugi, 2017). Kako deležniki na finančnem trgu nakazujejo, shranjujejo in ohranjajo lastništvo digitaliziranih sredstev, določata vrstniško omrežje (angl. peer-to-peer, v nadaljevanju P2P) in distribuirano beleženje podatkov, ki jim omogoča deljeno, točno zgodovino vseh transakcij v sistemu. Kriptografija nudi varen način izvedbe veljavne transakcije, kot tudi varen prenos in shranjevanje podatkov. Konsenzni algoritem nudi proces, da so transakcije potrjene in dodane k enotni evidenci, kar je pomembna lastnost, ko ima več kot en deležnik dovoljenje predlagati posodobitve evidence (Brainard, 2016).

Digitalne valute centralne banke (angl. Central Bank Digital Currency, v nadaljevanju CBDC), temelječe na DLT, bi delovale kot gotovina. V začetku bi centralna banka (v nadaljevanju CB) izdala digitalno valuto, potem bi krožila med bankami, podjetji in

potrošniki brez nadaljnjega vpletanja CB. Vpliv bi imela na tri glavna področja centralnega bančništva: plačila, finančno stabilnost in monetarno politiko (Shin, 2018). CB so v svoji vlogi operaterja in nadzornika plačilnega sistema in ostale infrastrukture finančnega trga ter pospeševalca razvoja in inoviranja plačilnega sistema zadolžene za spodbujanje varnih in učinkovitih plačilnih sistemov. Bolj točno, varnost plačilnih sistemov pogosto temelji na kakovosti upravljanja s tveganji (Bank for International Settlements, 2018; v nadaljevanju BIS). Plačila, obračuni in poravnave so s CBDC izpostavljene operativnim in varnostnim tveganjem, vprašanjem poravnave, pravnim tveganjem, vprašanjem upravljanja ter tveganjem upravljanja in zaščite podatkov (BIS, 2017). Kriptovalute CB se delijo na maloprodajne, kjer CB izda svojo kriptovaluto, izmenljivo z državnim denarjem, poleg gotovine in rezerv zastopajo tretjo komponento monetarne baze, in veleprodajne, ki imajo omejen dostop in so namenjene finančnim institucijam (Bech in Garratt, 2017). Uvedba CBDC verjetno ne bi spremenila osnovnega delovanja vpeljave monetarne politike, vključno z operacijami odprtega trga CB. Prav verjetno pa tudi ne bi učinkovala na diskrecijo CB, kot tudi ne na dospelost, likvidnost in kreditno tveganje sredstev (BIS, 2018).

V začetku 2016 so Banka Kanade, konzorcij za finančne inovacije R3, nekatere od glavnih kanadskih bank in institucija za plačilne storitve Payments Canada pričele s projektom Jasper s ciljem raziskovanja DLT za poravnavo medbančnih plačil. Sredstvo za poravnavo je bilo digitalno potrdilo o prejemu (angl. Digital Depository Receipt) kot zahtevek za kanadsko-dolarske vloge (Payments Canada in drugi, 2017; v nadaljevanju PC). Niso pa opazili prihrankov v primerjavi z obstoječim sistemom, prav tako je bil izpostavljen vdorom in tveganjem v delovanju (Global Banking News, 2018a; v nadaljevanju GBN). Šele v tretji fazi projekta Jasper so dokazali, da sta takojšen obračun in poravnava vrednostnih papirjev v evidenci izvedljiva. Gotovina centralne banke in sredstva so bila spremenjena v žetone za dokončanje takojšnje, neposredne poravnave sredstev na DLT (Accenture, 2018). Projekt Ubin od Monetarnega organa Singapurja, Združenja bank v Singapurju in drugih finančnih institucij se osredotoča na reševanje zastojev plačil in na mehanizem varčevanja z likvidnostjo pri bruto poravnavi v realnem času (angl. Real-time gross settlement, RTGS) (Accenture, 2017). Španska banka Santander je za svoje komitente v letu 2018 uvedla čezmejna plačila v sistemu DLT, imenovana One Pay FX, in s tem dvignila vrednost kriptovalut (GBN, 2018b). Od 2014 so Banka Anglije, Banka za mednarodne poravnave in Mednarodni denarni sklad analizirali vpliv Bitcoina (v nadaljevanju zapisujem z veliko začetnico naziv sistema Bitcoin, z malo začetnico pa istoimensko valuto bitcoin) na denar CB, še bolj pa učinek tehnologije verige podatkovnih blokov kot njegovo podstat in tehnologijo razpršene evidence na plačila in bančništvo (Bott in Milkau, 2016). Poleg uporabe DLT v plačilnem sistemu se lahko uporabi za prenos kateregakoli sredstva, ki je prikazan v digitalni obliki. Obstaja pomembna vzporednica pri na novo pojavljajočih se plačilnih sistemih Federal Reserve (FED), ameriške centralne banke, in med tem, kar se pojavlja pri regulatorjih na trgu vrednostnih papirjev (Hodrick, 2018). Banke, tudi Credit Suisse in JP Morgan, preizkušajo žetonirane različice tradicionalnih vrednostnih papirjev in fiat valut, da bi strankam omogočile trgovanje na DLT. S prenosom na žeton, ki je pravno

izvršljiv zahtevek za vrednostni papir, ta postane bolj likviden in preprostejši za trgovanje. Poravnave valutnih transakcij prek verige blokov omogočajo avtomatizirane plačilne sisteme z uporabo pametnih pogodb (McLellan, 2018). Ko finančne institucije obravnavajo verigo blokov in DLT, ni mišljena odprta, javna baza, ki vzdržuje kopije po vsem svetu, kot je Bitcoin veriga blokov, temveč različica verige blokov, ki je delujoča v njihovem podatkovnem centru ali zasebnem oblaku ali pa jo vodi zasebni organ. Edina izjema bi lahko bil poskus borze Nasdaq pri sledenju nad lastništvom vrednostnih papirjev z omrežjem Bitcoin (Crosman, 2022). Svetovna banka je prek Banke skupnosti narodov Avstralije izdala prvo obveznico, temelječo na verigi blokov na Microsoftovi računalniški platformi v oblaku Azure (Townsend, 2018).

Priložnosti, ki jih prinaša DLT, so izvedba transakcij na finančnih trgih pri nižjih stroških, povečana zanesljivost, celovitost in hitrost procesa poravnave. Medtem ko virtualnim valutam, kot je bitcoin, primanjkuje transparentnosti, imajo visoko cenovno volatilnost in nizke omejitve vstopa. Za zagotovitev celovitosti, transparentnosti in s tem zaščite investitorja sta nujno potrebni zakonodaja in nadzor trga (Bruhl, 2017). DLT se med sabo ločijo na podlagi dovoljenja, ali lahko vsak računalnik naloži evidenco in potrjuje transakcije, na podlagi zasebnosti, kateri računalnik lahko prebere in sproži transakcijo v evidenci, po hierarhiji, ali ima vsak računalnik kopijo evidence, in po odprtosti kode, kdo lahko predlaga izboljšavo kode za platformo evidence (Wadsworth, 2018). Glede na izbiro tehnoloških komponent DLT zajema vse od oblike, kjer finančni posredniki vpeljejo le nekaj ključnih komponent za izboljšanje svojih tehničnih platform, do druge malo verjetne skrajnosti, celovite ureditve za nadomestitev vseh njihovih funkcij. Med tema skrajnima oblikama so številne možnosti za prihodnjo finančno arhitekturo (Mills in drugi, 2016). Kriptovaluta bi lahko delovala kot decentralizirana avtonomna organizacija in izvajala operacije na odprtem trgu z uravnavanjem količine novega denarja, na podlagi spremembe bruto domačega proizvoda (BDP), inflacije in obtočne hitrosti denarja (Hayes, 2016). Mehanizmi, ki neposredno vplivajo na vrednost kriptovalut, so ponudba in povpraševanje po njih, privlačnost za vlagatelje in razvoj svetovnih finančnih indikatorjev (Ciaian in drugi, 2016). Za tiste s konsenznim mehanizmom dokaza o delu so pomembne spremenljivke za njihovo rudarjenje: cena električne energije, poraba energije za rudarjenje, realne tržne cene kriptovalut in zahtevnost algoritma, ki se poveča z rudarjeno količino (Hayes, 2015).

DLT ima potencial povečati učinkovitost plačilnih procesov. Tehnologija je dostopna, vendar še ne povsem vpeljana. Potrebno je prepoznati njene prednosti, slabosti, priložnosti in nevarnosti. Ko bo sistem s pilotnimi projekti utrjen, je po učinku mreže pričakovati njegovo razširitev na globalno raven. V osnovi je treba najti učinke DLT na plačila, obračune in poravnave. Pri rabi kriptovalut CB pa je treba ločiti med dvema tipoma, prvim, namenjenim medbančnemu poslovanju, in drugim, namenjenim splošnemu obtoku. Za dosego večje hitrosti, varnosti, stroškovne učinkovitosti in transparentnosti transakcij z DLT se je treba soočiti s številnimi izzivi, ki jih opredelim tudi v svojem magistrskem delu.

Namen magistrskega dela je proučiti izboljšave transakcij z uporabo CBDC na razpršeni evidenci, v fazah plačila, obračuna in poravnave.

Cilji magistrskega dela so:

- Pregledati obstoječe prakse in modele digitalizacije valut v okviru centralnih bank ter oceniti njihov vpliv na pospeševanje transakcij in zmanjšanje stroškov v plačilnih sistemih.
- Raziskati omejitve, ki jih prinaša uporaba DLT v obstoječih plačilnih sistemih, ter proučiti, kako te ovire vplivajo na obsežno uporabo tehnologije.
- Oceniti vpliv DLT na povečanje učinkovitosti, zmanjšanje stroškov in izboljšanje zanesljivosti transakcij, ob upoštevanju specifičnih predpisov in varnostnih zahtev.
- Kvalitativno ovrednotiti v kolikšni meri DLT zmanjšuje stroške in pospešuje transakcijske procese v bančništvu.

Magistrsko delo obravnava teorijo in empirične ugotovitve znanstvenih oziroma akademskih člankov ter ostalih relevantnih publikacij na temo tehnologije razpršene evidence pri plačilih v bančništvu. Z metodo deskripcije opišem posamezne izraze in z metodo kompilacije povzamem dela drugih avtorjev ter jih z metodo sinteze združim v tematska poglavja. Delo podkrepim tudi z znanjem, pridobljenim na podiplomskem študiju, in s spoznanji, pridobljenimi s trgovanjem s kriptovalutami.

S pomočjo induktivno-deduktivne metode sklepam o lastnostih DLT v bančnem sektorju s posameznih primerov na splošno in obratno. Komparativna metoda mi služi za to, da kot izhodišče vzamem trenutni digitalni sistem v bančništvu in ga primerjam s sistemom, temelječim na DLT. Za tehnologijo izvedem tudi analizo prednosti, slabosti, priložnosti in nevarnosti. Uporabim tudi metodo spraševanja z delno strukturiranimi intervjuji in anketami odprtega tipa, torej kvalitativno metodo zbiranja podatkov za pridobitev informacij o poskusih vpeljave DLT (njene hitrosti, varnosti, stroškov, transparentnosti in ostalih informacij, opredeljenih med cilji), ki jih naslovim na strokovne sodelavce centralnih in poslovnih bank ter stopim z njimi v stik prek stikov na njihovih uradnih spletnih straneh. Diskusija zajema tako primarne kot sekundarne vire, v rezultatih je analizirano stanje in predviden razvoj sektorja z uporabo DLT.

V začetku dela predstavim tehnologijo razpršene evidence in z njo povezane elemente ter nadaljujem z vpeljavo tehnologije v plačilni sistem. Poiščem povezavo med kriptovalutami in CBDC. Značilnosti zadnjih *de facto* predstavljajo lastnosti plačil, kliringa in poravnave z omenjeno tehnologijo. V raziskovalnem delu obravnavam ugotovitve centralnih bank, povezane z uporabo valute na razpršeni evidenci pri plačilih, ter največjega združenja poslovnih bank in finančnih institucij za digitalizacijo gotovine z namenom izboljšave transakcij.

2 PREDSTAVITEV TEHNOLOGIJE RAZPRŠENE EVIDENCE

2.1 Terminologija tehnologije razpršene evidence

V magistrskem delu se pogosto pojavljajo izrazi, povezani z informacijsko tehnologijo, ki pa imajo specifičen pomen. Razširljivost (angl. scalability) je zmogljivost sistema, da ohranja učinkovitost kljub povečanemu obsegu uporabe. Prožnost (angl. flexibility), za kar uporabljam besedo prilagodljivost, se nanaša na hitro odzivanje sistema na spremembe, kar zajema: modularnost (kjer je možno dodajati ali odvzemati dele, t. i. module, ne da se bi s tem zmotilo delovanje sistema), razširljivost in interoperabilnost (s programskimi vmesniki (angl. application programming interface, API)). Celovitost (angl. integrity) pomeni, da so podatki, sistemi in procesi takšni, da informacije ostanejo nespremenjene in brez napak. Obstojnost (angl. resilience) opisuje hitro vzpostavitev delovanja sistema po nepredvidenih dogodkih in napakah v delovanju, vključuje tudi zasilne (angl. redundancy) sisteme in toleranco napak. Širši pomen predstavlja robustnost, ki pomeni, da sistem ohranja stabilno delovanje, tako da ga napake ne prizadenejo. Usklajevanje (angl. reconciliation) služi preverjanju, da so primerjani podatki poenoteni z izvornimi. P2P-delovanje predstavlja omrežje, kjer si računalniki izmenjujejo podatke neposredno in delujejo kot strežnik in uporabnik hkrati. Vozlišča (angl. nodes) predstavljajo točke v omrežju oziroma napravo ali računalnik, povezan z omrežjem. Na tehnologijo razpršene evidence (angl. distributed ledger technology) se v nadaljevanju sklicujem s kratico DLT. Izraz verifikacija se uporablja v DLT-transakcijah in pomeni preverjanje natančnosti in pristnosti podatkov transakcije, medtem ko validacija pomeni overjanje oziroma preverjanje veljavnosti z zagotavljanjem zakonitosti in skladnosti transakcije s pravili in politikami omrežja.

2.2 Temelji tehnologije razpršene evidence

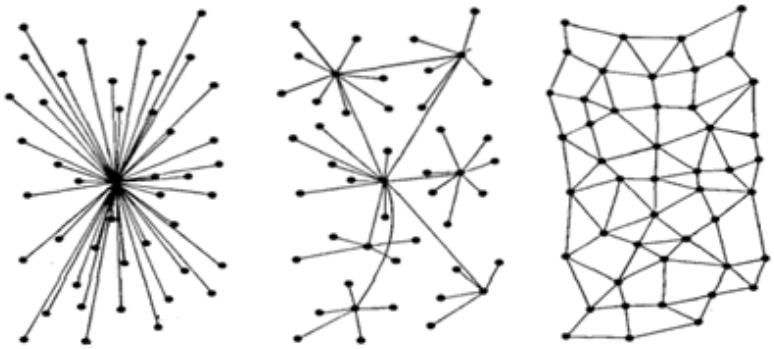
Tehnologija razpršene evidence beleži transakcije in pogodbe na različnih lokacijah in pri različnih subjektih ter nima osrednjega skrbnika, torej je decentralizirana. Temelji na P2P-omrežju in konsenznem algoritmu za kopiranje, razporejanje in usklajevanje digitalnih podatkov med napravami, t. i. vozlišči (angl. nodes). Vsaka naprava zabeleži transakcijo in z glasovanjem izbere, katera različica je prava, na ta način vsa vozlišča posodobijo evidenco. Varnost omogočajo kriptografski ključi in elektronski podpisi, prav tako vse shranjene informacije postanejo nespremenljiva baza podatkov (Wattenhofer, 2017). Sistem se deli na javno dostopen in na sistem, dostopen le zasebnim uporabnikom, razlikuje se lahko tudi po uporabi konsenznih algoritmov (Oliver, 2018). V nadaljevanju so navedene lastnosti, značilne za DLT (Mathis, 2016):

- razpršenost (distribuiranost): vsi udeleženci v omrežju imajo popolno kopijo evidence, kar omogoča popolno transparentnost,
- anonimnost: identiteta udeležencev je psevdonimna ali anonimna,
- časovni žig: vsak blok je časovno označen,

- soglasnost: vsi udeleženci soglašajo o verodostojnosti vsakega zapisa,
- nespremenljivost: vsi potrjeni zapisi so nepovratni, torej se jih ne da spreminjati,
- varnost: vsak zapis posebej je šifriran,
- programirljivost: ustvariti se da pametne pogodbe.

Možnost vpogleda in vnosa pri centraliziranih evidencah ima le skrbnik, takšne evidence so spremenljive in se morajo za izvedbo transakcij usklajevati z zunanjimi evidencami. V decentraliziranem sistemu ni enotnega skrbnika z nadzorom nad vso obdelavo procesov, so pa pooblaščene osebe, ki lahko vnašajo podatke v evidenco; takšen tip javne evidence je dostopen ostalim le na vpogled. V primeru distribuiranega sistema se obdelava transakcij odvija na več mestih, vsakdo lahko v okviru pravil omrežja vpisuje in dostopa do evidence (Anderson, 2019). Na sliki 1 so za različne vrste sistemov s črtami ponazorjene povezave, s točkami pa vozlišča oziroma naprave.

Slika 1: Centraliziran, decentraliziran in distribuiran sistem



Vir: Schneider (2019).

Različne vrste decentraliziranih sistemov so: (1) arhitekturni – določa ga število naprav v sistemu, potrebnih za njegovo delovanje, (2) politični – število skrbnikov in (3) racionalni – delovanje sistema le kot celote. DLT je politično decentraliziran, saj noben ne upravlja z njim, arhitekturno decentraliziran, nima centralne točke izpostavljene odpovedi, vendar je logično centraliziran, saj ima eno skupno dogovorjeno (konsenzno) stanje in sistem deluje kot en računalnik. Pozitivna lastnost DLT se nanaša na eno centralno bazo, kjer gre za koristno zvrst logične centralizacije. Z odpravo te oblike bi bilo omogočeno delovanje delov omrežja na geografskih območjih s slabo internetno povezavo (Schneider, 2019).

DLT uporablja konsenzni mehanizem, s katerim večina udeležencev omrežja sklene soglasje v zvezi z vrednostjo podatka ali predlagano transakcijo, ki se potem posodobi v evidenci. Pravila in postopki vzdržujejo usklajen nabor pristnih podatkov med udeleženimi vozlišči. Povezanim napravam omogoča skupno delovanje, četudi nekatere izmed njih odpovedo (Cline in drugi, 2016).

Pogosto prihaja do zamenjave pojmov tehnologije razpršene evidence s tehnologijo verige blokov, saj je bila slednja več let od njenega nastanka edina oblika DLT. Kasneje so se pojavile še novejše oblike DLT – Hashgraph, Directed Acyclic Graph (DAG), Holochain in Radix, opisane v nadaljevanju. Skupne lastnosti vseh omenjenih tehnologij so decentralizacija, konsenzni mehanizem, nespremenljivost podatkov, transparentnost in varnost. Ločnice pa so v tem, kako vozlišča konsenz dosežejo, in v strukturi beleženja podatkov. Med glavna konsenzna mehanizma za validiranje transakcij in dodajanje blokov k verigi pri tehnologiji verige blokov spadata dokaz o delu in dokaz o deležu (Cline in drugi, 2016). Struktura podatkov je v verigi blokov in po žetonih. Druge zvrsti imajo kot konsenzni mehanizem v rabi usmerjeni aciklični graf (angl. directed acyclic graph, DAG), ki je tudi struktura shranjevanja podatkov, ali toleranco napake; podatki se lahko tudi beležijo v obliki hashgrapha.

Verige blokov so načeloma javno dostopne, pri ostalih tehnologijah je dostop omejen. Struktura podatkov in konsenzni mehanizem v verigi blokov otežujeta razširljivost, pri ostalih, kot je DAG, je razširljivost večja in lahko obdelajo več transakcij na sekundo. Upravljanje je lahko decentralizirano s konsenzom, doseženim znotraj skupnosti, ali bolj centralizirano, kjer odločitve sprejemajo izbrane skupine udeležencev (Rauchs in drugi, 2018). Med tehnologije razpršene evidence torej spadajo:

- Veriga blokov (angl. blockchain): Začetki segajo v osemdeseta leta, ko je David Chaum leta 1983 uvedel kriptografijo za avtomatizacijo plačil in anonimnost. Leta 1991 so raziskovalci predstavili časovno označene dokumente, leta 2004 je Hal Finney razvil ponovljivi dokaz o delu, prelomnica pa je bila leta 2008, ko je Satoshi Nakamoto izdal belo knjigo o Bitcoinu, ki opisuje decentralizirano valuto in blockchain (Tripathi in drugi, 2017). Zapisi transakcij so shranjeni v evidenci kot veriga blokov. Izvedba transakcije vozlišča v omrežju se potrdi s ključem skupaj s predhodno transakcijo in se kot takšna shrani v evidenco. Na ta način postane nespremenljiva in neizbrisna. Udeleženci v omrežju lahko ustvarjajo kovance z različnimi konsenznimi mehanizmi. Bloke transakcij potrjujejo rudarji (subjekti, ki s posebno programsko opremo poskušajo pridobiti novo kriptovaluto), lahko jih preložijo na kasneje ali prekličejo. Omejitve ima pri razširljivosti v obdelavi transakcij (National Archives and Records Administration, 2019; v nadaljevanju NARA).
- Hashgraph je produkt korporacije Swirlds in vsebuje dva protokola. Obdela lahko na tisoče transakcij na sekundo. Prvi protokol skrbi za pretok informacij med vozlišči, drugi pa služi doseganju konsenza o vrstnem redu transakcij. Omrežje je zasebno in dostopno le pooblaščenim uporabnikom, njegova javna oblika se imenuje Hedera Hashgraph. Ta je počasnejša in ima konsenzni mehanizem podoben delegiranemu dokazu o deležu, kjer se z glasovanjem določi delegate za validiranje (Baird in drugi, 2019).
- Usmerjeni aciklični graf (angl. distributed acyclic graph, DAG) je podatkovna struktura grafa, ki poteka enosmerno. Transakcije so med seboj povezane zaporedno in aciklično, tako da se transakcija prek druge ne veže več sama nase. DAG je mreža povezanih

vozlišč, kjer se mora vsaka transakcija povezati z vsaj dvema predhodno potrjenima transakcijama, preden je lahko sama potrjena, za kar rudarjenje ni potrebno. Omogoča vzporedno potrjevanje več transakcij hkrati (Popov, 2018).

- Holochain je platforma za decentralizirane aplikacije (angl. decentralised applications, DApps) z vrstniškim omrežjem za dosego dogovora med udeleženci. Vsaka naprava v omrežju dobi svojo varno evidenco in lahko deluje samostojno in hkrati tudi sodeluje z vsemi drugimi napravami v omrežju. Strukturo podatkov ima v obliki razpršene heš (angl. hash) tabele, ki omogoča večjo razširljivost in učinkovitost v primerjavi z verigo blokov (Harris-Braun in drugi, 2018).
- Radix/Cerberus (nadgradnja Tempa) je javna decentralizirana evidenca, ki temelji na konsenznem protokolu logičnega števca. Sledi načelu linearne razširljivosti, čemur služijo uporabna struktura, razdrobljenost podatkov in omogočanje popolne decentralizacije z uporabo logičnega števca; konsenz vpelje le pri nasprotujočih si dogodkih (Casar in drugi, 2020).

2.3 Tehnične lastnosti tehnologije razpršene evidence

Decentraliziranost pomeni odpravo posrednikov, večjo učinkovitost, varnost ter izboljšanje avtomatizacije. Finančna industrija šteje sledljivost in poenostavljeno usklajevanje med ključne prednosti DLT (Kuhn in drugi, 2019). Zgodnja faza njenega razvoja se odraža v njeni večji izpostavljenosti in postopnosti pri sprejemanju. Glavna težava je v razširljivosti, izboljšave so potrebne tudi v interoperabilnosti.

DLT omogoča medvrstniški prenos digitalne vrednosti v obliki žetonov med dvema stranema in decentralizirano hranjenje evidence z odpravo potrebe po posredniku ali centralnem organu, zadolženem za nadzor nad evidenco. Transakcije posledično potekajo pri nižjih stroških, hitreje in so bolj razširljive. Vsi udeleženci omrežja imajo šifrirano kopijo celotne razpršene evidence. Z dosegom konsenza so spremembe vnesene in omrežje je posodobljeno v realnem času, kar omejuje prevare in odstrani stroške usklajevanj (Kuhn in drugi, 2019).

DLT omogoča večje hitrosti in učinkovitosti z zmanjšanjem zamud pri obdelavi pri plačilih, kliringih in poravnavah z umikom posrednikov in avtomatiziranjem procesov. Ročno usklajevanje ni potrebno, zato lahko DLT prispeva k bistveno nižjim stroškom, saj DLT sistem vsebuje distribuirane dejanske podatke in zato ni potrebe po usklajevanju ene baze podatkov z bazo podatkov nasprotne strani. Dodatni razlogi za nižje stroške so lahko cenejše vzdrževanje infrastrukture DLT, kot tudi zmanjšanje zaostanka plačil in omejevanje prevar. Po ocenah banke Santander v letu 2015 bi DLT finančni industriji prihranil 15–20 milijard dolarjev letno (IBRD, 2017).

Omogoča bolj obstojen sistem kot običajne centralizirane baze podatkov in ponuja boljšo zaščito pred različnimi vrstami spletnih napadov zaradi svoje razpršene narave, ki odstrani

enotno točko napada. Torej prispeva k večji varnosti na internetu. DLT je še vedno v zgodnji fazi razvoja in še vedno so prisotni resni pomisleki glede njegove robustnosti in obstojnosti. Še posebej za prenose velikih vrednosti, razpoložljivosti primerljive strojne opreme in programskih aplikacij ter zadostnega števila usposobljenih strokovnjakov. Veliki dolgoletni igralci v informacijski tehnologiji (v nadaljevanju IT), kot sta IBM in Microsoft, kot tudi v finančnem sektorju, Visa in Mastercard, so pričeli z razvijanjem produktov in storitev DLT, ki bi sčasoma uživali enako raven zaupanja, kot jo dandanes ponujajo običajni sistemi IT.

Različice odprtih razpršenih evidenc se soočajo s težavami v razširljivosti verige blokov, natančneje v hitrosti potrjevanj transakcij. Obstoječe prosto dostopne verige blokov imajo omejeno hitrost transakcij. Na primer Bitcoin lahko obdela le 4–7 transakcij na sekundo zaradi omejitve pri velikosti bloka na 1 megabajt (MB). Čeprav bi se dalo blok povečati, potrebuje več časa za napredovanje po omrežju in poveča tveganje nastajanja vilic oziroma oblikovanja prevladujočih alternativ različic verig blokov. To težavo bi se dalo sčasoma rešiti in najbolj izstopa prav v sistemu Bitcoin. Zaprti sistemi, kot je Ethereum, naj bi imeli večjo prepustnost. Takšni sistemi imajo večjo razširljivost in lahko obdelajo večje količine transakcij, kar dosežejo na račun bolj centralizirane, manj transparentne platforme, ki odpravi veliko prednosti razpršene odprte narave javnih sistemov DLT, zato jim primanjkuje globalnega dosega.

Različni sistemi DLT morajo biti interoperabilni z drugimi evidencami in integrirani v obstoječe sisteme za umestitev v finančni sistem. Integracija DLT v finančno infrastrukturo, kot so plačilni sistemi ali sistemi poravnav, zahteva koordinacijo in sodelovanje med različnimi industrijami in predstavlja velike stroške. Platfroma Corda, produkt konzorcija R3, in Fabric, rezultat projekta Hyperledger, sta primera razvoja DLT za finančni sektor.

Vsaka programska oprema vsebuje tehnične pomanjkljivosti. Statistično gledano, obstaja 15–50 skladenjskih napak, t. i. hroščev, na 1.000 vrstic kode. Primer napada leta 2016 na decentralizirano avtonomno organizacijo na Ethereumu je pokazal, da so lahko pomanjkljivosti pametnih pogodb izrabljene. Spletna varnost temelji na razpršeni naravi evidence in na domnevi, da napadalcem ne more uspeti spremeniti osrednjih algoritmov DLT-omrežja. Eden od možnih napadov na odprto razpršeno evidenco s konsenznim mehanizmom je 51 % napad, kjer zlonamerni akter prevzame 51 % omrežne računalniške moči in lahko uspešno vpliva na izid konsenza. Zanesljivost predpostavke, da noben subjekt nikdar ne more upravljati z več kot polovico računalniške moči vseh strežnikov na določeni verigi blokov, je odvisna od robustnosti omrežja. Do sedaj še ni prišlo do neposrednega vdora v razpršeno evidenco (IBRD, 2017).

2.4 Regulativni izzivi tehnologije razpršene evidence

Pametne pogodbe so povezane s samodejnim usklajevanjem podatkov in izvršitvijo dogovorov. Nespremenljivost, čeprav dobra za revizijo, povzroča težave pri reklamacijah plačil. Odprto vprašanje je še pri dokončnosti poravnave transakcije. Izziv predstavljajo tudi

razlike v pravosodjih pri mednarodnih plačilih. Model vodenja otežuje nadzor s strani regulatorjev. Ugotavljanje identitete pa je tudi ključna komponenta pri zagotavljanju skladnosti z zakonodajo. Pomanjkljivost se pojavi pri pomanjkanju zasebnosti pred drugimi udeleženci.

DLT omogoča programiranje avtomatskega izvrševanja dogovorov na podlagi predhodno sprejetih kriterijev. Takšna oblika programa se imenuje pametna pogodba, npr. plačilo računa ob prejemu naročene pošiljke, delniški certifikati, ki sami izplačujejo dividende, ali pa plačilo za opravljeno delo. Tudi centralizirani sistemi omogočajo pametne pogodbe, le da je potrebno usklajevanje obeh strani, kar traja bistveno dlje. Z DLT sta obe strani z opravljeno transakcijo soglasni hkrati, saj imata obe isto kopijo evidence.

DLT omogoča nespremenljivo in preverljivo revizijsko sled transakcij digitalnih ali fizičnih sredstev. Čeprav je v večini primerov nespremenljivost zaželena, lahko povzroči težave pri povračilih, zato pa je možna povratna transakcija, ki je izvedena ločena transakcija za vrnitev pravic digitalnega sredstva prvotnemu pošiljatelju za reklamacijo kot pri delovanju zahtevkov pri sistemih plačilnih kartic. Originalna evidenca v tem primeru še vedno ostane (IBRD, 2017). To nastane kot posledica povezane verige kriptografskih zapisov, kajti sprememba enega zapisa povzroči neveljavnost algoritma kriptografske funkcije razpršitve (ponekod omenjana bolj pravilno kot funkcija zgostitve) oz. heša (angl. hash) nadaljnjih zapisov. Spremembe bi torej zahtevale ponovno programiranje celotne verige (Kuhn in drugi, 2019).

Odsotnost centralizirane infrastrukture in centralnega organa vodi v pomisleke o učinkovitem upravljanju celotne infrastrukture. Ustvarjanje vilic pri Ethereumu in predlogi za spremembe protokola Bitcoin pričajo o tem, kako težko je doseči odločitev o kritičnih spremembah na infrastrukturi DLT. Regulatorji v finančnem sektorju vzpostavljajo učinkovite sisteme upravljanja za centralno infrastrukturo in regulirane subjekte. Pri odprtem DLT je pogosto nejasno, za koga veljajo dogovori o upravljanju, v nasprotju z zaprtim tipom DLT, kjer ima administrator opredeljene naloge pri upravljanju. Skladnost z zakonodajo in industrijski standardi morajo biti še vpeljani. Nekateri regulatorji po svetu aktivno proučujejo tehnologijo, toda zakonodajni okviri, namenjeni DLT, so še v nastajanju.

V plačilnih in poravnalnih sistemih v okolju razpršene evidence so določeni pomisleki povezani z dokončnostjo transakcije. V plačilnem sistemu na DLT je konsenzni mehanizem v rabi za validacijo transakcij in zagotavljanje, da so dodane v evidenco na varen in nespremenljiv način, le kot take so dokončne, kar pa traja predolgo. Neskladja so tudi med zakonodajami v čezmejnih sistemih razpršene evidence v zvezi s podatki in transakcijami. Nadzorovanje odprtih razpršenih evidenc je posebej zahtevno, saj nimajo nadzora s strani pravnega subjekta, v nasprotju z nadzorovanjem zaprtih zasebnih evidenc, kjer po navadi obstaja administrator ali lastnik sistema, ki je predmet predpisov.

Za vpeljavo v finančni sistem morajo sistemi DLT izpolnjevati zahtevi poznavanja svoje stranke (angl. Know Your Client, KYC) in skrbnosti pri ugotavljanju (angl. Customer Due Diligence, CDD) znotraj predpisov proti pranju denarja (angl. Anti-Money Laundering, AML) oz. boja proti financiranju terorizma (angl. Combating the Financing of Terrorism, CFT). Večina odprtih DLT prikrije identiteto udeležencev omrežja s šifriranjem z uporabo javnega ključa, kar je na meji zakonitega in omogoča transakcije z nepreverjenimi osebami. Veliko menjalnic, kot npr. Coinbase, ponuja hitrejše preverjanje in krajši čas transakcij, če uporabniki potrdijo več osebnih podatkov, da izpolnijo zahteve KYC. Zaprti DLT rešuje to težavo, ker je dostop do omrežja nadzorovan in se po navadi zahteva preveritev identitete udeleženca (IBRD, 2017).

Zakonodaja ne dopušča psevdoanonimnosti pred določenimi institucijami. Pri kriptovalutah verige blokov dopuščajo udeležbo le z identifikatorji. Verige blokov z omejenim dostopom lahko izbirajo način identifikacije (Kuhn in drugi, 2019). V odprtih evidencah so vse transakcije na voljo in vidne vsem članom omrežja, čeprav so lahko šifrirane in je identiteta uporabnika prikrita, ni zagotovljena zasebnost. V nekaterih okoliščinah se lahko o identiteti udeleženca sklepa na podlagi vzorcev transakcij ali po drugih pokazateljih. Zaprte razpršene evidence se soočajo z isto težavo. To je eden od ključnih pomislekov pri vnašanju DLT v infrastrukturo finančnih trgov, ki ga naslavljata Corda in Fabric (IBRD, 2017).

3 PLAČILNI SISTEM OD KLIRINGA DO PORAVNAVE

Denar in plačilni sistemi so notranje povezani, razvijali so se skupaj in ta povezava je razvidna iz vloge CB, ki zagotavljajo tako stabilnost valute kot plačilnih sistemov za nemoteno delovanje gospodarstva.

Zgodovinsko je do izmenjave prišlo s predmeti z notranjo vrednostjo, kot so npr. zlati kovanci. V 16. stoletju so hranilnice zlata imele knjige bančnih vlog svojih strank, kar je omogočalo plačila z vnašanjem sprememb v njih namesto fizične izmenjave sredstev. Sistem je deloval le za stranke iste banke. Z večanjem potrebe po medbančnih plačilih se je pojavila centralna klirinška banka, kjer so lahko vse banke članice imele odprte račune in s tem poenostavile medbančna plačila.

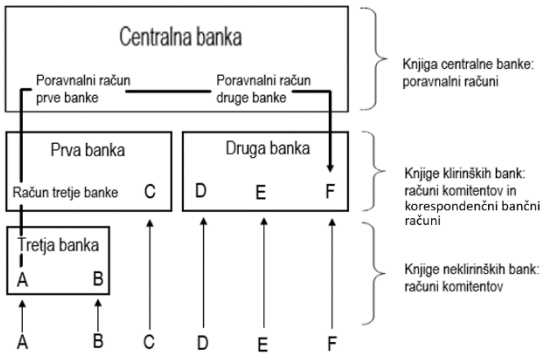
V sodobnih časih se plačila izvedejo tako, da se zmanjša stanje na računu plačnika in poveča stanje na prejemnikovem računu za isti znesek. Postopek je po stoletjih ostal enak, razlika je le v tehnologiji beleženja salda in njegovega prenosa med bankama. Tehnološki razvoj zadnjih petdeset let je vplival na plačilni sistem na dva načina. Zapisi in knjige so se spremenili iz fizične v elektronsko obliko, kar je povečalo hitrost transakcij in zmanjšalo operativna tveganja. Pojav inovativnih tehnologij dopušča nove plačilne metode, kot so npr. mobilna plačila.

V središču centraliziranega plačilnega sistema je evidenca s poravnavami pri klirinškem centralnem organu, vlogo po navadi prevzame centralna banka. Poslovna finančna institucija

ima bilanco stanja zabeleženo v knjigi CB, pa tudi odraženo v lastni knjigi. Posamezni komitenti, podružnice ali celo manjše banke potem hranijo bilance stanj pri tej instituciji, kar se spet odraža v njihovi lastni knjigi.

Slika 2 ponazarja plačilo z računa A na račun F prek številnih posrednikov, ki preverijo vsak korak v postopku. Udeleženci imajo vpogled samo v svoja sredstva in obveznosti. Puščice navzgor ponazarjajo depozite, puščica navzdol pa plačila (Ali in drugi, 2014).

Slika 2: Potek plačil v centraliziranem večstopenjskem sistemu



Vir: prirejeno po Ali in drugi (2014).

3.1 Plačilni sistem na razpršeni evidenci

Plačilo se prične s komunikacijo plačilnega orodja, npr. kreditne kartice, s sprejemno napravo, kot je čitalcem kartic. Oddan je nalog za plačilo in po preveritvi, ali ima plačnik dovolj razpoložljivih sredstev, se mu odobri transakcija. Kliring je pošiljanje informacije o finančni transakciji banki prejemnika plačila in plačnika za določitev plačilnega zneska. Poravnava je izpolnitev obveznosti med plačnikom in prejemnikom plačila in zaključek transakcije.

