UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA ALTERNATIVNIH TEHNOLOGIJ DECENTRALIZIRANIH FINANC ZA BANČNE DEPOZITE

Ljubljana, september 2025 JERNEJ ŠTOJS

IZJAVA O AVTORSTVU

Podpisani Jernej Štojs, študent Univerze v Ljubljani Ekonomske fakultete, avtor predloženega dela z naslovom Analiza alternativnih tehnologij decentraliziranih financ za bančne depozite, pripravljenega v sodelovanju z mentorjem red. prof. dr. Alešem Groznikom

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 pisnih del UL EF, 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 pisnih del UL EF;

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 Univerze v Ljubljani Ekonomski fakulteti 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 preko 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 22. 9. 2025 Podpis študenta: 

POVZETEK

Magistrsko delo obravnava alternativne tehnologije decentraliziranih financ (DeFi) kot možno alternativo bančnim depozitom. Teoretični del zajema pregled tradicionalnega finančnega sistema, tehnologije veriženja blokov, tehnologij decentraliziranih financ in analizo vodilnih DeFi protokolov. Empirični del temelji na intervjujih s strokovnjakoma s področja bančništva in tehnologije veriženja blokov. Ugotavlja, da DeFi protokoli ponujajo potencialno večjo donosnost v primerjavi s tradicionalnimi bančnimi depoziti, vendar so izpostavljeni pomembnim tveganjem, predvsem na področju varnosti in regulacije. Ključno vlogo pri uspešni uporabi DeFi rešitev imajo uporabniška izkušnja, pravna zaščita ter možnost integracije v obstoječi bančni sektor. Ugotovitve kažejo, da DeFi ponuja privlačno, a še nezrelo alternativo bančnim depozitom. Študija zaključuje, da je za dolgoročno uveljavitev DeFi kot alternative bančnim depozitom nujna regulacija, razvoj varnostnih mehanizmov ter krepitev zaupanja uporabnikov.

KLJUČNE BESEDE: decentralizirane finance, bančni depoziti, tehnologija verige blokov, tveganja, regulacija

CILJI TRAJNOSTNEGA RAZVOJA

ABSTRACT

The master's thesis examines alternative decentralized finance (DeFi) technologies as a potential substitute for bank deposits. The theoretical part provides an overview of the traditional financial system, blockchain technology, decentralized finance technologies, and an analysis of leading DeFi protocols. The empirical part is based on interviews with experts in banking and blockchain technology. It finds that DeFi protocols offer potentially higher returns compared to traditional bank deposits but are exposed to significant risks, particularly in the areas of security and regulation. User experience, legal protection, and the possibility of integration into the existing banking sector play a key role in the successful adoption of DeFi solutions. The findings indicate that DeFi represents an attractive yet still immature alternative to bank deposits. The study concludes that for the long-term establishment of DeFi as an alternative to bank deposits, regulation, the development of security mechanisms, and the strengthening of user trust are essential.

KEY WORDS: decentralized finance, bank deposits, blockchain technology, risks, regulation

SUSTAINABLE DEVELOPMENT GOALS

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
DAO – (angl. Decentralized Autonomous Organization); Decentralizirana avtonomna organizacija
DeFi – (angl. Decentralized Finance); Decentralizirane finance
DSR – (angl. Dai Savings Rate); Dai varčevalne obresti
EVM – (angl. Ethereum Virtual Machine); Ethereum navidezni stroj
LTV – (angl. Loan to Value Ratio); Razmerje med vrednostjo zavarovanja in izposojenim zneskom
MKR – Maker
SEC – (angl. Securities and Exchange Commission); Ameriška komisija za vrednostne papirje in borzo
USD – (angl. United States Dollar); Ameriški dolar
USDT – Tether

1 UVOD

Banke so depozitno-finančne ustanove in pomemben del finančnega sistema. Ena od osnovnih funkcij, ki jo imajo, je sprejemanje depozitov varčevalcev in upravljanje z njimi. Za banke so depoziti varčevalcev tudi ena od oblik zadolževanja. Depozit pomeni, da varčevalec položi denar na bančni račun, banka pa se pogodbeno obveže, kdaj mu bo denar vrnila in kakšne obresti bo plačala za upravljanje tega denarja (ATVP, brez datuma).

Centralne banke določajo obrestne mere, ki vplivajo na celoten finančni sistem, tudi na varčevalce (Schiller, 2022). V Sloveniji se varčevalci trenutno soočajo z izredno nizkimi obrestnimi merami na depozite (Zveza potrošnikov Slovenije, brez datuma). Varčevalci se sami odločajo, kako bodo upravljali svoje depozite, ki so del širšega pojma osebnih financ, katerih glavna komponenta je upravljanje z njimi. Medtem ko je to za nekatere varčevalce zelo stresno, pa za druge predstavlja zmožnost doseči finančno in socialno varnost ter samostojnost (Muske in Winter, 2004). Možnost nalaganja kapitala in njegovega upravljanja z dobo interneta in tehnološkim prebojem ni več namenjeno samo bogatim, ki so nekoč bili edini predstavniki na trgu kapitala, ampak je možen dostop vsem investitorjem, tudi majhnim varčevalcem (Balkovec, 2000).

Decentralizirane finance (angl. Decentralized Finance, v nadaljevanju DeFi), ki temeljijo na tehnologiji veriženja blokov, s svojim hitrim razvojem ponujajo alternativo tradicionalnemu finančnemu sistemu (Busayatananphon in Boonchieng, 2022). DeFi protokoli, kot so MakerDAO, Aave in Compound, med drugim omogočajo varčevalcem, da svoje depozite prenesejo na protokol verige blokov (angl. Blockchain Protocol) in s tem zaslužijo donos za kripto depozit, kot bi na banki za fiat depozit. Donos zaslužijo zaradi zagotavljanja likvidnosti v protokolu (Shah in drugi, 2023).

Raziskave so pokazale, da DeFi ponujajo transparentnost, varnost in enostaven dostop do globalnih finančnih storitev, kar omogoča posameznikom, da izkoristijo donose brez posrednikov, ki bi zaračunavali dodatne stroške (Busayatananphon in Boonchieng, 2022).

V magistrskem delu želim pregledati literaturo o tradicionalnem finančnem sistemu, tehnologiji veriženja blokov in DeFi. Raziskati in poudariti želim tveganja in izzive, ki so prisotni v tradicionalnem finančnem sistemu, kot tudi v DeFi. Poleg tega bom preučil metodologijo, ki je bila uporabljena v znanstvenih in strokovnih delih za določanje tveganj v DeFi. Zaradi hitrega napredka in malo regulatorne ter zakonodajne podlage v primerjavi s tradicionalnimi financami, je pravilno določanje tveganj ključno za varno in vzdržno rast DeFi.

Na trgu je veliko DeFi protokolov in zaradi preglednosti ter čim boljšega dostopa do podatkov, se bom osredotočal na največje tri protokole po skupni zaklenjeni vrednosti (angl.

Total Value Locked). Predstavil bom upravljanje, delovanje, poslovni model in možnost donosa na depozit v protokolu.

Skupaj z zgoraj omenjenimi dejavniki bom v raziskavi preučil, ali lahko funkcionalnost služenja obrestnih mer za kripto depozit v DeFi, služi kot učinkovita alternativa bančnim depozitom. Poudarek bom namenil uporabniški izkušnji, regulaciji in pravni zaščiti uporabnikov, varnosti in tveganjem, poslovnemu modelu tradicionalnega bančništva in DeFi ter integraciji tehnologij DeFi v banke. To so ključne stvari, ki so varčevalcem pomembne, ko se odločajo o alternativnih rešitvah bančnim depozitom. V zaključku bom povzel ključna spoznanja, ugotovitve in dosežene rezultate moje raziskave. Na podlagi uporabljenega pristopa bom predlagal tudi nadaljnje korake za izboljšanje in razvoj na tem področju.

Skozi magistrsko delo želim raziskati področje tehnologije veriženja blokov in tehnologije DeFi, ki ponujajo alternativno možnost za bančni depozit. Upravljanje osebnih financ in spremljanje vseh možnosti, ki so na trgu, jemljem kot intelektualni izziv, ki zadeva vsakega posameznika, ki želi poskrbeti za socialno, osebno in finančno varnost sebe ali svoje družine. Gre za kompleksno področje, saj imamo varčevalci zelo oseben in subjektiven odnos do naše lastnine in zato ga je treba naslavljati analitično in objektivno. S pridobljeno analizo bo magistrsko delo služilo kot dober vodič za tiste, ki so odprti do alternativnih možnosti za donose na depozit, ki jih danes ponujajo protokoli DeFi.

Namen magistrskega dela je ugotoviti trenutno stanje DeFi tehnologij in preučiti ali lahko tehnologije DeFi, služijo kot alternativa bančnemu depozitu in podati predloge za nadaljni razvoj DeFi protokolov.

Prvi cilj je na podlagi primarnih podatkov, zbranih v okviru izvedene kvalitativne raziskave, analiza tehnološke možnosti za kripto depozit v DeFi, kot alternativa bančnim depozitom, ki je smiselna in ustrezna z regulatornega vidika, vidika uporabe za posameznika, varnosti, donosa in tveganja, ki ga s tem sprejme. Drugi cilj je s pomočjo teorij vezanih na to področje in empirične raziskave analiza prednosti in slabosti DeFi depozitov v primerjavi z bančnimi depoziti ter podati predloge, ki bodo uporabni za nadaljnji razvoj DeFi. Ključno je, da bodo predlogi premišljeno sestavljeni in realno uporabni.

Ob navedenem namenu in ciljih bom v magistrskem delu odgovoril na temeljno raziskovalno vprašanje, ki se glasi: »Ali znotraj protokolov DeFi obstaja tehnološka možnost za alternativo bančnim depozitom?«.

Magistrsko delo bo sestavljeno iz teoretičnega in empiričnega dela. Pri sami izdelavi magistrskega dela bom uporabil različne metode dela. Uporabljene bodo metoda deskripcije, s katero bom predstavil definicije tujih in domačih avtorjev, metoda kompilacije, saj bom povzemal nekatera spoznanja in stališča drugih avtorjev ter empirično metodo znanstvenega raziskovanja.

V magistrskem delu bom uporabil primarne in sekundarne podatke. V prvem delu bom uporabil sekundarne podatke in pregledal teoretično literaturo o tradicionalnem finančnem sistemu, tehnologiji veriženja blokov, pametnih pogodbah in DeFi.

V drugem delu bom s pomočjo empirične metode zbral primarne podatke. S kvalitativno raziskavo bom opravil delno strukturirana intervjuja s strokovnjakoma s tega področja. Podatke bom uporabil za dodatno analizo tehnologij DeFi kot alternative bančnemu depozitu in jih primerjal z že obstoječimi študijami s tega področja. Določil bom pozitivne ter negativne lastnosti protokolov, kot alternativo bančnemu depozitu. Na podlagi rezultatov bom v diskusiji predstavil ključne ugotovitve in priporočila ter omejitve za nadaljnjo raziskovanje.