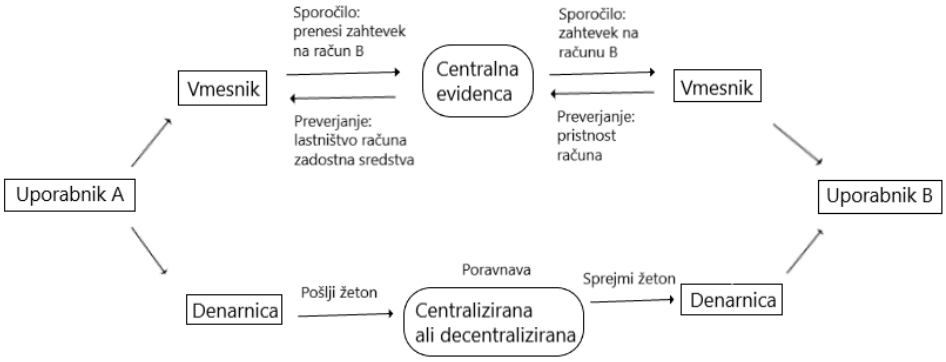
Pri tehnologiji razpršene evidence plačnik izkazuje lastništvo nad sredstvi z digitalnim podpisom. Potrjevanje pri DLT zajema kliring in poravnavo obenem, konsenz o tem, ali je transakcija potrjena, je dosežen med vozlišči omrežja. Tu ni razlike med pošiljanjem informacij o finančni transakciji in dokončni izmenjavi denarja. Plačila na DLT niso izpostavljena tveganju, da ne bi bila poravnana po končani izmenjavi informacij o plačilu in število udeležencev v plačilnem postopku je manjše (Wadsworth, 2018). Na sliki 3 je prikazan potek plačil v običajnem plačilnem sistemu v primerjavi s sistemom digitalnih žetonov.

Razpršene javne evidence temeljijo na teoriji iger, kjer optimalne odločitve izhajajo iz možnih odločitev nasprotnikov, in konceptu verjetnosti za določitev zaporedja transakcij. Bitcoin je nedeterminističen, potrditve dokončnosti transakcij so posledica verjetnosti. V

takšnem sistemu je težko slediti računovodskim načelom in izpolniti zahteve revizije. To ponuja priložnost, da se ustvari nov trg zavarovanja tveganj (Bott in Milkau, 2016).

Obračun in poravnava transakcije obsegata omrežje udeležencev, sredstvo ali skupino sredstev za prenos med udeleženci ter postopek prenosa, ki opredeljuje korake in obveznosti, povezane s transakcijo. Neposredni udeleženci so finančne institucije, kot so banke in posredniki, posredni udeleženci pa so končni uporabniki, kot so gospodinjstva in podjetja. Sredstvo je lahko katerikoli finančni instrument, kot je monetarni instrument, vrednostni papir, blago ali izvedeni finančni instrument.

Slika 3: Potek plačil z žetonom ali na računu



Vir: prirejeno po Mancini-Griffoli in drugi (2018).

Prenos sredstev poteka v štirih fazah: predložitev, validacija ali preverjanje veljavnosti, preverjanje izpolnjevanja pogojev in poravnava. Pošiljatelj predloži plačilno sporočilo plačilnemu sistemu, kjer poteka postopek validacije, preden je potrjeno, zajema lahko varnostne ukrepe, kot so verifikacija ali preverjanje pristnosti identitete pošiljatelja in celovitosti sporočila, da ni prišlo do poseganja vanj. Če sistem potrdi plačilo kot veljavno, preveri, ali je zadoščeno pogojem za poravnavo, kot je razpoložljivost zadostnih sredstev ali odobrenega kredita za poravnavo. Dokončnost poravnave, kar pomeni brezpogojno poravnanost in nepovratnost, je ponekod dosežena šele po nakazilu na račun prejemnika.

Kriptografija pri DLT se uporablja za dokazovanje identitete in šifriranje podatkov. Za potrditev prenosa sredstev se uporabi javni ključ. Udeleženec lahko ustvari digitalni podpis z zaupno poverilnico oz. zasebnim ključem. Za potrditev pripadnosti obravnavanega sredstva udeležencu, ki je transakcijo sprožil, lahko drugi upravičeni udeleženci v omrežju potrdijo verodostojnost vpisa v evidenco, tako da jo dešifrirajo z matematičnim algoritmom in z javno dostopnim ključem lastnika sredstev.

Poenostavljeno povedano, javni ključ ima podobno vlogo kot obesna ključavnica, saj je namenjen zaklepanju oziroma šifriranju. Zasebni ključ je namenjen tej isti ključavnici za njeno odklepanje oziroma dešifriranje. Elektronski podpis ustvari pošiljatelj s svojim zasebnim ključem in prejemnik lahko preveri pošiljateljev podpis z javnim ključem.

Kriptografija se lahko uporabi za šifriranje informacij transakcije v evidenci, tako da lahko le določeni udeleženci razkrijejo podrobnosti vsake transakcije. Šifrirani razpršeni zapisi v evidenci zagotovijo tudi večjo zasebnost, prav tako pomagajo pri delovanju konsenznega mehanizma (Mills in drugi, 2016).

Atomskost transakcij je mehanizem poravnave, ki temelji na načelu dostave proti plačilu, povezuje prenos dveh sredstev na tak način, da zagotovi prenos enega sredstva samo takrat, ko se opravi prenos drugega sredstva. Izid poravnave je, da si obe strani uspešno izmenjata sredstvi ali pa se transakcija ne zgodi. V informatiki se takšno vzajemno pogojenost omenja kot atomskost transakcije (European Central Bank in Bank of Japan, 2018; v nadaljevanju ECB in BoJ).

Mehanizem rešuje različna tveganja plačilnih sistemov, eno od njih je kreditno tveganje, ki nastane, ko postane banka plačnica insolventna in dolguje veliko količino denarja drugim članicam sistema. Drugo je likvidnostno tveganje, ko banka članica, sicer solventna, nima sredstev za poravnavo plačila v določenem časovnem roku. Tretje je operativno tveganje, pri katerem banka, vpletena v plačilno transakcijo, preneha delovati, začasno ali stalno, zaradi nekega dogodka, kot je npr. napaka v informacijski tehnologiji (IT) (Ali in drugi, 2014).

DLT omogoča večjo preglednost nad lastništvom, hkrati pa varen in hiter prenos pri nižjih stroških in v odsotnosti posrednika. Standardizacija bi pripomogla k njegovi razširjenosti. Z vidika varnosti in zaščite je v celoti šifriran in ne vključuje centralnega organa ali zaupnega zunanjega upravitelja. Hitrost poravnave je skoraj takojšnja. Z P2P-poravnavo doseže stroškovno učinkovitost, saj naredi posrednike odvečne. Transakcija postane dokončna z nespremenljivim zapisom.

Izzivi sistema so operativni, tehnološki, pravni in drugi. Razširjenost je upočasnjena zaradi pomanjkanja standardizacije in interoperabilnosti v namenih uporabe, kot tudi v različnih zakonodajah. Težave v varnosti povzročata pomanjkanje zasebnosti oz. prevelika transparentnost. Dokončnost ni popolnoma v skladu z zahtevami predpisov, in tudi to, kako se spoprijeti z reklamacijami, še ni jasno. Morebitna rešitev bi bila, da bi pooblaščena vozlišča izvajala nadzor nad sistemom (Hodrick, 2018).

3.2 Delovanje plačilnega sistema na verigi blokov z rudarjenjem

Pri plačevanju s kritovalutami, kot je bitcoin, imajo ključno vlogo rudarji. Konkurenca jih vodi v nakup vedno bolj zmogljive strojne opreme v zameno za plačilo v digitalni valuti, od navadnih centralno procesnih enot (angl. Central Processing Unit, CPU) prek grafičnih procesorjev (angl. Graphics Processing Unit, GPU) do specializiranih integriranih vezij (angl. Application-Specific Integrated Circuit, ASIC). Že v letu 2014 so ocene porabljene električne energije znašale toliko kot letna poraba električne energije za državo Irsko. Proizvodni stroški Bitcoin transakcije znesejo med 5 in 10 dolarjev, za primerjavo je pri

transakcijah v enotnem območju plačil v evrih (angl. Single Euro Payments Area – SEPA) v Evropi strošek manj kot 1 cent in manj kot 1 dolar pri mednarodnih transakcijah Združenja za svetovno medbančno finančno telekomunikacijo (angl. Society for Worldwide Interbank Financial Telecommunication – SWIFT).

Postopek potrjevanja v Bitcoinu poteka z javljanjem transakcije omrežju, primerljivo s hitrostjo pošiljanja elektronske pošte, ustvarjanjem novih blokov v načrtovanih 10 minutah, čakanjem v vrsti za obdelavo na približno 20.000 transakcij oz. 130 minut, zagotovilom o nakazilu po šestih blokih oz. 60 minutah, in sicer s knjigovodsko dokončnostjo transakcije. Plačila s kreditnimi karticami so hitrejša in njihova potrditev poteka v realnem času. Sistemi takojšnjih plačil, kot sta npr. SEPA Instant Credit Transfer in TIPS (angl. Target Instant Payment Settlement), lahko transakcijo izvedejo v manj kot desetih sekundah (Bott in Milkau, 2016). Na verigi blokov so tekoče transakcije poslane v omrežje, združene skupaj v blok in posredovane v evidenco za potrjevanje. Vozlišča tretjih oseb, t. i. rudarjev, se odločajo, katero transakcijo potrditi glede na zaslužek za opravljeno storitev, poleg tega pa dobijo tudi novo ustvarjeno valuto.

Za potrditev transakcij mora rudar priskrbeti dokaz o delu oz. najden heš (angl. hash) ali razpršitev, ki zastopa vse podrobnosti o bloku in vsake posamezne transakcije v njem. Sestavljen je iz niza črk in številk. Če se podrobnosti transakcije spremenijo, se heš tudi spremeni, zato se kriptografija s heši uporablja za potrjevanje verodostojnosti informacij. Heš se poišče z reševanjem šifriranega matematičnega problema z izključno uporabo procesne moči računalnikov. Potrebnih je sistemsko zastavljenih 10 minut za rešitev problema, kar se odraža tudi v stroških rudarjenja. Omrežje je seznanjeno s hešem dokaza o delu in če vozlišča soglašajo k dodajanju bloka k verigi, dosežejo konsenz. Bloki so dodani k verigi samo v primeru, ko večina omrežja prenese kopijo nove verige blokov (Wadsworth, 2018).

3.3 Pomen preverjanja identitete udeležencev v plačilnih sistemih

Pri prenosu sredstev v gotovinski obliki je pomembno, da se da prepričati o avtentičnosti sredstva plačila, v digitalni obliki pa je v ospredju preverjanje identitete plačnika in prejemnika plačila. Na razpršeni evidenci lahko domnevno zlonamerni akter, z večjim številom psevdonimnih identitet, prevzame nadzor nad večjim delom omrežja, kar je poimenovano 51 % napad, česar tudi zasilni sistemi (angl. redundancy) ne morejo preprečiti. Eden od načinov reševanja te težave je ustanovitev zaupne agencije za overjanje identitet. Pojav nekaj glavnih netransparentnih skupnosti rudarjev (angl. mining pools) je spremenil ekosistem Bitcoin v *de facto* centralizirano vodenega. Tudi programsko kodo za Bitcoin razvijajo določene skupine, čeprav je formalno odprtega vira (Bott in Milkau, 2016).

Posredniki so zadolženi tudi za nadzor finančnih transakcij na internetu, npr. preverjanje zadostnega stanja na računu pred izvedbo nakupa. Z zmanjševanjem asimetrije informacij oziroma izkoriščanja neseznanjenosti ene strani in tveganja moralnega hazarda oziroma bolj

tveganega ravnanja na račun druge stranke povečujejo učinkovitost trga. Uveljavljajo pogodbena določila in pridobivajo informacije o strankah, tudi o njihovi zanesljivosti. Z večanjem trga postanejo storitve preverjanja bolj pomembne, saj se udeležene strani ne poznajo, zato se zanašajo na posrednike za zagotavljanje varnosti transakcij in uveljavljanje pogodbenih določil.

Posredniki zaračunavajo pristojbine za kupca in prodajalca, saj sama ne moreta učinkovito preveriti vseh ključnih informacij, povezanih s transakcijo. S posredniki pa nastane tveganje zasebnosti zaradi izrabljanja osebnih informacij, saj dostopajo do podatkov transakcij, in tveganje cenzure oziroma izločanja transakcij, saj odločajo o izvedbi transakcij. Z vedno večjim deležem digitalizacije ekonomske in družbene aktivnosti je zaščita podatkov zahtevna in razkrivanje informacij vse bolj pogosto. Primeri iz preteklosti so kraje številk socialnega zavarovanja, kot je bil vdor v bonitetno agencijo Equifax v letu 2017, in podatkov s kreditnih kartic, kot je bilo kršenje pravil pri podatkih trgovca oblačil Target v letu 2013, ali predaja podatkov o strankah oglaševalcem.

Tehnologija verige blokov prepreči razkrivanje informacij tretji strani, udeležencem trga omogoča preverjanje podrobnosti transakcije in uveljavljanje pogodb. Omogoča preverjanje informacij o transakciji z ohranjanjem zasebnosti. Dopušča preveritev verodostojnosti zadevnih informacij, npr. kreditne sposobnosti, ne pa celotnega vpogleda v informacije, npr. zapisov preteklih transakcij (Catalini in Gans, 2019).

Sistem pa ima tudi svoje pomanjkljivosti, saj sistem upravljanja identitet temelji na ključih, ki se jih ne da obnoviti. Ključa se ne da povezati z gotovostjo z identiteto, saj ni tretje strani, ki bi ga certificirala. Če se ključ izgubi, ne obstaja odgovorni subjekt zanj, tako ostanejo sredstva stalno zaklenjena. Preklicati ga tudi ne more nihče v primeru kraje ali izpostavljenosti. Tako ne obstaja način, da bi se javilo omrežju, da določen ključ ni več za rabo in se ga ne sme sprejemati (Le Borne in drugi, 2016).

Digitalizacija je znižala stroške preverjanja transakcij na neznatne. Preverjanje opravljajo avtomatizirani procesi in digitalne metode avtentikacije, DLT torej zagotavlja preverjanje brez posrednikov. Vsakršno lastnost transakcije oziroma informacijo o vpletenih subjektih in predmetu izmenjave na razpršeni evidenci se vedno lahko preveri oz. revidira z nizkimi stroški, v realnem času in s strani kateregakoli udeleženca na trgu.

Zaupanje v posrednika je nadomeščeno z zaupanjem v izvorno kodo in pravila konsenza. Ta pravila določajo, kako razpršeno omrežje doseže dogovor o pravem stanju deljenih podatkov, ki jih mora vzdrževati za namene dobro delujočega tržišča. Razpršeni podatki predstavljajo pretekle transakcije in neporavnana stanja.

Pametne pogodbe zajemajo pravila in podatke za izvedbo določenih operacij (zagon aplikacij, preveritev uveljavljenosti pogodbenega dogovora). Institucije, vpletene v transakcijo, lahko vnaprej soglašajo o pravilih poravnave in uskladitvi izmenjave, tako kot tudi o postopku reševanja sporov in izpeljavi revizij. Zaupni neodvisni oraklji (sistemi za

nudenje zunanjih informacij) zagotavljajo odzivanje finančnih pogodb na nove informacije iz tržnega okolja. Tako se lahko vršijo izvedeni finančni instrumenti, vezani na zunanje podatke. Pametne pogodbe lahko zberejo informacije iz več virov, da ocenijo, ali mora biti plačilo izvedeno. Tudi pri avtomatiziranem preverjanju posrednikom ostanejo še naloge zagotavljanja skladnosti s predpisi in tržne varnosti, ravnanja v primeru povračila stroškov in potrjevanja informacij, ki zahtevajo delovno intenzivno preverjanje.

Javljalniki interneta stvari so ključnega pomena pri razširitvi nabora pogodb, ki so lahko avtomatizirane na verigi blokov, ker se jih lahko uporabi pri odjemu informacij iz stvarnega okolja (npr. prek senzorjev, GPS-naprav) in nadomesti delovno intenzivna preverjanja s stroškovno učinkovito strojno opremo (Catalini in Gans, 2019).

3.4 Čezmejni plačilni sistem

Tehnologija razpršene evidence lahko prispeva k hitrejšim čezmejnim bančnim transakcijam, večji konkurenci ponudnikov plačilnih storitev, zmanjšanju kreditnega in likvidnostnega tveganja. Po točkah so navedene posledice uvedbe DLT pri čezmejnih plačilih (van Ginneken, 2019):

1. Hitrejše čezmejne medbančne transakcije pomenijo nižje oportunitetne stroške, ki izhajajo iz dostopanja do denarja.
2. Manjše vstopne ovire zaradi prehoda iz večstopenjskega v razpršen bančni sistem vodijo v povečano konkurenco ponudnikov plačilnih storitev, kar se odraža v nižjih stroških transakcij.
3. Zamenjava korespondenčnih bank (finančnih institucij, ki opravljajo bančne storitve za drugo banko, pogosto za mednarodne transakcije) v plačilnem procesu s transparentno platformo pomeni tudi boljše storitve za stranke.
4. Kreditno tveganje (tveganje nevračila denarja) med banko plačnico in prejemnico na platformi se zmanjša z medvrstniškim plačilnim mehanizmom zaradi atomske poravnave. Na ta način ni potrebnega več toliko denarja, namenjenega kritju pred tveganjem neporavnave.
5. Zadržana likvidnost na računih nostro, kjer banka hrani sredstva v tuji valuti pri tuji korespondenčni banki, se lažje sprosti, zato je likvidnostno tveganje manjše.
6. Izboljšava storitev in povečanje dobičkov zaradi takojšnje in stalne razpoložljivosti sta privlačni za korporativne stranke.
7. Uvedba CBDC v mednarodna plačila s strani poslovne banke bi naredila trg nekonkurenčen s prednostjo prvega na trgu in ekonomijami obsega. Enaki pogoji za vse udeležence so mogoči z izdajo denarja s strani CB.
8. Strošek prehoda in upravljanja platforme je treba primerjati s stroški sistema bruto poravnave v realnem času. V prehodnem času je treba vzdrževati obe infrastrukturi hkrati, zato so stroški prehoda visoki.

9. Banke bi s storitvami korespondenčnega bančništva zaslužile manj, slabša povezanost med njimi bi se odrazila v višjih stroških. Po drugi strani bi tehnološke inovacije in predpisi krepili konkurenco med njimi in vplivali na nižje stroške njihovih strank.

Poslovne banke lahko hranijo likvidna sredstva za omogočanje plačil v denarnici evidence zunaj delovnega časa sistema bruto poravnave v realnem času (angl. Real-Time Gross Settlement, v nadaljevanju RTGS). Pravna tveganja so večja zaradi razlike v zakonodajah in morebitnega samostojnega organa med udeleženimi centralnimi bankami. Zajemanje poslovnih bank, prvotno delujočih pod drugo zakonodajo, in korporativnih strank razširi naloge CB, saj morajo preveriti svoje nove stranke (angl. Know Your Client, KYC), kar lahko povzroči težave pri skladnosti in pravna tveganja. Nižja dobičkonosnost korespondenčnega bančništva lahko banke prisili v bolj tvegane izdaje posojil, da nadomestijo izgubljene prihodke, kar lahko vodi do tveganja v finančni stabilnosti (van Ginneken, 2019).

Pričakovana rast čezmejnih plačil v obdobju od 2016 do 2022 je bila z 22 bilijonov ameriških dolarjev (v nadaljevanju USD) na 30 bilijonov USD kar znese 5,5 % letnega prirasta v malo- in veleprodaji skupaj. V upadu je število korespondenčnih bank, in sicer od 2011 do sredine 2017 je bil upad 8 %. Današnja čezmejna plačila so draga, trajajo več dni in jim primanjkuje transparentnosti v stroških in času dostave. To je posledica zapletenosti čezmejnih plačil in poravnav, ki vključujejo vpletenost več subjektov v izvedbo transakcije, obsežne predpise (proti pranju denarja, proti financiranju terorizma, v poznavanju svoje stranke), kot tudi različne tehnične in operativne standarde, zastarele sisteme in infrastrukture. Težave v razvoju varnega, učinkovitega in vključujočega mednarodnega sistema še dodatno poslabšajo različne zakonodaje posameznih pravosodij.

K zmanjšanju stroška plačila prispeva zmožnost samodejne obdelave, kar je težko zagotoviti prek več subjektov in lokacij. Če ponudnik storitev pošiljatelja ni prisoten na lokaciji prejemnika in zato ne more sprejeti sredstev tam, se mora zanesti na drugo finančno institucijo, da izpelje transakcijo namesto njega. Temelj čezmejnih plačil in poravnav je že stoletja povsod model korespondenčnega bančništva. Še vedno je edino takšen model prisoten v vsaki državi oziroma za vsako valuto in ga lahko uporabi vsak imetnik bančnega računa. Toda število bank, ki ponujajo to storitev, je v upadanju (Bank of Canada in drugi, 2018; v nadaljevanju BoC).

Skupna raziskava, ki so jo objavile CB Kanade, CB Združenega kraljestva in CB Singapurja se osredotoča na potencial CBDC v izboljšanju kreditnega tveganja nasprotne strani pri medbančnih čezmejnih plačilih in poravnavah. Veleprodajni CBDC je omejen le na finančne institucije in trge. Sodobni model čezmejnih plačil za poravnavo obveznosti poslovnih bank temelji na sistemu RTGS. Pri nakazilih med subjekti različnih pravosodij prihaja do časovnih zamikov, zato so nasprotne strani izpostavljene kreditnemu in poravnalnemu tveganju svojih korespondentov.

Z raziskavo je bilo ugotovljeno, da veleprodajni CBDC znotraj enega pravosodnega sistema nima bistvenih prednosti v primerjavi z obstoječim. Čezmejni CBDC bistveno izboljša kreditno, plačilno in poravnalno tveganje nasprotne strani. Prednosti vključujejo tudi 24-urno dostopnost, anonimnost in odpravljanje kreditnega tveganja nasprotne strani za vse udeležence. Veleprodajni CBDC vpliva tudi na prihodnjo vlogo CB in njen nadzor nad sistemom (Ward in Rochemont, 2019).

3.5 Plačilni sistem kot decentralizirana avtonomna organizacija

3.5.1 Povezanost plačilnega sistema z ekonomsko stabilnostjo

Glavna vloga CB je izdajanje in upravljanje s ponudbo valute v gospodarstvu. Monetarni organ uravnava oskrbo z in umik denarja za vzdrževanje splošne makroekonomske stabilnosti oziroma nizke inflacije in polne zaposlenosti. Uravnavanje ponudbe denarja je doseženo z naborom političnih orodij za posredno ali neposredno vplivanje na ponudbo ali povpraševanje po valuti.

Neposredni ukrepi zajemajo operacije na odprtem trgu, kjer banka ustvarja denar s kupovanjem državnih obveznic z uporabo novo izdanega denarja. Tudi nekonvencionalna monetarna orodja lahko vnesejo likvidnost na trge, kot je kvantitativno rahljanje oziroma kupovanje tveganih vrednostnih papirjev (npr. zavarovanimi s hipoteko) na odprtem trgu.

Posredni ukrepi za nadzor nad ponudbo denarja zajemajo mehanizme za določanje obrestne mere kot orodja za dosego ekonomskih ciljev. Sodobna gospodarstva so znotraj povezana z obrestno mero, ki vpliva na vse, od porabe potrošnikov in korporativnih investicij do vladnega dolga in neto izvoza. Ključna obrestna mera, ki jo CB določi, služi kot temelj za vse druge obrestne mere posojil in tako učinkovito določa strošek izposojanja ter vrednost denarja. Poenostavljeno zapisano, obrestna mera določa ceno denarja.

Z višanjem obrestne mere se zavira gospodarsko rast. Dražja posojila vplivajo na zmanjšano potrošnjo, zmanjša se tudi kreditna sposobnost. Donosnost projektov vpliva na izdajo korporativnih obveznic, saj korporacije z njimi odplačujejo obresti. Obrestne mere vplivajo na vse finančne trge: na lastniški in dolžniški kapital, izvedene finančne instrumente, trg deviz in trg blaga.

Pomembna naloga CB je skrb za ekonomsko stabilnost z nadzorom plačilnega sistema, ki je pomemben del infrastrukture sodobnih gospodarstev, dovoljuje brezhibno kupovanje ter prodajo obeh potrošniških in poslovnih dobrin in storitev. Zaupanje v to, da bodo vsakodnevne transakcije poravnane v realnem času, pripomore k uporabnosti denarja. Denar je uporaben le takrat, ko je sprejet in obstaja zanesljiva plačilna infrastruktura zanj.

Z uravnavanjem ponudbe denarja je CB v središču plačilnega sistema, predvsem zaradi elektronske izmenjave med zasebnimi plačilnimi sistemi in lastnim poravnalnim računom.

Za izvajanje svojih operacij so kot uporabnice teh sistemov izpostavljene napakam v njihovem delovanju. Zgodovinsko so pogosto bile njihove lastnice in upravljavke (TARGET, TARGET2 in poravnave dolgov pri CB).

Ko se banke ali finančne institucije soočajo z insolventnostjo, lahko CB posreduje kot posojilodajalec v skrajni sili. Takšna podjetja je treba reševati, sicer ima to izjemno negativen vpliv na gospodarstvo. Posojilodajalec v sili ne deluje le za zaščito bančnih institucij, temveč tudi posameznikov, ki imajo depozite pri takšnih institucijah, in preprečuje prekomerno dvigovanje vlog na bankah. Ko so finančne institucije prisiljene v izposojo od CB, signalizirajo trgu, da se približuje ali pa je prisotna gospodarska kriza. V vsakodnevnem poslovanju se ta oblika pomoči ne uporablja.

Zgodovinsko so zasebne banke in sindikati prevzemali vlogo posojilodajalca v skrajni sili. Vlade so tudi že priskočile na pomoč kot posojilodajalec v skrajni sili z reševanjem finančnega sektorja, npr. takrat, ko sta bila bančni sektor in avtomobilska industrija reševana iz državnega proračuna po propadu investicijske banke Lehman Brothers leta 2008.

Posojilodajalec v skrajni sili spodbuja prekomerno tveganje in moralni hazard, ker se banka zaveda, da bo rešena, če se bliža propadu, zato jemlje posledice tveganih dejanj manj resno. Za digitalno valuto bi bilo to zelo težko zagotoviti, tako bi moral biti posojilodajalec v skrajni sili zasebni ali državni organ ali pa ga ne bi bilo, če bi tveganje moralnega hazarda presegalo tveganje stečaja (Hayes, 2016).

3.5.2 Digitalna valuta centralne banke kot podstat plačilnega sistema decentralizirane avtonomne organizacije

Da bi DLT lahko zadostil vlogi decentralizirane avtonomne organizacije (angl. Decentralized Autonomous Organization, v nadaljevanju DAO) v vlogi CB, bi moral iz sedanjih izhodišč tehnologije razpolagati z neomejeno možnostjo ponudbe kriptovalute. Pomembne lastnosti bi še bile zagotavljanje anonimnosti, izvajanje transakcij v realnem času in uravnavanje ponudbe denarja glede na razmere v gospodarstvu. Tak sistem bi deloval po principih polnega rezervnega bančništva. Zanj bi bila potrebna razširljivost za pokritje potreb po transakcijah v gospodarstvu.

Sistem bi imel algoritme za zaupno izvrševanje dogovorov oz. pametne pogodbe in bi bil zastavljen kot monetarni organ na verigi blokov za avtomatizirano ustvarjanje valute. Posegel bi lahko na trg z operacijami odprtega trga z namenom uravnavanja ponudbe denarja v primeru kriznih razmer: prekomerna inflacija ali deflacija, visoka brezposelnost in recesija. Valuta bi delovala *de facto* kot DAO, sprejemala samostojne odločitve in se odzivala na realne finančne trge. Na zmanjšanje valute bi vplivala z odkupom ali pa nevtralizacijo s prenosom na neaktivne denarnice. Kupovala bi tujo valuto na trgu deviz in stabilizirala cene z nakupom vrednostnih papirjev (Hayes, 2016).

Decentralizirana avtonomna organizacija je (Wang in drugi, 2019):

1. razpršena, cilje dosega s pristopom od spodaj navzgor z usklajevanjem med vozlišči,
2. avtomatizirana, saj računalniška koda upravlja s sistemom, konsenz je dosežen znotraj avtonomne skupnosti uporabnikov, kar prispeva k nižjim stroškom delovanja,
3. z lastnimi pravili delovanja, kar se navezuje na pametne pogodbe, sistem nagrajevanja udeležencev je transparenten in sorazmeren z razporeditvijo dela med njimi.

CB imajo veliko svobodnega preudarka oz. diskrecije pri oblikovanju in implementaciji odločitev. Nepredvidljivost obrestne mere povzroča nestabilnost finančnih trgov. Napačna pričakovanja glede gibanja ključne obrestne mere lahko vplivajo na povečano cenovno volatilnost. Sodobna gospodarstva so prevelika in prezapletena za monetarno diskrecijo, zato ravnanje po vnaprej določenih strogih pravilih zmanjšuje ekonomsko negotovost.

Javnim odločevalcem za uspeh na volitvah koristi kratkoročno povečanje proizvodnje in zaposlitve, kar pa vpliva na dolgoročno inflacijo in prihodnjo nestabilnost. CB mora zato izvajati nepriljubljene ukrepe, ki jih politika ne bi. Državne oblasti lahko sledijo politiki visoke inflacije za monetarno financiranje oz. monetizacijo dolga. Takšna politika je pogosto predhodnik propada nacionalnih gospodarstev. Odplačevanje dolga z inflacijo je preprosto, zato avtonomni monetarni organ z mandatom za stabilno inflacijo služi kot varovalni mehanizem (Hayes, 2016). Že Ricardo (1824) je omenjal potrebo po neodvisnosti CB od političnih pritiskov s pravico ustvarjanja denarja ločeno od moči odločanja, kako ga potrošiti. S preprečevanjem CB, da bi financirala državni proračun, in z neodvisnostjo sprejemanja odločitev.

Hayes (2016) predpostavlja naslednji princip delovanja decentraliziranega bančnega sistema. Težko izvedljivo je, da bi kriptovalutni sistem sam zastavljal ciljno obrestno mero. Določanje te je značilnost sodobnih monetarnih politik, vendar obstajajo drugi načini vplivanja na ceno denarja: digitalna valuta še vedno lahko dosega cilje monetarne politike z uravnavanjem količine ustvarjenega novega denarja s podobnim učinkom. Spreminjanje količine ponudbe denarja je enakovredno spreminjanju obrestne mere. Obrestna mera in količina denarja sta notranje povezani, s tem, da višja obrestna mera podraži denar, tudi zmanjšanje ponudbe novega denarja ima podoben učinek.

Če gospodarstvo raste prehitro, se mora zmanjšati ustvarjanje denarja tekom naslednjega obdobja. To ima podoben učinek dvigovanju obrestne mere, ker naredi denar redkejši. V splošnem se za spodbujanje bolj stroge monetarne politike tekom nekega časovnega intervala število enot valute na blok zmanjša (npr. s 25 na 10 kovancev na blok) in čas med tvorjenjem blokov podaljša (npr. z 10 na 15 min), za izvajanje ekspanzivne monetarne politike spodbujanja gospodarske rasti se zgodi ravno nasprotno (Hayes, 2016).

4 VLOGA KRIPTOVALUT V RAZVOJU DIGITALNIH VALUT CENTRALNE BANKE, TEMELJEČIH NA TEHNOLOGIJI RAZPRŠENE EVIDENCE

Kot je bilo omenjeno na začetku magistrskega dela, se je kot prva v vrsti tehnologij razpršene evidence pojavila tehnologija verige blokov. Kasneje so nastajale nove inovativne metode distribuiranega beleženja podatkov in tako se je razvil pojem tehnologija razpršene evidence, ki zajema vse tehnologije z enakim konceptom delovanja. Ločnica obstaja tudi med tehnologijo verige blokov in kriptovaluto bitcoin. Slednja temelji na tej tehnologiji v obliki žetona. Kriptovalute lahko temeljijo na marsikateri tehnologiji razpršene evidence, žeton pa je oblika, ki zagotavlja njihovo neponovljivost, veriga blokov pa nespremenljivost. Ravno zaradi kriptovalute, kot je bitcoin, je govora o CBDC, ki so le delno centralizirane. Kriptovalute prepredajo značilnosti, ki vplivajo na celotno učinkovitost plačil. V nadaljevanju omenjam bistvene oziroma takšne, v katerih odstopajo od današnjih sredstev plačil.

Že v letu 2015 je bilo v obtoku več kot 600 digitalnih valut z različnimi protokoli za procese in potrjevanje transakcij in z različnimi načini rasti ponudbe njihovih enot. Ta fragmentiranost oziroma raznoterost predstavlja oviro pri širši rabi in sprejetosti, v raznih iniciativah lahko predstavlja oviro pri doseganju kritične mase, potrebne za realizacijo mrežnih učinkov, torej takšnih, kjer se korist z večanjem števila udeležencev povečuje.

Glede na svojo omejeno razširjenost je število transakcij v obdelavi pri sistemih kriptovalut bistveno manjše kot pri tistih, s katerimi upravljajo širše sprejeti maloprodajni plačilni sistemi. Ali so sistemi kriptovalut sposobni obdelati bistveno večje število transakcij, je še odprto vprašanje. Nekateri prepoznavnejši sistemi kriptovalut so intenzivni v porabi električne energije za ustvarjanje računalniške moči, namenjene obdelavi majhnega števila transakcij. Izboljšave v procesni moči in hitrosti ter nižanje stroškov programske in strojne opreme prispevajo k razširljivosti in večji učinkovitosti. Drugi sistemi digitalnih valut domnevno potrebujejo manj virov za delovanje.

Nepopolna anonimnost ali psevdonimnost nekaterih sistemov digitalnih valut lahko odvrneta nekatere udeležence finančnega sistema od neposredne uporabe ali ponudbe digitalne valute svojim strankam, saj se težko izpolni zahteve potrjevanja identitete pri transakcijah digitalnih valut. Transakcije niso eksplicitno vidne v javnih evidencah, vendar je iz podatkov izvedljivo sklepati o njihovih udeležencih.

Digitalne valute na razpršeni evidenci morajo zagotoviti konsenz med udeleženci v omrežju, da dosežejo enotnost evidence o zgodovini transakcij in stanjih računov. Sočasno lahko obstoji več različic evidence. Tehnični in varnostni pomisleki so povezani s tem, da udeleženci omrežja lahko potrdijo nelegitimno evidenco in se tretja stran na ta način okoristi.

Trajnostna naravnanost poslovnega modela je lahko poseben izziv za nekatere sisteme digitalnih valut. Motivi za preverjanje in vključevanje transakcij v evidenco so neposredno povezani z zaslužki od izdaje valute, slednja pa ima omejitev v končno izdani količini oziroma se njena količina zmanjšuje v intervalih. Primanjkuje pravih motivov za delovanje sistema, ko se ponudba nove digitalne valute zmanjša ali preneha. Možna rešitev je tudi višanje pristojbin na transakcije za nadomestitev izgube prihodka pri ustvarjanju novih enot digitalne valute. To pa lahko negativno vpliva na povpraševanje po valuti in delovanje sistema na dolgi rok (BIS, 2015).

Način upravljanja je model skupnostnega samoupravljanja, ki pa ne ponuja zadostne mere zaupanja, transparentnosti in odgovornosti za potrebe finančne industrije. Model je povsem odprt, kjer se lahko vsakdo pridruži in spremlja transakcije. Toda dostopati bi morali le pooblaščeni udeleženci in presojati o legitimnosti aktivnosti na omrežju (Le Borne in drugi, 2016).

Obstaja tveganje izgube sredstev za uporabnike. Vdori lahko spodkopavajo uporabniško zaupanje v sistem digitalne valute. Če uporabnik ne razpolaga več s podatki o lastništvu nad enotami digitalne valute, shranjenimi na razpršeni evidenci, je zelo verjetno, da do teh enot ne bo več mogel priti. Nekateri uporabniki digitalnih valut zaupajo posrednikom pri shranjevanju informacij v zvezi z njihovim lastništvom enot digitalne valute glede varnosti, da preprečijo izgubo zaradi računalniških vdorov, operativnih napak ali nezakonite pridobitve.

Digitalne valute na razpršeni evidenci ponujajo nižji strošek transakcij kot druge metode plačevanja, še posebej pri čezmejnih plačilih. Transakcije teh sistemov ne potrebujejo posrednikov za pomoč pri plačilih, kar vpliva na nižje stroške obdelave. Toda stroški transakcij teh sistemov niso vedno transparentni in obstajajo tudi drugi stroški, kot so pristojbine za menjavo digitalne valute v državno valuto pri uporabnikih s stanjem računa, izraženim v enotah digitalne valute.

Preprostost uporabe je po navadi ključnega pomena za sprejetost plačilnih metod in mehanizmov in lahko zajema dejavnike, kot so število korakov v plačilnem procesu, intuitivnost postopka in enostavnost integracije z ostalimi procesi. Uporaba digitalnih valut in razpršene evidence je lahko bolj zaželena zaradi navedenih prednosti v primerjavi z obstoječimi metodami. Veliko ponudnikov poskuša izboljšati in olajšati uporabnikovo izkušnjo v sistemih digitalnih valut.

Če se uporabniki odločijo obdržati sredstvo digitalne valute, sprejeto kot plačilo, jih lahko prizadenejo stroški in izgube, povezane s cenovnimi in likvidnostnimi tveganji, ko se na primer ne da izstopiti pravočasno iz naložbe zaradi manjše tržne kapitalizacije. Ta tveganja niso zanemarljiva ob dani volatilnosti in motnjah trga, do katerih prihaja pri nekaterih bolje poznanih sistemih digitalnih valut. Medtem ko nekateri uporabniki iščejo špekulativne dobičke na podlagi volatilnosti, za večino variabilnost menjalnih tečajev predstavlja oviro k

širši sprejetosti. Kakšen je razpon, za katerega bi se zmanjšala cenovna volatilnost, če se bi sistemi digitalnih valut uporabljali široma, je še odprto vprašanje, saj na dolgi rok obstaja tveganje izgube hranjenih digitalnih valut z ničelno notranjo vrednostjo.