Omejitve raziskave so omejen dostop do nekaterih sekundarnih podatkov zaradi občutljivosti finančnih informacij in hitrih sprememb v DeFi sektorju, ki lahko vplivajo na aktualnost zbranih podatkov in ugotovitev.

2 TRADICIONALNI FINANČNI SISTEM

Tradicionalni finančni sistem predstavlja temelj globalnega gospodarstva in vključuje različne finančne institucije, finančne trge in finančne instrumente, ki delujejo pod nadzorom centralnih bank in drugih finančnih regulatorjev. Ta sistem zagotavlja centralizirano regulacijo in stabilnost, kar je ključno za zaupanje v finančne trge in gospodarstvo kot celoto. Glavni akterji v tem sistemu so banke, centralne banke, investicijske družbe ter drugi finančni posredniki (Ribnikar, 2003).

Delovanje finančnih trgov je možno zaradi finančnih institucij, saj te omogočajo prenos denarja od subjektov s presežnimi denarnimi kapacitetami, k tistim, ki imajo produkcijske naložbene priložnosti. Finančne insitucije tako igrajo ključno vlogo pri izboljšanju učinkovitosti gospodarstva (Mishkin in Eakins, 2023).

Finančne institucije delimo na finančne posrednike in agentske finančne institucije. Finančne posrednike ločimo na: depozitne in nedepozitne finančne posrednike, odvisno od tega, ali zbirajo finančna sredstva z bančnimi vlogami ali ne. Primer depozitnih finančnih posrednikov so poslovne banke. V tradicionalnem finančnem sistemu imajo te banke vlogo kot posredniki med varčevalci in posojilojemalci. Poslovne banke sprejemajo depozite od subjektov z denarnimi presežki ter ta sredstva uporabijo za odobritev posojil subjektom, ki teh presežkov nimajo. Dohodek ustvarjajo predvsem z razliko med obrestnimi merami na depozite in obrestnimi merami na posojila. Poslovne banke zagotavljajo tudi vrsto drugih finančnih storitev, kot so plačilni sistemi, storitve za upravljanje premoženja ter izdajanje finančnih instrumentov (Mishkin, 2016).

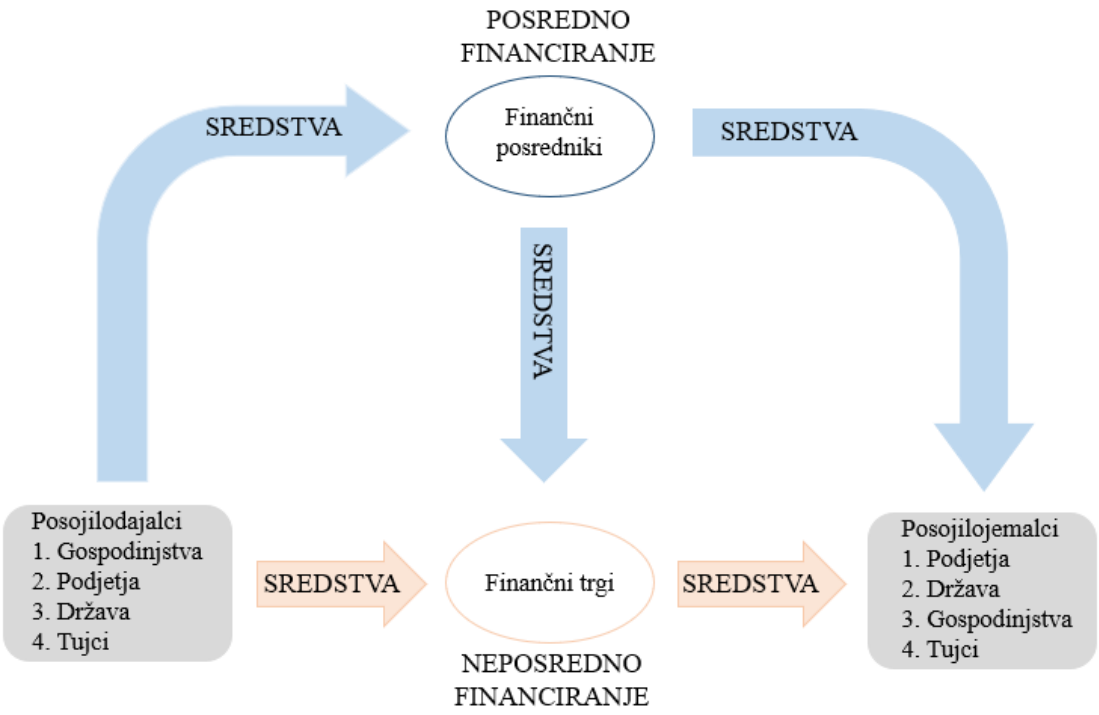
Poleg poslovnih bank so pomembni tudi drugi finančni posredniki, kot so investicijske banke, zavarovalnice in pokojninski skladi. Investicijske banke financirajo podjetja prek

izdajanja vrednostnih papirjev, zavarovalnice pa zagotavljajo zaščito pred finančnimi tveganji. Pokojninski skladi omogočajo varčevanje in dolgoročno investiranje za posameznike (Cecchetti in Schoenholtz, 2015).

2.1 Funkcija finančnih trgov in finančnih posrednikov

Kot navajata Mishkin in Eakins (2023), se preko finančnih trgov premikajo sredstva od subjektov, ki so privarčevala presežna sredstva z manjšo porabo od svojih prihodkov, k tistim, ki jim primanjkuje sredstev. Kot je prikazano na sliki 1, se tisti, ki imajo presežke in posojajo sredstva, nahajajo na levi strani, tisti, ki si morajo izposoditi sredstva za financiranje svojih izdatkov, pa na desni. Puščice kažejo, da sredstva tečejo od varčevalcev k posojilojemalcem preko dveh poti. Pri neposrednem financiranju si posojilojemalci neposredno izposojajo sredstva od posojilodajalcev na finančnih trgih s prodajo vrednostnih papirjev. Po drugi strani pri posrednem financiranju finančni posredniki - poslovne banke upravljajo in izposojajo sredstva od varčevalcev in jih nato preko posojil posojajo naprej posojilojelamcem.

Slika 1: Neposredno in posredno financiranje



Vir: prirejeno po Mishkin in Eakins (2023).

Struktura finančnih trgov - direktne finance (Mishkin in Eakins, 2023):

- Trgi dolžniških in lastniških vrednostnih papirjev. Sredstva na finančnem trgu se pridobijo z izdajo dolžniških instrumentov (obveznice, krediti) z obrestmi do zapadlosti

ali z izdajo delnic, ki predstavljajo lastništvo podjetja in prinašajo dividende brez roka zapadlosti.

- Primarni in sekundarni trgi. Primarni trg je finančni trg, na katerem se novi vrednostni papirji, kot so obveznice ali delnice izdajo s strani držav ali podjetij in prodajo kupcem na trgu. Sekundarni trg je finančni trg, na katerem se lahko preprodajajo že izdani vrednostni papirji. Izdajanje vrednostnih papirjev na primarnem trgu po navadi vodijo investicijske banke ali za to specializirane finančne institucije.
- Borzni in izvenborzni trgi. Sekundarni trgi delujejo na dva načina: preko borz, kot je Newyorška borza vrednostnih papirjev, kjer se transakcije izvajajo centralizirano preko ene lokacije. Po drugi strani pa se predvsem obveznice prodajajo preko izvenborznih trgov, kjer trgovci preko trgovalnih sistemov ponujajo konkurenčne cene brez centralizirane lokacije.

Struktura finančnih posrednikov - indirektne finance (Mishkin in Eakins, 2023):

- Finančni posredniki, ki izboljšujejo delovanje finančnih trgov s tem, da zagotavljajo storitve, ki znižujejo stroške, upravljajo tveganja in rešujejo informacijske težave. Posredno financiranje vključuje finančne posrednike, ki delujejo kot posredniki med posojilodajalci-varčevalci in posojilojemalci-porabniki. Ti posredniki si izposojajo sredstva od varčevalcev in jih nato posojajo posojilojemalcem.
- Ključne prednosti finančnih posrednikov so zmanjševanje transakcijskih stroškov z izkoriščanjem ekonomije obsega ter zagotavljanje likvidnostnih storitev. Poleg tega posredniki z diverzifikacijo sredstev in zmanjševanjem izpostavljenosti posameznim tveganjem naredijo poslovanje manj tvegano.
- Finančni posredniki prav tako rešujejo problema asimetričnih informacij. Prvi je adverzna selekcija, ko tvegani posojilojemalci iščejo posojila. Drugi problem je moralno tveganje, ko se posojilojemalci po prejemu posojila začnejo ukvarjati z bolj tveganimi dejavnostmi. S preverjanjem in nadzorom posojilojemalcev posredniki zmanjšujejo ta tveganja.
- Ekonomija obsega omogoča finančnim institucijam, da ponujajo več storitev in znižujejo stroške z uporabo istih informacijskih virov. Vendar to lahko vodi do konflikta interesov, kjer različni cilji lahko privedejo do zavajajočih ali prikritih informacij, kar negativno vpliva na učinkovitost trga.

Glede na tipe finančnih posrednikov, poznamo (Mishkin in Eakins, 2023):

- depozitne institucije (poslovne banke);
- pogodbene varčevalne institucije (zavarovalnice, pokojninski skladi);
- investicijske posrednike.

2.2 Tveganja v tradicionalnih financah

Varnost depozitov je tesno povezana s tveganji, ki so prisotni v tradicionalnem finančnem sistemu. Analiza tveganj v tradicionalnih financah bo omogočila izhodišče za primerjavo s tveganji, ki jih prinaša uporaba alternativnih tehnologij DeFi za bančne depozite, kar je predstavljeno v nadaljevanju magistrskega dela.

Tradicionalni finančni sistem se sooča s številnimi tveganji, ki lahko ogrozijo stabilnost finančnih institucij in negativno vplivajo na gospodarstvo. Ta tveganja so posledica strukture poslovanja finančnih institucij, makroekonomskih sprememb in dinamične narave finančnih trgov. Med ključna tveganja sodijo likvidnostno, kreditno, tržno in operativno tveganje, ki lahko vplivajo na uspešnost finančnih institucij ter njihovo odpornost na finančne šoke (Burton in Brown, 2014).

2.2.1 Likvidnostno tveganje

Likvidnostno tveganje nastane, kadar finančne institucije nimajo zadostnih likvidnih sredstev za izpolnitev svojih kratkoročnih obveznosti. To tveganje je zlasti prisotno pri bankah, ki imajo na eni strani obveznost do varčevalcev (depoziti), na drugi strani pa so vključene v dolgoročne posojilne pogodbe. V obdobju nenadnih zahtev po dvigu depozitov lahko banke postanejo nelikvidne, kar privede do t. i. bančne panike. Likvidnostno tveganje se je povečalo med globalno finančno krizo leta 2008, ko je propad finančnih institucij povzročil motnje na kreditnih trgih (Acharya in drugi, 2009).