Sistemi digitalnih valut na razpršeni evidenci pogosto nimajo načina podajanja reklamacij, ker imajo nepreklicna plačila, kar zmanjšuje tveganje prejemnika plačila, da bi bilo plačilo povrnjeno plačniku zaradi prevare ali povračila bremenitve. Čeprav je lastnost privlačna za prejemnike plačil oz. trgovce, lahko odvrne sprejetost in uporabo s strani plačnikov oz. potrošnikov.

Digitalne valute na razpršenih evidencah bi lahko ponujale hitrejši kliring in poravnavo transakcij, kot sta v običajnih sistemih. Toda nabor inovacij, ki ni povezan z digitalnimi valutami, kot je npr. hitrejši maloprodajni plačilni sistem, tudi naslavlja povečano povpraševanje po večji plačilni hitrosti. Poleg tega sistemi bruto poravnave v realnem času že podpirajo veleprodajne finančne trge in zagotavljajo zmogljivosti za zelo hitra plačila in poravnave zneskov velikih vrednosti.

Digitalne valute na DLT so odprta omrežja z globalnim dosegom. Ti sistemi ne razlikujejo med uporabniki glede na kraj in tako dopuščajo prenos vrednosti ne glede na lokacijo. Hitrost transakcije ni odvisna od kraja plačnika in prejemnika plačila. Decentralizirana zasnova sistemov digitalnih valut bi pomenila težavno implementacijo zakonov, s katerimi bi nacionalne oblasti uvedle omejitve na čezmejne transakcije.

Nekateri sistemi digitalnih valut na DLT lahko zagotovijo transakcije, ne da bi razkrili osebne ali plačilne podatke. Privlačnost zasebnosti podatkov s psevdonimnostjo ter izogibanja bankam in oblastem lahko deloma vodi želja izogniti se zakonom in predpisom. Na ta način so sistemi digitalnih valut, povezani s svojim globalnim dosegom, privlačni za nedovoljeno rabo. Toda obstajajo tudi legitimni razlogi, zakaj imajo uporabniki raje anonimne plačilne metode, ko prejemnik plačila ni zaupen za zaščito razkritih informacij. Do tega lahko pride pri transakcijah med dvema stranema pri spletni prodaji.

Trženje tehnologije in učinki ugleda lahko pripomorejo k razširjenosti tehnologije. Sistemi digitalnih valut na razpršeni evidenci so inovativna metoda plačevanja. Trgovci lahko vidijo koristi pri sprejemanju plačil prek sistema digitalne valute kot spodbudo za povpraševanje po njihovih izdelkih in storitvah. Uporabnike lahko ti sistemi privabijo preprosto tudi zaradi novosti tehnologije (BIS, 2015).

Če povzamem poglavje, predstavlja razdrobljenost kriptovalut oviro za krepitev mrežnih učinkov, omejitve so pri njeni razširljivosti, psevdonimnost je v nasprotju z izpolnjevanjem zahtev poznavanja svoje stranke, zaščiti pa tudi ne zasebnosti podatkov, obstaja možnost ustvarjanja vilic oz. nelegitimne verige blokov, kriptovalutam primanjkuje dodatnih finančnih spodbud po poteku izdaje celotne količine denarja, imajo vprašljiv model upravljanja, prisotni so pomisleki glede varnosti, predstavljajo nižje stroške čezmejnih plačil, so intuitivne za uporabo, toda imajo cenovna tveganja, likvidnostna tveganja, težavo

v nepreklicnosti plačil, globalni doseg otežuje sprejemanje predpisov ter so lahko zanimive za trg kot inovacija.

4.1 Konsenzni mehanizem dokaza o delu in z njim povezano rudarjenje na verigi blokov za izvedbo transakcij v plačilnem sistemu

V tem razdelku pišem o podrobnostih rudarjenja, natančneje, kako na stroške proizvodnje kovancev oz. porabljene električne energije vplivajo zahtevnost rudarjenja, hitrost proizvodnje enot in kriptografski algoritem v rabi. S konsenznim mehanizmom se potrjuje transakcije na razpršeni evidenci, zato mu namenjam posebno pozornost v tem poglavju.

Proizvodnja kriptovalut, kot je bitcoin (v nadaljevanju BTC), je podobna konkurenčnemu trgu blaga, saj rudarjenje poteka, dokler se mejni stroški ne izenačijo z mejnimi prihodki. Rudarjenje poteka s specializirano strojno opremo, zmogljivejšo od običajne, in je merjeno s heš/sekundo (H/s). Zmogljivejši računalnik ima boljše možnosti najdbe bloka, zato je konkurenčen. Zanesljivost protokola dokaza o delu omogoča procesno delo računalnika. Vrednost BTC primarno izhaja iz njegove uporabe in potrebe po transakcijah. V stroških proizvodnje je zajeta tržna cena kriptovalute, cena električne energije, učinkovitost energije rudarjenja in zahtevnost rudarjenja.

Večina kriptovalut ima podoben nabor vgrajenih spremenljivk kot bitcoin:

1. Celotna ponudba denarja je število kadarkoli ustvarjenih kovancev; pri BTC je natanko 21 milijonov enot.
2. Vsak rudarjen blok vsebuje določeno število enot, s katerim je rudar nagrajen. Prvotno je blok BTC vseboval 50 BTC, na vsake štiri leta se količina razpolovi.
3. Blok se z rudarjenjem zaradi prilagajanja zahtevnosti poišče v povprečju v enakem časovnem intervalu. BTC-bloki so najdeni v povprečju na vsakih 10 minut.
4. Omrežje preveri dosežen povprečen čas bloka na podlagi predhodno rudarjenih blokov. Pri BTC sistem po 2016 najdenih blokih preveri, ali je odstopanje od 10-minutnega povprečja v času ustvarjanja bloka. Če je daljše od 10 minut, sistem poveča zahtevnost iskanja novih blokov, tako da je 10-minutno povprečje ponovno vzpostavljeno.
5. Algoritem kriptografske funkcije razpršitve (heš) je uporabljen kot podlaga za protokol. Pri BTC kot pri večini altkovancev je v rabi SHA-256d, ostali sistemi uporabljajo algoritem, imenovan scrypt.

Večje število transakcij se odraža v agregirani računalniški moči, vloženi v rudarjenje, kar prispeva k višji vrednosti kovanca. Racionalni rudar zasleduje dobiček na način, da uporablja vire za rudarjenje, dokler mejni strošek ne preseže mejnega prihodka, takrat umakne uporabo računalniške moči iz omrežja in jo nameni v drugo. Uporabljena procesna moč je sorazmerna z zahtevnostjo rudarjenja, saj se z višanjem omrežne moči zahtevnost rudarjenja povečuje, da ohrani vnaprej programiran čas bloka. Tako se da s stopnjo zahtevnosti posredno oceniti agregatno moč rudarjenja.

Število najdenih kovancev na minuto je negativno povezano z njegovo vrednostjo. Gre za razširitev zakona o padajoči mejni koristnosti. To pomeni, da hitrost tvorjenja enot znižuje ceno. Če je proizvedenih mnogo kovancev na blok ali pa so bloki najdeni v hitrem zaporedju, jim to znižuje vrednost. Po drugi strani redkost na blok poveča vrednost. Na to vplivata plačilo za ustvarjen blok in čas nastajanja bloka.

Razmerje med rudarjenimi kovanci in nerudarjenimi iz celotne ponudbe denarja je pozitivno povezano z vrednostjo kovanca. Omejitev prihodnje ponudbe denarja je eksogena, zato manjši odstotek nerudarjenih enot poveča redkost in kovancu poveča vrednost. Relativna redkost se izračuna kot količnik med številom najdenih kovancev in celotno ponudbo denarja. V empirični raziskavi Hayes (2015) ni uspel potrditi tega kot hipoteze, verjetno zaradi načina definiranja celotne ponudbe kovancev. V sistemu Bitcoin je število omogočenih decimalnih mest osem, vendar se da število teh mest neomejeno povečevati. Ko celotna ponudba denarja doseže zgornjo mejo, se enote enostavno deli, npr. s 100.000.000 BTC, kar ne preprečuje nastanka enote 0,00000001 BTC.

Altovanci, temelječi na scrypt algoritmu, imajo višjo vrednost, *ceteris paribus*, kot kovanci, temelječi na SHA-256d. Sistem scrypt je nadgradnja protokola SHA-256d, na katerem temelji BTC. Scrypt je bil vpeljan za onemogočanje izrivanja rudarjev s slabšo strojno opremo. Posledično potrebujejo scrypt altkovanci v povprečju več računalniške moči na enoto kot kovanec z uporabo algoritma SHA-256d. Relativna zahtevnost algoritma vodi v relativno vrednost. Trajnost kriptovalute je pozitivno povezana z njeno vrednostjo. Dlje kot je kriptovaluta v rabi in obstoju, večjo ima vrednost. V konkurenčnem okolju altkovancev (drugih, kot je bitcoin) so poraženci izrinjeni, tako s časom pridobiva na vrednosti.

Odločitev o rudarjenju je torej odvisna od cene električne energije, energetske porabe na enoto moči rudarjenja, vrednosti BTC in zahtevnosti rudarjenja. Na običajnih trgih blaga se ponudba spremeni, da se prilagodi spremembam v povpraševanju. Ponudba BTC je drugačna, s spreminjanjem zahtevnosti se uravnava linearno rast ponudbe. Cenovna elastičnost ponudbe se udejanji s prilagajanjem zahtevnosti rudarjenja (Hayes, 2015).

4.2 Volatilnost kriptovalut kot pomanjkljivost plačilnih sistemov

V tem razdelku obravnavam mehanizme, ki neposredno vplivajo na vrednost digitalne fiat valute. Na ravnotežje vplivajo tržna kapitalizacija valute, njena obtočna hitrost in splošna raven cen. Ponudba kovancev je določena s količino kriptovalute v obtoku, ki je javno poznana in definirana vnaprej. Povpraševanje je določeno po njeni vlogi kot posredniku v menjavi, cena je posledica ravnotežja med ponudbo in povpraševanjem. Kovancev ne izda CB ali vladni organ. Ponudbo in povpraševanje po kriptovaluti vodi špekulativno ravnanje vlagateljev, kajti za digitalne valute obrestne mere ne obstajajo in dobički so zgolj ustvarjeni s spremembo cene. Razvoj svetovnih financ, ki jih predstavljajo borzni indeksi, kot je Dow Jones, tečaji deviz, kot je dolar za evro, in cena nafte dolgoročno močno vplivajo na vrednost kriptovalute.

Povpraševanje po kriptovaluti v obtoku je sorazmerno splošni ravni cen dobrin in storitev in velikosti gospodarstva kriptovalute ter obratno sorazmerno obtočni hitrosti, ki meri pogostost nakupa dobrin in storitev z enoto kriptovalute in je pogojena z oportunitetnimi stroški hranjenja. Na popolnih trgih nastopi cenovno ravnotežje kriptovalute takrat, ko se cena kriptovalute s povečanjem obtočne hitrosti in količine kriptovalute zniža, toda naraste z velikostjo gospodarstva kriptovalute (tržna kapitalizacija) in ravnjo cen.

Ker je kriptovaluta fiat valuta, nima notranje vrednosti ali, drugače povedano, nima vrednosti v ozadju, ki bi izhajala iz njene potrošnje ali uporabe v proizvodnji, kot npr. pri zlatu. Vrednost fiat valute izhaja iz zaupanja, da bo obdržala vrednost tudi v prihodnje oziroma delovala kot posrednik v menjavi. To je pomembno za kriptovaluto, kajti kot nova valuta še uveljavlja tržni delež med bodočimi uporabniki. Ker je valuta digitalna, je bolj izpostavljena spletnim napadom, ki lahko destabilizirajo sistem in povečajo volatilnost cen. Stroški transakcij vplivajo na to, katero kriptovaluto vlagatelji izberejo, njihov izbor pa ima učinek na njeno vrednost.

Globalni makroekonomski in finančni razvoj izkazujejo borzni indeksi, devizni tečaji in cene nafte. Naštete spremenljivke vplivajo na ceno kriptovalute. Ugodnejši makroekonomski in finančni razvoj lahko spodbudi uporabo kriptovalute v trgovanju in menjavi in tako okrepi povpraševanje po njej, kar lahko ima pozitiven vpliv na ceno kriptovalute.

Inflacija in cenovni indeksi so drugi pomembni indikatorji makroekonomskega in finančnega razvoja. Cena nafte je eden od glavnih virov povpraševanja in stroškovnih pritiskov, ki je zgodnji pokazatelj pojava inflacije. Če cena nafte signalizira potencialne spremembe v splošni ravni cen, to lahko vodi do depreciacije ali apreciacije kriptovalute. Tudi menjalni tečaj lahko odraža pojav inflacije in ima tako pozitiven vpliv na ceno kriptovalute (Ciaian in drugi, 2016).

4.3 Vodilna kriptovaluta bitcoin kot odraz tehnologije razpršene evidence v plačilnih sistemih

Že v letu 2016 je Bitcoin upravljal z 10,5 milijard dolarjev in imel več kot 150 milijonov dolarjev dnevne menjave. Še vedno pa ne more nadomestiti samostojnega monetarnega organa. Sistem Bitcoin je decentraliziran denar na verigi blokov in ima vlogo hranilca vrednosti in posrednika v menjavi. Varnost plačilnega sistema in njegova uporaba sta pomembni za njegov obstoj. Varnost transakcij še ni bila ogrožena, prav tako še ni bil ponarejen. Konsenzni mehanizem na omrežju anonimnih in oddaljenih vozlišč ne potrebuje centralnega nadzora.

Po Aristotelu so za funkcionalnost denarja nujne štiri lastnost (v Smithin, 2002): obstojnost, prenosljivost (velika vrednost glede na velikost in težo), deljivost (zamenljivost), notranja vrednost (neodvisnost vrednosti od drugih objektov). Ali kriptovaluta, kot je BTC, ustreza omenjenim pogojem? (1) varnost je izredno visoka in transakcije v strukturi verige blokov

so trajne, (2) lahko se dostopa do njega z vsakega računalnika ali mobilne naprave, povezane z internetom, (3) BTC se lahko razdeli na 8 decimalnih mest, najmanjši se imenuje *satoši* in je tudi zamenljiv. Kljub vsemu pa njegovo uporabo zavirajo pomanjkljivosti, ki so opisane v nadaljevanju.

Zgornja meja BTC je 21 milijonov kovancev, s to količino se rudarjenje zaključi, saj na voljo ni več novih kovancev. Umetna zgornja meja povzroča naraščajoče deflatorno valuto. Ob stalni ponudbi in z večanjem povpraševanja po denarju pridobiva vsak kovanec na vrednosti, ki raste skladno s prebivalstvom in naraščanjem BDP. Za dosego učinkovitosti ne bi smel imeti omejitve. Rešitev je lahko uporaba deležev BTC kot enote (milijardinka BTC ali nano-BTC npr.) v vsakodnevnem poslovanju, toda razpolagati z neomejeno ponudbo denarja je vseeno boljše.

Omrežje BTC lahko obdela do sedem transakcij na sekundo (v nadaljevanju tns), kar je dovolj za notranji BTC-trg, vendar zanemarljivo v primerjavi z nacionalnim. Plačilni sistem VISA opravi z okoli 1.700 tns (teoretično 35-krat več), PayPal, ki je bistveno manjše omrežje, se v povprečju spoprime s 193 transakcijami na sekundo. Za tekoče delovanje gospodarstva mora biti sistem zmožen sprotne obdelave več tisoč tns. Velikost bloka je omejena in povezana s tns ter omogoča le 1 MB (2.000–2.500 transakcij) prostora za shranjevanje podatkov. Z naraščanjem količine transakcij se mora vsak blok znatno povečati.

BTC-transakcije potrebujejo programiranih 10 minut za rudarjenje bloka, preden so potrjene. Prejemniki plačil jih imajo raje potrjene večkrat, od tri do šestkrat, kar lahko traja do ene ure in je nesprejemljivo za veliko večino dnevnih transakcij, ki morajo biti izvedene in potrjene takoj. Napadi v obliki distribuirane zavrnitve storitev (angl. Distributed Denial-of-Service, DDoS) na omrežje oz. onesposabljanja strežnika s preveliko obremenitvijo lahko povzročijo upad hitrosti pod pričakovano in niso značilni le za sisteme digitalnih valut.

Naslovi v BTC so psevdonimni in ne anonimni, kar pomeni, da se prave identitete na omrežju lahko razkrije posredno s spleta ali z analizo vzorcev transakcij na verigi blokov. Predpisi proti pranju denarja so zahtevani s strani finančnih institucij, toda gotovinski denar je anonimen. Za zaščito zasebnosti posameznikov in približevanje lastnostim gotovine bi za kriptovaluto moralo veljati isto.

BTC ima poleg stalne stopnje tvorjenja enot, enega bloka na deset minut, tudi pravilo za zmanjšanje količine najdenih BTC v vsakem bloku približno na vsaka štiri leta. Torej ima vnaprej določeno rast ponudbe denarja. Friedmanovo pravilo predpostavlja enakomerno stopnjo rasti količine denarja za CB, neodvisno od stanja gospodarstva (Friedman, 1948). To prispeva k bolj obvladljivim splošnim ravnem cen in učinkovitejšim tržnim obrestnim meram.

Preostali kovanci ali alternativni kovanci, kot jih naslavlja literatura, ali *altcoins* skušajo rešiti eno ali več omenjenih težav BTC. Npr. dash, prvotno imenovan darkcoin, omogoča povsem anonimne transakcije na verigi blokov s hitrimi potrditvami in povečanjem velikosti

bloka. Digitalna valuta lahko obstaja tudi na verigi blokov z distribuiranim dovoljenjem, kjer je vsako vozlišče v omrežju poznan in zaupen subjekt, in ne samo kot decentralizirani monetarni sistem. S tem se zmanjša potreba po dragem in energetsko potratnem rudarjenju ter bistveno poveča hitrost in število transakcij. Poslovne banke in finančne institucije lahko zastopajo takšna vozlišča (Hayes, 2016).

4.4 Doseganje ekonomske stabilnosti in večje zanesljivosti plačilnih sistemov s stabilnimi kovanci

Stabilni kovanci ohranjajo vezavo z uradnim številcem (*numeraire*), po navadi ameriškim dolarjem. Obstajajo štiri vrste stabilnih kovancev: Prvi je stabilni kovanec, krit s fiat valuto, ki je vezan ena na ena na ameriški dolar ali drugi obstoječi številec. Tether je vodilni primer takšne valute kot popolnoma zavarovane kriptovalute, vezane na dolar.

Vsak kovanec je krit z enakim zneskom depozitov oziroma vlog ameriškega dolarja, hranjenih pri poslovnih bankah do leta 2018 na Tajvanu, po tem letu pa z večino sredstev na Bahamih. Tether omogoča svojim uporabnikom anonimnost, kot jo imajo gotovinske transakcije, hkrati ima transakcije, preverljive na Bitcoinovi verigi blokov. Izkazal je obljubljeno mero stabilnosti skozi večletno obdobje z izjemo kratkega časa aprila 2017, od poletja 2020 do sedaj pa ni imel posebnih nihanj v svoji vrednosti (Eichengreen, 2019).

Stabilni kovanec Terra USD (UST) v povezavi s Terra Luno ima za ohranitev vezave 1 UST na 1 USD vzpostavljen sistem dvojnega žetona. Z odmikom cene UST od vrednosti dolarja se odzove ponudba žetonov Lune. Ob povečanem povpraševanju po UST in njegovem dvigu cene nad 1 USD sistem ustvari nove kovance UST z uničenjem, t. i. sežigom, kovancev Lune. Ob zmanjšanem povpraševanju po UST in padcu njegove cene pod 1 USD sistem z ustvarjanjem oz. s t. i. kovanjem Lune z njo odkupi in sežge žetone UST (Quiroz-Gutierrez, 2022). Kovanec se je pojavil leta 2018, odgovorna oseba zanj je bil Do-Kwon iz Terraform Labs, v maju 2022 pa je prišlo do strmoglavljenja njegove vrednosti. Ustanovitelj je bil prijet zaradi finančne goljufije v Črni gori marca 2023 na podlagi obtožnic Združenih držav Amerike in Koreje (Kuzmanovic in Savic, 2023).

V drugo kategorijo spadajo stabilni kovanci, kriti s kriptovaluto. V tem primeru se drugo kriptovaluto hrani za kritje stabilnega kovanca. Ta različica osvobodi izdajatelja opravka z bankami, ki lahko imajo dvome o ponujanju storitev platformi, ki se jo lahko uporablja za nezakonite namene. Težava nastane v tem, ker vrednost kritja niha, saj kritje ni v obliki stabilnega kovanca. Ker lahko vrednost kritja pade, morajo kripto stabilni kovanci, da bi bili kredibilni, biti prekapitalizirani, kar podraži njihovo upravljanje v primerjavi s fiat kritimi stabilnimi kovanci. Vodilni kripto kriti stabilni kovanec, imenovan DAI, je imel v času pisanja trikratni količnik kritja. Vrednost kritja lahko pade kadarkoli pod vrednost izdaje kovanca, ne glede na presežno kritje so ti kovanci izpostavljeni prekomerni menjavi.

Tretja kategorija je delno krit stabilni kovanec, kamor je sodil tudi v času pisanja kovanec, poimenovan Saga, ki ga je razvijala neprofitna organizacija Saga Monetary Technologies. Izvajala je preveritev zahtev proti pranju denarja, saj je platforma uporabljala verigo blokov za zagotavljanje anonimnosti transakcij med udeleženimi stranmi. Projekt je stremel k nižjim stroškom transakcij in večji razširljivosti sistema.

Krit je bil z delnimi rezervami enot posebnih pravic črpanja na Ethereumu. Zaradi nezaupanja v valutno vezavo je obstajalo tveganje, da bi prišlo lahko do prekomerne zamenjave. Kajti njegova vrednost je izhajala iz kombinacije dejavnikov, kot so zaupanje v trg, uporabnost kot menjalno sredstvo, naložbena privlačnost in prihodnji obeti gibanja vrednosti. Nižanje njene volatilnosti, bodisi zaradi večanja baze uporabnikov, še ni zagotavljalo nadaljevanja trenda v prihodnosti. V začetku leta 2021 se je projekt iz nepojasnjenih razlogov zaustavil (Sadeh Man, 2020).

CB, soočene s takšno situacijo, se po navadi odzovejo na dva načina. Devalvirajo valuto, kar zmanjša obveznosti do rezerv, toda to ni skladno z utemeljitvijo stabilnega kovanca, saj spodkopava zaupanje vanj in v njegov tržni delež. Lahko tudi z vsiljenim nadzorom nad denarjem omeji dostop vlagateljem do njihovih rezerv. Toda omejevanje zamenljivosti kriptožetona v fiat valuto je v nasprotju s principi stabilnega kovanca.

Četrta oblika je stabilni kovanec brez kritja. V rabi ima pametne pogodbe za upravljanje ponudbe digitalnega kovanca s ciljem vzdrževati njegovo vrednost proti dolarju. Platforma izdaja tako digitalne kovance kot digitalne obveznice. Pametne pogodbe prodajajo obveznice za kovance, ko cena zadnjega upade, in kovanec za obveznico, ko dolarska cena kovanca naraste.

Investitorji vlagajo v obveznice kljub manjši likvidnosti in večji nominalni vrednosti zaradi dividend v obliki digitalnega kovanca. Dividende so financirane iz zaslužka od izdaje denarja, ki ga dobi platforma pri prodaji dodatnih kovancev. Nekateri nekriti stabilni kovanci izdajajo tudi delnice, kjer njihovi prejemniki samodejno prejmejo dodatne kovance, ko je potreba po dodatni izdaji in so vse obveznice izplačane.

Ohranjanje takšnih shem je odvisno od uspeha rasti platforme, kajti brez rasti uporabnikov stabilnih kovancev ni dodatne izdaje, s katero je plačano imetnikom obveznic. S prodajo obveznic se prepreči upad vrednosti kovanca pod nominalno vrednost. Platforma pridobi kovance, ki so zunaj obtoka, vendar je treba te presežke odpraviti ali zamrzniti, da se ohrani vrednost kovanca. Ne sme se jih vnesti nazaj v obtok za izplačilo dividend imetnikom obveznic, da se s tem ne ogrozi vezave.

Četudi platforma raste, lahko dvomi o njeni trajnosti omajejo njeno stabilnost. Skeptičnost o tem, ali lahko ustvari zadosten zaslužek od izdaje denarja v prihodnosti za izplačilo lastnikom obveznic, vpliva na vlagatelje tako, da zmanjšajo svoje povpraševanje po obveznicah, kar podraži odvzem preseženih kovancev iz obtoka platforme in krepi dvome.

Vlagatelji niso pripravljeni kupiti dodatnih obveznic ne glede na ceno in platforma zato ne more preprečiti upada cene stabilnega kovanca (Eichengreen, 2019).

5 VPLIV CENTRALNOBANČNIH DIGITALNIH VALUT NA UČINKOVITOST PLAČILNIH SISTEMOV

5.1 Razvoj centralnobančnih digitalnih valut iz kriptovalut na tehnologiji razpršene evidence

Sprva je bila ideja, da bi koncept kriptovalute deloval revolucionarno na bančni sistem, kjer bi z eno od svojih glavnih lastnosti, decentraliziranostjo, odpravil centralno bančništvo. V nadaljevanju je opisan prvi takšen poskus države. Kasneje pa so ravno CB v tehnologiji kriptovalut odkrile lastnosti, ki bi jim omogočile uresničitev svoje digitalne gotovine. Njen prenos bi ostal medvrstniški, vendar bi lahko omogočala sledljivost za odvrnitev od nezakonite rabe in preprečevanje davčnih utaj. Za razliko od fizičnega denarja bi lahko bila še obrestonosna in programirljiva za namembnost uporabe. Omrežje bi bilo razpršeno med zaupnimi vozlišči finančnih institucij, ki bi potrjevale transakcije. Tako sistem ne bi temeljil na dokazu o delu, ki je energetsko potraten in ima omejitve pri razširljivosti.

Prevzem zunanje valute, kot je BTC, za zakonito plačilno sredstvo je sprva uzakonila južnoameriška država Salvador v času predsedovanja Nayiba Bukeleja leta 2021. Finančni prilivi salvadorskih zdomcev so prispevali 20 % letnega BDP države, primorani pa so bili plačevati visoke transakcijske stroške v višini 400 milijonov dolarjev letno, 70 % prebivalstva ni imelo bančnega računa pred vpeljavo BTC. Po njegovi uvedbi se ga je začelo posluževati 24 % prebivalstva. BTC omogoča hitra, stroškovno učinkovita čezmejna plačila in ne zahteva bančnega računa. V državi sta kljub temu obveljali dve valuti, BTC in ameriški dolar.

Vlada je ponudila denarnico za BTC, imenovano Chivo, in kot spodbudo namenila 30 ameriških dolarjev bonusa vsakemu uporabniku. Transakcije so potekale na omrežju Lightning, kjer se validiranje izvaja zunaj verige blokov in se kasneje zabeleži nanjo, kar prispeva k večji razširljivosti oziroma nižjim stroškom in večji hitrosti. Sistem se je soočal s tehničnimi težavami. Država namerava tudi izdati dolgoročne obveznice za financiranje svojih BTC projektov. Turizem se je povečal za 81 % v letu 2022 v primerjavi z obdobjem pred pandemijo covida in država je postala privlačna za tuje naložbe (Kshetri, 2022).

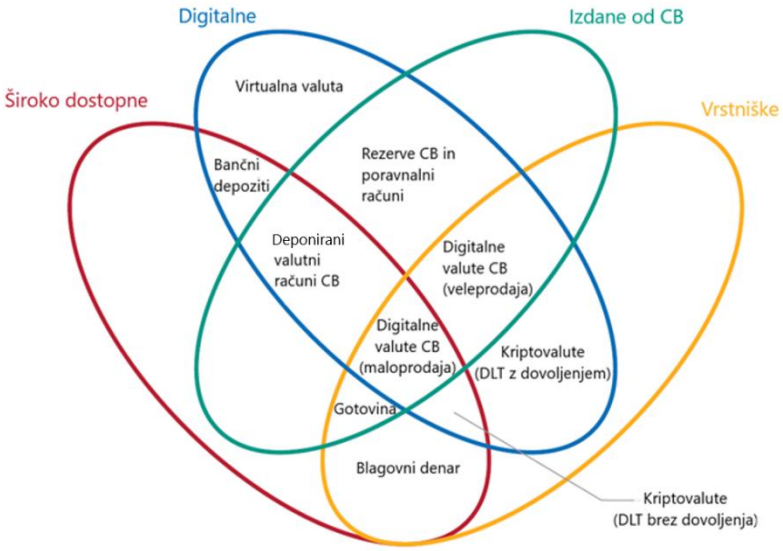
5.2 Značilnosti centralnobančne digitalne valute, odražene v plačilnih sistemih

Za delovanje plačilnega sistema, temelječega na tehnologiji razpršene evidence, je potrebna uvedba uradne kriptovalute po odloku CB. Po Shinu (2018) bi takšna zvrst denarja delovala kot gotovina – ustvarila bi jo CB, nato bi bila v obtoku med bankami, podjetji in potrošniki.

Takšna kriptovaluta bi bila izmenjavana med udeleženci realnega sektorja na razpršeni evidenci, kjer CB ne bi bilo treba voditi računov, prav tako bi CB z zaprtim dostopom v sistem določala zaupna vozlišča.

Tri poglavitne značilnosti kriptovalut so: (1) digitaliziranost (predstavljajo priročno plačilno sredstvo, zavarovano s šifriranjem za preprečitev ponarejanja in prevar pri transakcijah), (2) niso nikogaršnja obveznost, četudi so ustvarjene zasebno, nimajo možnosti unovčitve, njihova vrednost izhaja samo iz bodočih pričakovanj o njihovi sprejetosti in (3) dopuščajo digitalno P2P-izmenjavo (Shin, 2018).

Slika 4: Razvrstitev oblik denarja po značilnostih



Vir: Shin (2018).

Na sliki 4 je denar razvrščen med štiri lastnosti – izdajatelja, obliko, dostopnost in transferni mehanizem. Izdajatelj je lahko centralna ali poslovna banka, lahko pa tudi ni izdajatelja kot v primeru blagovne menjave. Obliko lahko ima fizično, kot je bankovec ali kovanec, ali pa je v digitalni obliki. Dostopen je lahko za splošno rabo, kot so bančne vloge, ali pa omejeno, kot so rezerve CB. Zadnja lastnost opisuje transferni mehanizem, ki je lahko P2P ali prek posrednika, kot je pri vlogah.

Denar je zasnovan na dva načina, kot žeton ali kot dobroimetje na računih. Denar na žetonu (npr. bankovci in kovanci) je lahko izmenjan na P2P-način, kar je izključno odvisno od zmožnosti preverbe prejemnika plačila o verodostojnosti plačilnega sredstva, zato je pri gotovini težava v možnosti ponarejanja. Sistem, kjer je denar na računu, temelji izključno na zmožnosti preverjanja identitete imetnika računa (Shin, 2018), zato je težava s sredstvi na računu kraja identitete. V primeru digitalnih žetonov lahko pride tudi do elektronske poneverbe ali podvojene potrošnje. Zadnje pomeni trošenje istih enot kriptovalute večkrat zapored s podvajanjem.

V prikazu so navedene tri oblike digitalnega denarja CB; ena na računu in dve na žetonu. Zadnji dve se razlikujeta po tem, kdo ima dostop do njih, kar vpliva na njuni različni možnosti uporabe. En je plačilni instrument v splošni rabi pri maloprodaji, drugi pa je žeton za digitalne poravnave z omejenim dostopom v veleprodaji in je v rabi med finančnimi institucijami (BIS, 2018).

CBDC je lahko na žetonu, kot sta bila v letu 2014 predlagana Fedcoin in Bitdollar. To pomeni, da se pri izdaji enote CBDC prenašajo od enega do drugega ekonomskega subjekta neodvisno od CB, kot sedaj krožijo bankovci. CBDC pa je lahko odražen kot stanje na računu subjektov pri CB. CBDC ima le delne značilnosti kriptovalut. Bitcoin, Litecoin ali Ether uporabljajo razpršeno evidenco in šifriranje za zagotavljanje njihove verodostojnosti. Za delovanje centralnobančnega sistema lahko CBDC prav tako temelji na sedanji tehnologiji RTGS, ki je bolj zrela in uveljavljena. Optimalna izbira lastnosti izhaja iz namembnosti CBDC. CBDC za zagotavljanje varnih plačilnih storitev potrebuje druge lastnosti kot v vlogi instrumenta monetarne politike.

Tabela 1 med seboj primerja nekaj tipičnih sredstev, podobnih denarju, in opredeljuje njihove značilnosti. Pogoj, da je sredstvo opredeljeno kot CBDC, sta prvi dve značilnosti, navedeni v prvem stolpcu, ostale pa so predmet izbire. Bančne rezerve so elektronske in na računu, niso kriptovalute, saj ne delujejo na razpršeni evidenci, nudijo izplačilo obresti, dostopne so omejenemu številu udeležencev, bankam in ostalim finančnim institucijam. Njihov glavni cilj je imeti vlogo instrumenta monetarne politike, za manjši del gospodarstva ponujajo tudi varne in učinkovite plačilne storitve in služijo kot instrument za finančno stabilnost, kar pomeni, da niso povsod dostopne (Meaning in drugi, 2018).

Tabela 1: Karakteristike CBDC in drugih sredstev, podobnih denarju

	CBDC	Rezerve	Bankovci CB	Vloge	Bitcoin	Ethereum
Obveznost CB	✓	✓	✓	✗	✗	✗
Elektronski	✓	?	✗	✓	✓	✓
Povsod dostopen	?	✗	✓	✓	✓	✓
Obrestonosen	?	?	✗	?	✗	✗
Izmenljiv 1:1*	?	✓	✓	✓	✗	✗
Kriptovaluta	?	✗	✗	✗	✓	✓
Žeton ali stanje na računu	?					

** z ostalimi obveznostmi CB, vključuje =* ✓ *, ne vključuje =* ✗*, izbirno =* ? *,*

stanje =  *, žeton =*  *;*

Vir: prirejeno po Meaning in drugi (2018).

CBDC je valuta na DLT in vpliva na finančno stabilnost, v tem pomenu je drugačna od zasebno izdanih kriptovalut, ki nimajo jasnega sistema upravljanja, pristojne institucije, pravnih okvirjev in so načeloma brez kritja. CBDC lahko izboljša dostopnost do digitalnih plačil potrošnikom, ki jim bančne storitve niso na voljo bodisi zaradi previsokih stroškov bančnih storitev ali prevelike oddaljenosti od ponudnikov. Pomanjkljiva digitalna pismenost je še vedno lahko ovira. Tudi nezanemarljiv del prebivalstva v visoko razvitih državah presenetljivo nima zadostne dostopnosti bančnih storitev.

Stroški upravljanja z gotovino na ravni Evropske unije (v nadaljevanju EU) znašajo 0,5 % BDP, CBDC je cenejši za upravljanje. V primerjavi z zanemarljivimi stroški hranjenja CBDC naj bi bili stroški gotovine kot hranilca vrednosti med 0,5 in 1 % njene vrednosti; med katere so šteti stroški hrambe, transporta, zavarovanja in varovanja. V nasprotju z bančnimi računi CBDC ne bi bil izpostavljen kreditnemu in likvidnostnemu tveganju. Ta prednost lahko prikrajša zasebne banke glavnega vira financiranja, ki v evroobmočju znaša 20 % njihovega financiranja in lahko negativno vpliva na ceno in ponudbo bančnih posojil. Prehod na CBDC lahko sproži prekomerno dvigovanje bančnih vlog (Agur in drugi, 2018). Manj vlog pri poslovnih bankah (v nadaljevanju PB) pomeni zmanjšanje tokov finančnih posojil, saj banke z vlogami financirajo svoja sredstva za posojanje, manjši obseg naložb in manjšo gospodarsko rast (Niepelt, 2018).

Gotovina se kot sredstvo izmenjuje na način P2P in izdajatelj ni seznanjen o transakcijah, je povsod dostopna, imetje je anonimno in nima obrestnega donosa. CBDC je alternativa za gotovino, ki je tudi P2P, vendar lahko vpelje spremembe na preostalih omenjenih področjih. Za delovanje veleprodajnih plačilnih sistemov s tehnologijo razpršene evidence namesto sedanjega sistema RTGS se lahko uvede CBDC, dostopen le bankam in drugim finančnim institucijam. Širša javnost ne bi imela dostopa do takšnega CBDC, ampak le izbrane institucije, in ne bi bil obrestonosen, sistem bi vzdrževal nominalne zneske računov. Čeprav ima CB v običajnem RTGS osrednjo vlogo, bi v tem modelu bila le še en igralec več, obdržala bi nadzor nad dostopom in zaračunavala vodenje računa.

Da bi CBDC lahko čim bolje nadomestil gotovino, bi moral prevzeti naslednje značilnosti: vseprisotnost, saj z gotovino lahko rokuje vsakdo, anonimnost, kajti uporabnik ni poznan, in ne bi bil obrestonosen. Za izdajanje, obtok in umik gotovine je potrebna draga infrastruktura, zato bi oblasti bile pripravljene zamenjati gotovino z digitalno različico. Denar se tudi s časom obrabi, umaže in je prenosljiv za bolezni ter s krajo in ponarejanjem prispeva h kriminalu. Digitalna različica bi bila bolj učinkovita, čistejša in varnejša.

CBDC lahko služi kot učinkovitejši instrument monetarne politike v bližini ničelne obrestne mere, t. i. ničelne spodnje meje, in lahko poseže v negativno obrestno mero. Takšen CBDC bi bil povsod dostopen, da doseže javnost in v končni fazi nadomesti bankovce v rabi, obrestonosen, da zajame koristi digitalnega denarja, ki jih prinaša pozitivna ali negativna obrestna mera, in anonimen, da je podoben gotovini.