V odziv na to je leta 2015 v Bruslju začel delovati Enotni mehanizem za reševanje (angl. Single Resolution Mechanism), ki je mehanizem za reševanje in obvladovanje finančnih težav bank. Ustanovljen je bil kot del širšega projekta za vzpostavitev Bančne unije v Evropski uniji, s čimer se je želelo okrepiti stabilnost in zaupanje v bančni sektor po finančni krizi (Banka Slovenije, brez datuma). Cilj Enotnega mehanizma za reševanje je zagotoviti usklajen in učinkovit pristop k reševanju bank na ravni Evropske unije. Njegova naloga je zagotavljanje likvidnosti v izrednih razmerah. To pomeni, da Evropska centralna banka, finančnim institucijam v kriznih situacijah zagotovi likvidnost, s čimer prepreči širjenje panike in zagotovi stabilnost finančnega sistema (Benediktsdottir in drugi, 2011).

2.2.2 Kreditno tveganje

Kreditno tveganje pomeni, da posojilojemalci ne bodo sposobni izpolniti svojih finančnih obveznosti. Neplačila posojil lahko ogrozijo finančno stabilnost bank, saj te institucije ustvarjajo pomemben delež svojih prihodkov prav iz posojilnih obresti. Globalna finančna kriza leta 2008 je bila močno povezana s kreditnim tveganjem, saj so posojilojemalci množično neplačevali hipotekarna posojila, kar je povzročilo propad nepremičninskega trga in propad številnih finančnih institucij (Evropska komisija, 2021).

Finančne institucije za obvladovanje kreditnega tveganja uporabljajo različne ukrepe, kot so natančno ocenjevanje kreditne sposobnosti posojilojemalcev, oblikovanje rezerv za potencialna neplačila ter zahteve po zavarovanju posojil. V zadnjih letih so regulatorji uvedli višje kapitalske zahteve, ki so namenjene obvladovanju kreditnih tveganj in preprečevanju finančnih kriz (Acharya in drugi, 2009).

2.2.3 Tržno tveganje

Tržno tveganje izhaja iz nihanja cen finančnih instrumentov, kot so obveznice, delnice, denarne valute in izvedeni finančni instrumenti. Spremembe v obrestnih merah, inflaciji, povpraševanju in ponudbi ter širših makroekonomskih dejavnikih lahko vplivajo na vrednost teh instrumentov in s tem na uspešnost finančnih institucij (Gürünlü in drugi, 2019).

Za obvladovanje tržnega tveganja finančne institucije pogosto uporabljajo strategije diverzifikacije portfeljev in kritja z izvedenimi finančnimi instrumenti, kot so opcije in terminske pogodbe. Prav tako institucije vzpostavljajo sisteme za spremljanje tržnih tveganj v realnem času, da lahko hitro reagirajo na tržne spremembe (Harvey in drugi, 2021).

2.2.4 Operativno tveganje

Operativno tveganje se nanaša na tveganja, povezana z notranjimi procesi, sistemi in človeškimi napakami v finančnih institucijah. Med tovrstna tveganja sodijo napake v poslovanju, napadi kibernetske varnosti, goljufije in tehnične napake. Zaradi digitalizacije in vse večje uporabe tehnologije v finančnem sektorju postaja operativno tveganje vse bolj pomembno. Kibernetski napadi, napake v programski opremi in nepravilnosti v obdelavi podatkov lahko povzročijo velike finančne izgube ali celo sistemske motnje. Finančne institucije uporabljajo vrsto ukrepov za zmanjšanje operativnih tveganj, vključno z vzpostavitvijo notranjih kontrol, revizij ter naložb v kibernetsko varnost in sisteme za varno obdelavo podatkov. Prav tako morajo imeti institucije vzpostavljene načrte za obvladovanje tveganj in zagotavljanje neprekinjenega poslovanja v primeru večjih motenj (Robertson, 2015).

3 TEHNOLOGIJA VERIŽENJA BLOKOV

V drugem poglavju je predstavljen tradicionalni finančni sistem, ki opravlja funkcije finančnega posredništva in zagotavlja različne vrste bančnih storitev. V tretjem poglavju je predstavljena tehnologija za možno alternativo sedanjemu finančnemu sistemu, ki kljub tehnološkemu napredku in digitalizaciji za svoje delovanje še vedno potrebuje veliko posrednikov. V tem poglavju je podrobneje predstavljena tehnologija veriženja blokov, ki omogoča decentralizirane procese v financah, brez posrednikov.

Tehnologijo veriženja blokov lahko opredelimo kot inovativno digitalno tehnologijo, ki povezuje kriptografske metode, napredno upravljanje s podatki in mehanizme za zagotavljanje preverljivosti ter varnega beleženja transakcij med udeleženci v omrežju. Opredelimo jo lahko tudi kot digitalno knjigo zapisov (angl. Distributed Ledger), ki se nenehno povečuje. Deluje kot skupna varna baza podatkov, kjer vsak udeleženec hrani svojo kopijo zapisov. Ti zapisi se lahko posodobijo le ob soglasju vseh udeležencev, ki sodelujejo v določeni transakciji. Nato se posamezne transakcije združujejo v bloke, ti bloki pa so med seboj povezani v verigo. Delovanje poteka tako, da subjekti najprej predlagajo transakcijo, omrežje vozlišč pa jo preveri in po doseženem soglasju vključi v nov blok. Vsi podatki iz verige blokov se kopirajo na številna razpršena vozlišča v omrežju, kar zagotavlja robustnost in decentraliziranost (Andoni in drugi, 2019).

Tehnologija veriženja blokov za svoje delovanje ne potrebuje centralne avtoritete ali zaupanja vrednega posrednika. Namesto tega temelji na kolektivnem upravljanju in soglasju med vozlišči. S tem tehnologija veriženja blokov rešuje dve stvari: problem zaupanja med uporabniki in težavo koncentracije moči v rokah posameznega subjekta (Elrom, 2019).

Večina ljudi je za tehnologijo veriženja blokov prvič slišala po izumu Bitcoina leta 2008. Nekateri strokovnjaki to tehnologijo opisujejo kot revolucijo, medtem ko drugi zagovarjajo stališče, da bo njen razvoj bolj evolucijski in da bo preteklo še veliko časa, preden jo bomo uporabljali vsakodnevno. Tehnologija veriženja blokov spreminja način obdelave in shranjevanja podatkov ter izvajanje transakcij. Z njo lahko preoblikujemo obstoječe poslovne modele, državna upravljanja in družbene strukture, a njena popolna vključenost zaradi same kompleksnosti tehnologije zahteva čas. Veliko je še namreč tehničnih izzivov, regulatornih ovir in potreb po prilagoditvi obstoječih sistemov (Bashir, 2018).

Osnovno delimo tehnologijo veriženja blokov na (Paxos, 2024):

- Omrežja z dovoljenji. To so omrežja z omejenim dostopom, kjer administratorji nadzorujejo, kdo lahko sodeluje v protokolu.
- Omrežja brez dovoljenj. To so omrežja z odprtim in neomejenim sodelovanjem v protokolu.

Poznamo štiri vrste tehnologije veriženja blokov (Paxos, 2024):

- Javni protokol verige blokov: omogoča prosto sodelovanje vsem udeležencem. Vsak lahko dostopa do podatkov, izvaja transakcije in sodeluje pri potrjevanju. Omrežje je popolnoma odprto in transparentno, kjer ni omejitev pri vstopu v omrežje.
- Zasebni protokol verige blokov: dostop in sodelovanje sta strogo nadzorovana in centralizirana. Ta določa, kdo lahko sodeluje v omrežju in kakšne pravice ima. Vsi udeleženci morajo biti preverjeni in potrjeni.
- Konzorcijski protokol verige blokov: skupina entitet skupaj upravlja omrežje in določa pravila sodelovanja. Udeleženci so vnaprej znani in preverjeni, običajno gre za povezane organizacije s skupnimi poslovnimi interesi.

- Hibridni protokol verige blokov: združuje lastnosti odprtega in zaprtega sistema. Del funkcij je javno dostopen vsem, medtem ko so določeni deli omrežja dostopni le pooblaščenim udeležencem. To omogoča fleksibilnost pri določanju ravni zasebnosti in dostopa.

3.1 Omrežje

Tehnologija veriženja blokov je porazdeljen sistem oziroma omrežje. Definiramo jo lahko tudi kot tehnologijo porazdeljene glavne knjige, ki se uporablja kot decentralizirana platforma (Ammous, 2022). Vozlišče je posamezna enota v omrežju in deluje kot točka komunikacije, obdelave in shranjevanja podatkov. Navadno je to računalnik s pomnilnikom in procesorsko močjo. Vsa vozlišča so si sposobna pošiljati in sprejemati sporočila med seboj (Joker.si, brez datuma).

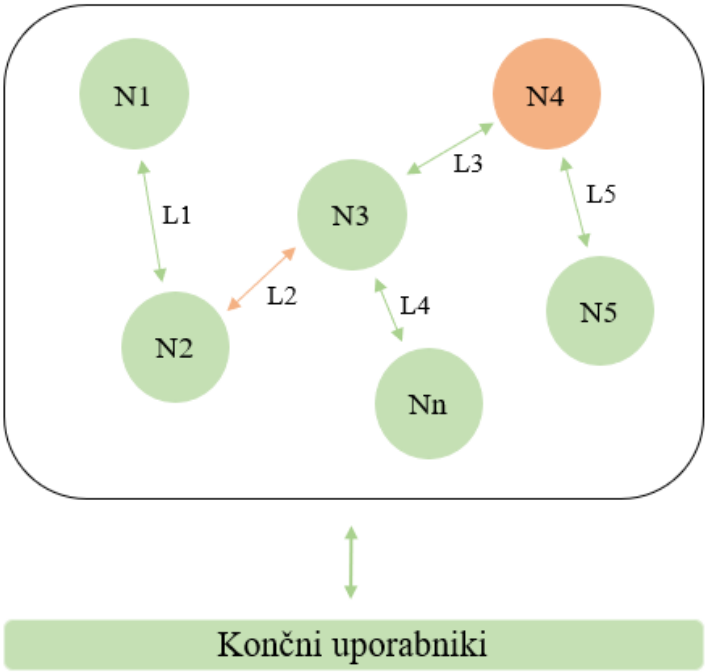
Vozlišča v verigi blokov delimo na dve kategoriji, ki opravljata različne funkcije za delovanje omrežja. Prvo skupino predstavljajo rudarji (angl. Miners), ki so odgovorni za ustvarjanje novih blokov in potrjevanje transakcij. Obenem ustvarjajo (rudarijo) nove enote kriptovalut. Delujejo v omrežjih, ki temeljijo na dokazu o delu. Drugo skupino sestavljajo podpisniki blokov (angl. Validators), katerih glavna naloga je preverjanje veljavnosti transakcij in digitalno podpisovanje novih blokov v omrežju. To zagotavljajo s konsenzom. Podpisniki blokov delujejo v omrežjih dokaza o deležu (Bashir, 2023).