V izogib bančnim krizam bi moral CBDC biti dostopen prebivalstvu na računih pri CB. Za njega bi bila potrebna identifikacija kot pri bančnih vlogah ter izjemoma obrestonosnost, kar je utemeljeno s predpostavko, da so bančne krize posledica delnih rezerv, saj so vloge posojilojemalcem na voljo na vpogled. S ponudbo vlog javnosti CB prekine povezavo med vlogami in posojili ter prepreči bančne krize (Agur in drugi, 2018). Če se CBDC uvede, bo na voljo skupaj z ostalimi plačilnimi sredstvi, vključno z gotovino. CBDC ima možne prednosti, kot je obrestni donos, vendar je lahko gotovina bolj zaželena zaradi anonimnosti pri transakcijah (Mohammad in Davoodalhosseini, 2018).

5.3 Brezgotovinska družba

Raba gotovine se vztrajno zmanjšuje zaradi enostavnosti plačil s karticami, aplikacijami in brezstično. Čeprav je malo verjetno, da bi CB umaknila gotovino iz plačilnega sistema, se nenaklonjenost do uporabe gotovine z negativnimi eksternalijami veča. Gotovina ne omogoča sledljivosti, kar lahko vodi do davčnih utaj, pranja denarja in nezakonitih transakcij. Gotovina predstavlja tudi večja tveganja pri njenem prevozu in pri plačilih, ker ni beležene izmenjave. V prihodnosti bi se lahko oblasti odločile za umik gotovine za zmanjšanje kriminala in povečanje davčnih prihodkov. Zaslužek od izdaje denarja bi se s CBDC povečal, saj bi bila količina celotnega denarja v obtoku večja, toda upravljanje gotovine in CBDC hkrati predstavlja tudi povečan administrativni strošek CB.

CBDC lahko izboljša učinkovitost in varnost plačilnih sistemov v splošnem obtoku, kot tudi za večje zneske. Na strani maloprodaje se razvija načine povečanja učinkovitosti plačil, npr. na plačilnih (angl. Point of Sale, POS) terminalih, na spletu in na način P2P. Uvedba veleprodajnega CBDC omogoča hitrejše poravnave in daljši delovni čas. CBDC lahko nadomesti denar z manjšo nominacijo s ponudbo digitalnega drobiža. Banka Koreje je aprila 2017 izvedla poizkus družbe brez kovancev, kjer so kupci lahko naložili drobiž na predplačniško kartico, namesto da bi ga sprejemali v fizični obliki. Izdelava kovancev jih je v letu 2016 stala okoli 43 milijonov evrov.

Brezgotovinska družba bi pomenila, da ne bi bilo razpoložljivih kovancev ali bankovcev in bi bil ves denar izmenjan v digitalni obliki. Trenutno ni predvidenega izvzema bankovcev in kovancev, toda z naraščanjem števila digitalnih transakcij in z upadanjem dviga gotovine z bankomatov se razviti svet bliža družbi z manj gotovine. Kriptovalute lahko vplivajo na obliko plačilnega sistema, zato je v interesu oblasti, da to področje nadzorujejo. Verodostojna rešitev bi bila digitalna valuta z jamstvom CB (Ward in Rochemont, 2019).

Čeprav ne obstaja povsem brezgotovinska družba, lahko preference potrošnikov, konkurenčni pritiski na podjetja, iskanje dobička bank in vladni ukrepi za spodbujanje brezgotovinskih transakcij pripeljejo k temu. Na Švedskem je le 15 % transakcij gotovinskih in predstavljajo le 1 % vrednosti BDP. Trgovci in gostinci se lahko odpovejo sprejemanju gotovine. Polovica bank ne posluje več z njo. Ponekod so banke za prehod v brezgotovinsko družbo uvedle vladne digitalne valute za nadomestitev kovancev in bankovcev. Zagovorniki

tega trdijo, da so takšne transakcije bolj praktične in da bi se zmanjšale kriminalne aktivnosti. K temu prehodu naj bi prispevala tudi digitalizacija družbe. Tudi banke prispevajo k temu z odstranitvijo bankomatov in poslovalnic. Tudi pandemija je prispevala k temu (Duignan, 2022).

Slabosti brezgotovinske družbe bi lahko bile (Duignan, 2022):

- izključevala bi posameznike, ki nimajo dostopa do bančnih računov,
- lahko bi dopuščala posege v zasebnost transakcij,
- tudi manjše tehnološke napake, vdori, naravne nesreče bi lahko onemogočili dostop do sredstev, plačila in nakupe,
- vlagatelji ne bi mogli dvigniti denarja v fizični obliki, da bi ga rešili. Tudi pri notranjem reševanju, kjer dolgove prevzamejo vlagatelji,
- vlagatelji se ne bi mogli izogniti negativnim obrestnim meram.

Maloprodajni CBDC je obveznost države, kar je velika prednost pred zasebno izdanimi digitalnimi valutami. Poslovni motiv ponudnikov zasebnega e-denarja, ki stremijo k maksimiziranju svojih dobičkov, ni v skladu z vlogo fiat valute. Vlade izplačujejo socialne transfere s fiat valuto, toda če bi imel zasebno izdan e-denar monopol, bi to povzročilo izgube pri prejemnikih iz naslova socialnega zavarovanja v primerjavi z ostalo družbo, bodisi zaradi menjalnega tečaja ali provizij pri menjavi (Ward in Rochemont, 2019).

Digitalni denar mora služiti kot zakonito plačilno sredstvo za vse plačilne transakcije. Prednost uradne valute je v ekonomijah obsega, torej večji ekonomičnosti zaradi razsežnosti uporabe, in mrežnih učinkih oziroma koristi zaradi splošne sprejetosti. Ena od možnih načinov plačila je digitalna valuta na elektronskem žetonu, analogna gotovini ali predplačniškim karticam z naloženim dobroimetjem.

Posamezniki in podjetja bi lahko imeli račune digitalne gotovine pri CB. V zgodovini bančništva so lahko nekatere fizične osebe imele račune pri CB Anglije. CB ne želijo izrivati poslovnih bank pri nudenju storitve hranjenja vlog, saj CB tudi nadzorujejo te iste banke. Tak način delovanja bi lahko ogrozil finančno stabilnost, npr. ob pričetku finančnih kriz bi komitenti začeli prenašati sredstva s PB na CB.

Digitalni denar bi bil vnesen v obtok prek namenskih računov pri nadzorovanih depozitnih institucijah, ki bi del sredstev hranile v rezervah pri CB. Tak pristop bi krepil konkurenco med ponudniki digitalne gotovine in zaščitil zasebnost posameznih transakcij ter lajšal primerno uveljavljanje zakonov. Mehanizem zagotavljanja digitalne gotovine bi bil podoben oskrbi z mnogimi drugimi javnimi dobrinami, kot so voda, elektrika ali javni prevoz.

Plačila na ta način potekajo naglo, varno in pri zanemarljivih stroških, na preprost način z bremenitvijo plačnikovega računa digitalne gotovine in dobropisom računa digitalne gotovine prejemnika plačila. Število goljufij pri transakcijah se zmanjša z enostavnimi metodami, kot je preverjanja identitete v dveh korakih. Posamezniki in podjetja bi morala

imeti možnost hranjenja sredstev v zasebnih finančnih institucijah in plačevati z zasebnimi oblikami plačil in fizičnim denarjem. Ko postane digitalna gotovina priročna in povsod dostopna, se povpraševanje po fizični valuti hitro zmanjša (Bordo in Levin, 2019).

CBDC stremi k temu, da postane s P2P-prenosom podoben gotovini, priročen za plačila v realnem času, obstojen in robusten v delovanju, zagotavlja zasebnost pri zakoniti izmenjavi, vsem dostopen ter omogoča čezmejna plačila (Auer in Böhme, 2020). Značilnosti CBDC bi torej bile, da ga CB izda v digitalni obliki, si ga ima vsakdo pravico lastiti, ni zgolj namenjen finančnim institucijam, je enaka valuta kot bankovci in depoziti CB, menjalni tečaj bankovcev in digitalne gotovine z ničelnimi obrestmi bi vedno bil ena na ena, uporabljalo bi se ga kot sredstvo pri maloprodajnih plačilih ter tretje strani ne bi bile vpletene v transakcijo, da preverijo in izvršijo plačilo (Grym in drugi, 2017).

V učinkovitem denarnem sistemu bi moral posrednik v menjavi služiti tudi vlogi varnega hranilca vrednosti, ki ima enako stopnjo donosa kot ostala netvegana sredstva. Drugače povedano, oportunitetni stroški hranjenja denarja bi morali biti enaki nič oz. opuščene alternative ne bi bile za to nič boljše ali slabše. Ta lastnost je ena od temeljnih razlogov za vpletenost javnega sektorja v ponudbo denarja, bodisi z izdajo centralnobančne valute ali pooblastila zasebno izdanemu denarju. Vsaka čisto zasebno izdana oblika denarja, ki je ne krije vlada, je predmet notranjega tveganja neizplačila in zato ne more služiti kot zanesljiv posrednik v menjavi ali stabilna obračunska enota. Fizični denar ni obrestonosen in je zato pomanjkljiv hranilec vrednosti v večini okoliščin. Pri stopnji inflacije 2 % se prava vrednost denarja oz. njegova kupna moč vztrajno znižuje. Izgube zaradi inflacije imajo enak učinek kot regresivni davek (glavarina), kjer plačajo večji delež dohodkov manj premožni, saj je fizična valuta predvsem v rabi družin s povprečnim dohodkom in malih podjetij, medtem ko premožni posamezniki in velike korporacije hranijo sredstva v skladih denarnega trga (vlagajo v nizkotvegane dolžniške vrednostne papirje), torej obrestonosnih računih z visoko likvidnostjo. Zvišanje inflacije situacijo zgolj poslabša.

Računi digitalne gotovine lahko imajo enak obrestni donos kot državne obveznice in postanejo varen hranilec vrednosti. Tako kot poteka izplačilo obresti za rezerve PB in izdaja obrestonosnih obveznosti širšemu naboru finančnih institucij s strani CB, tako so računi digitalne gotovine podobno umeščeni v sistem, PB prejmejo obresti na rezerve pri CB in izplačujejo obresti svojim vlagateljem.

V tem pogledu lahko služi obrestna mera na digitalni denar kot glavno orodje monetarne politike CB. Običajno bi bila obrestna mera pozitivna, v primeru resnih negativnih šokov pa bi CB lahko znižala obrestno mero digitalne gotovine pod ničlo in s tem spodbudila okrevanje gospodarstva ter ohranjala cenovno stabilnost. Zagotavljanje stabilne obračunske enote olajša ekonomske in finančne odločitve posameznikov in podjetij. Sistem digitalne gotovine bi se odzival s prilagajanjem obrestne mere. Možnost negativne obrestne mere pomeni, da CB nima prepričljive utemeljitve za pozitivno povprečno stopnjo inflacije. S tem

bi monetarna politika zagotavljala pravo cenovno stabilnost v skladu z indeksom cen življenjskih potrebščin (Bordo in Levin, 2019).

Da bi kriptovaluta CB ustrezala kriterijem plačilnega sredstva in hranilca vrednosti in z značilnostmi učinkovito vplivala na plačila, monetarno politiko in finančno stabilnost, mora imeti naslednje lastnosti, ki so zaradi večje preglednosti razporejene tudi v tabeli 2 (BIS, 2018):

1. Razpoložljivost oziroma dostop do digitalnih valut CB je omejen na delovne ure; manj kot 24 ur na dan in pet dni na teden. Po novem bi lahko bile dostopne neprestano ali tekom posebej določenih ur, kot je v času delovanja plačilnih sistemov za velike zneske.
2. Digitalne valute na žetonih lahko omogočajo različne stopnje anonimnosti, podobno kot pri zasebnih digitalnih žetonih. Po drugi strani lahko večja anonimnost napram CB privede do neizpolnjevanja zahtev o preprečevanju pranja denarja ali financiranja terorizma.
3. Transferni mehanizem za prenos denarja poteka na način P2P v primerjavi z vlogami, pri katerih je posrednik banka. Omenjene valute so lahko prenesene na oba načina.
4. Obrestni donos imajo vse digitalne obveznosti (v zagotavljanju dobrin in storitev v zameno za vrednost denarja) CB. V digitalni obliki je tehnično izvedljivo izplačevanje tako pozitivnih kot tudi negativnih obresti na žetonu ali pa stanju na računu. Z obrestno mero se da vplivati na povpraševanje po takšni valuti ali pa jo prilagoditi ključni obrestni meri CB. Njena raba je možna tako v vele kot maloprodajnem sistemu. Prav tako bi obrestna mera vplivala na njeno privlačnost kot posrednika v menjavi.
5. Omejitve: z zgornjo mejo oz. kapico na rabo ali hranjenje digitalne valute centralne banke (CBDC) se lahko upravlja možne neželene učinke ali namembnost njene uporabe. Z vpeljavo omejitve se naredi CBDC manj uporabno za veleprodajna plačila v primerjavi z maloprodajnimi.

Tabela 2: Ključne značilnosti oblik denarja centralnih bank

	Obstoječi denar CB		Digitalne valute centralnih bank (CBDC)		
	Gotovina	Rezerve in saldi poravnav	Maloprodajni		Veleprodajni
			Žeton	Račun	Žeton (izključno)
Stalna razpoložljivost	DA	NE	DA	IZBIRNO	IZBIRNO
Anonimnost do CB	DA	NE	IZBIRNO	NE	IZBIRNO
Medvrstniški (P2P) prenos	DA	NE	IZBIRNO	NE	IZBIRNO
Obrestonosnost	NE	IZBIRNO	IZBIRNO	IZBIRNO	IZBIRNO
Omejitve (kapica)	NE	NE	IZBIRNO	IZBIRNO	IZBIRNO

DA= obstoječa ali verjetna značilnost, IZBIRNO = možna značilnost, NE = ni tipična ali možna značilnost.

Vir: prirejeno po BIS (2018).

CBDC se bi približal značilnostim gotovine s P2P-prenosom, takojšnjo poravnavo, zasebnostjo, obstojnostjo, če infrastruktura zataji, in bi bil povsod dostopen. Za razliko od

gotovine se ga uporablja na internetu, tehnologija je varnejša pred krajo in nezakonito rabo. Lahko se jo naredi prilagodljivo novim oblikam elektronskih transakcij, kot sta plačilo med napravami (angl. Machine-to-Machine, M2M) ali internetu stvari. Na ta način ustreza vedno bolj digitaliziranemu okolju.

Sistem mora biti razširljiv in prilagojen razvoju dostopnih naprav (pametnih telefonov, pametnih ur, osebnih računalnikov, interneta stvari) za splošen dostop, kar vodi do večje finančne in digitalne vključenosti in obstojnosti. Gotovini primerljiv CBDC kljub tehnični izvedljivosti izplačila obresti nima predvidene obrestonosnosti. Večji izziv bi bil za dostopne naprave, ki ne bi bile povezane z omrežjem, ker bi se moral sistem ažurirati glede na tekoče obrestne mere v času transakcij. Nekaj morebitnih rešitev je še predmet raziskav.

Povečana varnost plačil in prilagodljivost naredita infrastrukturo CBDC izredno zanesljivo. V primeru izpada elektrike ali nedelovanja mobilnega omrežja lahko z neodvisnimi napravami s splošnim dostopom, digitalno denarnico za CBDC, doseže obstojnost. Obstojnost pred spletnimi napadi je še en pomemben vidik njenega delovanja. Izvedljivo je ustvariti denar z veliko mero zasebnosti pri plačilih in hkrati skladnostjo z zakonodajo, ki določa razkritje informacij, kot je izpolnjevanje zahteve proti pranju denarja. Doseči anonimnost na ravni gotovine bi vodilo do nezakonitih aktivnosti in ne bi bilo skladno s predpisi.

Interoperabilnost CBDC oziroma integracija z obstoječimi plačilnimi sistemi končnim uporabnikom omogoča medsistemske prenose; z njimi bi obstoječim sistemom bila omogočena nakazila s CBDC (BoC, 2020). Določitev namembnosti uporabe CBDC lahko razvrsti CBDC v dve kategoriji: na voljo širši javnosti oziroma potrošnikom kot maloprodajni CBDC ali omejen na poslovne banke in klirinške družbe kot veleprodajni CBDC.

Za maloprodajni CBDC je treba opredeliti najbolj učinkovit distribucijski mehanizem za razporejanje in shranjevanje za dosego njegovih programskih ciljev in čim večjo vključenost vseh upravičenih udeležencev. Določiti je treba, kje je CBDC hranjen, saj je lahko hranjen neposredno na računih pri CB, na računih pri sodelujočih PB, če delujejo kot posredniki za distribucijo, ali na debetnih karticah, izdanih s strani državnih organov.

Možnost obrestnega donosa CBDC s strani CB lahko vpliva na njegovo namembnost kot veleprodajnega ali v splošni rabi. Ta odločitev ima učinek na relativno privlačnost do lastništva CBDC. Pri maloprodaji to vpliva na to, ali imajo vlagatelji raje prihranke v CBDC pri CB ali običajne vloge pri poslovnih bankah. To v zameno vpliva na zneske in stabilnost vlog poslovnih bank, stanje PB na njihovem računu in aktivnost posojanja. Izplačila obresti na CBDC konkurirajo tistim v PB in izvajajo pritisk na dvig obrestnih izplačil poslovnih bank svojim vlagateljem. Za maloprodajni in veleprodajni CBDC morajo biti učinki na monetarno politiko, načrtni ali nenačrtni, temeljito proučeni.

Anonimnost transakcij bi spodbudila več potrošnikov k uporabi CBDC kot zasebne in P2P-alternative gotovini. Toda povračila transakcij, ki so posledice prevar, naredi bolj zahtevna, prav tako prepoznavanje nezakonitih aktivnosti in obnovitev izgubljenih sredstev. Če ima CB močne motive uporabiti CBDC proti pranju denarja, utaji davkov, za preganjanje korupcije ali za nadzor nad tokovi denarja in namene spremljanja, bo manj naklonjena omogočanju anonimnosti. Četudi CB ali država uvede CBDC, lahko vpleteni v nezakonito ali prikrito dejavnost za te namene še vedno nadaljujejo z uporabo gotovine in drugih alternativ, kot so kriptovalute, ki zagotavljajo zasebnost.

Zgornja meja na računu in pri transakcijah določa količino CBDC, ki je lahko v lasti ali prenesena v enem znesku po navodilih CB. Takšne omejitve lahko omilijo učinke vpeljave CBDC v sistem in tveganje pranja denarja. V okvirih maloprodajnega CBDC bi lahko CB omejila količino CBDC, ki jo lahko ima ali prenese državljan, da bi zmanjšala negativne posledice. Te vključujejo možnost prekomernega dvigovanja bančnih vlog ali nižje povpraševanje po bančnih vlogah, če državljani prepoznajo CBDC kot varnejšo obliko za hranjenje svojega denarja kot v vlogah PB. V okviri veleprodaje lahko CB omeji PB uporabo CBDC za plačila velikih vrednosti (World Economic Forum, 2019; v nadaljevanju WEF).

5.4 Veleprodajni plačilni sistemi z digitalnimi valutami centralnih bank

Veleprodajni CBDC na DLT je v fazi preverjanja koncepta. Obstoječi veleprodajni plačilni sistemi so pri koncu svojega tehnološkega cikla, v nesodobnih programskih jezikih in z dragim vzdrževanjem baz podatkov. Banka Kanade v projektu Jasper in Monetarni organ Singapurja v projektu Ubin preverjata sistem RTGS na platformi DLT. Plačila v sistemu RTGS so vsakodnevno obravnavana posamezno, v realnem času in s knjigovodsko dokončnostjo. Za razliko od maloprodajnih sistemov imajo veleprodajni sistemi dostop omejen na ožji krog uporabnikov. Potrjevanje transakcij z dokazom o delu, namenjeno preprečevanju dvojnega trošenja, kot je lahko v maloprodajnih sistemih, ni potrebno, saj CB razpolaga z bolj varčnim načinom zaupnega notarja, kjer izbrana skupina vozlišč potrjuje transakcije.

Ključni izziv pri uporabi kateregakoli CBDC je, kako prenesti denar CB na razpršeno evidenco. Tako Jasper kot Ubin uporabljata t. i. digitalno potrdilo o depozitu (angl. Digital Depositary Receipt, v nadaljevanju DDR), ki je zahtevek za rezerve, na podlagi katerih CB izda digitalne žetone na razpršeni evidenci. Projekt Jasper uvaja tudi mehanizem za varčevanje z likvidnostjo (angl. Liquidity-Saving Mechanism, v nadaljevanju LSM) oz. mehanizem pobota na platformi DLT (združevanje naročil in transakcij več tržnih udeležencev v eno transakcijo). Oba projekta dokazujeta, da so transakcije na razpršeni evidenci lahko izvedene v realnem času (Bech in Garratt, 2017).

Doprinos DLT pri plačilih, ugotovljen v projektu Jasper, je (PC in drugi, 2017):

- učinkovitejša obdelava administrativnih plačil in boljša usklajenost znotraj in med finančnimi institucijami (v nadaljevanju FI),
- manjša verjetnost dragih napak in sporov med udeleženimi FI,
- morebitne izboljšave pri prepoznavanju sankcioniranih subjektov in zagotavljanju jasnih in doslednih revizijskih sledi finančnih transakcij,
- ohranjanje transparentnosti sistema in boljši nadzor za CB in regulatorje,
- ohranjanje informacijske zasebnosti med FI,
- izboljšana avtomatizacija z uporabo pametnih pogodb.

Payments Canada, upravljalec kanadskih plačilnih sistemov, je v začetku leta 2016 v sodelovanju z Banko Kanade, konzorcijem za finančne inovacije R3 in nekaterimi glavnimi kanadskimi bankami pričel s projektom Jasper s ciljem raziskovanja uporabe DLT za poravnavo medbančnih plačil. S tem je CB prvič sodelovala v DLT-poskusu z zasebnimi finančnimi institucijami.

Cilj prve faze projekta je bil vzpostavitev veleprodajnih sistemov medbančne poravnave na Ethereum DLT-platformi in preverba njegovih zmožnosti izmenjave vrednosti v obliki CB digitalnih poravnalnih sredstev. Sredstvo poravnave je bilo digitalno depozitno potrdilo, ki je odražalo zahtevek do kanadskodolarskih vlog na računih Banke Kanade. Le banke, udeležene v projektu Jasper, so lahko nakazovale z uporabo DDR. Potrebni so bili tudi postopki za jamčenje kanadskih dolarjev v zameno za DDR in obratno, to je pomenilo možnost unovčitve DDR v zameno za kanadske dolarje.

V drugi fazi projekta, septembra 2016, se je prešlo z Ethereum DLT na platformo R3, imenovano Corda. Vpeljan je bil koncept vozlišča zaupnega notarja kot osrednjega dela konsenznega protokola. Platforma omogoča atomske transakcije in mehanizem za varčevanje z likvidnostjo. Osrednji element LSM je čakalna vrsta z algoritmom za sprotno poravnavo sklopov plačil, kot si sledijo po vrsti na njihovi neto osnovi. Poboti spodbujajo učinkovito financiranje in omogočajo tekoče delovanje dnevnih plačil (PC in drugi, 2017).

V tretji fazi projekta Jasper se je razširilo preverjanje koncepta druge faze z od konca do konca integriranim procesom poravnave vrednostnih papirjev. Namen je bil doseči takojšen obračun in poravnavo dostave proti plačilu (angl. Delivery versus Payment, v nadaljevanju DvP) in s tem dokazati možnost opravljanja poprodajne poravnave oz. DvP in prenosa lastništva delnic na platformi DLT. Zmožnost takojšnje poravnave transakcij bistveno zmanjša tveganje nasprotne strani, kjer ena stran ne izpolni svoje obveznosti, in sprosti kritje. Payments Canada, operater kanadskega sistema velikih plačilnih transakcij (angl. Large Value Transfer System, LVTS), posodablja kanadski plačilni sistem, Banka Kanade podpira ta podvig. Takšni plačilni sistemi lahko izboljšajo plačilno aktivnost Kanadčanov, kot tudi zavarujejo in naredijo kanadski finančni sistem bolj učinkovit (BoC, Boe & MAS, 2018).

Monetarni organ Singapurja (angl. Monetary Authority of Singapore, v nadaljevanju MAS) je v sodelovanju s tehnološkim podjetjem R3, ki se ukvarja s tehnologijo verige blokov, in z neimenovanim konzorcijem največjih svetovnih finančnih institucij novembra 2016 preveril koncept poenostavitve medbančnih plačil. Skupni projekt, poimenovan Ubin, je temeljil na singapurskem dolarju (v nadaljevanju SGD) na evidenci kot žetonu. Projekt je bil simbolno poimenovan Ubin po singapurskem otoku, ki je razpolagal z zalogami granita za tlakovanje nasipa med otoškim Singapurjem in celinskim Johorjem in nudil temelj za bilateralno trgovanje in sodelovanje. Na prispodoben način projekt Ubin združuje igralce industrij v prizadevanju za skupno ustvarjanje prihodnosti poslovanja in načina življenja ljudi s tehnološkimi inovacijami. Cilji projekta so: varnejša in učinkovitejša singapurska finančna industrija z zmanjšanimi tveganji in stroški doma in v mednarodnem okolju. Omogočanje singapurskemu finančnemu ekosistemu (tj. sistemu finančnih trgov, sistemov in institucij) globalne konkurenčne prednosti. Proučevanje priložnosti DLT za igralce v industriji ter spreminjanje in razvoj njihovih vlog. Projekt Ubin naslavlja vprašanja v šestih različnih fazah, ki potekajo po vnaprej predvideni časovnici (Deloitte in drugi, 2018):

1. Digitalizacija singapurskega dolarja: V tej fazi MAS in R3 raziskujeta uporabo CBDC oz. žetonirano različico SGD za medbančna plačila.
2. Notranja medbančna nakazila: V tej fazi MAS in Združenje bank Singapurja (angl. Association of Banks Singapore, ABS) raziskujeta medbančna nakazila na DLT in proučujeta nekatere funkcionalnosti RTGS, kot sta razvrščanje transakcij po prioriteti in reševanje zastojev plačil.
3. Dostava proti plačilu na DLT: V tej fazi MAS in singapurska borza (angl. Singapore Exchange, SGX) sodelujeta pri doseganju domače DvP-poravnave na dveh ločenih platformah verige blokov.
4. Plačilo proti plačilu (angl. Payment versus Payment, v nadaljevanju PvP) za čezmejne poravnave: V tej fazi je cilj oceniti izvedljivost čezmejne DvP.
5. Delujoči model: Cilj je oceniti vpliv DLT na obstoječe zakonodajne okvire in tržne procese.
6. Čezmejno DvP in PvP: Cilj je uporabiti zbrane ugotovitve za izvedbo čezmejnih poravnav tako plačil kot vrednostnih papirjev.

Sodelovanje med CB Singapurja in Kanade, ob podpori JP Morgan in tehnološkega podjetja Accenture, v projektu Jasper-Ubin je uspešno dokazalo zmožnost poravnave žetoniranih digitalnih valut med različnima platformama verige podatkovnih blokov. Izvedene so bile atomske plačilne transakcije, kjer so vse opravljene naenkrat ali pa nobena, med kanadskim dolarjem in singapurskim dolarjem, in to med dvema različnima DLT-platformama, kjer izmenjava poteka z »zgoščeno časovno zaklenjeno pogodbo« (angl. Hash Time Locked Contracts, v nadaljevanju HTLC), tj. pametno pogodbo, s katero se transakcija izvede vzajemno. Pogoji za izvedbo običajno vključujejo zagotovitev kriptografske funkcije razpršitve, ki jo mora prejemnik dešifrirati, da odklene transakcijo. Časovno zaklenjeni vidik HTLC zagotavlja, da se transakcija izvede le v določenem časovnem intervalu. Bolj preprosto povedano, za izvršitev transakcije je potreben heš in določen čas, izvede se zunaj

verige bloka. Projekt izhaja iz tega, da RTGS na DLT-sistemih temelji na različnih platformah v vsaki državi, v tem primeru na Cordi v Kanadi in na Quorumu v Singapurju. Na ta način je bila uspešno izpeljana čezmejna atomska transakcija med valutama in platformama (BoC in Monetary Authority of Singapore, 2019; v nadaljevanju BoC in MAS).

5.5 Maloprodajni plačilni sistemi z digitalnimi valutami centralnih bank

Maloprodajni CBDC, takšen, namenjen splošni rabi, je obstoječ kot stanje na računu ali kot sredstvo na elektronskem žetonu. Prva oblika je digitalni CBDC, podoben veleprodajnemu, vendar dostopen širši javnosti. Njegov izdajatelj je CB ali za to pooblaščeni subjekt in je pristojen za njegovo izdajanje, distribucijo, shranjevanje in vzdrževanje. Izdaja CBDC za splošno rabo omogoča širši javnosti neposredni dostop do računov pri CB. Uporabnik lahko do CBDC dostopa prek mobilne aplikacije (e-denarnice) ali drugih mehanizmov. Vele- in maloprodajni CBDC kot stanje na računu nimata lastnosti anonimnosti, kot jo ima gotovina pri transakcijah, saj mora uporabnik biti predhodno prijavljen, preverjen in odobren s strani CB, preden lahko ima odprt račun za maloprodajni CBDC pri njej.

Maloprodajni CBDC-žeton je podoben gotovini in je dostopen širši javnosti. Ključne razlike med maloprodajnim CBDC na računu in žetonih so v tem, kako je ustvarjen, distribuiran, shranjen in prenesen. Maloprodajni CBDC izda CB in ga lahko razporedi med poslovne banke (v nadaljevanju PB) ali druge pooblaščene finančne institucije za nadaljnji prenos na širšo javnost, ki nato shrani CBDC lokalno na kartici, mobilni aplikaciji (denarnici) ali na drugih nosilcih, podobnih trenutni vpeljavi denarja v finančni tehnologiji (FinTeh), kot je dobroimetje na mobilnem telefonu. Še več, anonimnost je dodatna pomembna lastnost, ki razlikuje obe obliki CBDC (Opare in Kim, 2020).

Pomanjkljivosti, povezane z rastjo kriptovalut v zasebnem sektorju, so lahko razlog za razvoj maloprodajnega CBDC. Od prihoda BTC v letu 2009 so naložbe v zasebne kriptovalute hitro narasle. Njihova uporaba za namene plačil ostaja skromna, saj pretirana volatilnost cen ponuja izziv njihovi uporabnosti kot stabilnemu plačilnemu sredstvu. Računalniško intenziven proces za ustvarjanje kriptovalut povzroča ogromno okoljsko breme. Rudarjenje za BTC je v letu 2018 po porabi moči primerljivo električni porabi celotne države Singapur. Lastništvo kriptovalut in njihova uporaba sta anonimna, saj so lahko računi ustvarjeni pod umetno ustvarjenimi imeni, zato nastopijo pomisleki glede zahtev AML in CFT. Kriptovalute se soočajo s težavo v razširljivosti, ker je vsaka transakcija, zabeležena v evidenci, poslana vsem uporabnikom v sistemu, kar vodi v omrežje z eksponentno rastjo števila beleženih transakcij. Če bodo v prihodnje zasebne kriptovalute postale pomemben del plačilnega sistema, bi to imelo podoben učinek odpovedi lastni valuti kot pri t. i. dolarizaciji gospodarstva, kar pomeni izgubo nadzora nad monetarno politiko. Nekaj držav je pričelo z omejevanjem in prepovedjo zasebnih kriptovalut, večina jih ohranja nevtralni ali omejeni nadzor nad njimi. Motiv CB za razvoj maloprodajnega CBDC je lahko zmanjšanje povpraševanja po zasebnih kriptovalutah (Agur in drugi, 2018).

Interes za koncept maloprodajnega CBDC izražajo CB in akademska sfera. Morda je najbolj v teh krogih prepoznaven fedcoin. FED naj bi ustvaril kriptovaluto, podobno BTC. Za razliko od BTC, bi samo FED imel možnost ustvarjati fedcoin in zamenljivost z gotovino in rezervami bi bila v pariteti, torej izenačena ena na ena. Fedcoini bi bili ustvarjeni ali izničeni le v primeru, da bi enaka vsota gotovine ali rezerv bila vpeljana ali odvzeta. Fedcoin bi bil kot gotovina decentraliziran pri transakcijah in centraliziran v ponudbi. Švedska CB Riksbank med prvimi dopušča možno lastno izdajo maloprodajnega CBDC (Bech in Garratt, 2017).

Maloprodajni CBDC lahko nudi vlogo skoraj brezplačnega posrednika v menjavi, stabilno obračunsko enoto in varnega hranilca vrednosti ter ohrani zaupanje, saj za njega jamči država. Nekdanja Facebookova Libra, zasebno izdani stabilni kovanec, je oživela razpravo o CBDC. CB se odzivajo na realnost tako javnih kot zasebnih digitalnih valut, ki postajajo del globalnega monetarnega sistema, v njihovem interesu je, da ne nazadujejo ali pa niso izrinjene.

Nekdanji Facebook, sedaj Meta, je junija 2019 pod vodstvom tedanjega podpredsednika Davida Marcusa napovedal izdajo digitalne valute libra, razvijalci so cilj opredelili kot »omogočitev preproste globalne valute in finančne infrastrukture za opolnomočenje ljudi«. Vrednost kovanca bi bila krita iz rezerv realnih sredstev, ki bi bila sestavljena iz košarice bančnih vlog in kratkoročnih državnih vrednostnih papirjev. Košarica valut, na katero bi bila vezana vrednost libre, bi bila podobna posebnim pravicam črpanja, košarici petih glavnih svetovnih rezervnih valut Mednarodnega denarnega sklada (IBM in OMFIF, 2019). Konec leta 2020 je bil projekt preimenovan v Diem.

V letu 2022 je banka Silvergate odkupila sredstva projekta Diem, s čimer se je zadeva zaustavila. Projekt bi spodbujal finančno vključenost, brezplačne P2P-transakcije in cenejše stroške spletnih nakupov. Kovanec bi imel nižjo volatilnost kot npr. BTC, saj bi bil vezan na košarico mednarodnih valut. Upravljanje bi bilo centralizirano, kar bi po mnenju razvijalcev povečalo njegovo učinkovitost in razširljivost. CB ne bi mogle vplivati na monetarno politiko prek denarnih agregatov, zato so nasprotovale takšnemu projektu. Diem bi zahteval tudi preveritev identitete uporabnikov in izpolnjeval zahteve proti pranju denarja (Crosman, 2022).

Razlog, da je švedska CB omenila možnost izdaje digitalne oblike denarja, namenjene širši javnosti, oziroma e-krone, je, da vedno manj Švedov uporablja gotovino, predvsem zaradi hitre digitalizacije družbe, ki prav tako vpliva na načine plačevanja. Marca 2017 se je izvršilni odbor Riksbanke odločil pričeti s projektom e-krone, ki je proučeval obseg izdaje e-krone kot komplementa gotovini. Gotovina je državni denar v fizični obliki, v nasprotju z zasebno izdanim digitalnim denarjem PB, ki ga širša javnost uporablja za opravljanje plačil. Projekt e-krone proučuje učinkovitost trga zasebnih plačilnih sistemov, blažitev možnih težav brezgotovinske družbe z državnim digitalnim denarjem in učinke e-krone na finančni sistem (Soederberg, 2019).

E-krona lahko postane novodobna krona v elektronski obliki kot dopolnilo fizični gotovini. Javnost bi lahko še vedno imela dostop do centralnobančnega denarja. E-krona bi lahko omogočala tudi delovanje plačil v kriznih obdobjih, česar se od zasebnega sektorja ne da pričakovati. V izrednih razmerah, ko zasebni plačilni sistemi lahko zatajijo, bi e-krona delovala kot alternativni sistem in tako v celoti povečala stabilnost plačilnega sistema ter ga naredila bolj varnega in učinkovitega.

Ponudnikom plačilnih storitev bi omogočila konkurenčno infrastrukturo. To bi koristilo inovacijam in zniževanju provizij. Opiše se jo lahko kot švedsko krono, ki se jo lahko hrani na računu pri Riksbanki ali pa je shranjena lokalno, npr. na kartici ali v mobilni aplikaciji. Oba tipa e-krone imata v ozadju evidenco za beleženje transakcij in lastniških pravic digitalne krone, kar naredi transakcije e-krone sledljive.

Za uporabo e-krone pri spletnih nakupih ali v fizičnih trgovinah bi platforma s temeljno evidenco e-krone morala biti interoperabilna s številnimi drugimi sistemi in subjekti. Banke in druga podjetja morajo biti zmožna pridružitve platformi, da bi lahko razvijala in ponujala plačilne storitve gospodinjstvom in podjetjem. Nujna sta sistem za preprečevanje pranja denarja in sistem za poravnave e-krone med platformami.

V formalnopravnem smislu je e-krona na žetonu opredeljena kot elektronski denar, medtem ko je e-krona na računu podobna bančni vlogi. E-krona je lahko v obtoku na enak način kot gotovina in z njo bi razpolagala gospodinjstva in podjetja ne glede na lokacijo. Odprtje računa e-krone je lahko pod enakimi pogoji kot pri odprtju računa pri zasebni banki. Za Riksbank je vpeljava e-krone v skladu s spodbujanjem varnega in učinkovitega plačilnega sistema. E-krona na žetonu je že v skladu z zakonodajo banke, toda e-krona na računu še nima opredeljenih jasnih nalog Riksbanke (Sveriges Riksbank, 2018).

5.6 Angažiranost centralnih bank pri vpeljavi tehnologije razpršene evidence v plačilne sisteme

Na podlagi poročila Banke za mednarodne poravnave, objavljenega januarja 2019, je bilo v teku raziskovanje in preverjanje delovanja CBDC pri 40 centralnih bankah. Uporaba tehnologije razpršene evidence predvsem za CBDC je pritegnila pozornost CB zaradi potenciala, ki ga ima pri naslavljanju dolgotrajnih izzivov, kot so finančna vključenost, plačilna učinkovitost ter operativna in internetna obstojnost plačilnega sistema. CB proučujejo več primerov uporabe razpršene evidence, da bi našle nove možnosti uporabe in izboljšale neučinkovite procese.