Vozlišča so lahko poštena, pokvarjena ali zlonamerna. Vozlišče, ki kaže iracionalno vedenje, se imenuje bizantinsko vozlišče. Poimenovano je po problemu bizantinskih generalov, ki so ga prvič opredelili Lamport in drugi (1982). To je računalniški problem, ki se pogosto pojavlja pri delovanju tehnologije veriženja blokov. Nedosledno vedenje bizantinskih vozlišč je lahko zlonamerno in škoduje delovanju celotnega omrežja. Problem nastane pri potrjevanju transakcij, kjer niso vsa vozlišča zaupanja vredna. Zato različne tehnologije veriženja blokov uporabljajo različne tehnike za preverjanje in potrjevanje transakcij. Najbolj znana sta algoritma oziroma mehanizma soglasja: sistem dokaza o delu (angl. Proof of Work), ki se uporablja za delovanje omrežja Bitcoin in sistem dokaza o deležu (angl. Proof of Stake), ki se uporablja za delovanje omrežja Ethereum. Ta mehanizma omrežju pomagata sinhronizirati podatke in ohraniti varnost (Bashir, 2023).

Izziv načrtovanja omrežij, je usklajevanje med vozlišči in robustnost. Tudi, če nekatera vozlišča odpovedo ali se prekinejo omrežne povezave, mora omrežje nadaljevati z obratovanjem. Ta problem je že dolgo časa področje raziskav o porazdeljenih sistemih. (Zheng in drugi, 2017).

Na sliki 2 je prikazan manjši primer omrežja. Ta ima šest vozlišč, od katerih je eno (N4) bizantinsko vozlišče, kar lahko vodi do neskladnosti podatkov. L2 je povezava, ki je prekinjena ali počasna, kar lahko privede do razdelitve omrežja (Bashir, 2023).

Slika 2: Primer manjšega omrežja



Vir: prirejeno po Bashir (2018).

Lastnosti omrežja (Bashir, 2023):

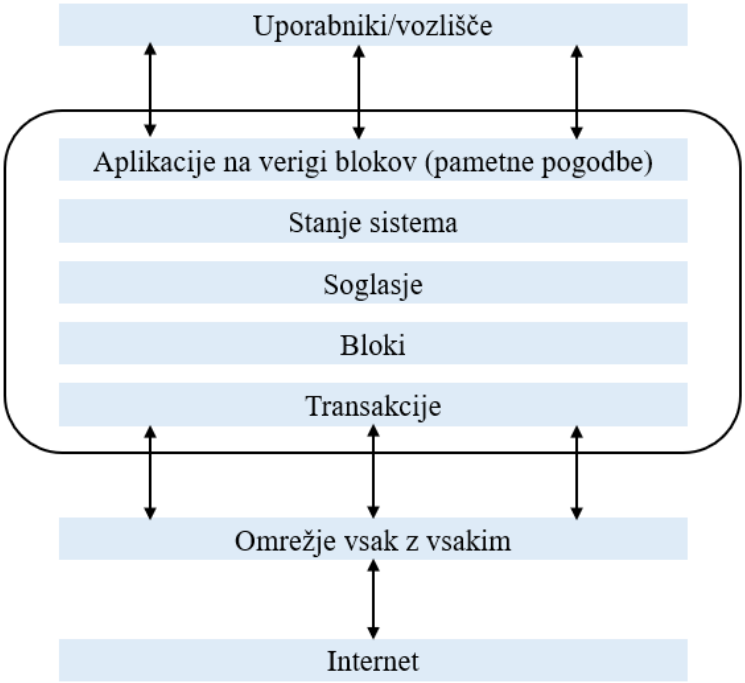
- Neposredna komunikacija vsakega z vsakim (angl. Peer to Peer). V omrežju ni centralnega nadzornika ali posrednika, saj vsi udeleženci komunicirajo neposredno drug z drugim. To omogoča neposredno izmenjavo denarnih transakcij med udeleženci brez vključevanja tretje osebe (banke).
- Porazdeljena glavna knjiga je zbirka podatkov, ki so razpršeni v omrežju računalnikov in ni centralizirana. Porazdeljena je med vozlišča v omrežju, kjer vsako vozlišče hrani svojo kopijo podatkov.
- Kriptografska zavarovanost porazdeljene glavne knjige. Kriptografija ščiti glavno knjigo pred manipulacijami. Varnost je zagotavljena zaradi: nezavrnljivosti podatkov, celovitosti podatkov in avtentikacije izvora podatkov.
- Princip samo dodajanja (angl. Append Only) pomeni, da se podatki lahko dodajajo v verigo blokov le v časovno urejenem zaporedju. Ko so podatki enkrat dodani v verigo blokov so praktično nespremenljivi. Teoretično jih je mogoče spremeniti le v primeru, če bi združena vozlišča uspela pridobiti več kot 51 odstotkov moči celotnega omrežja.
- Posodabljanje s konsenzom je ena najpomembnejših lastnosti tehnologije veriženja blokov. Zaradi tega je decentralizirana, saj nobena centralna avtoriteta nima nadzora nad posodabljanjem glavne knjige. Vsaka posodobitev v verigi blokov se preveri po merilih, ki jih določa protokol, in se vanjo vnese šele po tem, ko je med vsemi sodelujočimi vozlišči v omrežju dosežen konsenz o resnici. Za konsenz se uporabljajo različni algoritmi za doseganje soglasja, ki zagotavljajo, da se vse strani strinjajo o končnem stanju podatkov in resnici v omrežju. Infrastruktura verige blokov je večplastna in deluje

s pomočjo interneta, ki je osnovni komunikacijski sloj za omrežje. Zaradi interneta deluje direktna komunikacija vsakega z vsakim in omogoča: transakcije, bloke, mehanizme konsenza in pametne pogodbe. Vsi ti elementi delujejo skupaj kot en logičen sistem v okviru sistema vsakega z vsakim.

- Vozlišča povezana z verigo blokov izvajajo različne operacije, kot so: doseganje konsenza, preverjanje transakcij in obdelavo podatkov.

Na sliki 3 je prikazano delovanje omrežja verige blokov.

Slika 3: Omrežje verige blokov



Vir: prirejeno po Bashir (2023).

Blok je skupek transakcij, ki so logično združene in organizirane. Transakcija predstavlja zapis dogodka, na primer prenos denarja z računa pošiljatelja na račun prejemnika. Blok je sestavljen iz transakcij, njegova velikost pa se razlikuje glede na vrsto in zasnovo uporabljene verige blokov. V blok je vključeno tudi sklicevanje na prejšnji blok, razen če gre za izvorni blok (angl. Genesis Block). Izvorni blok je prvi blok v verigi blokov, ki je vgrajen v kodo ob prvem zagonu verige blokov. Struktura bloka je prav tako odvisna od vrste in zasnove verige blokov (Yaga in drugi, 2018).

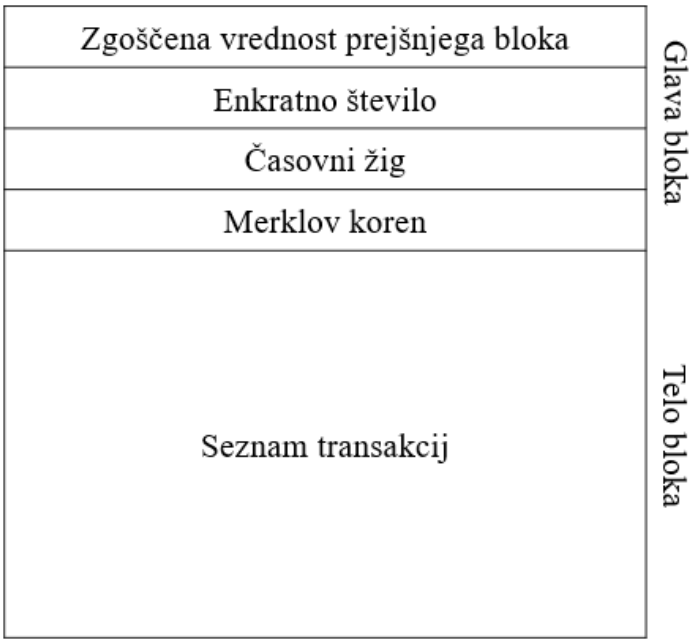
Glava bloka vsebuje (Bashir, 2023):

- verzijo bloka;
- zgoščeno vrednost prejšnjega bloka, ki zagotavlja pravilen vrstni red blokov;
- koren Merklovega drevesa, ki predstavlja zgoščeno vrednost vseh v paru zgoščenih vrednosti;

- časovni žig;
- naključno enkratno število (angl. Nonce), ki se generira ter uporabi samo enkrat in je rešitev uganke, ki jo iščejo rudarji pri algoritmu dokaza o delu;
- težavnost algoritma dokazovanja dela.

Merklov koren (angl. Merkle Root) je zgoščena vrednost vseh vozlišč Merklovega drevesa. Pri tehnologiji veroženja blokov je za potrjevanje transakcij cilj minimizirati porabo procesorske moči in hkrati zagotavljati maksimalno raven varnosti. Merklova drevesa se uporabljajo za preverjanja transakcij, kjer te niso razporejene po zaporednem vrstnem redu, ampak imajo drevesno strukturo, imenovano Merklovo drevo. V Merklovem drevesu vsako vozlišče vsebuje zgoščeno vrednost in je povezano s svojim nadrejenim vozliščem v hierarhičnem razmerju starš-otrok. Merklov koren je v verigi blokov prisoten v glavi bloka in predstavlja zgoščeno vrednost vseh transakcij v bloku. Zaradi tega je za preverjanje vseh transakcij potrebno preveriti samo Merklov koren, namesto da bi preverjali vsako transakcijo posebej (Drescher, 2017). Na sliki 4 je prikazana struktura bloka, ki je sestavljen iz glave bloka (angl. Block Header) in telesa bloka (angl. Block Body).

Slika 4: Struktura bloka



Vir: prirejeno po Antonopoulos in Wood (2018).

3.2 Sestavni deli omrežja

Drescher (2017) pravi, da je omrežje sestavljeno iz pet sestavnih delov:

- Naslov, ki je unikatna oznaka za uporabo v transakcijah verige blokov za označevanje pošiljateljev in prejemnikov. Naslov je javni ključ ali izpeljan iz javnega ključa in se

lahko uporabi večkrat. Da uporabniki preprečijo sledenje in se izognejo povezovanju transakcij s skupnimi naslovi, lahko za vsako transakcijo ustvarijo nov naslov.
- Transakcija predstavlja prenos vrednosti iz enega naslova na drugega.
- Transakcijski skript za izvajanje omejenih vnaprej določenih ukazov in transakcij.
- Navidezni stroj (angl. Virtucal Machine) je okolje za računalniške programe, ki omogočajo izvajanje pametnih pogodb.
- Pametne pogodbe so programi, ki se izvajajo na vrhu verige blokov in vsebujejo ukaze, ki se izvedejo samodejno, ko so izpolnjeni vnaprej določeni pogoji. Pametne pogodbe niso na voljo pri vseh vrstah verig blokov.