CB se razlikujejo po izraženem zanimanju in motivaciji za raziskovanje in preizkušanje te tehnologije. Nekatere banke so napredne in so pričele s proučevanjem te tehnologije že v letu 2014, izvedle so več pilotnih projektov in jo celo ponekod uvedle. Druga skupina institucij izkazuje zanimanje za to tehnologijo na način, da raje obširno spremlja dejavnost sorodnih institucij v zasebnem sektorju, vključno z naložbeno aktivnostjo v kriptovalute.

Zadnja skupina še ni namenila virov za raziskovanje DLT in nima tega namena bodisi zaradi drugih prioritet ali zaradi mnenja, da DLT v tej fazi ne ponuja dovolj prednosti z upoštevanjem tehnološke nezrelosti in tveganj.

Do sedaj še ni bilo opravljene zanesljive in temeljite kvantitativne analize učinkov CBDC ali drugih načinov vpeljave DLT v gospodarstvo. To dejstvo lahko predstavlja oviro za sprejetost pri snovalcih politik. Nekaj raziskav je vneslo obstoječe modele, da bi ocenile, kako CBDC deluje na BDP ali blaginjo v državi. Po izsledkih člankov avtorji sklenejo, da imajo obstoječi modeli omejene zmožnosti pri ocenjevanju posledic glede na zapletenost okoliščin (WEF, 2019).

Odbor za plačila in tržno infrastrukturo (angl. Committee on Payments and Market Infrastructures, CPMI) pri Banki za mednarodne poravnave (angl. Bank for International Settlements, v nadaljevanju BIS) je v 2018 izvêdel raziskavo, kjer je sodelovalo 63 CB, ki zajemajo 80 % pravosodij, o vpeljavi CBDC. Od tega 41 v tržnih gospodarstvih v vzponu in 22 v razvitih, ki tudi pokrivajo 80 % svetovnega prebivalstva in preko 90 % svetovne proizvodnje. Okoli 70 % vprašanih subjektov se ukvarja z obravnavo CBDC, kar je rahlo v porastu v primerjavi s predhodnim letom. Ostali so načeloma iz manjših držav ali pa imajo druge prednostne naloge. Nekatere CB se zanašajo na raziskave, izvedene s strani mednarodnih organizacij (še posebej BIS) ali regionalnih mrež, kot je Svetovalno-delovna skupina za finančno tehnologijo v Karibski skupnosti (angl. Caribbean Community, CARICOM). Od angažiranih CB jih polovica pokriva tako CBDC za splošno rabo kot veleprodajnega, okoli tretjina se jih osredotoča zgolj na prvega in okoli osmina zgolj na drugega. Vse CB so pričele delo, povezano s CBDC, s teoretičnimi in konceptualnimi raziskavami in si načeloma delijo svoje študije z namenom splošnega razumevanja področja dela. Polovica jih je prešla v fazo preizkušanja oz. preverjanja koncepta v praksi, kar predstavlja povečanje za 15 odstotnih točk v letu 2017.

Veliko CB tako v razvitih kot tudi tržnih gospodarstvih v vzponu poskuša ustvariti veleprodajni plačilni sistem z razpršeno evidenco, sem spadajo projekti, kot so kanadski Jasper, singapurski Ubin ali pa južnoafriški Khokha. Le pet CB je do 2019 izvedlo maloprodajne pilotne projekte, kot so e-peso ali e-krona, ki so trenutno le raziskovalne narave. Vedno več je sodelovanja med CB za preverjanje konceptov čezmejnih plačil in dogovorov o poravnavi vrednostnih papirjev, kot sta projekt Stella v sodelovanju med Evropo in Japonsko ter samostojni skupni projekt Kanade, Anglije in Singapurja.

Kot razloge za delo na tem področju so razvrstile že predpostavljene od bolj do manj pomembnega. Med motivi v ospredju za malo- in veleprodajni CBDC sta bili varnost plačil in plačilna učinkovitost znotraj države, kot najmanj pomembna razloga so presenetljivo za maloprodajnega navedle čezmejno plačilno učinkovitost, za veleprodajnega pa finančno vključenost. Na podlagi gospodarske razvitosti vprašanih sta tistim v vzponu najbolj pomembna razloga plačilna učinkovitost in finančna vključenost, najmanj pa čezmejna

plačilna učinkovitost. Za razvita gospodarstva pa sta varnost plačil in finančna stabilnost najpomembnejša, finančna vključenost pa najmanj pomembna.

CB gospodarstev v vzponu navajajo, da so podpiranje digitalizacije, vzpostavitev neformalne ekonomije in boj proti finančnemu kriminalu eni od glavnih razlogov za uvajanje CBDC. Nekatera napredna gospodarstva mika manj gotovine v obtoku ali celo brezgotovinska družba. Na kratki rok, v obdobju do treh let, 85 % CB ni imelo predvidene izdaje kateregakoli tipa CBDC. Nobena ni imela predvidene uvedbe veleprodajnega CBDC, dve od gospodarstev v vzponu pa sta imeli predvideno uvedbo splošnega CBDC v tem obdobju. Srednjeročno, v obdobju do šestih let, je imela le ena banka predvideno izdajo veleprodajnega CBDC. Verjetnost izdaje obeh tipov CBDC v prihodnje je enaka ne glede na to, da ima CBDC za splošno rabo navidezno večjo operativno zapletenost in večji učinek na gospodarstvo.

Predpogoj za izdajo CBDC je, da je CB pooblaščena zanj. Četrtina CB ima ali pa bo kmalu zadolžena za izdajo CBDC, medtem ko jih ena tretjina ni in pri četrtini še ni jasno, ali sploh kdaj bo. Velika negotovost ni nenavadna, kajti naloge CB izhajajo še iz časov pred pojavom kakršnihkoli elektronskih sistemov, kaj šele kriptovalut. Kljub temu se s seznanjanjem z omenjenim področjem negotovost v zvezi z njegovo izdajo zmanjšuje (Barontini in Holden, 2019).

6 IZVEDBA EMPIRIČNEGA DELA O TEHNOLOGIJI RAZPRŠENE EVIDENCE V PLAČILNIH SISTEMIH

6.1 Metodologija raziskave

V obravnavo uvajanja tehnologije razpršene evidence v bančni sistem in z njo povezanih plačil, obračunov in poravnav sem zajel CB in PB. Uporabil sem kvalitativno metodo znanstvenega raziskovanja, natančneje dva delno strukturirana intervjuja s predstavnikoma CB Norveške in mednarodnega konzorcija PB Fnality, in ankete odprtega tipa s predstavniki CB Hondurasa, Kolumbije, Poljske, Slovaške, dvema iz Švedske in Španije. Raziskava je bila izvedena v prvi polovici leta 2021.

Odprta vprašanja respondente vodijo v razpravo o naslednjih področnih tematikah, zato respondente sprašujem o:

- prednostih tehnologije razpršene evidence (angl. Distributed Ledger Technology, DLT) pri plačilih, obračunih in poravnavah (angl. Payments, Clearing and Settlement, PCS);
- izzivih in tveganjih DLT pri PCS. Za argumentiranje stališč o DLT pri PCS sem izhajal iz del Kuhn in drugi (2019) in Hodrick (2018). Ward in Rochemont (2019) izpostavljata CBDC kot protiutež kriptovalutam;

- nadaljnjem razvoju in časovni opredelitvi faz vpeljave DLT pri PCS. Projekta, kot sta Jasper po PC in drugi (2017) in Ubin po Deloitte in drugi (2018), sta se razvijala v več fazah, zato predvidim vprašanje o vpeljavi DLT v PCS na primerljiv način;
- opredelitvi vloge malo- in veleprodajne digitalne valute (CBDC) pri PCS. BIS (2018) opredeljuje dve obliki CBDC in njuno posledično vlogo v PCS. Shin (2018) še bolj podrobno izpostavlja pomen CBDC za delovanje plačilnega sistema;
- pomenu žetonov in pametnih pogodb pri PCS. Žetone na verigi blokov omenjajo Rauchs in drugi (2018) kot strukturo podatkov. Po Mathis (2016) programirljivost DLT dopušča tudi pametne pogodbe.

Nezavezujoč del vprašalnika poizveduje po:

- področjih uporabe DLT znotraj bančništva zunaj PCS. V plačilnih sistemih so še zaledni sistemi, v katerih se lahko uporabi DLT, kot trdijo Ali in drugi (2014), so plačilni sistemi povezani z denarnim sistemom.
- najbolj primernih zvrsteh tehnologije DLT in konsenznega mehanizma pri PCS in utemeljitvi zakaj. Med glavna konsenzna mehanizma, ki se navezujeta na verigo blokov, po Cline in drugi (2016) spadata dokaz o delu in dokaz o deležu.
- glavnih konzorcijih, platformah in infrastrukturah v rabi pri razvoju DLT pri PCS. Prej omenjena Jasper in Ubin sta delovala na platformah Corda in Quorum (BoC in MAS (2019).

Primarne vire sem ovrednotil tudi s sekundarnimi s komparacijo in sintezo. K raziskavi so bile vabljene vse CB, sedem jih je sodelovalo v raziskavi, nadaljnjih šest, Švica, Japonska, Evropska centralna banka (ECB), Hrvaška, Bolgarija in Slovenija, mi je posredovalo povezave do gradiv. S predstavnikom CB Sejšelov se dogovori o intervjuju niso udejanjili. Odzvali so se tudi iz CB Združenega kraljestva, Danske, Salomonovih otokov, Kirgizije, Indije, Estonije in Brunejev, vendar do sodelovanja ni prišlo zaradi drugih njihovih obveznosti, presežka formalnosti ali odlašanja. V stik sem stopil tudi s Payments Canada, ki omogoča transakcije velikih vrednosti med tamkajšnjimi finančnimi institucijami, predlagali so mi dodatno gradivo. Tudi iz BIS so mi ponudili povezave do gradiv. V sektorju poslovnih in investicijskih bank je bilo težavno pridobiti prave elektronske naslove zadevnih bank. Posledično je ponudnik e-poštnih storitev avtomatsko preusmeril mojo elektronsko pošto med vsiljeno pošto, saj sem pošiljal ogromno število sporočil na nepreverjene naslove. Od nekaj 100 poslanih elektronskih sporočil sem imel le zanemarljiv odziv. Dobil pa sem sogovornika iz banke ING iz Amsterdama, zadolženega za mednarodno blockchain iniciativo za plačila, imenovano Fnality, pri njihovi banki, in se sestal z njim prek videoklica prek aplikacije Zoom. Pri banki Nordea iz Helsinkov in Banki Monte dei Paschi iz Siene sem imel kontaktni osebi pripravljeni sodelovati v intervjuju, toda ga kljub temu nisem uspel izvesti, saj se nismo uspeli časovno uskladiti. Pogovora in prispevki k tematskim vprašanjem so bili opravljeni v prvi polovici leta 2021.

6.2 Respondenti

V raziskavi so s pisnimi odgovori ali pogovorom prek videopovezave sodelovali predstavniki CB (1) Hondurasa, (2) Kolumbije, (3) Poljske, (4) Slovaške, (5) Švedske, (6) Španije in (7) Norveške ter zasebnega konzorcija finančnih institucij z (8) Nizozemske. V nadaljevanju so zapisani njihovi odzivi, kjer se na njih sklicujem s CB, kratico države in zaporedno številko ustrezne priloge. Na konzorcij Fnality se sklicujem z okrajšavo FN in številko priloge. Njihovi odzivi so v prilogah v istem zaporedju, kot so navedeni v tabeli 3.

Tabela 3: Sodelujoče centralne banke in konzorcij finančnih institucij

Institucija, respondent, položaj, kontakt	**Oznaka za sklic**
BANCO CENTRAL DE HONDURAS Edas Encarnación Lazo Mercado *Vodja oddelka za informiranje javnosti / Sektor za institucionalne odnose* transparencia@bch.hn	CB-HN-1
BANCO DE LA REPÚBLICA COLOMBIA Fabio Mauricio Pinzón Gonzáles *Generalni direktor za upravljanje s tehnologijo* fpinzogo@banrep.gov.co	CB-CO-2
NARODOWY BANK POLSKI Anna Wójcicka *Svetovalka – Oddelek plačilnih sistemov* anna.wojcicka@nbp.pl	CB-PL-3
NÁRODNÁ BANKA SLOVENSKA Oddelek za komuniciranje info@nbs.sk	CB-SK-4
SVERIGES RIKSBANK dr. Björn Segendorf *Višji svetovalec, Oddelek za plačila, Sektor za analize in politiko delovanja* bjorn.segendorff@riksbank.se in David Lööv *Ekonomist, Generalni sekretariat, Oddelek za pilotni projekt E-krone* david.loov@riksbank.se	CB-SE-5
BANCO DE ESPAÑA Tajništvo *Vršilec dolžnosti generalnega direktorja za finančne inovacije in tržno infrastrukturo, Carlos Conesa Lareo* dga.fimi@bde.es	CB-ES-6
NORGES BANK Peder Østbye *Posebni svetovalec* peder.ostbye@norges-bank.no	CB-NO-7
ING (INTERNATIONALE NEDERLANDEN GROEP) Jan Lebbe *Vodja konzorcija mednarodnih plačil na verigi blokov pri ING* jan.lebbe@ing.com	FN-8

Vir: lastno delo.

7 ANALIZA MNENJ STROKE O TEHNOLOGIJI RAZPRŠENE EVIDENCE V PLAČILNIH SISTEMIH

7.1 Vpeljava tehnologije razpršene evidence

Od svojih sogovornikov iz CB sem uspel izvedeti, da so v različnih fazah preverjanja koncepta ali pa se neposredno sploh ne ukvarjajo z raziskavami pri vnosu DLT v plačilne sisteme.

CB-HN-1 ni obravnavala ne malo- ne veleprodajne CBDC, prav tako je nima v sistemu. Tudi CB-PL-3 (polj. Narodowy Bank Polski, v nadaljevanju NBP) nima na voljo dovolj informacij, ki bi jih lahko delila z mano, saj je razširjenost uporabe DLT v sistemih PCS na Poljskem zanemarljiva. Uporabnih izkušenj s CBDC ne morejo predstaviti, saj niso izvajali poskusov, kajti uprava NBP v tem času ni izrazila naklonjenosti še njegovi možni uporabi. Uporabljale pa so ga druge institucije na Poljskem, kot je Centralno depotna družba vrednostnih papirjev (polj. Krajowy Depozyt Papierów Wartościowych, KDPW), ki uporablja DLT za elektronsko glasovanje, da vlagateljem na srečanjih delničarjev javnih podjetij omogoči glasovanje na daljavo. Prav tako se tehnologija uporablja za evidentiranje zapisnikov glavnih srečanj (oddanih dokumentov in glasov) kot javno nespremenljivo evidenco. Na Poljskem se DLT v financah uporablja kot trajni nosilec podatkov, ki služi preverjanju pristnosti dokumentov, izmenjanih med finančnimi institucijami in strankami, s časovnim žigom. Največja banka na Poljskem (PKO Bank Polski) skupaj s klirinško hišo (polj. Krajowa Izba Rozliczeniowa, KIR) vpeljuje omenjeni sistem. Dokumenti zajemajo pogodbe in cenike bančnih storitev in so hranjeni v sistemu DLT v oblaku.

Na CB-SK-4 so omenili, da v evrosistemu spremljajo napredek na področju DLT in da je Kitajska eden od pionirjev testiranja DLT za CBDC. Razpravljalo tudi o projektu Diem (nekdanjem Facebookovem kovancu libri). Tudi ECB je opravila anketo v januarju 2021 o CBDC, odloča se namreč o obliki digitalnega evra.

CB-SE-5 se namreč tudi ukvarja s preverjanjem koncepta oziroma pilotnim projektom maloprodajnega CBDC, kjer preizkušajo rešitev, temelječo na DLT. Ocenjujejo tehnologijo, njene prednosti, slabosti in se še ukvarjajo z njo, zato so nekatera vprašanja za njih prezgodnja za dokončno sklepanje. V središču koncepta je dvostopenjski sistem, kjer CB Švedske (v nadaljevanju Riksbank) edina ustvarja CBDC – e-krone, igralci na trgu, kot so banke in ponudniki plačilnih storitev (angl. Payment Service Provider, v nadaljevanju PSP), služijo kot distributerji e-krone končnemu uporabniku. Deluje na podoben način, kot poteka razdelitev denarja dandanes. So sredi svojega dela in morajo še veliko storiti, preden lahko podajo kakšno zaključno trditev z zornega kota Švedske. Pilotni projekt proučuje tehnično rešitev za e-krono. O tem, ali bi sploh začeli z zagonom e-krone, še ni sprejetih odločitev in tudi ne, na kateri tehnologiji razpršene evidence bi temeljila ter kakšno vlogo bi imela pri reševanju težav s poravnavami. Informacije o stanjih na računih in o transakcijah

uporabnikov e-krone ne bi bile shranjene v osrednji evidenci Riksbanke, ampak razpršene znotraj omrežja e-krone in upravičenih ponudnikov plačilnih storitev za distribucijo e-krone po omrežju, kjer bi bil podatek, vezan na določenega ponudnika, viden le njemu samemu. Preizkušajo rešitev na podlagi DLT, kjer informacije v zvezi s transakcijami e-kron niso na voljo vsakemu ponudniku plačilnih storitev v omrežju, temveč samo tistim, vpletenim v transakcijo. Proučujejo, ali je možno, da Riksbanka ostane v sedanji vlogi, obenem pa ne hrani osrednje evidence oz. informacij končnih uporabnikov. Informacije, povezane z uporabniki e-krone in njihovimi transakcijami, so distribuirane med PSP, ki imajo opravka s strankami. Na ta način bi se ohranila vloga CB ločeno od končnega uporabnika in njegovih informacij. Oceniti skušajo vrednostni prispevek švedskega CBDC. Kar zadeva vprašanja poravnav, je še vedno v raziskovanju.

Drugi respondent s CB-SE-5 je tudi izpostavil, da se poraja vprašanje, kako bi takšna nova tehnična rešitev bila uporabljena z zakonodajnega vidika za PCS. Način in možnost uporabe pri PCS se spremlja v njihovem pilotnem projektu, vendar še niso prišli do zaključkov. Predpogoj pilotnega projekta je, da bi morala biti e-krona v omrežju ustvarjena s strani Riksbanke tako kot bankovci in kovanci in na isti način ne bi smela biti v pristojnosti ponudnikov plačilnih storitev ali zasebnih bank, ki jih razporejajo do končnih uporabnikov. Nejasnosti so, ali je omrežje e-krone, ki ga razvijajo v pilotu, lahko obravnavano kot sistem poravnav, saj je denar CB v omrežju, odgovor na to bo podala zakonodaja in je ključen.

Po besedah CB-ES-6 je razvoj DLT v prihodnosti odvisen od zmožnosti industrije, da izvede uspešne primere uporabe. Evropska komisija (v nadaljevanju EK) zato uvaja pilotni režim tržne infrastrukture za DLT ob zagotavljanju zaščite potrošnikov, učinkovitosti trga in finančne stabilnosti. Evrosistem trenutno preverja možnost izdaje CBDC oziroma kako narediti centralnobančni denar na razpolago v digitalni obliki za uporabo pri maloprodajnih plačilih. Odločitev v času ankete še ni bila sprejeta, razvijajo koncept, izvajajo poskuse uporabe, zbirajo mnenja javnosti in sodelujejo z deležniki.

Po izjavi CB-NO-7 skupaj s CB Švedske intenzivno proučujeta CBDC. Kljub vsemu je po njihovem mnenju Skandinavija namenila premalo pozornosti poravnavam vrednostnih papirjev (v nadaljevanju VP) na DLT. Center za inovacije BIS je v projektu Helvetia preizkušal sredstva in CBDC, oba v obliki žetonov za poravnavo vrednostnih papirjev. Glede uporabe DLT za CBDC sledijo razvoju trga. Regulatorji delujejo po principu, da mora zakonodaja določati ukrepe sorazmerne tveganjem, kar je še vedno v razvoju za prenos na DLT.

EK je predlagala zakonodajne okvire za kriptosredstva. Predlagana je bila tudi zakonodaja za DLT v običajni plačilni infrastrukturi oz. pri poravnavi vrednostnih papirjev, ki udeležencem omogoča preizkušanje DLT v varnem okolju in pod ustreznimi pogoji. DLT se preizkuša v različnih infrastrukturah in s tem se pridobiva več znanja o tveganjih, zakonodajnih in finančnih vprašanjih. Od rezultatov teh preizkusov je odvisno, ali bo vpeljana v prihodnosti. Poteka tudi testiranje kriptosredstev za decentralizirane finance

(angl. Decentralized Finance, DeFi) (sistem finančnih produktov in storitev, ki deluje brez posrednikov) in če je mogoče imeti običajna sredstva v takšnih infrastrukturah, kar bi morda prispevalo k določenim koristim. Trenutno gre za novo tehnologijo, ki mora biti preverjena, če so lahko tveganja zmanjšana in je lahko v zakonodajne okvire umeščena za uporabo v vsakdanjih financah. Center BIS za inovacije, kjer poteka sodelovanje med nekaterimi CB in CB Švice (nem. Schweizerische Nationalbank, SNB) ter infrastrukturo za poravnavo vrednostnih papirjev podjetja za finančne storitve SIX Group AG, upravlja z decentralizirano infrastrukturo oz. žetoniranimi sredstvi, neke vrste veleprodajni CBDC.

CB-NO-7 je upravni organ, regulator, in tudi ponudnik denarja, kot prvi spremljajo zasebne iniciative z zakonodajnega vidika in njihove CBDC-projekte. Veliko držav ima takšne projekte in preverjajo uporabnost DLT v tem kontekstu. Na Norveškem je malo uporabe gotovine, okoli 4 %, večina plačil je v obliki bančnih nakazil.

Tabela 4: Aktivnosti centralnih bank, povezane s preizkušanjem DLT pri PCS

Država CB	**Aktivnosti CB, povezane s preizkušanjem DLT pri PCS**
Honduras	– Se ne ukvarja z DLT.
Poljska	– Tehnologije ne preizkušajo. – Centralno depotna družba za vrednostne papirje: e-glasovanje. – Poslovna banka s klirinško hišo: trajni nosilec podatkov.
Slovaška	– Spremljajo razvoj maloprodajnega CBDC: evrosistem, Kitajska, Meta-Diem. – Izhajajo iz odločitev evropskih institucij.
Švedska	– Dvostopenjski sistem. – Podatki razpršeni med PSP in vidni le udeleženim v transakcijo.
Španija	– EK uvaja preko evrosistema pilotno infrastrukturo, ki nudi zaščito potrošnikov, učinkovitost trga in finančno stabilnost. – Evrosistem se ukvarja z uvedbo maloprodajne valute.
Norveška	– Skupaj s Švedsko preizkušajo DLT za PCS. – BIS: projekt Helvetia (VP) => zakonodaja sorazmerna tveganjem. – EK predlagala zakonske okvire za kriptosredstva in DLT v običajni plačilni infrastrukturi ter pri poravnavi VP. – Kriptosredstva v decentraliziranih financah (DeFi). – Švica in švicarska borza SIX: veleprodajni CBDC. – Regulator: spremljajo iniciative, zakonodaja takšna, da so ukrepi sorazmerni tveganjem, 4 % gotovine.

Vir: lastno delo.

CB-SK-4 trdi, da področje finančne tehnologije na Slovaškem določa evropska zakonodaja v pristojnosti Slovaške nacionalne banke in Ministrstva za finance Slovaške republike. DLT je termin za tehnologije, ki omogočajo skupno evidenco, deljeno v omrežju računalnikov. Vloga žetonov in pametnih pogodb pri PCS je lahko uporabna in lahko vodi k velikemu napredku. Kar zadeva sprejetost in uporabo, je po njihovem mnenju vse odvisno od skupnega dogovora na ravni evropskih institucij. V tabeli 4 so zbrane izkušnje CB z uporabo tehnologije razpršene evidence v plačilnih sistemih. Kjer lastnih izkušenj nimajo, so predstavljena opažanja, povezana z vpeljavo tehnologije.

7.2 Prepoznane prednosti in priložnosti

Po izjavah CB-CO-2 potekajo običajna plačila v centraliziranem okolju, kjer imajo enotno točko odpovedi celotnega sistema. V preteklosti je prišlo do neprilik, npr. v Banki Anglije, kjer so plačila v celoti prenehala delovati za nekaj ur in s tem začasno zaustavila gospodarstvo države ali regije. Tega pri DLT ni, zato kot CB verjamejo, da je primerna tehnologija za takojšnja plačila in obstojnost veleprodajnega CBDC. Veleprodajni CBDC je lahko v pomoč nadaljnjemu razvoju sistemov, podobnim RTGS. V manjših gospodarstvih lahko po njihovem mnenju maloprodajni CBDC izboljša učinkovitost plačil v državi. Žetoni in pametne pogodbe prispevajo k povečanju učinkovitosti, varnosti, zasebnosti in k boljšemu nadzoru nad kreditnim tveganjem.

Po mnenju CB-PL-3 so glavne prednosti DLT, da po zasnovi zagotavlja varnost podatkov transakcij, saj več omrežnih vozlišč hrani celotno zgodovino transakcij. Arhivi transakcij so zaščiteni pred spreminjanjem ali z drugimi besedami, vsaka priredba zgodovine transakcij je opazna. Veliko zagovornikov DLT navaja avtomatizacijo transakcije, izvedene pod pogoji, opredeljenimi v kodi, s t. i. pametnimi pogodbami, kot prednost DLT. Toda DLT ni predpogoj za avtomatizacijo transakcij, odvisnih od spremenljivk znotraj sistema ali zaznanih s senzorji zunaj sistema. Razčlenjenost podatkov zagotavlja preverljiv in nespremenljiv zapis.

CB-SK-4 izpostavlja kot prednost hitrejše in bolj tekoče procese na področjih, kjer so procesi veljali za dolgotrajne, okorne, polne frikcij, predolge in predrage, tako v kliringu in plačilih kot v poravnavi. Subjekti, udeleženi v čezmejna plačila različnih pravosodij, dajejo prednost DLT, saj sistem korespondenčnega bančništva upočasni in podraži transakcije. Primer so mednarodna plačila med evroobmočjem in zunaj njega.

CB-SE-5 še ni opredelila bistvenih prednosti, ugotavlja pa, da lahko DLT izboljša načelo dostave proti plačilu, mehanizem poravnave poslov z vrednostnimi papirji, ki povezuje prenos vrednostnih papirjev in prenos denarnih sredstev, na način, s katerim se zagotovi, da se dostava vrednostnih papirjev opravi samo, če se opravi ustrezno plačilo. DLT predstavlja drugačna operativna tveganja kot tehnologija v rabi in cenejši način izgradnje nove finančne infrastrukture. Vloga CBDC je pri čezmejnih plačilih in v poravnavi vrednostnih papirjev, torej povsod, kjer dostava proti plačilu dandanes ne obstaja.

Po mnenju CB-ES-6 so prednosti DLT pridobitve v učinkovitosti na splošno. Odbor za plačila in tržno infrastrukturo (angl. Committee on Payments and Market Infrastructures, CPMI) pri BIS prepoznava naslednja področja prednosti: povečanje hitrosti obdelave od konca do konca, nižje stroške obdelave s pomočjo kriptografije, hitrejše in bolj transparentno usklajevanje podatkov, omogočanje transakcij v realnem času, kar se odraža v večji kreditni sposobnosti in cenejšem upravljanju z likvidnostjo, avtomatizirana orodja za pogodbe (pametne pogodbe) ter sledljivost, ki po drugi strani krati zasebnost.

Za CB-ES-6 imata tehnologiji žetonov in pametnih pogodb možnost izboljšanja učinkovitosti plačil. Študije so se osredotočale še posebej na možnosti programirljivega denarja in programirljivih plačil. Eno od najbolj obetavnih področji zunaj plačil je digitalna identiteta oziroma skladnost z zahtevami preverjanja svoje stranke, kar poudarja tudi CPMI. Po izjavah CB-NO-7 je prednost DLT v pametnih pogodbah, saj je tveganje tretje strani zmanjšano, in v njeni obstojnosti. CBDC lahko nudi konkurenco v primeru, da banke ali druge plačilne sheme pridobijo na tržni moči in se jo lahko uporabi za preventivno ukrepanje.

Za CB-NO-7 je CBDC lahko rešitev v sili, ko bančno plačilno omrežje odpove. CBDC je lahko orodje za soočanje s temi izzivi, saj ohranja možnost državnega nadzora in zmožnost izvajanja monetarne politike. Ni zaželeno, da bi CBDC preveč posegel v delovanje bank. Še vedno bo zasebni sektor ohranjal zagotavljanje kreditov, ne bo pa pojavljanja zasebnih posojil na bilančnem računu CB. CBDC ne sme izkrivljati ali zavirati finančne stabilnosti na način, da bi vsi naenkrat dvigovali bančne vloge in vlagali v CBDC. Lahko se ga obravnava kot neke vrste digitalno gotovino, saj je obveznost CB kot gotovina in je zanimiv zaradi različnih razlogov namembnosti, zato vsaka banka izhaja iz svojega stališča za njegovo uveljavitev.

7.3 Prepoznane slabosti in izzivi

CB-HN-1 meni, da je izziv vpeljave DLT v PCS njegova zgodnja faza razvoja, razumevanje tehnologije s strani javnosti in institucij ter sprejetost s strani državnih organov, ne nazadnje pa tudi vprašanje zaupanja v tehnologijo samo. DLT primanjkuje jasnih zakonskih okvirov pri njegovi uporabi ter tehnično usposobljenega kadra za njegovo razširitev. Na CB-CO-2 menijo, da sta način upravljanja sistema in določanje novih pravil glede zasebnosti podatkov nujna. Preveč udeležencev ima dostop do informacij, med drugim vrstniške institucije.

CB-PL-3 izpostavlja razlike v tveganjih, odvisne od zasnove sistema DLT, v ukrepih proti pranju denarja in proti financiranju terorizma (AML/CFT). Slabosti so nižja hitrost in hkrati visoka poraba virov za izvajanje konsenznih algoritmov, veliko virov za shranjevanje zaradi obsežnosti podatkov, pa tudi vprašanje dokončnosti poravnave, ki je odvisna od konsenznega mehanizma in je potemtakem nedeterministična oz. verjetnostna v primeru, ko ne izključuje vilic, prav tako je povratnost transakcij skoraj nemogoča, zato nastopijo težave pri vračilih bremenitve računa za zagotavljanje pravic potrošnikov.

CB-SK-4 meni, da se bodo izzivi in tveganja zmanjševali s časom. Ker se izvedenih operacij prek DLT ne da preklicati, s tem reklamacije niso možne. To je težava pri potrošniških plačilih. Pravila za preklic nakazil in reklamacije so jasno opredeljena znotraj okvirov nakazil SEPA (angl. Single Euro Payments Area) kot tudi direktive EU za ponudnike plačilnih storitev PSD2 (angl. Payment Services Directive). Kot izziv vidijo tudi novost tehnologije. Ker zahteva specifična znanja in veščine, so mnenja, da potrošniki z vidika finančne vključenosti še niso pripravljeni nanjo. Na področju plačil, kliringa in poravnave so zadovoljni z razpoložljivimi tehnologijami, kot sta RTGS TARGET2 (angl. Trans

European Automated Real-time Gross Settlement Express Transfer System) pri plačilih in TARGET2-securities (T2S) pri poravnavi vrednostnih papirjev, ki so tudi v skladu z zakonodajo. Po njihovem mnenju zgolj inovacija sama, čeprav so do njih sprejemljivi, ne zadostuje kot razlog za zamenjavo enega sistema z drugim. Področje CBDC je obravnavano tudi na evropski ravni, kjer naj bi bili izzivi še v varnosti, zaščiti podatkov in uveljavljanju zahteve proti pranju denarja.

Po mnenju CB-SE-5 je trenutna zakonodaja prilagojena uveljavljeni tehnologiji, zato se lahko pojavijo nova pravna tveganja. Do pravnih tveganj v mednarodnem poslovanju pride zaradi različnih pravosodij. Težave se pojavljajo tudi pri razširljivosti. Pojavijo se lahko tudi nepredvidena operativna tveganja. CB-ES-6 pravi, da so izzivi trenutna razširljivost, pomanjkanje interoperabilnosti na platformi, sistemi upravljanja, knjigovodska dokončnost poravnav, operativno in varnostno tveganje ter robustnost in obstojnost DLT-platform. Po mnenju CB-NO-7 negotovi pravni okviri predstavljajo tveganje v zvezi z lastniškimi pravicami žetonov, prevzemanjem odgovornosti in zato ostajajo odprta tudi zakonodajna vprašanja.

7.4 Pravice v upravljanju plačilnih sistemov na razpršeni evidenci

Dostopnost sistema razpršene evidence se da prilagoditi. Na CB-PL-3 ga delijo na javnega in zasebnega; v prvem upravljajo vozlišča anonimni uporabniki, v drugem pa so uporabniki pooblaščeni s strani administratorja. Druga delitev se nanaša na dodeljene pravice uporabnikom. V primeru polnih pravic lahko vozlišča izvajajo transakcije, imajo vpogled v stanje evidence in potrjujejo transakcije, z omejenimi pravicami imajo vozlišča le ožji nabor pravic.

Na CB-SK-4 prepoznajo delitev na podoben način. Obstaja več vrst DLT glede na to, kdo lahko bere, ustvarja ali vključuje transakcije za stalno v evidenco. V glavnem se razlikujejo med tremi tipi: zasebni napram javni DLT, kjer je razlika v dostopnosti do omrežja; glede na omejitve, kjer se razlika nanaša na omejitve udeležencev pri izvajanju transakcij na DLT, ter na dovoljenje za potrjevanje transakcij, kjer se razlika nanaša na osebo, ki ji je dovoljeno potrjevanje transakcij, ali je to kdorkoli na DLT ali samo nekateri člani.

Na CB-NO-7 so mnenja, da javne verige blokov, kot je Ethereum, s pametnimi pogodbami ne ustrezajo pogojem za CBDC. Obstojnost omrežja ponuja DLT-infrastruktura, kjer je potrebno dovoljenje za dostop. Načeloma bi CBDC lahko deloval tudi v centralnem registru in tam ponujal podatke na vpogled in storitve. Uporaba pametnih pogodb na takšnem omrežju je po njihovem prepričanju bolj smiselna. Obtok CBDC na zunanjih registrih DLT prinaša določena tveganja in lahko škoduje ugledu banke, saj povzroča določene pravne obveznosti, ki si jih CB ne želi. DLT lahko pripomore k zagotavljanju zaželenih lastnosti CBDC, zato je vsekakor pomemben v povezavi z njim.

7.5 Področja uporabe, tipi tehnologij, platforme in raziskovalna združenja

Kar zadeva področij uporabe, na CB-CO-2 menijo, da se zunaj področja plačil lahko DLT uporabi pri CBDC, dostavi proti plačilu (angl. Delivery versus Payment, DvP), upravljanju sredstev skozi njihovo celotno obdobje, kot so vrednostni papirji in obveznice. Z vidika CB-SK-4 so področja PCS najbolj primerna za uporabo DLT. Je tudi nekaj drugih primerov uporabe, ki ne spadajo v kategorijo financ, kot so arhiviranje podatkov, upravljanje z identiteto, sledenje podatkom, storitve javne uprave itn. Razvijanje in testiranje raznih vrst DLT še ni zaključeno. CB-SE-5 pravi, da se zunaj plačil DLT lahko uporablja za zagotavljanje skladnosti, shranjevanje in izmenjavo podatkov, za boj proti pranju denarja itn.

Glede tipov tehnologij v CB-CO-2 menijo, da bi načeloma bila v rabi praktična toleranca bizantinske napake (angl. practical Byzantine Fault Tolerance, v nadaljevanju pBFT), saj gre za zaprte verige blokov med zaupnimi vozlišči, ki so regulirane in nadzorovane s strani vladne agencije. Pri pBFT konsenzni mehanizem kljub nedelujočim ali zlonamernim vozliščem sklene dogovor, tako da vodilno vozlišče pošlje poizvedbo ostalim vozliščem, na podlagi katere izloči škodljivo vozlišče. Celo RAFT-konsenz je lahko praktičen, kjer je vsako vozlišče zelo zanesljivo oziroma manj izpostavljeno vdorom. RAFT je podoben BFT, le da je vodilno vozlišče določeno z glasovanjem, prav tako je pri Paxosu, ki je še bolj zapleten. Število transakcij na sekundo je ključnega pomena za katerikoli PCS. V CB-ES-6 so tehnološko nevtralni, toda vsaka rešitev, vnesena v PCS, mora po njihovem mnenju zagotavljati varno in učinkovito infrastrukturo finančnega trga, tudi z zakonsko gotovostjo v smislu knjigovodske dokončnosti.

Dokaz o delu je za CB-NO-7 le način, kako se izogniti zaupni tretji strani za potrjevanje pri Bitcoinu, Ethreumu ipd., kot CB tega ne potrebujejo. Temelj njihovega registra je zaupanje vanj, na ta način lahko opravijo svoje naloge. Dokaz o delu in ostali razpršeni konsenzi, odvisni od zaupnih vozlišč, niso povezani s CB, zato ni treba utemeljiti CBDC na konsenznem mehanizmu, ki se zanaša na dokaz o delu, ker bi bil le potrata energetskih virov. Lahko je uporaben za verigo blokov pri drugih kriptovalutah, kjer ni zaupne tretje strani, kajti CB je zaupna tretja stran. DLT za CBDC bi bil na omrežju z zahtevanim dovoljenjem za pravice dostopa in upravljanja, kar lahko ima nekatere prednosti, kot sta obstojnost in programirljivost za uporabo pametnih pogodb. CBDC se lahko tudi nahajajo na drugih omrežjih DLT na žetonu, ki je krit s primarno valuto, in se jih tam uporabi za poravnave in storitve. Ta omrežja lahko temeljijo na različnih konsenznih mehanizmih. Tak konsenzni mehanizem, da se izogne zaupanju v centralno stran, ni potreben, ker so centralna stran, ki naj bi se ji zaupalo.