3.2.1 Pametne pogodbe

Koncept pametnih pogodb je že leta 1994 prvi predstavil Nick Szabo. Szabo (1994) pametno pogodbo opredeljuje kot elektronski transakcijski protokol, ki izvršuje pogoje pogodbe. Cilj je zadovoljiti pogodbene pogoje in njihovo izvrševanje brez posrednika. Z njimi je želel odpraviti tako zlonamerne kot nenamerne napake ter zmanjšati potrebo po zaupanja vrednih posrednikih. Pametne pogodbe se lahko implementirajo v katerikoli industriji, vendar je trenutno največ primerov uporabe povezanih s finančno industrijo. Čeprav je bila ideja zasnovana že v zgodnjih 90-ih letih, je svoj pravi potencial dosegla šele z izumom Bitcoina in nadaljnjim razvojem tehnologije veriženja blokov. Leta 2009 je bila v omrežju Bitcoin implementirana ena prvih praktičnih oblik pametnih pogodb. Transakcije so se lahko izvajale med uporabniki v omrežju, po principu vsak z vsakim, brez potrebe po zunanjem posredniku (Nakamoto, 2008).

Pametna pogodba je varen in nespremenljiv računalniški program, ki predstavlja dogovor med udeleženci ter se samodejno izvaja (Buterin, 2014). Sestavljena je iz množice programske kode in podatkovnih struktur, ki se decentralizirano izvajajo preko kriptografsko zaščitenih transakcij na omrežju (Bach in drugi, 2024). Izvrševanje pametne pogodbe poteka sočasno na vseh vozliščih znotraj omrežja. Doseganje soglasja glede novega stanja med vozlišči je ključno, da se lahko rezultat trajno zapiše v verigo blokov (Antonopoulos in Wood, 2018). Zaradi vgrajene nespremenljivosti kode v verigi blokov lahko pametna pogodba deluje kot zaupanja vreden samostojni posrednik. Pametne pogodbe lahko izvajajo zapletene izračune, trajno shranjujejo podatke, upravljajo s stanji in samodejne prenesejo sredstva med računi (Buterin, 2014).

Značilnost pametnih pogodb je njihova predvidljiva narava, kar pomeni, da morajo enaki vhodni podatki dosledno ustvariti enake izhodne rezultate. Da se izvajajo pravilno, pametne pogodbe ne morejo delovati s podatki zunaj svojega neposrednega okolja, saj bi to lahko vodilo v nepredvidljivo delovanje. Pametne pogodbe morajo vedno zagotavljati enak rezultat ne glede na to, katero vozlišče v omrežju jih izvaja. To zagotavlja robustnost in zanesljivost sistema (Zheng in drugi, 2017).

Ključne lastnosti pametnih pogodb so (Buterin, 2014):

- Samodejna izvršljivost. Pogodba se izvrši samodejno ob izpolnitvi vnaprej določenih pogojev. Ni potrebe po ročnem posredovanju ali nadzoru. Izvajanje je nepristransko in temelji izključno na programski kodi. Zaradi programske kode zmanjšuje možnost človeških napak in pristranskosti.
- Nespremenljivost. Ko je pametna pogodba nameščena v verigo blokov, je ni mogoče spreminjati. Zagotavlja varnost in zaupanje med udeleženci. Preprečuje naknadne manipulacije s pogodbenimi pogoji. Prav tako omogoča sledljivost in sled vseh transakcij.
- Semantična pravilnost. Natančno mora odražati namen in dogovor med strankami. Programska koda mora biti napisana tako, da nedvoumno izraža pogodbene pogoje. Cilj je predvidljivosti v vseh možnih scenarijih.
- Varnost je zagotovljena z uporabo kriptografskih mehanizmov za zaščito transakcij. Odporna je proti različnim vrstam napadov in manipulacij, kot so nepooblaščene spremembe in dostopi.

3.2.2 Oraklji

Oraklji so ponudniki zunanjih podatkov pametnim pogodbam, saj same dostopa do njih nimajo. Ker so verige blokov izolirane, so oraklji vmesnik, ki omogoča povezavo med kodo v pametni pogodbi in zunanjimi viri podatkov. Zagotavljajo, da lahko pametna pogodba deluje natančno in se izvede, tudi če je odvisna od podatkov zunaj omrežja na katerem je zgrajena. To omogoča aplikacijam iz različnih panog nemoteno interakcijo s pdoatki v resničnem svetu. Oraklji zagotavljajo podatke o (Bashir, 2023):

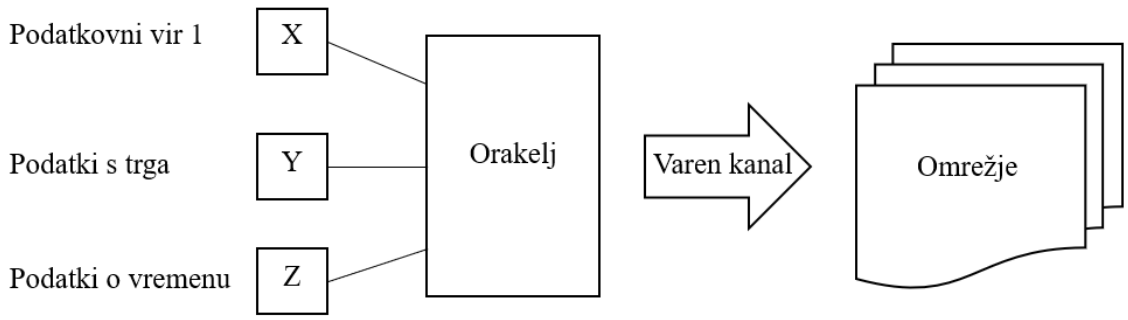
- finančnih trgih;
- vremenu;
- novicah iz realnega sveta;
- pametnih napravah s senzorji, ki so povezane z internetom;
- transportu, logistiki in drugih.

Poznamo več vrst orakljev (Chainlink, brez datuma):

- vhodni oraklji, ki podatke pridobivajo iz resničnega sveta in jih dostavljajo v omrežje;
- izhodni oraklji, ki omogočajo pametnim pogodbam pošiljanje ukazov zunanjim sistemom (sprožitev bančnih plačil);
- medverižni oraklji, ki omogočajo branje in pisanje informacij med različnimi omrežji, zagotavljajo interoperabilnost za prenos podatkov in sredstev ter omogočajo uporabo sredstev izven njihove izvorne verige;
- računsko omogočeni oraklji, ki izvajajo varne izračune zunaj omrežja zaradi tehničnih, pravnih ali finančnih ovir.

Slika 5 prikazuje osnovni model sistema oraklja in pametne pogodbe.

Slika 5: Sistem oraklja in pametne pogodbe



Vir: prirejeno po Chainlink (brez datuma).

3.2.3 Decentralizirana avtonomna organizacija

Decentralizirana avtonomna organizacija (angl. Decentralized Autonomous Organization, v nadaljevanju DAO) je oblika organizacijske strukture brez centralnega vodstva, katere člani si delijo skupni cilj: delovati v najboljšem interesu organizacije. Največkrat DAO prevzemajo obliko organiziranih skupnosti, ki se same usmerjajo in upravljajo prek pametnih pogodb, brez prisotnosti centralne avtoritete ali upravljalske hierarhije. DeFi protokole najbolj pogosto upravljanjo DAO (Axelsen in drugi, 2022).

DAO deluje preko interakcij in koordinacije od spodaj navzgor. Upravljajo jo neodvisni in racionalni agenti. S takšno organizacijsko strukturo rešuje problem principala in agenta ter s porazdeljenim sistemom upravljanja zmanjšuje tveganje za neracionalne odločitve (Axelsen in drugi, 2022).

V DAO so vsi člani lastniki organizacije in imajo moč odločanja o njenem razvoju. Običajno se predlagane spremembe zapišejo v obliki predloga za izboljšavo, o katerem se nato javno glasuje. Člani DAO izražajo svoje odločitve preko upravljavskih žetonov po principu večji delež žetonov imaš, sorazmerno več glasovalnih pravic imaš. Upravljalske žetone se lahko tudi trguje na borzah kriptovalut. Odločitve DAO se izvedejo s spreminjanjem kode pametne pogodbe (Hassan in De Filippi, 2021).

V akademski literaturi je veliko razprave o prednostih in slabostih decentraliziranega upravljanja v DAO. Sun in drugi (2024) so ugotovili, da decentralizacija privede do počasnejšega odločanja in neučinkovitosti. V praksi je upravljanje tudi nepopolno decentralizirano, saj pogosto končne odločitve sprejemajo razvijalci in ustanovitelji DAO, ki imajo v lasti največ upravljalskih žetonov.

3.3 Tehnologije decentraliziranih financ

Decentralizirane finance temeljijo na tehnologiji veriženja blokov, ki je predstavljena v prejšnjem poglavju magistrskega dela. V tem poglavju so predstavljene tehnologije decentraliziranih financ, ki predstavljajo eno izmed najpomembnejših inovacij na področju financ. Obravnavani so temeljni pojmi, tehnološka zasnova, ključne lastnosti, tveganja in regulativni izzivi. Namen poglavja je podati celovit pregled nad tehnologijami DeFi, ki omogoča razumevanje njegovega delovanja in razlik v primerjavi s tradicionalnim finančnim sistemom.

3.3.1 Opredelitev decentraliziranih financ

Od nastanka Bitcoina leta 2008 je tehnologija veriženja blokov močno spremenila tradicionalne finance. DeFi so omogočile demokratizacijo finančnih storitev in ustvarile naložbene priložnosti v žetonske oblike sredstev. Glavna sprememba se je zgodila za finančne institucije, ki so zmanjšale svojo centralizirano in dominantno vlogo (Zetzsche in drugi, 2020).

DeFi so decentraliziran finančni sistem, ki temelji na tehnologiji veriženja blokov in pametnih pogodbah. Gogel (2021) opredeljuje DeFi kot finančne aplikacije za finančne rešitve, zgrajene s pametnimi pogodbami, ki delujejo na tehnologiji veriženja blokov. Zagotavljajo finančne storitve, kot so plačila, posojanje, izposojanje, trgovanje, naložbe, zavarovanja in upravljanjem premoženja. So razvijajoča se oblika finančnih storitev in aplikacij, ki delujejo brez tradicionalnih centraliziranih posrednikov, kot so banke ali druge finančne institucije (Chen in Bellavitis, 2020).

Prednost DeFi je odprtost in dostopnost. Storitve so na voljo vsem uporabnikom brez tradicionalnih ovir in postopkov, kot so preverjanje identitete, državljanstva in plačilne sposobnosti. Celoten sistem je odprt in vse transakcije so javno preverljive na verigi blokov, kar povečuje zaupanje med uporabniki in zmanjšuje možnosti za goljufije (Schär, 2021).

Upravljanje DeFi protokolov poteka preko DAO, kjer lahko uporabniki protokola sodelujejo pri odločanju o spremembah in razvoju. Takšno upravljanje je drugačno od tradicionalnega korporativnega upravljanja, saj omogoča demokratizacijo odločevalskih procesov v finančnem sektorju (Qin in drugi, 2021).

3.3.2 Tehnologije decentraliziranih financ

Tehnologije DeFi so primarno prisotne na omrežju Ethereum, čeprav se razvijajo tudi tehnologije na drugih omrežjih. V DeFi velja temeljno načelo »koda je zakon«. Vsa pravila in pogoji delovanja so zapisani v programski kodi pametnih pogodb, ki so po namestitvi na verigo blokov nespremenljive (Werner in drugi, 2021).

Tehnologijo DeFi ločimo na pet slojev (StandICT, 2022):

- poravnalni sloj;
- sloj sredstev;
- protokolni sloj:
- aplikacijski sloj;
- agregacijski sloj.

Primarni sloj tehnologij DeFi, je poravnalni sloj. Njegova funkcija je zagotavljanje soglasja o zaporedju veljavnih transakcij, ki določajo novo stanje v verigi blokov in shranjevanje podatkov o celotnem stanju vseh pametnih pogodb. Poznamo dve vrsti poravnalnih slojev (StandICT, 2022):

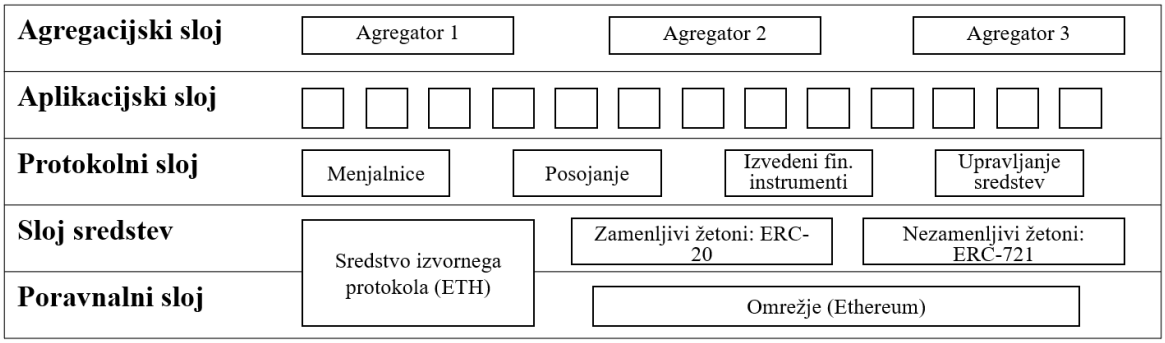
- Protokol 1. sloja (angl. Layer-1 Protocol), ki uporablja lasten protokol soglasja kot vir resnice za potrjevanje transakcij.
- Protokol 2. sloja (angl. Layer-2 Protocol), ki je sekundarni sloj. Deluje na vrhu verige blokov 1. sloja in se uporablja za povečanje hitrosti in širšo uporabnost. Za potrjevanje transakcij, ki se izvajajo na tem sloju uporablja protokol soglasja 1. sloja.

Funkcionalnost pametnih pogodb je ključna za delovanje sloja sredstev in protokolnega sloja. Sloj sredstev je sestavljen iz žetonov, ki imajo različne funkcije. Poznamo uporabniške žetone za dostop do storitev, upravljalske žetone za odločanje v protokolu, digitalna potrdila o pologu sredstev v pametno pogodbo in nezamenljive žetone. Za ustvarjanje žetonov se uporabljajo standardizirane specifikacije pametnih pogodb. Najpogostejši je standard ERC-20, ki je bil razvit v omrežju Ethereum in ga danes uporablja večina združljivih omrežij. Protokolni sloj je odgovoren za delovanje vsake DeFi aplikacije, kjer ena ali več samostojnih pametnih pogodb določa pravila delovanja protokola (StandICT, 2022).

Aplikacijski sloj je spletni uporabniški vmesnik, ki povezuje digitalno denarnico s pametno pogodbo. Spletni uporabniški vmesnik omogoča varno interakcijo z DeFi protokoli, kjer digitalne denarnice služijo kot orodje za kriptografsko podpisovanje in potrjevanje transakcij v omrežju (StandICT, 2022).

Na ravni agregacijskega sloja DeFi aplikacije temeljijo na načelu povezljivosti različnih protokolov in so zasnovane kot modularni gradniki. To omogoča medsebojno delovanje pametnih pogodb na različne načine. Integracija več različnih DeFi aplikacij omogoča razvoj finančnih produktov, ki presegajo zmožnosti posameznega protokola in so v tradicionalnem finančnem sistemu težko izvedljivi ali celo nemogoči (Harvey in drugi, 2021). Zaradi integracije lahko pametne pogodbe komunicirajo med seboj in se samodejno izvajajo tudi med več protokoli. V primerih, kjer samodejna integracija ni možna, lahko uporabniki ročno povezujejo različne DeFi aplikacije (StandICT, 2022). Slika 6 prikazuje tehnologijo DeFi, kjer so prikazani agregacijski sloj, aplikacijski sloj, protokolni sloj, sloj sredstev in poravnalni sloj.

Slika 6: Tehnologija DeFi



Vir: prirejeno po Schär (2021).

3.3.3 Lastnosti decentraliziranih financ

Lastnosti po katerih se DeFi razlikujejo od tradicionalnih financ so (Kitzler in drugi, 2023):

- Delujejo brez skrbništva (angl. Non Custodial), saj noben posrednik, kot sta banka ali borzni posrednik, nima v skrbništvu sredstev uporabnikov.
- So dostopne (angl. Permissionless), saj lahko vsakdo, brez posebnih dovoljenj uporablja obstoječe aplikacije ali razvije nove funkcionalnosti z novo programsko kodo.
- So transparentne, saj lahko vsakdo s potrebnimi tehničnim znanjem raziskuje in revidira stanje protokolov.
- Protokoli DeFi so sestavljivi (angl. Composable), kar omogoča povezano delovanje med različnimi protokoli.

3.3.4 Tveganja v decentraliziranih financah

Ker so DeFi še nezrel in hitro rastoči sektor finančne industrije, tu obstajajo nova finančna tveganja. Prav tako je ekonomska teorija v ozadju nekaterih DeFi aplikacij eksperimentalne narave in velikokrat ni dolgoročno obstojna. DeFi vključujejo tudi uporabo kriptovalut, ki imajo velika cenovna nihanja (Weingärtner in drugi, 2023).

Klasifikacija tveganj predstavlja metodološki pristop k sistematičnemu razumevanju in kategorizaciji različnih vrst tveganj. Teoretične temelje za tovrstno kategorizacijo je postavil Markowitz (1952), kjer je vpeljal razliko med sistematičnim in nesistematičnim tveganjem. Ta teorija predstavlja osnovo moderne portfeljske teorije. Sistematična tveganja zajemajo dejavnike, ki vplivajo na celoten trg in na njih posameznik nima vpliva. Med tovrstna tveganja uvrščamo makroekonomske dogodke, kot so recesije, politična nestabilnost in naravne katastrofe. Nasprotno nesistematična tveganja predstavljajo dejavnike tveganja na katera posameznik ali organizacija lahko vpliva. Slednje vključujejo dejavnike, kot so finančne odločitve, spremembe v vodstveni strukturi, način upravljanja in druge (Weingärtner in drugi 2023).

Sistematična tveganja DeFi delimo na (Weingärtner in drugi, 2023):

- Tržna tveganja: tveganje tržne manipulacije, trgovalno tveganje, tveganje obrestne mere, likvidnostno tveganje in valutno tveganje.
- Regulatorna in zakonodajna tveganje.
- Zunanja tehnološka tveganja: kriptografsko tveganje, tveganje orakljev, tveganje razširljivosti in rasti ter protokolno tveganje.

Nesistematična tveganja DeFi delimo na (Weingärtner in drugi, 2023):

- Finančna tveganja: kreditno tveganje in tveganje nasprotne stranke.
- Operativna tveganja: upravljalsko tveganje, tveganje skladnosti poslovanja, tveganje odvisnosti, tveganje resničnih informacij, strateško tveganje in tveganje ugleda.
- Notranja tehnološka tveganja: tveganje pametnih pogodb in tveganje kibernetskega napada.

3.3.5 Regulacija decentraliziranih financ

Skupna zaklenjena vrednost v DeFi je bila na dan 14. novembra 2024 129 milijard USD (DefiLlama, brez datuma). Zaradi velikosti industrije je učinkovita regulacija ključnega pomena za prihodnji razvoj. Cilj regulacije je po eni strani zagotoviti ustrezno zaščito uporabnikov, a hkrati ohraniti prostor za nadaljnje inovacije in razvoj (Axelsen in drugi, 2022).

Za finančne institucije, ki delujejo v tradicionalnih financah je izpolnjevanje regulatornih zahtev stroškovno potratno. Stroški povezani z regulacijo lahko znašajo tudi do 25 % vseh operativnih stroškov. Za DAO, ki trenutno razvijajo DeFi protokole, bi bilo izpolnjevanje enako strogih zahtev skladnosti poslovanja izjemno zahtevno ali celo ekonomsko nemogoče. Regulatorna skladnost namreč zahteva izpolnjevanje številnih pogojev, kot so: ustrezna raven kapitala in likvidnosti, centraliziran kontroling, ločitev določenih funkcij, jasno hierarhijo upravljanja in redno poročanje regulatorjem (Axelsen in drugi, 2022). Malcolm (2024) meni, da obstaja tveganje, da bi uporaba obstoječe regulacije lahko privedla do klasičnih in tudi povsem novih regulatornih tveganj. Zato je v prihodnosti nujna prilagoditev regulacije za nov in še nejasno opredeljen koncept DAO. DAO namreč ni subjekt v obliki pravne ali fizične osebe, ki lahko odgovarja za svoje obveznosti, ki nastanejo z njegovim delovanjem.

Axelsen in drugi (2022) pravijo, da je trenutno najbolj pogosto vprašanje, na kakšen način regulirati DeFi. Regulatorni organi se soočajo z izzivom oblikovanja ustrezne zakonodaje za tehnologijo, ki deluje avtonomno, brez neposrednega človeškega upravljanja. Za učinkovito regulacijo DeFi je potreben celovit pristop, ki temelji na sodelovanju med regulatornimi institucijami in deležniki v industriji. Avtorji menijo, da je prvi korak k uspešni regulaciji enotno razumevanja temeljnih konceptov DeFi tehnologije med vsemi deležniki ter jasna

opredelitev razlik v primerjavi s tradicionalnimi financami. Drugi korak je določitev kritičnih tveganj v DeFi.

Po drugi strani Malcolm (2024) meni, da bi bilo za začetek učinkovite regulacije potrebno določiti dva ključna elementa regulatornega okvira. Prvi so standardi za preprečevanje pranja denarja in financiranja terorizma, kjer so že na voljo napredne tehnološke rešitve za preverjanje sankcijskih seznamov. Drugi element je določitev minimalnih kibernetskih standardov in varnostnih ukrepov v DeFi. Razvijalci so z orodji, ki omogočajo transparentnost pametnih pogodb in njihovih upravljavskih mehanizmov na verigi blokov že razvili rešitve, ki prispevajo k višji varnosti v DeFi. Posledično se je leta 2023 zmanjšalo število vdorov v DeFi protokole. Izgubljenih je bilo za 54 % manj sredstev, v vrednosti 1,1 milijarde ameriških dolarjev (Chainalysis Team, 2024). Malcolm (2024) tudi navaja, da je za izboljšanje varnosti ključna uporaba naslednjih varnostnih ukrepov:

- revizije pametnih pogodb v DeFi protokolih;
- uporaba programov za odkrivanje varnostnih pomanjkljivost;
- sodelovanjem s specializiranimi podjetji za kibernetsko varnost;
- Rekt test, narejen po vzoru Joel testa. Test z uporabo dvanajstih preprostih vprašanj, nadomesti kompleksen Bizantinski proces ocenjevanja.