Širše vprašanje za CB-NO-7 je, ali je DLT potreben za ohranjanje nekaterih lastnosti gotovine in ohranjanje zaupanja v plačilni sistem. Značilnosti gotovine so torej tiste, ki jih mora CBDC imeti in pogojujejo vpeljavo tehnologije, kar pomeni, da so pomembne lastnosti tehnologije in ne tehnologija sama. Po mnenju CB-SE-5 bo veleprodajni CBDC verjetno na

žetonu. Področje, ki je osredotočeno na pametne pogodbe, so trgovinske finance, kjer se veliko pridobi z avtomatizacijo administrativnih procesov. To je lahko vključeno v veleprodajni CBDC-sistem. V finančnem sektorju bo prevladoval DLT, za katerega bo zahtevano dovoljenje za dostop.

CB-SE-5 oz. Riskbank še ni določila tipa tehnologije za e-krono kot javnega plačilnega sredstva. Kakšno vlogo naj bi imel CBDC v povezavi s poravnavo je zelo pomembno vprašanje z zakonskega vidika in zelo verjetno precej odvisno od tega, kako bo, tehnično gledano, vnesen morebitni CBDC. Njihov pilotni projekt spremlja e-krono kot rešitev v raziskovanju na platformi podjetja R3, imenovani Corda.

Kot prepoznavne platforme CB-CO-2 omenja R3 Cordo, ki ni običajna veriga blokov. V svoji edinstveni obliki pripomore k večji zasebnosti in učinkovitejšemu doseganju konsenza. Obstaja tudi Linuxov projekt Hyperledger na platformi Fabric. Ripple je še vedno prepoznaven na prizorišču mednarodnih plačil za prenos velikih vrednosti. Eno večjih raziskovalnih združenj na področju DLT je po besedah CB-ES-6 v njihovi državi verjetno Alastria iniciativa, ki je zbrala največje število podjetij. Ne osredotoča se na plačila, vendar bodo morda pomembna za njih v prihodnje.

7.6 Ugotovitve konzorcija poslovnih bank in finančnih institucij

7.6.1 Vpeljava tehnologije

Fnality je konzorcij več kot 15 bank, po trditvah njihovega predstavnika FN-8 namenjen izboljšanju mednarodnih plačil na DLT z digitalizacijo obstoječega denarja. V ospredju delovanja iniciative je platforma, s katero bi odpravila posredništvo in zagotovila neprestano delovanje sistema.

V iniciativi so udeležene glavne banke, med njimi ECB, Zvezne rezerve (v nadaljevanju FED), Banka Japonske (BoJ), Banka Kanade (BoC) in Banka Anglije (BoE) – prisotne so banke iz Evrope in Združenih držav Amerike (z izjemo Mizuha), tudi borza NASDAQ je del tega. V projekt nameravajo vključiti še preostale banke. Faze širitve potekajo v dveh serijah, A in B. Začetna investicija v projekt Fnality je bila opravljena pri najmanj 15 bankah in ob koncu leta 2021 je delo potekalo že na seriji B. Prizadevajo si zbrati dodatna sredstva ostalih bank, stik imajo s Citibank, Goldman Sachs itn. Njihov cilj je vzpostaviti platformo za izboljšanje veleprodajnega CBDC in izboljšavo mednarodnih plačil prek DLT.

7.6.2 Mehanizem delovanja

Potek plačilnega procesa po izjavah predstavnika FN-8 ponazarja naslednji primer: nizozemska finančna institucija International Netherlands Group (ING) pošilja denar nasprotni strani, vendar ni lastnik tega denarja (npr. dolarjev), temveč posluje z denarjem

druge banke, saj nima dovoljenja za to pri CB. Ker ING nima dovoljenja pri FED, se zato njegovi dolarji nahajajo pri poslovni banki Bank of America (v nadaljevanju BoA), ki ima dovoljenje pri njih. Tako ING posluje z BoA, da poravna svoje dolarske transakcije.

S projektom Fnality bi bili dolarji digitalizirani, tako si jih ING ne bi rabil lastiti, imel pa bi v lasti digitalno različico ameriških dolarjev, kar bi poenostavilo proces pošiljanja denarja na primer banki Shell. Za pošiljanje denarja od ING do Shell mora ING poslati nalog BoA. BoA preveri znesek, zahtevo KYC in po potrebi zaustavi proces. Prav tako so omejitve glede delovnih ur FED. Vse to bi bilo izvzeto, če bi si ING lastil digitalno obliko ameriškega dolarja. Fnality skuša digitalizirati različne valute, ki si jih lahko banke lastijo in jih pošiljajo različnim nasprotnim stranem na platformi.

7.6.3 Prednosti in priložnosti

Predstavnik FN-8 je mnenja, da DLT poenostavi celoten mednarodni plačilni sistem poravnav. Trenutno ima veliko omejitev, kot je poslovni čas CB. Omejitve dovoljenj PB za opravljanje bančnih storitev vodijo v plasti korespondenčnega bančništva, množenja sporočil, procesov in zapletanja stvari, že samo v primeru ameriških dolarjev.

Pri zamenjavi v indijske rupije ali malezijske ringite je še več posrednikov v procesu. Z DLT nameravajo odstraniti vse posrednike pri vseh tipih transakcij. Sestavlja se nabor vseh subjektov, ki so v vrednostni verigi. Za plačila so to korespondenčne banke in CB, predvsem njihov poslovni čas. Denar je prenesen od enega subjekta k drugemu, stvari se poenostavijo, saj so odstranjene različne plasti in tako si banke lastijo neke vrste veleprodajni CBDC.

Maloprodajni CBDC je digitalni evro, kjer si posamezniki lastijo centralnobančni denar. Edini CB denar, ki si ga posamezniki lastijo trenutno, je gotovina. Denar na bančnih računih pripada banki, banka zanj potrebuje dovoljenje za bančne posle. Če ga nima, potem ameriški dolarji na računu niso pri ING, ampak so pri njeni korespondenčni banki. DLT omogoča digitalizacijo denarja in s tem poenostavitev mednarodnih plačilnih tokov. Pri nacionalnih plačilnih tokovih ING hrani evre in posluje z evropsko banko. Tak proces je precej preprost in ponuja takojšnja plačila, ING je del takega omrežja.

V omrežju takojšnjih plačil je pošiljanje denarja drugi banki, tudi z računom, odprtim pri ECB s TARGET2 (angl. Trans-European Real-Time Gross Settlement Express Transfer), preprosto in plačila potekajo tekoče. Pri poslovanju z banko, ki nima dovoljenja za zamenjavo evrov v ameriške dolarje, se naleti na težave, ker se deluje v tistih slojih, ki jih DLT odpravi.

Prednost so tudi pametne pogodbe, ki omogočajo dvoje stvari – denar naredijo programirljiv, pri pošiljanju programiranega denarja določeni osebi se npr. določi nakazilo 10 evrov, vendar le za nakup določene dobrine, npr. hrane in ne cigaret ali alkohola, kar se označuje kot pogojenost denarja. Z njimi se poveže eno transakcijo s plačilom: npr. multinacionalno

rudarsko in železarsko podjetje Rio Tinto namerava dobaviti aluminij kupcu. V trenutku prejema aluminija, s podpisanim pismom prejema, pametna pogodba izvede prenos sredstev z banke kupca na banko Ria Tinta oziroma določa vezavo ene finančne transakcije na drugo. Tako se z avtomatiziranimi transakcijami odpravi tveganje poravnave.

Če kupec kljub stečaju prejme aluminij, potem ostane Rio Tinto brez plačila in mora dobiti aluminij povrnjen. S pametno pogodbo za prejem aluminija ob izvedenem plačilu Riu Tintu se odpravi poravnalno tveganje in tveganje nasprotne strani. Transakcije se na ta način poveže med sabo, tako da brez izpolnjenega pogoja ni prenosa denarja. Če kupec ne razpolaga z denarjem, se dostava aluminija prekliče.

Tehnologija je uporabna tudi za druge stvari, kot je zamenjava evro za dolar. ING menja evre za dolarje pri ameriški finančni instituciji BNY Mellon. Izplača evre BNY Mellonu, nato BNY Mellon prenese dolarje ING, vendar je izpostavljen tveganju nasprotne strani, da ena od strani ne izpolni obveznosti. Če ING že prenese evre BNY Mellonu in preide BNY Mellon v stečaj, nastopi težava. Takšno tveganje se imenuje Herstatt tveganje, po istoimenski banki, ki je v letu 1974 šla v celoti v stečaj v zelo kratkem času. Povezovanje transakcij med seboj odpravi tveganje, da v trenutku prejetja evrov od ene strani nasprotna stran izroči dolarje.

Tretja največja prednost DLT pri plačilih in poravnavah je usklajevanje. Vsi udeleženci vidijo neposredno izvedbo plačila, saj ima vsak udeleženec kopijo dejanskih podatkov. Plačila na banki prek SWIFT potekajo tako, da banka prejme SWIFT sporočilo, ko se plačila poravnajo, in potem mora posodobiti podatke v svojem sistemu. Z neposredno povezanostjo plačilnih sistemov bi bile posodobitve takojšnje in bi bila SWIFT-sporočila odvečna. Z DLT se zmanjšajo delo in napake usklajevanj. Včasih je potrebna ročna sprememba podatkov, saj uskladitev ni avtomatska, da je nekaj prejeto in da je vpisano v lastne sisteme, kjer prihaja do napak usklajevanj. Pokliče se partnersko banko in dogovori o posodobitvi svojega sistema. Posodobitev v deljeni evidenci nima napak usklajevanj.

Tri prednosti so torej poenostavitev celotnega plačilnega toka z odstranitvijo in umikom posrednikov, kar se doseže z digitalizacijo sredstev, programirljivost je tudi pogojenost plačil, na ta način se odpravi tveganje poravnave in nasprotne strani in še napake usklajevanj.

7.6.4 Slabosti in tveganja

Največji izziv po besedah predstavnika FN-8 je sprejetost tehnologije s strani regulatorjev. DLT morajo odobriti vsi centralni deležniki, natančneje CB. Tudi prepoznavnost tehnologije je velik problem. Do tveganj pride v primeru stabilnega kovanca ali digitalne valute poslovne banke, ki jo izda npr. JP Morgan ali Meta (Facebook). Pri uporabi kriptovalut je posameznik izpostavljen velikemu tveganju nasprotne strani. Stabilni kovanci morajo imeti enakovredno kritje. Finančna tehnologija (FinTeh) izdaja tether in je tudi krit z denarjem, shranjenim na banki. Tak kovanec je lahko tudi krit z vrednostnimi papirji ali obveznicami. Le 25 % tethra

je kritega z gotovino in 75 % je kritega z vrednostnimi papirji, tako da nastopi kreditno tveganje oziroma tveganje neizplačila.

Drugič obstajajo tehnološka tveganja: Ali je DLT varna tehnologija ali pa je izpostavljena vdorom? Bi morala biti bolj varovana, čeprav ni enotne točke odpovedi? Za medsebojno povezovanje transakcij je potrebna interoperabilnost. Zelo enostavno je trditi, da so na voljo atomske zamenjave, kjer en dogodek dopušča drug dogodek, vendar je zato potrebna komponenta interoperabilnosti. Za premik k digitalnemu evru, ki bi zagotavljal zasebnost, ne da vsakdo na verigi blokov vidi, kdo opravlja transakcije, je potrebna komponenta zasebnosti, ki še vedno ni utrjena v DLT.

Omenjena so bila tri največja tveganja in izzivi poleg regulativne odobritve. Za denar CB oziroma regulirana plačila je potrebna odobritev regulatorja, za to si prizadevajo kriptovalute kot regulirane valute. Regulatorji so še vedno odgovorni za vse denarne tokove na svojem območju, zato je regulativna odobritev vsekakor velik izziv.

7.6.5 Prihodnji razvoj in faze implementacije

Zasebni sektor po navedbah predstavnika FN-8 skuša izboljšati tehnologijo, kar mu omogoča javni sektor. Zasebni sektor skuša vnašati izboljšave plačil na nereguliran način, kasneje se inovacije regulira, zato ima javni sektor stabilne kovance še vedno v obravnavi za sprejemanje predpisov. So pa strani, ki skušajo početi stvari na reguliran način. Fnality poskuša izgraditi takšno platformo in za to potrebuje odobritev vseh CB. So tudi druge iniciative: Odbor za plačila in tržno infrastrukturo pri BIS (CPMI) in drugi, kot je Odbor za finančno stabilnost (angl. Financial Stability Board, FSB), ki poskušajo izboljšati čezmejna plačila. Fnality je iniciativa zasebnega sektorja skupaj z javnim sektorjem. Tudi javni sektor poskuša narediti nekaj sam od sebe, vendar skuša izboljšati čezmejna plačila v skupnih prizadevanjih med javnim in zasebnim, kjer je Fnality največji primer česa takega.

Tudi investicijska banka JP Morgan je poskusila s projektom Ubin skupaj z Monetarnim organom Singapurja umestiti takšno platformo z veleprodajnim CBDC. Bank de France eksperimentira z veleprodajnim CBDC in z maloprodajnim CBDC, digitalnim evrom. Na tak način skušajo CB in regulatorji narediti nekaj sami.

Pri maloprodajnem CBDC (digitalni evro, digitalni dolar) so angažirane CB in regulatorji. Zasebni sektor se loteva projektov na nereguliran način in sčasoma po malem odpravlja tveganja, s katerimi upravlja. Na takšen način so sledili stabilni kovanci kriptovalutam. Primera, ko poskuša zasebni sektor ustvarjati skupaj z javnim, sta Fnality in projekt JP Morgan s CBDC.

Javno-zasebna partnerstva se ukvarjajo z mednarodnimi plačili, z digitalnim evrom. Z maloprodajnim CBDC se načeloma ukvarja javni sektor, čeprav sodeluje z bankami pri digitalnem evru. Kitajska ustvarja svoj digitalni juan skupaj s poslovnimi bankami. Digitalni

juan, maloprodajni CBDC, bo izdal ponudnik plačilnih storitev. Običajno bi ga izdale banke prek razpoložljivih denarnic in preverjale zahtevo KYC.

7.6.6 Področja uporabe

Predstavnik FN-8 meni, da bi maloprodajni CBDC bil digitalna oblika gotovine, ki bi zajemala 10 % digitalne valute. Veleprodajni CBDC bi še zmeraj omogočal poenostavitev pretoka denarja iz ene banke v drugo v 90 % digitalne valute. Banke med sabo lahko izvajajo poravnave z veleprodajnim CBDC. Pametne pogodbe omogočajo programirljivost, pogojenost in povezave različnih transakcij ene z drugo.

DLT se lahko uporablja v bančništvu na vseh področjih: z digitaliziranimi vrednostnimi papirji in obveznicami se lahko posluje mimo skrbniških bank in centralno depotnih družb (angl. Central Securities Depository, CSD). Digitalizirana so lahko pisma podpore (akreditivi) oziroma pismene izjave banke, da bo izplačala znesek pod določenimi pogoji, gre za digitalizirano posojanje. Iniciativa se posveča tudi projektu decentraliziranih financ oz. DeFi, ki združuje vse strani – opravljanje bančnih poslov z depoziti in posojili; banke sprejemajo depozite, da posojajo naprej svojim strankam. DeFi združuje vse strani skupaj. Uporaba je dobrodošla v trgovinskih financah, s čimer se ukvarja npr. inciativa Contour.

7.6.7 Tipi tehnologij in organizacije

Na koncu predstavnik iniciative FN-8 še poudarja, da za plačila absolutno ni primeren konsenzni protokol dokaza o delu, saj je preveč časovno potraten in neekološki. V rabi je toleranca napake, ki je zmogljivost sistema, da deluje pravilno kljub poljubnim, tudi zlonamernim napakam. Potrebna zmogljivost za opravljanje obsega poravnav na sekundo v maloprodajnem CBDC je npr. na božični dan v Londonu na tisoče transakcij na sekundo in tega se ne da doseči z dokazom o delu.

Opravka so imeli tudi s Hashgraphom, vendar vse, kar je možno tam, je izvedljivo tudi na zasebni verigi blokov. Za uporabo javne verige blokov je smiselno imeti dovolilnico za plačila. Za upravljanje z maloprodajnim CBDC je potrebno dovoljenje za dostop in upravljanje. Razširljivost je eden od izzivov DLT pri plačilih, kot tudi učinek na okolje.

Glavni konzorcij je Fnality, drugi je od JP Morgan in še trije so, ki poskušajo pričeti na tem področju, vendar niso konzorciji, rahlo izgubljajo tekmo. Platforma za JP Morgan je Quorum. Peta faza Ubina v Singapurju skupaj z JP Morgan je uporabljala zasebni oblak Ethereuma – Quorum, Fnality tudi uporablja zasebni oblak Ethereuma. Corda podjetja R3 uporablja notarje, ki so posredniki, njih je smiselno izločiti.

8 DISKUSIJA

8.1 Vpeljava tehnologije razpršene evidence

Po bankah sem poizvedoval, ali se ukvarjajo s preizkušanjem tehnologije DLT pri PCS, in ugotovil, da se CB-HN-1 s tem ne ukvarja. CB-PL-3 se aktivno ne ukvarja z njo, vendar so v njihovi državi uvedli DLT pri Centralno depotni družbi vrednostnih papirjev za elektronsko glasovanje. Po Mills in drugi (2016) je lahko plačilni instrument, kot je vrednostni papir, tudi na razpršeni evidenci. Tudi ena izmed PB skupaj s klirinško družbo overja dokumente na DLT na Poljskem. WEF (2019) omenja uporabo veleprodajnega CBDC za namene kliringa.

CB-SK-4 omenja, da se evrosistem ukvarja s tem, in ugotavlja, da je Kitajska med pionirji testiranja. Kot ločen primer navaja tudi projekt Diem, ki pa ga je po Crosman (2022) v letu 2022 odkupila banka Silvergate, s čimer se je projekt zaustavil. ECB je v letu 2021 opravila anketo v zvezi z digitalnim evrom. Sami tudi raziskujejo maloprodajni CBDC na DLT. Po Bech in Garratt (2017) je švedska Riksbanka šla najdlje pri razmišljanju o možni izdaji maloprodajnega CBDC.

Pri CB-SE-5 bi edini ustvarjali CBDC, ostale finančne institucije pa bi služile njegovi distribuciji. Po Soederberg (2019) se Švedska približuje družbi brez gotovine, zato je Riksbank omenil tudi možnost izdaje digitalne oblike denarja, namenjene širši javnosti. Informacije bi bile razpršene znotraj omrežja digitalne gotovine. Podatki bi bili vidni le ponudnikom plačilnih storitev (PSP), s katerimi ima uporabnik opravka. Tako bi se po Sveriges Riksbank (2018) ponudnikom plačilnih storitev omogočilo konkurenčno infrastrukturo. V tem primeru CB ne bi imela vpogleda v elektronsko poslovanje uporabnikov sistema. Tudi vprašanje poravnav je še nerešeno oz. ali je omrežje e-krone sistem poravnav. Tehnična rešitev je predmet zakonodaje, e-krona bi morala po njihovem ostati obveznost CB. CB-ES-6 trdi, da je vpeljava odvisna od uspešnih primerov praks. EK uvaja pilotni režim infrastrukture DLT, kjer so v ospredju zaščita potrošnikov, učinkovitost trga in finančna stabilnost. ECB proučuje maloprodajni CBDC.

CB-NO-7 sodeluje na DLT-projektih s CB Švedske. Skandinavija je premalo pozornosti namenila raziskavam DLT pri poravnavah vrednostnih papirjev. Po BoC, Boe & MAS (2018) je primer takšnega projekta v svetu Jasper, v katerem poskušajo doseči takojšen obračun in poravnavo dostave proti plačilu (DvP) na platformi DLT. Center za inovacije BIS je preizkušal to v projektu Helvetia. Sprejeti ukrepi morajo biti sorazmerni tveganjem in to se mora odražati v zakonodaji. EK je za kriptosredstva predlagala zakonske okvire. Zakonodaja je bila predlagana tudi za DLT v običajni plačilni infrastrukturi, ker različne infrastrukture izkazujejo različna tveganja, in pri poravnavi vrednostnih papirjev. Po IBRD (2017) so zakonodajni okviri še v nastajanju, težava nastopi med različnimi pravosodji. Po Deloitte in drugi (2018) je bil tudi cilj projekta Ubin v šesti fazi naslavljanje zakonodajnih

okvirov z DLT. Testira se tudi kriptosredstva v decentraliziranih financah. Center BIS za inovacije (CB-ji, CB Švice in borza SIX) preizkušajo neke vrste veleprodajni CBDC in spremljajo tudi zasebne iniciative. CB-SK-4 pa izhaja iz evropske zakonodaje, svojih pooblastil in svojega ministrstva za finance. Nadaljnji koraki so odvisni od odločitev evropskih institucij.

8.2 Prepoznane prednosti in priložnosti

CB-CO-2 poudarja, da v sistemu DLT ni enotne točke odpovedi. Po IBRD (2017) razpršena narava evidence naredi sistem bolj obstojen in omogoča večjo zaščito pred spletnimi napadi. Izpostavlja tudi, da je dober za takojšnja plačila in zagotavlja obstojnost, da je koristen za razvoj RTGS in da maloprodajni CBDC izboljša učinkovitost plačil v manjših gospodarstvih, prispeva k večji varnosti, zasebnosti in nadzoru nad kreditnim tveganjem. Po Ali in drugi (2014) mehanizem sistema prispeva k odpravi kreditnega tveganja, torej takšnega, ki nastane v primeru insolventnosti dolžnika.

CB-PL-3 meni, da zagotavlja varnost podatkov transakcij, nespremenljivost in sledljivost. Izpostavljajo pa, da avtomatizacija ni zgolj značilnost DLT. Po PC in drugi (2017) je že v projektu Jasper bila izkazana jasna in dosledna revizijska sled finančnih transakcij. CB-SK-4 meni, da so procesi hitrejši in bolj tekoči kot v korespondenčnem bančništvu, kjer so dragi in počasni. Po van Ginneken (2019) zamenjava korespondenčnih bank s transparentno platformo izboljša učinkovitost plačil. CB-SE-5 navaja, da je izboljšana dostava proti plačilu (DvP) in morebitna cenejša finančna infrastruktura. ECB in BoJ (2018) omenjata tudi prednost DvP, kjer je mehanizem transakcije atomskost poravnave, ki pomeni istočasno izmenjavo med obema stranema.

Tabela 5: Prednosti in priložnosti DLT pri PCS

Država CB	**Prednosti in priložnosti DLT pri PCS**
Kolumbija	– Ni enotne točke odpovedi, takojšnja plačila in obstojnost, učinkovitost, varnost, zasebnost, odpravljeno kreditno tveganje.
Poljska	– Varnost, nespremenljivost, sledljivost, (avtomatizacija).
Slovaška	– Hitrejši, bolj tekoči procesi, posebej pri čezmejnih plačilih.
Švedska	– Boljši DvP, drugačna tveganja, cenejša izgradnja infrastrukture.
Španija	– Splošna učinkovitost / CPMI: hitrejša obdelava, od konca do konca, nižji stroški (kriptografija), hitrejše in transparentnejše usklajevanje podatkov, transakcije v realnem času (kreditna sposobnost, cenejše upravljanje z likvidnostjo), pametne pogodbe, sledljivost na račun zasebnosti, programirljiv denar.
Norveška	– Pametne pogodbe (tveganje tretje strani zmanjšano), obstojnost, alternativa zasebnim sistemom za preventivno ukrepanje. Rešitev v sili, če bi zasebne kriptovalute destabilizirale gospodarstvo. Ponuja zanesljivo alternativo. Prilagajanje namembnosti.

Vir: lastno delo.

CB-ES-6 je mnenja, da so pridobitve v učinkovitosti na splošno. CPMI pri BIS navaja naslednje prednosti: večjo hitrost obdelave od konca do konca, nižje stroške obdelave s pomočjo kriptografije, hitrejše in bolj transparentno usklajevanje podatkov, transakcije v realnem času, kar vodi do večje kreditne sposobnosti in cenejšega upravljanja z likvidnostjo, pametne pogodbe in sledljivost (na račun zasebnosti). Po Kuhn in drugi (2019) se podatki v omrežju z dosegom konsenza uskladijo v realnem času. Z žetoni in pametnimi pogodbami se veča učinkovitost, denar in plačila postanejo programirljiva. Po Mathis (2016) je slednja ena od ključnih lastnosti DLT. Uporabi se ga lahko za digitalno identiteto, kot poudarja CPMI. Po Mills in drugi (2016) se kriptografija pri DLT uporablja tudi za dokazovanje identitete in šifriranje podatkov.

CB-NO-7 izpostavlja odpravljeno tveganje nasprotne strani z uporabo pametnih pogodb in njeno večjo obstojnost. Čezmejni CBDC po Ward in Rochemont (2019) bistveno izboljša kreditno, plačilno in poravnalno tveganje nasprotne strani. Omogoča vzpostavitev konkurence, če zasebne kriptovalute prekomerno pridobijo na moči, in se ga lahko uporabi za preventivno ukrepanje kot rešitev v sili. Kriptovalute po Ward in Rochemont (2019) lahko vplivajo na zasnovo plačilnega sistema, zato odločevalci iščejo rešitev v digitalni valuti, zajamčeni z njihove strani. V tabeli 5 so zbrane vse prepoznane prednosti in priložnosti razpršene evidence v plačilnih sistemih s strani respondentov centralnih bank.

8.3 Prepoznane slabosti in izzivi

CB-HN-1 izpostavlja zgodnjo fazo razvoja tehnologije in njeno razumevanje ter sprejetost s strani državnih organov. Po raziskavi WEF (2019) nekatere institucije niso namenile virov za raziskovanje DLT zaradi njene tehnološke nezrelosti in s tem povezanih tveganj. CB-HN-1 meni, da je zaupanje v tehnologijo ključno. Manjkata ji ustrezna zakonodaja in strokovno usposobljen kader. Tudi po IBRD (2017) tehnologija še ni v okvirih zakonodaje in industrijskih standardov.

CB-CO-2 skrbi zasebnost uporabnikov; po Hodrick (2018) težave v varnosti povzročata pomanjkanje zasebnosti oz. prevelika transparentnost. CB-PL-3 vidi kot težavo uveljavljanje zahtev AML/CFT, nižjo hitrost in visoko porabo energije; po Bott in Milkau (2016) so že v letu 2014 ocene porabljene električne energije znašale toliko kot letna poraba za državo Irsko. Kot problematične prepozna tudi obsežne vire za shranjevanje, vprašanje dokončnosti poravnav ter nepovratnost transakcij. Po Hodrick (2018) dokončnost ni popolnoma v skladu z zahtevami predpisov in tudi, kako se spoprijeti z reklamacijami, še ni jasno.

CB-SK-4 tudi moti nepovratnost transakcij, nezrelost tehnologije in primanjkovanje znanja širši javnosti o njej. Inovacija sama ni zadosten razlog za njeno vpeljavo po njihovem mnenju. Izzive na evropski ravni vidijo tudi v varnosti, zaščiti podatkov in uveljavljanju zahteve proti pranju denarja (AML). Po Agur in drugi (2018) sta lastništvo kriptovalut in njihova uporaba anonimna, saj so lahko računi ustvarjeni pod umetno ustvarjenimi imeni, zato nastopijo pomisleki glede zahtev AML in boja proti financiranju terorizma (CFT).

CB-SE-5 kot pomanjkljivost izpostavlja pomanjkanje ustrezne zakonodaje in različna pravosodja. Po IBRD (2017) so neskladja tudi med zakonodajami v čezmejnih sistemih razpršene evidence v zvezi s podatki in transakcijami. Po CB-SE-5 so tudi težave v razširljivosti in nepredvidena operativna tveganja, prav tako je nerešeno vprašanje poravnave. Tudi po Agur in drugi (2018) se kriptovalute soočajo s težavo v razširljivosti, ker je vsaka transakcija, zabeležena v evidenci, poslana vsem uporabnikom v sistemu, kar vodi v omrežje z eksponentno rastjo števila beleženih transakcij.

Tabela 6: Slabosti in izzivi DLT pri PCS

Država CB	**Slabosti in izzivi DLT pri PCS**
Honduras	– Zgodnja faza razvoja (nerazumevanje, nesprejetost, nezaupanje). – Pomanjkanje zakonodaje in usposobljenega kadra.
Kolumbija	– Upravljanje, pravila zasebnosti.
Poljska	– AML/CFT-tveganja, nižja hitrost, energetska potratnost, viri za shranjevanje, dokončnost poravnave in nepovratnost transakcij.
Slovaška	– Nepreklicne transakcije, nezmožnost reklamacij, novost tehnologije. – Na evropski ravni: varnost, zaščita podatkov, zahteva AML.
Švedska	– Pravna tveganja, tuje jurisdikcije, razširljivost in nepredvidena operativna tveganja, vprašanje poravnave.
Španija	– Razširljivost, interoperabilnost, sistem upravljanja, knjigovodska dokončnost, operativno in varnostno tveganje, robustnost in obstojnost.
Norveška	– Zakonodaja: lastniške pravice, odgovornosti, regulativna vprašanja.

Vir: lastno delo.

CB-ES-6 skrbijo razširljivost, pomanjkanje interoperabilnosti, sistem upravljanja, knjigovodska dokončnost poravnav, operativno in varnostno tveganje. Po BIS (2015) so tehnični in varnostni pomisleki povezani s tem, da udeleženci omrežja lahko potrdijo nelegitimno evidenco in se tretja stran na ta način okoristi. Izzivi v robustnosti in obstojnosti sistema so po IBRD (2017) posledica zgodnje faze razvoja, še posebej pri prenosih velikih vrednosti, razpoložljivosti primerljive strojne opreme in programskih aplikacij ter zadostnega števila usposobljenih strokovnjakov. CB-NO-7 poudarja negotove pravne okvire v zvezi z lastniškimi pravicami žetonov in prevzemanjem odgovornosti. Če uporabnik nima več dostopnega gesla, je po BIS (2015) zelo verjetno, da ne bo mogel doseči svojih sredstev. Nekateri lastniki kriptosredstev zato zaupajo posrednikom pri shranjevanju in varovanju svojih gesel. Tabela 6 povzema vse slabosti in izzive tehnologije razpršene evidence, ki jih pri plačilnih sistemih ugotavljajo respondenti.

8.4 Pravice v upravljanju plačilnih sistemov na razpršeni evidenci

CB-PL-3 opredeljuje ločnico med javnim in zasebnim DLT glede upravljanja vozlišč. Po Oliver (2018) se sistem deli na javno dostopen in na sistem, dostopen le zasebnim uporabnikom. Dalje se deli na pravice uporabnikov glede vpogleda v podatke, izvedbe transakcij in potrjevanja transakcij. Po Anderson (2019) se v primeru distribuiranega sistema

obdelava transakcij odvija na več mestih, vsakdo lahko v okviru pravil omrežja vpisuje in dostopa do evidence. CB-SK-4 deli DLT na to, kdo lahko bere, ustvarja ali vključuje transakcije v evidenco za stalno, na naslednje podtipe: zasebni ali javni, brez omejitev pravic ali z omejitvami pravic ter z dovoljenjem ali brez dovoljenja v upravljanju. CB-NO-7 je mnenja, da javne verige blokov ne ustrezajo pogojem za CBDC. Prav tako zunanji registri prinašajo določena tveganja CB. Po IBRD (2017) je implementacija zakonov pri odprtih razpršenih evidencah bistveno bolj zahtevna kot pri zaprtih, kjer je za njih odgovoren upravljalec sistema. Prav tako ima administrator pri zaprtem sistemu jasne naloge upravljanja, medtem ko pri odprtem ni definirano, za koga veljajo.

8.5 Področja uporabe, tipi tehnologij, platforme in raziskovalna združenja

Zunaj področja plačil, kliringa in poravnav banke vidijo področja uporabe še drugje. CB-CO-2 izpostavlja rabo še v dostavah proti plačilu (DvP) in sredstev skozi celotno obdobje od izdaje, trgovanja, korporativnih aktivnosti, poravnave do zapadlosti. CB-SK-4 v arhiviranju podatkov, upravljanju identitete, sledenju podatkom in v storitvah javne uprave. Po Wattenhofer (2017) vse shranjene informacije postanejo nespremenljiva baza podatkov. Ima pa sistem po Le Borne in drugi (2016) tudi svoje pomanjkljivosti v upravljanju identitet, saj temelji na neobnovljivih ključih. CB-SE-5 trdi, da v zagotavljanju skladnosti, shranjevanju, izmenjavi podatkov in proti pranju denarja. Po Catalini in Gans (2019) tudi pri avtomatiziranem preverjanju ostane posrednikom še naloga zagotavljanja skladnosti s predpisi in delovno intenzivno preverjanje informacij.

Za najbolj smiselne konsenzne mehanizme prepoznavajo naslednje. CB-CO-2 praktično toleranco napake (pBFT) in konsenz RAFT. V CB-ES-6 so indiferentni, poudarjajo pa pomen knjigovodske dokončnosti. Po Bott in Milkau (2016) je DLT nedeterminističen, zato so potrditve dokončnosti transakcij posledica verjetnosti. CB-NO-7 meni, da dokaz o delu (angl. Proof of Work, PoW) zagotovo ni primeren, saj izogibanje zaupni tretji strani ni utemeljeno. Za omrežje DLT bi bilo potrebno dovoljenje za pravice, kar nudi obstojnost in programirljivost, pa tudi možnost prenosa sredstev v druga omrežja DLT. Po Hayes (2016) digitalna valuta z razpršenim dovoljenjem omogoča bankam in finančnim institucijam, da upravljajo z vozlišči in nadomestijo energetsko potraten proces rudarjenja ter povečajo učinkovitost. Za CB-NO-7 so pomembne lastnosti tehnologije in ne tehnologija sama. Po BoC (2020) bi se CBDC približal značilnostim gotovine z medvrstniškim prenosom, takojšnjo poravnavo, zasebnostjo, obstojnostjo, če infrastruktura zataji, in bi bil povsod dostopen.

CB-SE-5 trdi, da bo sistem DLT potreboval dovoljenje za dostop in za pravice o upravljanju. Veleprodajni CBDC bo temeljil na žetonu, z njim bodo povezane trgovinske finance. Po Sveriges Riksbank (2018) je vpeljava e-krone za Riksbank v skladu s spodbujanjem varnega in učinkovitega plačilnega sistema. Tehnologija e-krone na žetonu je že v skladu z zakonodajo banke. Njihov pilotni projekt spremlja e-krono kot rešitev v raziskovanju na

platformi R3 Corda. Tudi v projektu Jasper po PC in drugi (2017) uporabljajo isto platformo s konceptom vozlišča zaupnega notarja v središču konsenznega protokola. Platforma omogoča atomske transakcije in mehanizem za varčevanje z likvidnostjo.

Banke omenjajo članske organizacije oziroma konzorcije in platforme za DLT. CB-CO-2 izpostavlja R3, Hyperledger in Ripple. Tudi IBRD (2017) navaja poleg platforme Corda, ki je produkt konzorcija R3, Fabric, rezultat projekta Hyperledger kot primer razvoja DLT za finančni sektor. CB-SE-5 uporablja platformo R3 Corda. CB-ES-6 navaja kot primer iniciativo Alastria, ki se sicer ne ukvarja s PCS.

8.6 Ugotovitve konzorcija poslovnih bank in finančnih institucij

8.6.1 Mehanizem delovanja

Določene banke nimajo dovoljenja za opravljanje bančnih poslov s tujo valuto v tujini, zato imajo pri korespondenčni banki odprte nostro račune. Z digitalizacijo valut bi postalo poslovanje v tuji valuti izvedljivo. Proces mednarodnih plačil bi se poenostavil, odstranjeni bi bili posredniki, predvsem korespondenčne banke (FN-8).

V primerjavi s posredniki so po Catalini in Gans (2019) stroški preverjanja transakcij z digitalizacijo zanemarljivi. Preverjanje namesto posrednikov opravljajo avtomatizirani procesi in digitalne metode avtentikacije. V mednarodnih plačilih bi uvedba CBDC s strani poslovne banke po van Ginneken (2019) naredila trg nekonkurenčen, k čemur bi prispevali prednost prvega na trgu in ekonomije obsega. Enake pogoje za vse udeležence bi zagotavljala CB z izdajo svojega denarja.

8.6.2 Prednosti in priložnosti

Delovnemu času CB se ne bi bilo treba prilagajati, saj so po van Ginneken (2019) denarnice v evidenci PB na voljo s stalno razpoložljivostjo. Zahteva o poznavanju svoje stranke oziroma dodatne preveritve stanj na računih, identifikacija strank in izpolnjevanje pogojev proti pranju denarja bi bile odvečne.

Več valut v menjavi ne bi predstavljalo dodatnih zapletov. Digitalizirane valute bi zastopale veleprodajno centralnobančno digitalno valuto. Toda po van Ginneken (2019) bi nove PB in korporativne stranke v tuji jurisdikciji predstavljale pravna tveganja. S pametnimi pogodbami se naredi denar programirljiv, določi se lahko njegovo namembnost, da se ga potroši lahko le za določene dobrine ali storitve. Tudi znesek uporabe, minimalni ali maksimalni ter rok uporabe (FN-8). Uvedba veleprodajnega CBDC po Ward in Rochemont (2019) omogoča hitrejše poravnave in daljši delovni čas. Določitev namembnosti uporabe CBDC po WEF (2019) lahko razdeli CBDC v dve kategoriji, dostopnega javnosti kot maloprodajni CBDC ali omejenega na finančne institucije kot veleprodajni CBDC.

Eden od možnih razlogov za razvoj maloprodajnega CBDC so po Agur in drugi (2018) pomanjkljivosti, povezane s povečano prisotnostjo kriptovalut v zasebnem sektorju. Maloprodajni CBDC ne bi bil družbeno koristen po Ward in Rochemont (2019), če bi ga izrinil zasebno izdan e-denar. Ponudniki v takšnih shemah stremijo k maksimiziranju svojih dobičkov, kar ni skladno z doktrino fiat valute. Po Grym in drugi (2017) bi valuta CB bila v digitalni obliki namenjena splošni uporabi, poenotena bi bila z državno valuto in izključevala bi posrednike.