Pri regulaciji DeFi je pomembna tudi stopnja anonimnosti uporabnikov. Javna omrežja so po zasnovi odprta in omogočajo preverjanje transakcij brez centraliziranih posrednikov. To je problematično zaradi slabe zasebnosti uporabnikov. Vsaka transakcija med naslovi ali interakcija s pametno pogodbo ostane za vedno zapisana in vidna na omrežju. To je privedlo do nastanka protokolov za izboljšanje zasebnosti. Ti uporabnikom omogočajo, da sredstva v protokol pošljejo z enega naslova in jih kasneje dvignejo z drugega naslova. Vsi pologi in dvigi so še vedno vidni na verigi blokov, vendar povezava med določenim pologom in pripadajočim dvigom ni več javno dostopna. To so začele izkoriščati tudi zlonamerne skupine ljudi, ki preko takšnih protokolov prenašajo sredstva iz nezakonitih virov (Buterin in drugi, 2024).

Zaradi tega so Buterin in drugi (2024) razvili protokol z imenom Privacy Pools, ki temelji na pametnih pogodbah. Namenjen je izboljšanju zasebnosti in odkrivanju slabih akterjev v omrežju. Protokol deluje na podlagi kriptografskega mehanizma z ničelnim znanjem (angl. Zero Knowledge Proof). Z njim uporabniki razkrijejo določene informacije njihove transakcije, ne da bi jim bilo treba razkriti celotno transakcijo in prikažejo, da je vir sredstev legitimen. Deluje tako, da ena stranka (dokazovalec) prepriča drugo stranko (preverjalec), da sredstva izvirajo iz legitimnega vira, ne da bi protokolu ali drugim uporabnikom v omrežju razkril kakršne koli dodatne informacije poleg dejstva o resničnosti te trditve. S tem se omogoči, da se pošteni uporabniki protokola lahko ločijo od nepoštenih uporabnikov. Pošteni uporabniki lahko dokažejo legitimnost svojih transakcij, medtem ko nepošteni ne morejo skriti zlonamerne dejavnosti. Protokol Privacy Pools omogoča tudi možnost, da uporabniki regulatorju, razkrijejo podrobnejše informacije in dokaze o svojem premoženju.

To je pomembno za centralizirane kripto borze, saj morajo zagotavljati, da je izvor sredstev, ki jih sprejmejo skladen z regulativo (Buterin in drugi, 2024).

3.4 Decentralizirano posojanje

DeFi protokoli preko likvidnostnih bazenov (angl. Liquidity Pools) usklajujejo ponudbo in povpraševanje po kriptovalutah. Določajo pravila za depozite kot tudi za posojila v protokolu. Posamezniki, ki vložijo svoje kriptovalute v likvidnostne bazene, se imenujejo vlagatelji. Tisti, ki si kriptovalute izposodijo, se imenujejo posojilojemalci. Vlagatelj lahko z depozitom ustrezne kriptovalute prispeva k večji likvidnosti v protokolu in za to zasluži obresti. Po drugi strani si posojilojemalci kriptovalute izposodijo in za to plačajo obresti. Te se razdelijo med protokol in vlagatelje, ki zagotovljajo likvidnost. Tako kot v tradicionalnih financah, tudi v DeFi obrestne mere določajo cene za posojila in depozite. Obrestne mere so večinoma odvisne od ponudbe in povpraševanja po likvidnosti znotraj protokola, kot tudi od tržnih razmer drugih DeFi protokolov. Ko je na trgu povpraševanje po posojilih visoko, nove likvidnosti ni možno zagotoviti z ustvarjanjem novega denarja, kot je to možno v tradicionalnih financah. Izposoditi je mogoče samo likvidnost, ki jo zagotovijo vlagatelji (Feige, 2024).

V nasprotju z bančnimi posojili se v DeFi kreditna sposobnost posojilojemalcev ne ocenjuje. Tako je obrestna mera za posojilo enaka pri vseh posojilih in dodatni kreditni pribitki ne obstajajo. Po drugi strani so zahteve po zavarovanju posojila višje (Qin in drugi, 2021). Ker je pametna pogodba nepsremenljivo določena in se avtomatsko izvaja, mora zavarovanje za posojilo vedno presegati 100 % vrednosti posojila. Zaradi tega v večini primerov ni slabega dolga. Posojilojemalci si lahko izposodijo le toliko, kolikor lahko pokrijejo s svojimi sredstvi (Aramonte in drugi, 2021). To posojilojemalce spodbuja tudi h konzervativnosti. Namreč če vrednost zavarovanja pade pod vnaprej določeno vrednostjo in posojilojemalec ne more zagotoviti dodatne likvidnosti za zavarovanje, se posojilo avtomatično likvidira. Z likvidacijo se poplača posojilo in protokolu plača še kazenske obresti ob likvidaciji (Feige, 2024).

Feige (2024) opozarja tudi, da je nezadostna likvidnost pogost problem v DeFi. Zasnova večine kriptovalut ne dovoljuje izdajatelju poljubnega izdajanja novih enot za zagotavljanje likvidnosti (Nakamoto, 2008). Fiksna ponudba je pogosto obravnavana kot prednost kriptovalut, ki naj bi domnevno ohranjale svojo vrednost, vendar ima fiksna ponudba tudi posledice pri posojanju. Zaradi fiksne ponudbe, bi se lahko pri posojanju kriptovalut potencialno ustvarila deflacijski pritisk in dolžniška deflacija. To je situacija, v kateri realna vrednost dolga sčasoma narašča zaradi deflacije. Breme obresti in plačil glavnice se v tej situaciji za posojilojemalce povečuje (Feige, 2024).

3.5 Integracija tehnologij DeFi s tradicionalnim finančnim sistemom

V drugem poglavju je bil predstavljen tradicionalni finančni sistem, v tretjem poglavju pa tehnologija veriženja blokov in DeFi tehnologije. Vprašanje je kako naj tradicionalni bančni sistem uporabi te tehnologije pri svojem poslovanju. Za zdaj še ne poznamo primerov bank ali finančnih institucij, ki bi se dnevno zanašale izključno na te tehnologije in jih uporabljale pri svojem poslovanju. Nekatere banke postopoma integrirajo tehnologije DeFi v svoje testne produkte in sklepajo partnerstva z DeFi platformami ter testirajo hibridne bančne produkte tako za varčevalce kot tudi za poslovanje med finančnimi institucijami. Te vidijo veliko potenciala predvsem v čez mejih plačilih, kliringu in poravnavi med finančnimi institucijami. Tehnologija DeFi lahko poceni transakcije in po drugi strani zmanjša operativna tveganja. Vendar pa avtorja navajata, da uvajanje tehnologij DeFi zahteva znatne naložbe v prilagoditev notranjih procesov in strategij bank ter finančnih institucij, naložbe v infrastrukturo ter skladnost z regulacijo. Brez teh sprememb uvedba tehnologij DeFi finančnim institucijam ne bo prinesla pričakovanih izboljšav (Adwani in Rao, 2025).

4 ANALIZA PROTOKOLOV V DECENTRALIZIRANIH FINANCAH

Medtem ko je v drugem in tretjem poglavju predstavljena teorija, predstavlja četrto poglavje uvod v empiričen del. V tem poglavju so podrobneje predstavljeni trije najbolj uveljavljeni protokoli v DeFi, ki omogočajo možnost za donos na depozit. Pomembno je omeniti, da se v DeFi sektorju vsak dan pojavi nova tehnologija, ki bi lahko bila primerna za analizo, vendar sem se s ciljem za čim bolj kvalitetno raziskavo osredotočal na največje in uveljavljene protokole, ki so tudi že bili analizirani v akademski literaturi. Prav tako so ti protokoli največji po višini vrednosti depozitov varčevalcev, kar pomeni, da jih je trg skozi leta delovanja prepoznal kot uveljavljeno tehnologijo za DeFi depozit.

Shah in drugi (2023) pravijo, da je bila na začetku uporaba kriptovalut omejena samo na trgovanje in vlaganje. Centralizirane platforme so postale priljubljene za omogočanje teh storitev. Zahteva centraliziranih platform je, da uporabniki prenesejo zasebne ključe svojih kripto sredstev na tretjo osebo. Tako so centralizirane platforme isti posredniki, kot so banke v tradicionalnem finančnem sistemu. Zasebnost uporabnikov je manjša, provizije za transakcije pa so višje. DeFi protokol namesto vključevanja tretje osebe, finančne storitve izvaja samostojno in nadzora nad sredstvi nima. Ko so izpolnjeni vnaprej določeni pogoji, program pametne pogodbe preveri te pogoje in ugotovi ali se transakcija izvede ali ne.

4.1 Sky

Sky protokol (predhodno znan kot MakerDAO) je eden prvih DAO na področju DeFi. Ustanovljen je bil leta 2015, delovati pa je začel leta 2017 z objavo bele knjige, ki je določila teoretične in tehnične temelje protokola. Sky protokol je med vodilnimi decentraliziranimi

platformami, ki delujejo na omrežju Ethereum in temelji na decentraliziranem upravljanju (Shah in drugi, 2023). Na dan 2. 2. 2025 je bila skupna zaklenjena vrednost v Sky protokolu 5,8 milijarde ameriških dolarjev (DefiLlama, brez datuma). Upravlja se z glasovanjem, glasovalno pravico pa ima vsak imetnik upravljavskega žetona Maker (v nadaljevanju MKR). En žeton v glasovalni pogodbi, predstavlja en glas. Cilj upravljanja je zagotavljanje finančne stabilnosti protokola in ohranjanje vrednosti stabilnega kovanca Dai (Sky Protocol, brez datuma).

Dai je decentraliziran stabilni kovanec, katerega vrednost je vezana na fiat valuto USD. Za razliko od centraliziranih stabilnih kovancev, kot je Tether (USDT), izdajanje Dai ne nadzoruje centralna entiteta. Novi Dai nastajajo preko zavarovanega kreditiranja. Posojilojemalci, ki si želijo izposoditi Dai, to naredijo s pologom kriptovalut na pametno pogodbo. V zameno protokol generira nov Dai in s kreditom zagotovi novo likvidnost posojilojemalcu (Sky Protocol, brez datuma).

4.1.1 Poslovni model

Poslovni model Sky protokola temelji na sistemu zavarovanih posojil, ki delujejo preko trezorjev (angl. Vaults). Posojilojemalci v trezor položijo ustrezno kriptovaluto, ki je zavarovanje za posojilo. Skozi celotno časovno obdobje kreditiranja morajo vzdrževati določeno razmerje med vrednostjo zavarovanja in izposojenim zneskom (angl. Loan to Value Ratio, v nadaljevanju LTV). Razmerje LTV je določeno v kodi pametne pogodbe (Artemis Crypto Fundamentals, brez datuma).