Tveganje poravnave odpravi na način, da naredi transakcije vzajemne tako, da se obe izvedeta sočasno. Na tak način se odpravi tveganje nasprotne strani oziroma neizpolnitve obveznosti ali neplačilo in poravnalno tveganje, povezano s časom dostave. Usklajevanje je prednost, saj ni ročnega vnosa in možnosti za napake, kajti podatki so vsem dostopni (FN-8). Atomskost transakcij je po ECB in BoJ (2018) mehanizem poravnave za prenos dveh sredstev na način, da zagotovi prenos enega sredstva istočasno s prenosom drugega sredstva. Izid poravnave je, da si obe strani uspešno izmenjata sredstvi ali pa transakcija sploh ni izvedena. Potrjevanje pri DLT po Wadsworth (2018) zajema kliring in poravnavo obenem, saj tu ni razlike med pošiljanjem informacij o finančni transakciji in dokončni izmenjavi denarja.

Zakonska podlaga za tehnologijo še ni dodelana, saj je tudi tehnologija še v razvojni fazi. Potrebna je njena odobritev s strani centralnih bank. Tveganje pri stabilnih kovancih je kreditno tveganje, nihče ne jamči za njihovo vrednost. Izpostavlja se tehnološka tveganja glede njene varnosti. Njena interoperabilnost še ni dosežena. Komponenta zasebnosti je tudi manjkajoča (FN-8).

Tveganje nasprotne strani in kreditno tveganje, ki nastopi v primeru insolventnosti dolžnika, po Ali in drugi (2014) rešuje atomskost transakcij. S takšno poravnavo se po van Ginneken (2019) kreditno tveganje na platformi zmanjša in z njim potreba po tolikšnem kritju za zavarovanje tveganja neporavnave. Do istega tveganja prihaja po Ward in Rochemont (2019) tudi pri nakazilih med subjekti iz različnih pravosodij zaradi časovnih zamikov. Tveganje nasprotne strani po BoC in drugi (2018) bistveno zmanjša zmožnost takojšnje poravnave transakcij in z njim potrebo po kritju.

Ročno usklajevanje med bazami podatkov nasprotnih strani za sisteme DLT po IBRD (2017) ni potrebno, kar zmanjšuje stroške, sistemi namreč razpolagajo z distribuiranimi dejanskimi podatki. Centralizirani sistemi po Kuhn in drugi (2019) tudi omogočajo pametne pogodbe, le da je potrebno usklajevanje obeh strani, kar je dolgotrajno. V DLT imata obe strani isto kopijo evidence in sta soglasni obenem.

8.6.3 Slabosti in tveganja

Regulatorji so v finančnem sektorju po IBRD (2017) zadolženi za učinkovito infrastrukturo upravljanja. Pri odprtem DLT ni reguliranega subjekta, ki bi bil predmet zakonodaje. Kljub

spremljanju tehnologije s strani regulatorjev morajo biti zakonodajni okviri še določeni in standardi vpeljani (FN-8). Ugotovljena prednost DLT pri plačilih v projektu Jasper po PC in drugi (2017) je ohranjanje transparentnosti sistema in boljši nadzor s strani regulatorjev. Nezrelost tehnologije po Kuhn in drugi (2019) predstavlja večjo izpostavljenost tveganjem in zato previdnost pri sprejemanju. Zgodnja faza razvoja tehnologije po IBRD (2017) lahko predstavlja pomanjkljivosti v njeni robustnosti in obstojnosti. Stabilni kovanec (Tether) po Eichengreen (2019) omogoča svojim uporabnikom anonimnost kot pri gotovini, preverljivost na verigi blokov in izkazuje relativno mero stabilnosti.

Tehnološka tveganja šteje med izzive sistema tudi Hodrick (2018). Razširjenost je upočasnjena zaradi pomanjkanja interoperabilnosti. Pomanjkanje zasebnosti oz. prevelika transparentnost povzročata težave v varnosti. Tehnični in varnostni pomisleki so po BIS (2015) povezani s potrditvijo nelegitimne evidence s strani udeležencev omrežja in na ta način z okoriščenjem tretje strani. Po IBRD (2017) morajo različni sistemi DLT biti med seboj interoperabilni in integrirani v razpoložljive sisteme za vključitev v finančni sistem. Umestitev DLT v plačilno infrastrukturo zahteva sodelovanje med industrijami in povzroča visoke stroške. Ravno tako so po IBRD (2017) v odprtih evidencah vse transakcije s psevdonimnimi identitetami vidne vsem članom omrežja. Iz vzorcev transakcij se da sklepati o identiteti udeleženca. Z isto težavo se soočajo tudi zaprte razpršene evidence, zato tudi Corda in Fabric namenjata pozornost reševanju tega vprašanja.

8.6.4 Prihodnji razvoj in faze implementacije

Kar zadeva proučevanje napredka na tem področju s strani raznih iniciativ, je npr. Odbor za plačila in tržno infrastrukturo (CPMI) pri BIS v letu 2018 po Barontini in Holden (2019) opravil obsežno raziskavo s 63 CB o vpeljavi CBDC.

Finančne institucije in banke so razvijale DLT v raznih projektih, kot je npr. projekt Ubin, ki je po Deloitte in drugi (2018) temeljil na singapurskem dolarju (SGD) na evidenci kot žetonu in projektu Jasper-Ubin, kjer je po BoC in MAS (2019) sodelovanje med CB Singapurja in Kanade (ob podpori JP Morgan in tehnološkega podjetja Accenture) uspešno dokazalo zmožnost poravnave žetoniranih digitalnih valut med različnima platformama verige podatkovnih blokov.

Način izdajanja digitalne valute po izjavi CB-SE-5 deluje po principu dvostopenjskega sistema, kjer sama (Riksbank) edina ustvarja CBDC e-krone, igralci na trgu, kot so banke in ponudniki plačilnih storitev, pa služijo kot distributerji e-krone h končnemu uporabniku. Po CB-SE-5 CBDC ne bi smela biti v pristojnosti ponudnikov plačilnih storitev ali zasebnih bank za dodelitev končnim uporabnikom.

8.6.5 Tipi tehnologij in organizacije

Tehnologija, primerna za CBDC, je toleranca napake (BFT), kjer sistem lahko kljub anomalijam nekaterih vozlišč deluje nemoteno. Dokaz o delu je energetsko potraten in ni potreben, ko je za sistem zadolžena zaupna institucija. Poleg tega ima tehnologija tudi težave z razširljivostjo. Hashgraph je primerljiv z zasebno verigo blokov, medtem ko bi CBDC deloval na javni verigi blokov, za katero je potrebno dovoljenje za dostop. Corda vključuje posrednike, kar je nezaželeno (FN-8).

Za dokaz o delu je po Wadsworth (2018) potrebnih sistemsko zastavljenih 10 minut za rešitev problema, kar se odraža tudi v stroških rudarjenja. Po Bott in Milkau (2016) so bile že v letu 2014 ocene porabljene električne energije primerljive z letno porabo Irske. Toleranco napake (BFT) kot konsenzni mehanizem v tehnologiji razpršene evidence omenjajo tudi Rauchs in drugi (2018).

Omrežje Hashgraph je po Baird in drugi (2019) zasebno in dostopno le pooblaščenim uporabnikom. Struktura podatkov in konsenzni mehanizem na verigi blokov naredi po Rauchs in drugi (2018) razširljivost težavno. Povečanje razširljivosti bi bilo potrebno za DLT po Hayes (2016) za pokritje potreb po transakcijah v gospodarstvu.

Tabela 7: Ugotovitve konzorcija poslovnih bank in finančnih institucij o DLT pri PCS

Ugotovitve konzorcija poslovnih bank in finančnih institucij o DLT pri PCS
– Digitalizacija denarja, veleprodajni CBDC in mednarodna plačila. – Transakcije v tuji valuti (nostro/vostro). – Poenostavi mednarodna plačila – nabor posrednikov, menjava valut. Gotovina obveznost CB, depoziti obveznost PB. Programirljivost denarja za določene dobrine. Atomska transakcija: odprava poravnalnega tveganja in tveganja nasprotne strani. Usklajevanje in transparentnost. – Pravni okvirji – odobritev s strani regulatorjev. Kreditno tveganje stabilnih kovancev poslovnih bank. Vprašanje varnosti, interoperabilnost in zasebnost. – Nereguliran način v reguliran način, javno zasebno partnerstvo. – Maloprodajni CBDC: veleprodajni CBDC v razmerju 1:9. – PoW ni primeren. Toleranca napake je zaželena. Hashgraph je kot zasebna veriga blokov, potrebne dovolilnice pri plačilih na javni verigi blokov. Razširljivost. Corda zaradi vozlišč notarjev ni zaželena.

Vir: lastno delo.

Koncept vozlišča zaupnega notarja kot osrednjega dela konsenznega protokola je stopil po PC in drugi (2017) v veljavo v drugi fazi projekta Jasper, septembra 2016, s prehodom z Ethereuma na platformo R3, imenovano Corda. Platformi, kot sta Corda v Kanadi in Quroum v Singapurju, povezuje po BoC in MAS (2019) projekt Jasper-Ubin, ki predpostavlja različne platforme za RTGS na DLT po državah. V tabeli 7 so izpostavljene vse glavne ugotovitve konzorcija Fnality.

9 SKLEP

Decentralizacija prispeva k večji hitrosti in nižjim stroškom transakcij. Plačila so možna v realnem času tudi tam, kjer v običajnih sistemih niso, to vodi v boljšo kreditno sposobnost in naredi upravljanje z likvidnostjo cenejše. Pametne pogodbe odpravijo kreditno tveganje, tveganje nasprotne strani in poravnalno tveganje, saj v t. i. atomski poravnavi pride do izmenjave med nasprotnima stranema istočasno. Prednost plačilnega sistema na tehnologiji razpršene evidence je tudi cenejša infrastruktura. Razpršena evidenca nima enotne točke odpovedi, kar okrepi obstojnost sistema. Hranjenje kopije podatkov prek mreže vozlišč nudi samodejno in takojšnje usklajevanje. Prav tako nudi centralnobančni sistem na razpršeni evidenci ukrepanje v sili, in sicer v primeru, če kriptovalute ogrozijo stabilnost gospodarstva. Že pri stabilnih kovancih obstaja tveganje neizplačila, saj nihče ne jamči za njihovo vrednost. Najizraziteje se izkazuje učinkovitost pri čezmejnih plačilih, saj je pri njihovem poteku polno trenj – z digitalizacijo fiat valut se poenostavi mednarodna plačila. To pomeni odpravo posrednikov (korespondenčnih bank in delovno intenzivnih preveritev) in neprestano delovanje sistema. Tehnologija omogoča transparentnost in nespremenljivo revizijsko sled. Programirljivemu denarju se lahko določi namembnost, npr. le za določene dobrine in storitve z zneskom in rokom uporabe.

Po drugi strani povzroča nespremenljivost težave pri povračilu sredstev. Anonimnost je lahko privlačna za nezakonite aktivnosti. Hkrati pa psevdoanonimnost dovoljuje vpogled v transakcije neupravičenim stranem. Možne slabosti so nezrelost tehnologije in temu primerno pomanjkanje zakonodaje. Pri nekaterih sistemih je dokončnost poravnave nedeterministična, torej verjetnostna, in ne izpolnjuje računovodskih standardov. Kriptovalute imajo težave pri razširljivosti, zasebnosti (saj ne izpolnjujejo pogojev poznavanja svoje stranke) in energetski potratnosti konsenznega mehanizma dokaza o delu. Pri njih obstaja tudi tveganje izgube dostopa do sredstev. Izboljšati je treba še njihovo interoperabilnost z drugimi sistemi tudi zaradi zagotavljanja atomskosti transakcij. Upravljanje je lahko težavno, če ni prisotnega osrednjega subjekta pri odločanju.

Monetarni sistem, s katerim upravlja CB, je neločljivo povezan s plačilnim sistemom. Pri finančnih institucijah bo imela tehnologija razpršene evidence zaprt dostop za upravljanje, pa tudi nadzor pristojnega organa. Digitalna valuta lahko obstaja tudi na verigi blokov z razpršenim dovoljenjem, kjer je vsako vozlišče v omrežju poznan in zaupen subjekt kot PB ali finančne institucije. S tem se zmanjša potreba po dragem in energetsko potratnem rudarjenju in bistveno povečata hitrost in število transakcij.

Brezgotovinska družba bi izključevala posameznike, ki nimajo dostopa do bančnih računov, lahko bi dopuščala posege v zasebnost transakcij, tudi manjše tehnološke napake, vdori, naravne nesreče bi lahko onemogočili dostop do sredstev, plačila in nakupe, vlagatelji ne bi mogli dvigniti denarja v fizični obliki, da bi ga rešili pred izgubo, in se ne bi mogli izogniti negativnim obrestnim meram. Digitalni denar bi bil vnesen v obtok prek namenskih računov pri nadzorovanih depozitnih institucijah, ki bi del sredstev hranile v rezervah pri CB – takšen

pristop bi krepil konkurenco. Tudi Fedcoin bi bil kot gotovina decentraliziran pri transakcijah in centraliziran v ponudbi.

Motivi za zamenjavo gotovine z njeno digitalno obliko bi lahko bili naslednji: ne zagotavlja sledljivosti, kar lahko omogoča nezakonite transakcije. Umik gotovine bi prispeval k zmanjšanju kriminala in povečanju davčnih prihodkov. CBDC je alternativa gotovini s P2P-izmenjavo, vendar za razliko od nje omogoča sledljivost, obrestonosnost in programirljivost za namembnost uporabe. DLT torej lahko pripomore k zagotavljanju zaželenih lastnosti CBDC. Potrebna je še odobritev regulatorjev.

LITERATURA IN VIRI

1. Accenture. (2017, 12. oktober). *Accenture, MAS and ABS Developing Distributed Ledger Technology Solutions for Settlement of Payments Using Central Bank Digital Currency*. https://research-ebsco-com.nukweb.nuk.uni-lj.si/linkprocessor/plink?id=20c05e93-6bd2-3126-bce4-b6dabd56f236
2. Accenture. (2018, 5. november). *Payments Canada, the Bank of Canada, TMX Group, Accenture and R3 Demonstrate Feasibility of Instantaneous Equity Settlement through Distributed Ledger Technology*. https://research-ebsco-com.nukweb.nuk.uni-lj.si/linkprocessor/plink?id=f651f5ef-53dc-3ae3-b414-b1f637922a76
3. Agur, I., Bergara, M., Bordo, M., Engert, W., Fernandez de Lis, S., Fung, B., Gnan, E., Levin, A., Niepelt, D., Judson, J., Masciandaro, D., Panetta, F., Pichler, P., Ponce, J. in Summer, M. (2018). *Do we need central bank digital currency? Economics, Technology and Institutions*. Larcier.
4. Ali, R., Barrdear, J., Clews, R. in Southgate, J. (2014). Innovations in Payment Technologies and the Emergence of Digital Currencies. *Bank of England Quarterly Bulletin, 54*(3), 262–275.
5. Anderson, M. (2019). Exploring Decentralization: Blockchain Technology and Complex Coordination. *Journal of Design and Science*. https://jods.mitpress.mit.edu/pub/7vxemtm3
6. Auer, R. in Böhme, R. (2020). The Technology of Retail Central Bank Digital Currency. *BIS Quarterly Review*. https://ssrn.com/abstract=3561198
7. Baird, L., Harmon, M. in Madsen, P. (2019). *Hedera: A Public Hashgraph Network & Governing Council*. Hedera Hashgraph.
8. Barontini, C. in Holden, H. (2019). *Proceeding with caution - a survey on central bank digital currency*. BIS.
9. Bech, M. in Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review*. https://ssrn.com/abstract=3041906
10. Bank for International Settlements. (2015). *Digital Currencies*. *Committee on Payments and Market Infrastructures Report*. BIS.

11. Bank for International Settlements. (2017). *Distributed ledger technology in payment, clearing and settlement: An analytical framework*. Committee on Payments and Market Infrastructures.
12. Bank for International Settlements. (2018). *Central bank digital currencies*. *Committee on Payments and Market Infrastructure & Markets Committee Report*. BIS.
13. Bank of Canada. (2020). *Contingency Planning for a Central Bank Digital Currency*. BoC.
14. Bank of Canada, Bank of England in Monetary Authority of Singapore. (2018). *Cross-Border Interbank Payments and Settlements: Emerging Opportunities for Digital Transformation*. KPMG Services Pte. Ltd.
15. Bank of Canada in Monetary Authority of Singapore. (2019). *Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (Jasper-Ubin Design Paper)*. Accenture.
16. Bordo, M. D. in Levin, A. T. (2019). Improving the monetary regime: the case for U.S. *Cato Journal, 39*(2), 383–405.
17. Bott, J. in Milkau, U. (2016). Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments. *Journal of Payments Strategy & Systems, 10*(2), 153–171.
18. Brainard, L. (2016). Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement. *Institute of International Finance Annual Meeting Panel on Blockchain*. Board of Governors of the Federal Reserve System.
19. Bruhl, V. (2017). Virtual Currencies, Distributed Ledgers and the Future of Financial Services. *Intereconomics/Review of European Economic Policy, 52*(6), 370–378.
20. Casar, F., Hughes, D., Primero, J. in Thornton, S. (2020). *Cerberus: A Parallelized BFT Consensus Protocol for Radix*. Radix.
21. Catalini, C. in Gans, J. (2019). *Some simple economics of the blockchain*. National Bureau of Economic Resarch.
22. Ciaian, P., Rajcaniova, M. in Kancs, d'A. (2016). The Economics of BitCoin Price Formation. *Applied Economics, 48*(19), 1799–1815.
23. Cline, B., Seibold, S. in Samman, G. (2016). *Consensus: Immutable Agreement for the Internet of Value*. KPMG LLP.
24. Conte de Leon, D., Stalick, A. Q., Jillepalli, A. A., Haney, M. A. in Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and, 11*(3), 286–300.
25. Crosman, P. (2015). Why Banks Are Testing Bitcoin's Blockchain (Without Bitcoin). *American Banker, 180*(84), 0.
26. Crosman, P. (2022). The road ahead for Meta’s Diem under Silvergate Bank’s ownership. *American Banker, 187*(28), 4–6.
27. Deloitte, Singapore Exchange in Monetary Authority of Singapore. (2018). *Delivery versus Payment on Distributed Ledger Technologies: Project Ubin*. Deloitte Consulting Pte, Ltd.

28. Duignan, B. (2022, 30. junij). *What Is a Cashless Society and How Does It Work?* https://www.britannica.com/story/what-is-a-cashless-society-and-how-does-it-work
29. European Central Bank in Bank of Japan. (2018). *Project Stella - Securities settlement systems: delivery-versus-payment in a distributed ledger enviornment*. ECB in BoJ.
30. Eichengreen, B. (2019). *From Commodity to Fiat and Now to Crypto: What Does History Tell Us?* National Bureau of Economic Research.
31. Fintech. (brez datuma). *Cryptocurrency: Blockchain* (5. izd.). Fintech Publishing.
32. Friedman, M. (1948). A monetary and fiscal framework for economic stability. *The American Economic Review, 38*(3), 245–264.
33. Global Banking News. (2018a, 15. junij). *Bank of Canada indicates it is not enthused by performance of blockchain*. https://research-ebsco-com.nukweb.nuk.uni-lj.si/linkprocessor/plink?id=cffeaa71-a8df-3535-ad9d-b9b7c46fe9bd
34. Global Banking News. (2018b, 13. april). *Bitcoin rallies following Santander's launch of payment service*. https://research-ebsco-com.nukweb.nuk.uni-lj.si/linkprocessor/plink?id=ea816421-e790-3675-ad52-a6771a555502
35. Grym, A., Heikkinen, P., Kauko, K. in Takala, K. (2017). Central bank digital currency. *BoF Economics Review, 5*.
36. Harris-Braun, E., Luck, N. in Brock, A. (2018). *Holochain: Scalable Agent-Centric Distributed Computing*. Ceptr, LLC.
37. Hayes, A. (2015). Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin. *Telematics and Informatics, 34*(7), 1308-1321.
38. Hayes, A. (2016). Decentralized Banking: Monetary Technocracy in the Digital Age. V *Tenth Mediterranean Conference on Information Systems Proceedings*. Association for Information Systems.
39. Hodrick, L. S. (2018). Payment Systems and the Distributed Ledger Technology. V M. D. Bordo, J. Bullard, M. Eichenbaum, J. Fernández- Villaverde, A. T. Levin, C. I. Plosser, D. Sanches, K. Warsh, M. Brunnermeier, J. H. Cochrane, C. L. Evans, S. Fischer, A. Krishnamurthy, L. E. Ohanian, E. Rosengren, J. B. Taylor in V. Wieland (ur.), *The Structural Foundations of Monetary Policy* (str. 131–136). Stanford University Press, Hoover Institution Press.
40. IBM in Official Monetary and Financial Institutions Forum. (2019). *Retail CBDCs: The next payments frontier*. OMFIF.
41. Kshetri, N. (2022). El Salvador's Bitcoin Gamble. *Computer (00189162), 55*(6), 85–89.
42. Kuhn, R., Yaga, D. in Voas, J. (2019). Rethinking Distributed Ledger Technology. *Computer (00189162), 52*(2), str. 68–72.
43. Kuzmanovic, J. in Savic, M. (2023, marec). Do Kwon Held in Montenegro Quarantine. https://www.bloomberg.com/news/articles/2023-03-28/crypto-mogul-do-kwon-held-in-montenegro-quarantine
44. Le Borne, F., Treat, D., Dimidschstein, F. in Brodersen, C. (2016). *SWIFT on distributed ledger technologies: Delivering an industry-standard platform through community collaboration* (Position paper). SWIFT SCRL.

45. Mancini-Griffoli, T., Peria, M., Agur, I., Ari, A., Kiff, J., Popescu, A. in Rochon, C. (2018). *Casting Light on Central Bank Digital Currency*. IMF.
46. Mathis, T. (2016). *Blockchain: A Guide to Blockchain, The Technology Behind Bitcoin, Ethereum and Other Cryptocurrencies*. Level Up Lifestyle Limited.
47. McLellan, L. (2018). *Banks ready blockhain tokens for debt and equity*. GlobalCapital.
48. Meaning, J., Dyson, B., Barker, J. in Clayton, E. (2018). *Broadening narrow money: monetary policy with a central bank digital currency*. Bank of England.
49. Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W. in Baird, M. (2016). Working Papers -- U.S. Federal Reserve Board's Finance & Economic Discussion Series. *Distributed ledger technology in payments, clearing, and settlement*, 1–34.
50. Mohammad, S. in Davoodalhosseini, R. (2018). *Central Bank Digital Currency and Monetary Policy*. Bank of Canada.
51. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
52. National Archives and Records Administration. (2019). *Blockchain White Paper*. NARA.
53. Niepelt, D. (2018). *Reserves For All? Central Bank Digital Currency, Deposits, and their (Non)-Equiavalence*. Munich Society for the Promotion of Economic Research - CESifo GmbH.
54. Oliver, P. (2018). *Blockchain 101: Distributed Ledger Technology (DLT)*. Independently Published.
55. Opare, E. A. in Kim, K. (2020). *Design Practices for Wholesale Central Bank Digital Currencies from the World*. The Institute of Electronics, Information and Communication Engineers.
56. Payments Canada, Bank of Canada in R3. (2017). *A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement*. *Project Jasper White Paper*. PC in BoC.
57. Popov, S. (2018). *Tha Tangle*. IOTA.
58. Quiroz-Gutierrez, M. (2022). "I didn't get out because I got greedy": Investors share losses on Luna Reddit forum as the coin drops 97% in 24 hours. *Fortune*. https://fortune.com/crypto/2022/05/11/luna-ust-reddit-stablecoins-crypto-crash
59. Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K. in Zhang, B. Z. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework*. Centre for Alternative Finance.
60. Ricardo, D. (1824). *Plan for the Establishment of a National Bank*. John Murray.
61. Sadeh Man, I. (2020, marec). *Saga's Whitepaper*. https://www.sogur.com/static/files/p/--08d9a3f2-0118-43aa-b7d8-9a77a966c319_Saga%2BWhitepaper%2BMarch%2B2020.pdf
62. Schneider, N. (2019). Decentralization: an incomplete ambition. *Journal of Cultural Economy, 12*(4), 265–285.
63. Schwab, K. (2016). *Četrta industrijska revolucija*. FrodX.

64. Shin, H. S. (2018). V. Cryptocurrencies: looking beyond the hype. *BIS Annual Economic Report*, 91–114.
65. Smithin, J. (2002). *What is money?* Routledge.
66. Soederberg, G. (2019). *Economic Comentaries: The e-krona now and for the future*. Sveriges Riksbank.
67. Sveriges Riksbank. (2018). *The Riksbank's e-krona project: Report 2*. Stockholm.
68. The International Bank for Reconstruction and Development. (2017). *FinTech Note, 1. Distributed Ledger Technology (DLT) and Blockchain*. The World Bank.
69. Townsend, M. (2018). World Bank To Issue First Ever Blockchain Bond. *Global Finance, 32*(8), 61.
70. Tripathi, G., Ahad, M. A. in Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal, 9*. https://doi.org/10.1016/j.dajour.2023.100344
71. van Ginneken, C. L. (2019). *Settlement of Cross-Border Transactions through Central Bank Digital Currency*. University of Twente.
72. Virmani, T. (2018, 20. november). *18 blockchain consortia you should know about*. https://medium.com/blockchain-blog
73. Wadsworth, A. (2018). Decrypting the role of distributed ledger technology in payments processes. *Reserve Bank of New Zealand Bulletin, 81*(5), 3–19.
74. Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L. in Wang, F. Y. (2019). Decentralized Autonomous Organizations: Concept, Model, and Applications. *IEEE Transactions on Computational Social Systems, 6*(5), 870–878.
75. Ward, O. in Rochemont, S. (2019). *Understanding Central Bank Digital Currencies (CBDC)*. Institute and Faculty of Actuaries.
76. Wattenhofer, R. (2017). *Distributed Ledger Technology: The Science of the Blockchain*. CreateSpace Independent Publishing Platform.
77. World Economic Forum. (2019). *Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today?* World Economic Forum.
78. Williams, I. (2020). *Cross-Industry Use of Blockchain Technology and Opportunities for the Future*. IGI Global.
79. Workie, H. in Jain, K. (2017). Distributed ledger technology: Implications of blockchain for the securities industry. *Journal of Securities Operations & Custody, 9*(4), 347–355.

PRILOGE

Priloga 1: Anketa odprtega tipa s predstavnikom Centralne banke Hondurasa

Questions regarding DLT in PCS (IT department) – Master Thesis

transparencia <transparencia@bch.hn> 11 February 2021 at 18:49
To: Daniel <daniel@valentine.si>

Hi Mr Valentine,

The following, are our answers to your first 5 questions:

1. What are the advantages of DLT in PCS?

Central Bank of Honduras (BCH) has not implemented yet, DLT in Payments, Clearing and Settlement (PCS) systems.

2. What are the challenges and risks of DLT in PCS?

Challenges: maybe, the maturity level of the PCS, and the authorities understanding and trust over the DLT technologies.

Risk: To implement DLT tech, without a clear regulation to use it, and strong technicall skills and dominion of this kind of technologies.

3. Future development and phases of implementation:

Not considired yet in BCH.

4. The role of wholesale and retail central bank digital currency in PCS:

None, digital currencies are not included yet on BCH PCS strategy.

5. The role of tokens and smart contracts in PCS:

Not aply at this time in BCH.

While the information provided is useful for your purposes, please acknowledge receipt, if you have any additional questions or comments, write or call that we will gladly assist you.

Attentive greeting,

Edas Encarnación Lazo Mercado

Jefe Sección de Información Pública

Departamento de Relaciones Institucionales

Banco Central de Honduras

Teléfonos 2216-1000 y 2262-3700 ext. 21421

Apartado Postal 3165

Correo electrónico: edas.lazo@bch.hn y transparencia@bch.hn

"Al Servicio de la Nación"

Priloga 2: Anketa odprtega tipa s predstavnikom Centralne banke Kolumbije

RE: NO-REPLY Registro de Petición - Atención al Ciudadano - Banco de la República C21-12527 - Regarding a question from Daniel in Slovenia

Pinzón González Fabio Mauricio <fpinzogo@banrep.gov.co> 9 February 2021 at 21:5
To: "daniel@valentine.si" <daniel@valentine.si>
Cc: Morales Rodríguez Camilo <cmoralro@banrep.gov.co>, Álvarez Benítez Julio Ernesto <jalvarbe@banrep.gov.co>, Robayo Abello Ivan Adolfo <irobayab@banrep.gov.co>, Penagos Bonilla Daniel Andrés <dpenagbo@banrep.gov.co>, Rodríguez Garzón Camilo Alfonso <crodriga@banrep.gov.co>, Medina Rodríguez Olga Patricia <pmedinro@banrep.gov.co>, Lozano Javier Enrique <Jlozan@banrep.gov.co>, Hómez Prada Deyssi Rocío <dhomezpr@banrep.gov.co>

Hi Daniel,

Here you have my best guess for your questions

1. ***What are the advantages of DLT in PCS?***

The traditional PCS runs in a centralized environment that it is a single point of failure for the whole system. There have been situations where the whole system, even in the UE or Bank of England where the PCS stopped completely for a few hours, paralyzing the economy of the country or region for that period

2. ***What are the challenges and risks of DLT in PCS?***

Since several parts have access to the same information and in some cases are peer institutions, governance and definition of new rules regarding public and private data into the DLT is a must

3. Future development and phases of implementation:

From the central bank perspective we believed is a nice technology for immediate payments and resilience of a wholesale CBDC (Central Bank Digital Currency)

4. ***The role of wholesale and retail central bank digital currency in PCS**:*

Wholesale may be helpful for Real Time Gross Settlement in further developments of these type of systems. In some small economies, retail CBDC can improve the efficiency of the country's PCS

5. The role of tokens and smart contracts in PCS:

Efficiency, Security, Privacy and Credit Risk control.

Additional questions:
6. Areas where DLT in banking could be used exceeding PCS?

CBDC, Delivery vs Payment, Asset Lifecycle Management (i.e. Securities & Bonds)

7. ***What type of DLT (e.g. blockchain, distributed acyclic graph, Hashgraph, etc.) i.e. what kind of consensus protocol (e.g. proof-of-work, proof-of-stake, practical Byzantine fault tolerance, etc.) is most appropriate for PCS and why?***

I believe PBFT because these normally are permissioned blockchains among trusted parties regulated and supervised by a government agent. Even RAFT consensus can be practical where every node is highly reliable (less vulnerable to hackers. TPS (transactions per second) are crucial measure in any PCS

8. ***Main consortiums, their platforms and the infrastructures they use involved in developing DLT in PCS:*** *R3 is the one that sounds a lot as DLT platform. It is DLT. It is not blockchain so solves privacy, consensus and efficiency in its particular design. There is also Hyperledger (open or Fabric from IBM). Ripple still sounds in the international payments arena. I am not familiar with consortiums regarding PCS.*

Regards

FABIO MAURICIO

PINZÓN GONZÁLEZ

General Director of Technology Management (CTO)

Carrera 7 # 14-78, piso 10
Bogotá D.C., Colombia
Tel. (571) 343 0547

fpinzogo@banrep.gov.co
www.banrep.gov.co

Móvil: 3104782463

Priloga 3: Anketa odprtega tipa s predstavnikom Centralne banke Poljske

Questions regarding DLT in PCS (IT department) – Master Thesis

Wójcicka, Anna <anna.wojcicka@nbp.pl> 10 February 2021 at 09:22
To: Daniel <daniel@valentine.si>
Cc: Listy <Listy@nbp.pl>

Dear Mr. Valentine,

in reply to your inquiry please find below the information based on our expertise.

1. What are the advantages of DLT in PCS?

To the best of our knowledge the main advantages of DLT are:

- Use of DLT ensures - by design - full backup of transaction data, as multiple network nodes store full history of transactions.

- Transaction records in PCS are protected from being changed or in other words modifications in transaction history can be detected.

Moreover, many proponents of DLT cite automation (so called "smart contracts", or automated transactions executed under conditions which are defined in the code of the "smart contract") as an advantage of DLT. It is worth noting that DLT is not a prerequisite for automation of transactions in PCS. Any system – centralized or distributed – can be designed in a way that allows automated execution of transactions depending on state of variables from inside the system or observed by sensors connected to the system.

2. What are the challenges and risks of DLT in PCS?

As the "DLT" category contains multiple variants of system design, e.g.: public (anyone can run a node, possibly without identifying themselves) vs private (only entities identified and certified by the system administrator can run a node), "permissionless" (all nodes have full rights to submit transactions, read the state of the ledger and verify transactions) vs "permissioned" (nodes may have only a subset of rights), the set of risks and challenges may be different depending on system design (e.g. AML/CFT risks are higher for public systems which do not require identification of users). It includes:

- lower speed (need for resources in order to execute consensus algorithms),

- redundancy of data requires storage resources,

- settlement finality dependent on consensus algorithm (if consensus algorithm does not exclude forks, then settlement finality is only probabilistic - i.e. probability of reversing the transaction can be close to zero but not zero),

- execution of consumer rights such as chargebacks can be problematic.

3. Future development and phases of implementation:

Please note that the scope of using blockchain technology in payments, clearing and settlements systems in Poland is negligible. Therefore Narodowy Bank Polski is currently not provided with sufficient information to present an assessment requested in question 3, 7 and 8.

Questions 4-5: The role of wholesale and retail central bank digital currency in PCS and the role of tokens and smart contracts in PCS.

Please be informed that at the moment the Management Board of the NBP refers negatively to the possibility of issuance of a digital currency by the Polish central bank. NBP does not conduct practical tests in the field of CBDC or the DLT technology itself. Therefore, NBP does not have any useful experience with wholesale or retail CBDC that could be shared with you.

However, you may wish to refer to the following analytical work on CBDC of the Bank for International Settlements, e.g.:

- Central bank digital currencies (2018; https://www.bis.org/cpmi/publ/d174.pdf)
- The technology of retail central bank digital currency (2020; https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf)
- Central bank digital currencies: foundational principles and core features (2020; https://www.bis.org/publ/othp33.pdf)

6. Areas where DLT in banking could be used exceeding PCS.

We would like to share some information about application of distributed ledger technology solutions in finance in Poland. It should be noted that these applications use DLT in order to take advantage of the Merkle tree property of blockchains and thus create a verifiable, hard-to-modify, database.

The most complex application of DLT in Poland was conducted by KDPW (Central Securities Depository of Poland) which implemented DLT eVoting application. It enables investors to remotely vote at general shareholder meetings of public companies using digital devices. DLT is used to record actions taken at general shareholder meetings (documents submitted, votes taken etc.) in order to create a public record of the meeting which cannot easily be modified afterwards. eVoting is a DLT system which includes shareholders/proxies, issuers, brokers and custodians. See: https://www.kdpw.pl/en/business/e-voting/Pages/default.aspx

The second most important area of application of DLT in finance in Poland is use of DLT for the so-called durable medium (verification of authenticity of documents exchanged between financial institutions and clients in order to prove the content of such document at a specified point of time in the past). Several banks in Poland, including PKO Bank Polski – the biggest bank in Poland, introduced in collaboration with the Clearing House (KIR) a durable medium system with use of DLT. The documents distributed using this system include contracts and price lists (for fees and commissions for banking services) are kept in the DLT system. The latest version of a durable medium in PKO Bank Polski uses DLT combined with cloud storage. See: https://www.kir.pl/en/clients/durable-medium/

We hope you will find the information useful. Should you have any further questions, please do not hesitate to contact us.

Yours sincerely

NBP Narodowy Bank Polski

Anna Wójcicka | Advisor
Payment Systems Department
phone +48 22 185 2527
email: anna.wojcicka@nbp.pl

Narodowy Bank Polski
ul. Świętokrzyska 11/21
00-919 Warszawa
Poland

We protect the value of money

[Quoted text hidden]

Priloga 4: Anketa odprtega tipa s predstavnikom Centralne banke Slovaške

Questions regarding DLT in PCS (IT department) – Master Thesis

info@nbs.sk <info@nbs.sk> 2 February 2021 at 08:27
To: Daniel <daniel@valentine.si>

Dear Daniel,

Thank you very much for your request. We are pleased that you contacted us with regards to your Master Thesis about Distributed Ledger Technology (DLT) in Payments, Clearing and Settlement (PCS). As you mentionned, you are trying to get responses from the professionals and you already did some research through academic articles and institutional reports.

As you know, the National bank of Slovakia is the National Competent Authority with regards to the Slovak financial market. It also makes part of the Eurosystem. Regulations and directives, finalized at the European level, are directly or with some modifications transposed into the national law. Regulation that the National Bank of Slovakia produces together with the Ministry of Finance SR is always impacted by the European legislative framework. This is also valid for several FinTech issues and areas, that are being or are soon going to be regulated.

Firstly, it is important to define the term "DLT". The Distributed ledger technology (DLT) is the term used to refer to those technologies that allow a common ledger to be shared across networks of computers. There are different types of DLTs depending on who can read, create or include transactions permanently on the ledger. There are usually distinguished following three types of DLTs: public versus private DLTs (distinction concerns accessibility of the network), unrestricted verus restricted DLTs (distinction concerns participants, restricted or unrestricted, who are able to create transactions in the DLT) and permissionless verus permissionned DLTs (distinction concerns the person, who is permitted to validate the transaction, whether it is anyone in the DLT network or only some members).

You can find more information on this topic on the following link:
https://www.nbs.sk/en/financial-market-supervision1/fintech/distributed-ledger-technology-dlt
(website of the National Bank of Slovakia dedicated to FinTech, section on DLT).

Pleas find below our responses to your questions:

1.What are the advantages of DLT in PCS?

One of the biggest advantages of the technology, such as DLT, is that it introduces quicker and smoother processes in those areas where they used to be tedious, cumbersome, full of friction, too long and expensive. This is valid for all areas, from payments, to clearing and settlement. Indeed, the DLTs are welcomed by those subjects that offer their services on cross border basis within different jurisdictions. If we take as an example correspodent banking or international payments between some countries, such as a Eurozone country and a non-Eurozone country, this process can be too long and expensive. DLT can be a true practical solution for improvement of such processes.

From the European perspective, for more information concerning the use of the DLT in market securities area, please check the documents such as ESMA (European Securities Market Authority) Report - The Distributed Ledger Technology Applied to Securities Markets:
https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
and also the Digital finance strategy of the European Commission:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591&from=EN
as well as the document from Bank of International Settlements – On the

future of securities settlement:
https://www.bis.org/publ/qtrpdf/r_qt2003i.pdf

For more information concerning the use of DLT in payments or clearing and settlements, please consult the document from the International Monetary Fund:
https://www.imf.org/en/Publications/fintech-notes/Issues/2020/06/25/Distributed-Ledger-Technology-Experiments-in-Payments-and-Settlements-49251

2.What are the challenges and risks of DLT in PCS?

Today, there are several challenges and risks associated with DLTs, but these will possibly decrease in the course of time. One of the challenges of the operations carried out through DLTs is that they cannot be called off and they are not claimable. In praxis, this is a serious problem. In payments, in case of consumer payments for example, this is not the case: rules concerning cancellation and claimability are clearly described, within the SEPA framework as well as in PSD2. In addition, the DLT as technology, is new. Thirdly, from the perspective of financial inclusion, consumers are not ready yet to use it, because it requires a very specific knowledge and skills.

In addition, concerning the domain of payments, clearing and settlement, we do have technologies that are suitable for now. For example the RTGS (Real Time Gross Settlements Systems) such as TARGET2 in payments or TARGET2-securities (T2S) in securities settlement, work well, they are regulated by a legislative framework and altough we are opened towards new innovations, we do not want to replace one system by another only because of innovation itself.

3.Future development and phases of implementation.

There are several developments foreseen in this area especially in the private sector. From the point of view of the European Central bank, please, see the web site dedicated to the topic of DLT:
https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html

For more information about testing and projects carried out through DLTs in different areas, please see Annex I. - List of DLT Experiments and Research in Payments and Settlements in the document from the International Monetary Fund:

https://www.imf.org/en/Publications/fintech-notes/Issues/2020/06/25/Distributed-Ledger-Technology-Experiments-in-Payments-and-Settlements-49251

4.The role of wholesale and retail central bank digital currency in PCS.

The question of wholesale and retail central bank digital currencies in PCS is a very important topic. The pros and cons of different alternatives are being discussed also on the European level from different perspectives, such as security, data protection, AML issues, etc.

Eurosystem is aware of the advancements in this field, especially in countries such as China for example (one of the pioneers in testing and implementation of the CBDC). There have also been lots of discussion introduced by the project Diem (former Libra project from Facebook).

The European Central bank has recently prepared a survey concerning digital currencies that was closed 12.1.2021. The results are now under review. Also the ECB should decide at the middle of the year 2021 whether to continue or not with the projext of digital euro, please see the report on the digital euro: https://www.ecb.europa.eu/euro/html/digitaleuro.en.html

Concerning research in this field, we advise you to consult more on this topic on the link of the Bank of International Settlements:
https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf

5. The role of tokens and smart contracts in PCS

The role of tokens and smart contracts in Payments, Clearing and Settlement can be useful and can lead towards a lot of improvement. However, again, concerning acceptance and use, everything depends on the common consensus agreed at the level of the EU institutions.

Several research papers have been produced by the European institutions in this field. Please see the document from Organization for Economic Co-operationand development on the topic of The Tokenisation of Assets and Potential Implications for Financial Markets: https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf

Please, see also the outcome of the work of the European Commission in the document Legal and regulatory framework of blockchain and smart contracts: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

Additional questions:

6. Areas where DLT in banking could be used exceeding PCS?

From our perspective, and also from the point of view of finance, the areas such as payments, clearing and settlement are the most prone for the use of the DLT. There are several other use cases which do not fall into the category of finance: such as data archiving, identitiy management, data protection, data tracking, government services, etc.

For more information, please see the document Exploring DLT and blockchain for alternative finance from the European Crowdfunding network:

https://eurocrowd.org/wp-content/blogs.dir/sites/85/2019/11/ECN_Exploring-DLT-and-Blockchain-for-alternative-finance_Nov2019.pdf

7. What type of DLT (e.g. blockchain, distributed acyclic graph, Hashgraph, etc.) i.e. what kind of consensus protocol (e.g. proof-of-work, proof-of-stake, practical Byzantine fault tolerance, etc.) is most appropriate for PCS and why?

The developments and testing of different types of DLTs are not yet finished nor finalized.

8. Main consortiums, their platforms and the infrastructures they use involved in developing DLT in PCS.

The answer to this question belongs rather to the entities of the private sector.

We hope that this answer was useful. We wish you a lot of luck with your Master Thesis.

Kind regards,

Communications Section
NBS

Priloga 5: Anketa odprtega tipa s predstavnikoma Centralne banke Švedske

VB: Questions regarding DLT in PCS – Master Thesis

Segendorff, Björn <bjorn.segendorff@riksbank.se> 15 December 2020 at 15:57
To: "daniel@valentine.si" <daniel@valentine.si>

Dear Daniel,

These are not easy questions but I have tried to provide answers in red below. Here is a link to a CPMI-report that you might find useful: https://www.bis.org/cpmi/publ/d157.htm. It is an early attempt by some central banks to think about what you ask.

Kind regards,

Björn

Björn Segendorf
Senior Adviser, Ph.D | Payment Department | Analysis and Policy Unit

SVERIGES RIKSBANK

103 37 Stockholm
Tel: +46 8 787 0678 | Mobil: +46 72 739 92 27 | Fax: +46 8 21 05 31
bjorn.segendorf@riksbank.se
www.riksbank.se

From: Registratorn
Sent: Monday, December 14, 2020 7:29:42 AM (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
To: Info AFS
Subject: VB: Questions regarding DLT in PCS – Master Thesis

Från: Daniel <daniel@valentine.si>
Skickat: den 13 december 2020 16:39
Till: Registratorn <Registratorn@riksbank.se>
Ämne: Questions regarding DLT in PCS – Master Thesis

Dear Sir/Madam,

I'm Daniel Valentine, 33, postgraduate student at the Faculty of Economics, University of Ljubljana / Slovenia. My master thesis is about Distributed Ledger Technology (DLT) in Payments, Clearing and Settlement (PCS). To conclude my work I have to gather information from professionals in this field first hand in addition to the research I have already done through academic articles and institutional reports. Therefore I would kindly like to ask if you could please elaborate on (at least the first five of) the following questions. We can also discuss the topics if preferred on live chat in Zoom.

1. What are the advantages of DLT in PCS? It is uncertain whether there are any substantial advantages. One possible advantage is that DLT provides a new way of achieving DvP (delivery-versys-payment). Another may be that the operational risks are different from those existing in the legacy technology that we otherwise use. It may also be a cheaper way to build a new financial infrastructure.

2. What are the challenges and risks of DLT in PCS? New legal risks may arise since existing legislation is written with legacy technology in mind. There may also arise legal risks from conflicting national legislation if DLT is used in a cross-border setting. Scalability. New technology tend to imply unforeseen operational risks.

3. Future development and phases of implementation:

4. The role of wholesale and retail central bank digital currency in PCS: Cross-border payments and security settlement where DvP not always exist today.

5. The role of tokens and smart contracts in PCS: Wholesale CBDC is likely to be tokenized. It is difficult to have an opinion on smart contracts. One area that is eyed when it comes to smart contracts is trade financing where there is a lot to gain from automation of the administrative process. This can of course be integrated in e.g. a wholesale CBDC-system.

Additional questions:

6. Areas where DLT in banking could be used exceeding PCS? Compliance, data storing and exchange for countering AML etc.

7. What type of DLT (e.g. blockchain, distributed acyclic graph, Hashgraph, etc.) i.e. what kind of consensus protocol (e.g. proof-of-work, proof-of-stake, practical Byzantine fault tolerance, etc.) is most appropriate for PCS and why? I don't have the technical knowledge to have a firm idea about this. What I do think is that we will only se permissioned DLT in the financial sector for the foreseeable future.

8. Main consortiums, their platforms and the infrastructures they use involved in developing DLT in PCS:

Your help would mean a lot to me on the way to achieving my goal – reaching my master's degree. Thank you for your tips and advice in advance!

Kind regards,

Daniel Valentine

Questions regarding DLT in PCS – Master Thesis

Lööv, David <David.Loov@riksbank.se> 4 January 2021 at 10:46
To: "daniel@valentine.si" <daniel@valentine.si>
Cc: Registratorn <Registratorn@riksbank.se>

Dear Daniel,

First of all I want to make clear that the Riksbank has made no decision on which kind of technology a possible e-krona would use if it were to be launched for the public.

What we are doing now is running a POC/pilot for a retail CBDC where we are testing a solution which uses DLT. And we are evaluating the technology and its pros and cons as we learn more during the work so many of your questions are a bit too early for us to give conclusive answers to.

I assume that you have read our official information of the solution we are testing? Or else I think it might be a bit hard to follow my answers because they will be based on what we are doing now. One key concept is that the solution we are testing now is re-using the two tier system where the Riksbank is the only creator of the CBDC (e-kronan) and actors on the market, like banks and other payment service providers, are distributors of the e-kronor to the end user. Much like the distribution of cash today. Unfortunately the answer I can give at the moment is not that informative since we are in the middle of our work and much is to be done before any firm conclusion can be drawn from a Swedish CBDC point of view.

1. What are the advantages of DLT in PCS?

   Answer: First of all I must stress that we are working on a pilot project that are investigating a technical solution that might be interesting for an e-krona. But there are no decisions made if an e-krona should be launched, what kind of technical solution it will be based on and also what kind of role it would have when it comes to issues regarding settlement etc. And as written above that is something that our work is aiming to answer from a Swedish CBDC point of view. We are now testing a solution which uses DLT but where the information on all the e-kronors in circulation and transaction are not distributed to every approved payment service provider in the network but rather just to those that are involved in a transaction of e-kronor. So the information of all the balances and transactions of the e-krona users is not stored at a central ledger at the Riksbank but rather distributed within the e-krona network and the payment service providers that are allowed to distribute e-kronor in the network. And distributing it so that only information that are relevant for a certain PSP are visible for that PSP.

   One argument that we are looking in to if it holds is that such type of DLT might enable a solution where the Riksbank remains its current role so that the RIksbank will not keep a central ledger and by that hold end-user information. The information regarding the users of e-kronor and their transactions will be distributed among the PSP's that have a relationship with the customers. And by that remaining the Riksbank role with no end-user relationship and information. Our aim for the pilot is to examine these kind of arguments to see if there are any substance in them from a Swedish CBDC point of view. What kind of role and status it would have in questions regarding settlement is also under investigation.

2. What are the challenges and risks of DLT in PCS?

Big question. I'm an economist so I'm not an expert on the technical issues regarding DLT so I'm not in a position to dive into hard tech issues and challenges regarding DLT in PCS. But the questions regarding DLT as suitable for

clearing and settlement is interesting and something that needs to be examined further.

3. Future development and phases of implementation:

What do you mean here? For our work in the pilot?

4. The role of wholesale and retail central bank digital currency in PCS:

Also a very big question where there no given answers at the moment. These are questions that we are working on and that are given a lot of attention in the global CBDC debate and work. And the field of CBDC is quite new. In our pilot project at the RIksbank we are looking investigating a retail CBDC so the questions regarding wholesale is another topic. What kind of role a CBDC should have in regards to settlement is a very big question from a legislative point of view and also probably much dependent on how a possible CBDC would be implemented technically. So it's hard to give any straight answers at the moment. It's not just a technical question but much dependent on regulatory issues. And once again something that we are investigating at the moment with our technical solution as a benchmark.

5. The role of tokens and smart contracts in PCS:

Once again the answers is based on what we are looking at in our CBDC-pilot project. The e-krona in the solution we are building and investigating are based on R3 Corda platform so for a general technical documentation of the tokens and smart contracts I would recommend reading technical documentation on Key concepts | Corda OS 4.6 | Corda Documentation.

When it comes to the broader question how this types of new technical solutions might be used for payments, clearing and settlements it is as mentioned above much of a regulatory issue as well. And if/how these types of technical solution could be adopted to be used for PCS is something that we are looking at in our pilot project. We have not finished this at the moment so we have not reached any final conclusions yet. But one premise of our pilot is that the e-krona in the network should be created by the Riksbank just like notes and coins, and just like notes and coins it should **not** be a claim on the PSP or private bank that distributes them to the end users. So the question if this e-krona network that we are developing in the pilot could be regarded as a settlement system (since it is central bank money in the network) is a key question and will depend on how the technical solution could be interpreted from a regulatory point of view.

I will have to take a look at the other questions later if I find the time. We are quite busy at the moment, but feel free to reply if you have any questions regarding our work.

I also recommend that you read our published material regarding our work in the pilot (if you haven't already). It is not that much at the moment but it might give you some background to what we are doing.

E-krona | Sveriges Riksbank.

Sincerely David

David Lööv
Economist | General secretariat | E-krona pilot division

SVERIGES RIKSBANK

103 37 Stockholm
Tel: +46 8 787 02 23 | Mobile: +46 72 991 64 82 |
david.loov@riksbank.se
www.riksbank.se

[Quoted text hidden]

Priloga 6: Anketa odprtega tipa s predstavnikom Centralne banke Španije

RV: Questions regarding DLT in PCS (IT department) – Master Thesis

DGA.FIMI@bde.es <DGA.FIMI@bde.es> 4 February 2021 at 13:37
To: daniel@valentine.si
Cc: infoweb@bde.es

Dear Daniel,

Please find below (in your email) answers to your questions.

Best regards,

Secretaría
Direccion General Adjunta de Innovación Financiera e Infraestructura de Mercado
Tel. +34 91.338.50.95
Ext.móvil: 34824
dga.fimi@bde.es
www.bde.es

BANCO DE ESPAÑA
Eurosistema

De: Daniel <daniel@valentine.si>
Enviado el: miércoles, 27 de enero de 2021 15:44
Asunto: Questions regarding DLT in PCS (IT department) – Master Thesis

Dear Sir/Madam,

I'm Daniel Valentine, 33, a postgraduate student at the Faculty of Economics, University of Ljubljana / Slovenia. My master thesis is about Distributed Ledger Technology (DLT) in Payments, Clearing and Settlement (PCS). To conclude my work I have to gather information from professionals in this field first hand in addition to the research I have already done through academic articles and institutional reports. Therefore I would kindly like to ask if you could please elaborate on (at least the first five of) the following questions. We can also discuss the topics if preferred on live chat in Zoom.

1. What are the advantages of DLT in PCS?

- Efficiency gains: DLTs are in general terms considered to offer efficiency gains. The CPMI ("Distributed ledger technology in payment, clearing and settlement") has identified several points where this efficiency gains could materialize:
    - Increasing the speed of end to end processing
    - Reducing the cost of processing, (i.e. by using cryptography)

- Increasing speed and transparency in reconciliation
- Allowing real time transactions, which could lead to reducing the cost of credit and liquidity management
- Automated contract tools such as smart contracts

The following document may also help you to complete this question: Distributed ledger technology in payments, clearing, and settlement – Federal Reserve (https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf)

- Traceability is also an advantage identified by the CPMI; however, it is important to leverage it with privacy. Therefore, you could either consider it an advantage or a challenge. Traceability in DLT is also mentioned in the following Banco de España article, which is not specific of PCS but may help you: https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/2018/T4/descargar/Files/beaa1804-art26e.pdf

2. What are the challenges and risks of DLT in PCS?

You can find some information on this in the Banco de España and the CPMI documents mentioned above. Basically, some of the challenges and risks of DLT in PCS are the following:

- Current scalability
- Current lack of interoperability between platforms
- Government systems
- Legal settlement finality
- Operational and security risk, robustness and resilience of DLT platforms

3. Future development and phases of implementation:

The future development of DLT will largely depend on the ability of the industry to develop successful use cases. As far as the public authorities is concerned, the objective is to make sure there is an adequate balance between innovation and well functioning and stability of the financial system. In this regard, the European Commission is working on introducing a pilot regime for DLT market infrastructures in order to enable the use of DLT while ensuring investor protection, market integrity and financial stability.

4. The role of wholesale and retail central bank digital currency in PCS:

The Eurosystem is currently examining the potential issuance of a CBDC, i.e. the possibility of making central bank money available in digital form for use in retail payments. No decision has been made yet. We are currently developing the concept, conducting practical experimentation, listening to the views of the broader public and engaging with stakeholder. You can find further information on this at:

https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html

5. The role of tokens and smart contracts in PCS:

Both technologies have the potential to improve efficiency in PCS. Recent studies have considered specifically the possibilities of programmable money and programmable payments such as Money in programmable applications – Bundesbank (https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf)

However, similar initiatives are arising out of the DLT context such as trigger solutions:

https://www.bundesbank.de/en/press/speeches/on-the-future-of-money-and-payments-843720

Additional questions:

6. Areas where DLT in banking could be used exceeding PCS?

One of the most promising areas is digital identity (compliance, KYC...). (Also mentioned by CPMI in the previously mentioned document)

7. What type of DLT (e.g. blockchain, distributed acyclic graph, Hashgraph, etc.) i.e. what kind of consensus protocol (e.g. proof-of-work, proof-of-stake, practical Byzantine fault tolerance, etc.) is most appropriate for PCS and why?

As central banks we are technology neutral, but any solution applied for PCS must ensure to fulfill the basic requirements for safe and efficient financial market infrastructures (https://www.bis.org/cpmi/publ/d101a.pdf), in particular as regards efficiency, safety and legal certainty (e.g. in terms of finality).

8. Main consortiums, their platforms and the infrastructures they use involved in developing DLT in PCS:

I am afraid we cannot offer you more detail than the public information already available in the internet. In the case of Spain, Alastria is probably the initiative that brings together the largest number of companies. It is not specific about PCS, but it could also be relevant for them in the future, so you may want to look into it if you have not done so yet.

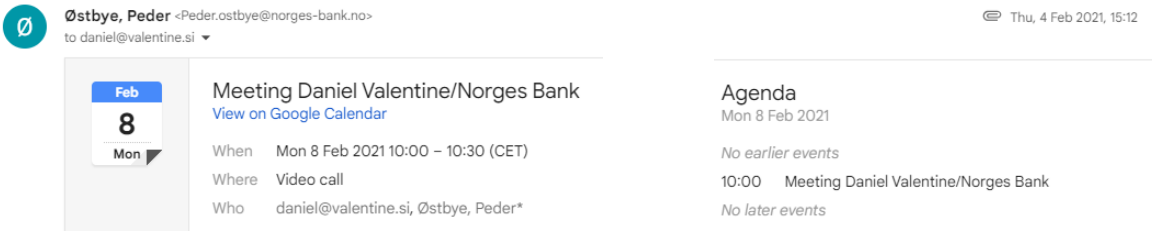
Your help would mean a lot to me on the way to achieving my goal-reaching my master's degree. If required please forward this e-mail to the IT department. Thank you for your tips and advice in advance!

Kind regards,

Daniel Valentine

Priloga 7: Intervju s predstavnikom Centralne banke Norveške

Prepis zvočnega posnetka z dne 8. 2. 2021

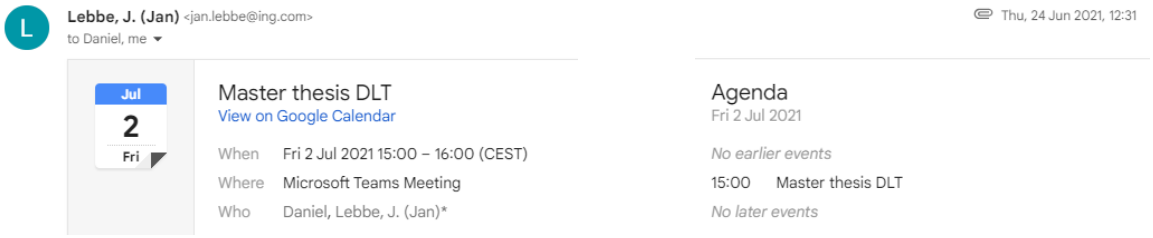


When it comes to at least Norway and Sweden what we have looked into and in particular in Sweden is the CBDC topic. When it comes to the testing and use of DLT in sort of traditional infrastructure for settlements of securities and these things, I don't think that we have done so much in Scandinavia. I guess you are aware of this BIS innovation hub and some project called Project Helvetia and then there they have tested out tokenized assets, and the use of some tokenised CBDC for security settlements. So I think what I can contribute most to here is that is kind of our consideration concerning the use of DLT in future CBDC if that is launched. We have looked into it, we follow the market and the development and there are certain advantages with DLT which is kind of emphasised in that project Helvetia from this innovation hub that you can have the benefits with smart contracts and maybe some resilience aspects. There are also certain risks. When it comes to the risks, you have everything from the kind of insecurities related to the basic legal framework like the property rights of the tokens and the responsibility if some things go wrong and things like that. And then you have the regulatory issues: Usually, regulators follow this principle of the same activity, same risks and same rules. So it's still under development how you can apply this to DLT. The EU Commission has recently proposed a regulatory framework for crypto assets and about that, they have also proposed regulations for the use of DLT within traditional payment/security settlement infrastructures where they kind of allow traditional participants to test out DLT within some safe i.e. within a compliant way. Different infrastructures are testing it out now, gaining more knowledge about the risks, regulatory issues, and financial issues. Depending on the results of these tests if they are successful they probably will be implemented in the future. There are a lot of benefits with smart contracts which can reduce some counterparty risks and can be utilized. There is also testing mostly for crypto assets with this decentralized finance and if you can have sort of more traditional assets on those infrastructures, maybe that will give some benefits, so far it's a new technology that needs to be tested. We will see in the future if the risks can be reduced and the regulatory framework can be put in place so it can be used for more mainstream finance. What this project Helevetia is, that it's elaborated more on the BIS innovation hub homepage. It's a test where the BIS innovation hub, which is a sort of collaboration between different central banks on innovation issues and the Swiss national bank and SIX, which is security settlement infrastructure, have cooperated and they test how you can perform settlements on a sort of decentralized infrastructure in some sense with tokenized assets and some wholesale CBDC version. As a central bank, we are in some sense authority a regulator and we also supply money. And of course, as an authority and as a regulator we look into the private initiatives from a regulatory perspective. Many countries have launched CBDC projects and they are looking into the usefulness of DLT in this context also in Norway we are looking into CBDC, and then a question arises what is the role of DLT in CBDC? CBDC can be considered as a sort of digital cash in the sense that it's a claim on the central bank as cash is and we are looking into this for various purposes, different central banks look into this from different perspectives. In Norway there is little use of cash, only 4 % of payments are done with cash, and most are done by bank payments, so kind of a broader question for us is if CBDC kind of necessary to preserve some of the properties of cash and preserve

the trust in the payment system. CBDC can fulfil certain roles, can be a contingency solution that is operational even if the bank payment network is not working, can provide some competition in case some banks gain market power or other payment suppliers gain market power and also serves a precautionary principle because there a lot of developments in the payment system and CBDC can be a way to meet some of these challenges that make it possible for us to preserve national control and the ability to perform monetary policy. We don't want CBDC to disrupt the bank too much, it will still be the role of the private sector to provide credit, private loans shouldn't come on the balance sheets of the central banks and we don't want it to distort or impede financial stability, because you can imagine that if CBDC is available, you can imagine a situation where many take out their bank deposits and put it in the central bank CBDC instead, so based on these things there are a lot of characteristics that CBDC should have and it is those that determine the technology if CBDC is launched, it is the characteristics that are important, it's not the technology. And then the question is if DLT has any role in facilitating a DLT that meets its objectives and characteristics. And then the DLT has some advantages, it's various ways that CBDC can interact with DLT, some think that CBDC could be issued on a smart contract on a public blockchain like Ethereum, but we don't see that public blockchains are ready for that yet. You can gain maybe some benefits by having a DLT infrastructure for CBDC for instance a permissioned variant of DLT you could imagine that if you had more validators for instance you could increase the resilience of the network. That may be the most kind of sensible alternative so far is that DLT is: CBDC is compatible with other DLT networks in various ways, which means that the CBDC could be based on some sort of central register but the data is represented in such a way that it could be compatible, you could look it into other DLT networks and then you can use the services there and that might contribute to the distribution of the CBDC but also to the development of services based on CBDC and also this network can provide some benefits when it comes to the use of smart contracts. But then there are risks if some CBDCs are circulating on external DLT registers it might give the CB some reputational risks we don't want, and it might give us some legal responsibilities we don't want, DLT is relevant when it comes to looking into CBDC but it is not the reason for why we're doing it. It might be an alternative technology to give a CBDC with those characteristics that we want CBDC to have. Well, Proof of Work is a way to avoid a trusted third party for validation and it's what's used in Bitcoin and some other cryptocurrencies and it's, for instance, Ethereum there are other alternatives like Proof of Stake but we are a CB so we don't need a …and it's central in its name so we don't think that is particularly useful for our register, because our kind of basis is that it's trust in our register and that we perform our tasks. The PoW or other distributed consensuses that are based on no trust will not be so relevant for a CB. So it is not needed that we base a CBDC on consensus mechanisms that are reliant on PoW, that would just be a waste of resources, it might be useful for Bitcoin and cryptocurrencies because there you don't have any trusted third parties, but the CB is a trusted third party. So it's an alternative. So if we use DLT in a CBDC network, if the kind of architecture is based on that then it would be based on some permissioned DLT network so that you can gain some advantages of a DLT like resilience and you can introduce some programmability that makes it possible to utilize smart contracts but it is also possible that, as I told you earlier, that CBDC exists in a register and then it can lock those CBDC. You can sort of wrap them onto other DLT networks and then they could be used there for settlements and services and those networks could be based on various consensus algorithms like PoW or PoS. But that would not be our register that would be some alternative register. This kind of consensus mechanism to avoid trust in a central party is not necessary for us because we are the central party that is supposed to be trusted.

Priloga 8: Intervju s predstavnikom mednarodnega konzorcija finančnih institucij Fnality

Prepis zvočnega posnetka z dne 2. 7. 2021



The main initiative of banks to improve international payments on DLT. Check the presentation of the BIS, and ECB, one is the digitization of money.

Fnality aims to create a platform where digitized existing currencies can send currencies towards the various counterparties 24/7 without any intermediaries, so the payment process is currently like that. If a client of ING wants to send money towards another party they do not own this money, they bank with a bank. Sometimes a bank does not have a licence with a certain central bank, if a bank doesn't have a licence with a certain central bank then they do not own for example dollars, ING does not have a licence with the FED then the dollars that they own are not sitting with ING are sitting with BoA, which is a bank who owns a licence with the FED. And then banks with ING, ING banks with Bank of America to settle their US dollar transactions. Now what Fnality is aiming to do is we are trying to to digitize the US dollars for ING not to own US dollars but to own the digital version of the US dollars and like that I can send this money towards the counterparty towards the bank of Shell, so this makes the process less complicated because if I as ING need to send money towards Shell, then ING needs to send this instruction to BoA, BoA receives this instruction which puts lead to blocking they do an amount check, they do KYC checks if they don't like certain things then the amount is blocked, they are limited towards the opening hours of the FED. So if ING owns the digital version of the US dollar, then they do not need to go via BoA they are not limited towards the opening hours of the FED. That is what we are trying to do with the various currencies. We're trying to digitize the various currencies so that we can own them and then we can send them towards the various counterparties on the platform and that's an initiative of all the banks. It is with the ECB, with the FED, with BoJ, with BoC, with the BoE, that's where we're trying to do this. Mitsuho is missing here and then here you have all the other banks in Europe and here you have the banks in the U.S. Also Nasdaq is part of that. The aim is to have the other banks by the end of this year, we're doing series B, so we did this with A the initial investments in Fnality we did with at least 15 banks, at the end of this year we are doing series B, we want to raise extra money with the various with other banks contact with Citibank, Goldman Sachs etc. The aim is to set up such a platform to improve wholesale CBDC and international payments via DLT.

What are the advantages of DLT in PCS? Simplification of the whole international payments settlement system. Currently, there are a lot of limitations. Central bank opening hours, limitations to commercial banks having the banking licence, this leads to doubling of, this leads to correspondent banking layers, multiplication of messages and processes, this complicates things, this is only for US dollars, if you would change this towards Indian rupees or Malaysian ringgits then you would have even more intermediaries in the process of money going from this part into the other. What DLT aims to do is to get rid of all intermediaries so for all kinds of transactions and now we are talking about payments for also other transactions we are making mapping of all the people who are in to the value chain and for payments we are seeing correspondent bank, central bank opening hours, DLT allows us to think about this and to simplify this, if you would digitize currencies, then we're not able to trade these currencies and obtain finality, then we transfer this money from here to there, then we simplify things, then we cut out varies layers and then we get towards something like this where the banks are owning some kind of wholesale CBDC. Retail CBDC - the digital Euro that is this. That is you and me

owning Central Bank money. Now we don't own CB money, the only CB money that we own is cash. The money that we have in our bank accounts is with our bank and if that bank does not have a banking licence then the US dollars that we have on our bank account is not even with ING, but is with the correspondent bank of ING. So DLT enabled us to digitize money, simplifying things. So what is the advantage of DLT in PCS? Simplification of the international payments flows. National payment flows, for example Euros, ING has Euros, so if you are banking with a European bank then this process is quite simple, you have instant payments for the moment, ING is part of the instant payment network, if you want to send money towards another bank who is also on the instant payments network who also has an account with ECB with TARGET2 then it can do that simply and then payments go quite smoothly. If you don't have a licence, if you are banking with a bank which doesn't have a banking licence and you want to exchange your Euros and turn it into US dollars and send it somewhere else. Then you are into problems because then you are working in these layers and that is something that DLT is trying to change, trying to simplify with digitization of payments.

The second advantage is that smart contracts enable us two things, first of all, to make money programmable as you can send money towards a person or you can give money towards a person but for example has some kind of programmation to it, that you say I gave you 10 Euros but you can only use it for buying food but not cigarettes not alcohol because you drink too much, programmability - conditionality of money, that's that you can link a certain transaction towards a payment, that you say for example Rio Tinto wants to move Aluminium towards Cargo, and you say as of the moment that Cargo receives that aluminium, and the letter of credit is signed then initially in the smart contract it is stated that money goes from the bank of Cargo to the bank of Real Tinto, so like that you link one financial transaction towards another. When you take away you automate transactions and you take away settlement risk because if aluminium goes to Cargo, Cargo receives it and that time Cargo goes bankrupt then Real Tinto doesn't get its money and needs to recuperate the aluminium, but if there is a smart contract that states and as of the moment that Cargo receives the aluminium the money goes towards the bank of Rio Tinto and there is no settlement risk, there is no counterparty risk. Link transactions towards each other, because if there's no if, there's no transfer of money, if Cargo doesn't have the money then the aluminium that is delivered gets barred. So you link both transactions to the error and you cut away risk towards your counterparty and that's for certain transactions delivery of goods but you can also do that for example for [unclear]. If you want to do a euro US dollar swap. Euros between ING, ING says I'm swapping dollars with BNY Mellon, I'm giving euros to BNY Mellon, then the euro go via this situation, BNY Mellon needs to give the US dollars towards ING but you have counterparty risk because if ING already gave the euros towards BNY Mellon, BNY Mellon goes bankrupt that is called Herstatt risk because that was once a bank Herstatt went broke overnight. All the money. If you link both transactions towards each other the euro and the us dollar then you don't have risk to your counterparties. As of the moment when you get the euros towards the other party, the other party gives you dollars linking those transactions eliminates risk.

The third big advantage of DLT in P&S is reconciliation, and reconciliation is that if a payment happens all the parties directly see that a payment happened because you have their copy of the truth now with SWIFT I showed you that as well, go via SWIFT. If the payments get settled then the bank receives a SWIFT message and then they need to reconcile that into their systems if you link the payment system directly towards the back of the system then you have instant updates then you do not need to work via those SWIFT messages. So the reconciliation part does not happen. With DLT you diminish your reconciliation efforts and errors. Sometimes you need to reconcile you do not get an automatic update you need to reconcile internally because you are based on a central database, the central database that needs to update you, that update with a fat figure you received something, you fill it into your systems, ah it's wrong you have reconciliation errors, you call your buddy bank in BNY then you say ok let's do a deal, we do a deal, you update that in your system, if you update that in a shared ledger then you don't get these reconciliation errors. So these are the three advantages, simplification of the whole payment stream, secondly, getting away and getting rid of intermediaries by the digitization of assets, programmability is also conditionality, getting rid of settlement and counterparty risk and thirdly, fourthly or fifthly reconciliation errors.

Challenges and risks of DLT: The biggest challenge is approval by regulators if you want to do something like this they need to have the approval of all the central parties, and central banks; recognition is a big problem. Risks of DLT in payments and settlement: If you have for example a stablecoin and a stablecoin or a commercial

bank digital currency which is issued by JP Morgan, which is issued by Facebook [unclear] of all those entities. If you do not have central bank money to do payments with and you have counterparty risk, counterparty risk called [unclear] issuing, FinTech [unclear] issuing then if you are using cryptocurrencies of course you face huge risk. It depends on the settlement currency that you are using. Cryptocurrency has a lot of risks, stablecoins risk on FinTech [unclear] issuing it but also it needs to be backed on 1 by 1. Tether is issued by the FinTech but is backed by money that is sitting at a certain bank, sometimes it is even not backed by money but is backed by securities, bonds etc. Only 25 % of Tether is backed by cash, and 75 % is backed by securities, so then you have credit risk. [unclear] settlement means that you're using. Secondly, you have technological risks, because is DLT the perfect technology that can be hacked normally and should be more secure, with no single point of failure nevertheless to get and to state that you can link transactions to each other you need to have interoperability because it's very nice to say we have atomic swaps if this happens then that happens but for that, you need an interoperability component or solution that works perfectly that is currently not yet the case if you want to move towards a digital euro and you want to make that digital euro private not that everybody on the blockchain sees who is doing transactions with what you need a privacy component, a privacy component is still not rock-solid in DLT. Those are the three biggest risks and challenges next to regulatory approval. If you want to have central bank money, if you want to make your payments regulated then you need to have the approval of a regulator and they are now trying to - cryptocurrencies as regulated - regulators are still responsible for all the money flows in their region. So regulatory approval is a big challenge.

Future development and phases of implementation: You have the private sector trying to improve that and then you need to have the public sector allowing it to do that, in the beginning, the private sector is trying to improve payments in an irregulated way. That's why the public sector, stablecoins, they're still regulating that, so there are a lot of flows that are going from one party to the other that are not regulated that the private sector is trying to achieve. First, the private sector is doing stuff in an irregulated way, then things are getting regulated and then some parties are trying to do things in a regulated way. Fnality is trying to do things in a regulated way. Fnality is trying to build such a platform and for that, you need to have the approval of all the central banks. There are other initiatives: CPMI and others at FSB are trying to enhance cross-border payments. Finality is an initiative of the private sector together with the public sector. Then you could also imagine that the public sector is still trying to do something by itself. But the public sector says they want to improve cross-border payments jointly between public and private. Fnality is the biggest example of that so JP Morgan tried with a project Ubin together with the Monetary Authority of Singapore also to put in place a platform like this. Also wholesale CBDC. Bank de France is experimenting with wholesale CBDC, with retail CBDC - digital euro, so central banks, regulators, trying to do something themselves, wholesale CBDC is normally joined the retail CBDC that are the central banks and the regulators trying to do something themselves and then you have it the digital euro, the digital dollar, you have massive things there. The private sector starts on its own in an irregulated way the- n the private sector to decrease a little bit of risk that they are doing. That's how stablecoins came into life after cryptocurrencies. The private sector trying to do something with the public sector that's for example Fnality and the projects of JP Morgan CBDC projects. With regards to international payments, you have these public-private partnerships about digital euros, retail CBDC normally means the public sector although the public sector also cooperates with the banks in the digital euro with the retail CBDC. China is doing for example its digital yuan also together with commercial banks. Here a retail CBDC will be done will be issued by a payment services provider and normally it will be the banks providing wallets or doing KYC for people's own general public CBDC. The retail CBDC is going to be a replacement for cash, 10 % of the money in circulation is currently cash, and 90 % is commercial bank money, which is also the division, retail CBDC will be also 10 % of the money in circulation. The digital euro will be 3000 euros per person maximum. Retail CBDC will be a digital version of cash, wholesale CBDC will still enable the simplification of money flowing from one bank to the other or commercial bank money, most of our money is in an account with a bank. Banks will do interbank settlements via wholesale CBDCs. Smart contracts enable programmability, conditionality and linking of various transactions to each other.

Areas where DLT in banking could be used: Everything. Securities, if you digitize bonds and equities, you do not need to go via custodians via CSDs, you can digitise letters of credit, digitize lending, and decentralised finance [DeFi] – that's another project I'm working on, making sure that all parties come together, banking is

deposits, loans, banks are taking deposits to lend towards borrowers towards their clients in DeFi we bring those parties together we can use DLT in banking in decentralised finance, in securities, trade finance, HQLAx, [unclear], Congo, Contour, these are the names of certain initiatives in those things.

What kind of consensus protocol is most appropriate for PCS: Not PoW, we do not want PoW, it takes too much time it is bad for the environment, and nobody wants proof of work, byzantine fault tolerance - yes, we are using that. But not PoW. You need to be able to do the number of settlements per second, retail CBDC if you want to do on Christmas day in London per second thousands of transactions you cannot do that with PoW so you need - We worked with Hashgraph and there are a lot of things. If you do things like that then you can do things on private blockchain. The question is do you want to do private blockchain or public blockchain it needs to be permissioned in payments if you want to do retail CBDC it needs to be permissioned. Scalability is one of the challenges of DLT in payments. Scalability is key and an environmental impact is also key.

Main consortia: Fnality, second consortium the one of JP Morgan, and there are three aiming to get a foot on the ground here but they do not have actual consortia. They are losing a little bit of the game. Platforms: For JP Morgan Quorum, we are going to give you the Ubin Phase 5 which is Singapore together with JP Morgan link that they are using, we are also using a private Ethereum cloud. I do not believe in Corda, they are working with notaries, notaries are intermediaries, and you do not want to have intermediaries, but R3 works with Corda.