Kot je razvidno iz enačbe (1), je mogoče LTV izračunati kot kvocient med zneskom posojila in tržno vrednostjo zavarovanja. Rezultat nam pove, kolikšen delež vrednosti zavarovanja predstavlja izposojeni znesek (Borgersen, 2017).

$$LTV = \frac{Znesek\ posojila}{Tržna\ vrednost\ zavarovanja} \tag{1}$$

V primeru, da vrednost zavarovanja pade pod določeno mejo, pametna pogodba avtomatsko sproži likvidacijo pozicije. Likvidacijska vrednost se porabi za poplačilo kredita in za plačilo likvidacijske provizije protokolu. Na primer, posojilojemalec lahko zastavi 1 Ethereum v vrednosti 4000 USD. S tem zavarovanjem dobi posojilo v Dai in ob tem ohrani svojo pozicijo v Ethereumu. Za posojilo plačuje obresti, ki predstavljajo prihodek tako za protokol, kot tudi za vlagatelje, ki zagotavljajo likvidnost v pametni pogodbi, imenovani Dai varčevalne obresti (angl. Dai Savings Rate, v nadaljevanju DSR) (Artemis Crypto Fundamentals, brez datuma).

Sky protokol je imel leta 2024 316 milijonov ameriških dolarjev bruto prihodkov. Od tega je 135 milijonov ameriških dolarjev plačal v DSR, ki lastnikom Dai stabilnega kovanca omogoča donos, ko z Dai žetoni zagotovijo likvidnost v protokolu (Dune, brez datuma).

DSR deluje kot bančni depozit za Dai, kjer se obrestna mera dinamično prilagaja glede na tržne razmere. Po plačilu v DSR je imel Sky protokol 181 milijonov ameriških dolarjev neto prihodkov. Glavni vir predstavljajo obresti, ki jih plačujejo posojilojemalci ob izposoji Dai. Drugi najpomembnejši vir prihodkov so naložbe v ameriške kratkoročne zakladne obveznice. Odkar je leta 2022 Ameriška centralna banka začela dvigovati obrestne mere, so takšne naložbe postale dober način za donos na likvidna sredstva v protokolu. To je tudi prva integracija tradicionalnih finančnih produktov v DeFi. Za Sky protokol, ki je DAO, to storitev upravljajo pravne osebe, odgovorne za upravljanje kripto sredstev. Ena od njih je BlockTower Capital Advisors LP, registrirana družba za investicijsko svetovanje pri ameriški Komisiji za vrednostne papirje in borzo (angl. Securities and Exchange Commission, SEC). Sredstva upravja v imenu Sky protokola in po navodilih, ki jih izglasujejo lastniki upravljalskega žetona MKR. Tretji vir prihodkov so likvidacijske provizije, ki se zaračunajo ob likvidaciji pozicij, zaradi nezadostnega zavarovanja kredita (Artemis Crypto Fundamentals, brez datuma).

Tabela 1 na levi strani prikazuje bruto prihodke, DSR, ki ga prejmejo vlagatelji ter neto prihodke, ki so izračunani med bruto prihodki in DSR. Podatki so predstavljeni v ameriških dolarjih za štiriletno obdobje od 2021 do 2024.

Tabela 1: Letni prikaz prihodkov in DSR Sky protokola za obdobje 2021–2024 (v USD)

Prihodki	**2024**	**2023**	**2022**	**2021**
Bruto prihodki	316.124.421	108.193.327	76.452.068	113.280.383
DSR	-135.058.847	-32.710.230	-10.101.231	-5.886
Neto prihodki	181.065.575	75.483.096	66.350.837	113.274.497

Vir: prirejeno po Dune (brez datuma).

4.1.2 Analiza možnosti donosa za depozit

Na Sky protokolu je možno z depozitom zaslužiti preko DSR. To je variabilna obrestna mera, ki jo vlagatelji zaslužijo s pologom in zaklepanjem svojih Dai stabilnih žetonov v pametno pogodbo DSR. Svoje Dai lahko varčevalci v pametni pogodbi DSR kadarkoli tudi odklenejo in z njimi prosto upravljajo. Nad sredstvi, ki so zaklenjena, imajo popoln nadzor. Višino obrestne mere aktivno določajo imetniki žetonov MKR z glasovanjem na verigi blokov. Obrestovanje se izvaja s kontinuiranim obračunavanjem vsako sekundo, glede na trenutno veljavno stopnjo DSR. Kot je razvidno iz enačbe (2), je mogoče končni letni znesek izračunati kot zmnožek glavnice z vsoto seštevka ena in povprečne letne obrestne mere, potenciranega s časom v letih. A je končni znesek, P glavnica, r letna obrestna mera in t čas v letih (Github, brez datuma).

$$A = P(1 + r)^t \tag{2}$$

DSR ima dva namena:

- Zagotavlja donos imetnikom Dai.
- Je eno od monetarnih orodij za uravnavanje povpraševanja po Dai, s čimer se vzdržuje njegova vrednost z vrednostjo ameriškega dolarja. Ko je cena Dai pod 1 ameriškim dolarjem, je potrebno povečati povpraševanje po Dai. To naredijo z dvigom obrestne mere in spodbudijo vlagatelje k nakupu in zaklepanju več Dai žetonov v DSR, obenem pa posojilojemalci hitreje poplačajo kredite, saj morajo plačevati višjo obrestno mero za posojilo. To zmanjša ponudbo Dai in poveča povpraševanje po Dai. Obratno velja, če je cena Dai nad 1 ameriškim dolarjem. Takrat se obrestna mera zniža in s tem spodbudi vlagatelje k manjšem zaklepanju Dai v DSR, obenem pa so krediti za posojilojemalce cenejši. To poveča ponudbo in zmanjša povpraševanje. Aktivno prilagajanje obrestne mere vzdržuje želeno razmerje Dai proti ameriškim dolarjem ena proti ena (MakerDAO, brez datuma).

Tabela 2 prikazuje uravnavanje cene Dai preko višine posojilne obrestne mere in DSR. Črka r označuje obrestno mero.

Tabela 2: Način uravnavanja cene Dai

Zmanjšanje ponudbe, r = 15 %	**Posojilna obrestna mera** (ponudba), r = 10 %	Povečanje ponudbe, r = 5 %
Dai = 0,95 $	Dai = 1 $	Dai = 1,05 $
Povečanje povpraševanja, r = 13,5 %	**Depozitna obrestna mera DSR** (povpraševanje), r = 8,5 %	Zmanjšanje povpraševanja, r = 3,5 %

Vir: lastno delo.

4.2 Aave

Aave protokol (v nadaljevanju Aave) je decentraliziran DeFi protokol, ki deluje na tehnologiji veriženja blokov. Uporabniki lahko Aave uporabljajo kot vlagatelji ali kot posojilojemalci. Vlagatelji zagotavljajo kripto sredstva v likvidnostne bazene in za to zaslužijo obresti, ki se obrestujejo vsako sekundo. Na drugi strani lahko posojilojemalci dostopajo teh sredstev pod pogojem, da zagotovijo prekomerno zavarovanje (angl. Overcollateralization) za posojilo (Aave Protocol, brez datuma).

Aave je največji DeFi protokol na trgu. Na dan 2. 2. 2025 je skupna zaklenjena vrednost znašala 35,3 milijarde ameriških dolarjev. Protokol deluje na več različnih omrežjih: Ethereum, Polygon, Avalanche in Arbitrum. Široka dostopnost omogoča nizke stroške transakcij in večjo priljubljenost med uporabniki (DefiLlama, brez datuma).

Za razliko od drugih DeFi protokolov, Aave omogoča, da lahko vsak ustvari posojilni likvidnostni bazen (angl. Lending Pool). To pomeni, da lahko teoretično uporabniki Aave posojajo in si izposojajo v katerikoli kriptovaluti. Takšna prilagodljivost je redkost na DeFi trgu in je ni mogoče najti v tradicionalnem bančnem posojanju. Aave je po svoji obliki

upravljanja DAO. Upravljajo ga imetniki istoimenskega upravljavskega žetona AAVE. Odločajo o ključnih stvareh protokola, kot je upravljanje prihodkov, prilagajanje tehničnih parametrov protokola in oblikovanje strateških odločitev protokola (Delphidigital, brez datuma).

4.2.1 Poslovni model

Aave služi prihodke s provizijami in obrestmi, ki jih plačujejo uporabniki protokola ob izposoji kripto sredstev, ob likvidacijah in bliskovitih posojilih (angl. Flash Loans). Aave razdeli del prihodkov med DAO in vlagatelje, ki z depoziti zagotavljajo likvidnost. Lastniki AAVE upravljalskega žetona preko sistema upravljanja prilagajajo višino obrestne mere za posamezne vrste posojila. Na obrestno mero za posojilo vplivajo njegova ponudba, tržna kapitalizacija, likvidnost trga in makroekonomski dejavniki, kot je aktualna višina ključne obrestne mere na trgu (Delphidigital, brez datuma).

Aave je imel leta 2024 469,5 milijonov ameriških dolarjev bruto prihodkov. Od tega je plačal 390,5 milijonov ameriških dolarjev obrestnih odhodkov vlagateljem, ki protokolu zagotovljajo likvidnost. Po plačilu obresti za depozite vlagateljem je imel Aave skoraj 79 milijonov ameriških dolarjev neto prihodkov (Token Terminal, brez datuma).

Tabela 3 na levi strani prikazuje bruto prihodke, obrestne odhodke, ki jih prejmejo vlagatelji ter neto prihodke, ki so izračunani med bruto prihodki in obrestnimi odhodki. Podatki so predstavljeni v ameriških dolarjih za štiriletno obdobje od 2021 do 2024.

Tabela 3: Letni prikaz prihodkov in obrestnih odhodkov Aave protokola za obdobje 2021–2024 (v USD)

Prihodki in odhodki	**2024**	**2023**	**2022**	**2021**
Bruto prihodki	469.524.232	118.513.490	185.035.895	362.110.813
Obrestni odhodki	390.529.754	100.463.656	164.731.603	324.855.684
Neto prihodki	78.994.478	18.049.834	20.304.292	37.255.129

Vir: prirejeno po Token Terminal (brez datuma).

4.2.2 Analiza možnosti donosa za depozit

Na Aave lahko uporabniki zaslužijo donos z depozitom stabilne kriptovalute v likvidnostne bazene. S tem zgotavljajo likvidnost na trgu, do katere lahko posojilojemalci dostopajo s prekomerno zavarovanimi krediti. V zameno ponudniki likvidnosti prejemajo variabilne obresti za depozit, ki se obrestujejo vsako sekundo, posojilojemalci pa pridobijo likvidnostna sredstva na podlagi svojega zavarovanja. Procesi posojanja, izposojanja, odplačevanja in likvidacij se izvajajo decentralizirano, brez posrednikov preko pametnih pogodb. Vsak likvidnostni bazen ima določene številne parametre, kot so: višina obrestne mere,

konfiguracija rezerv, stopnja zavarovanja in druge. Te parametre potrdijo imetniki AAVE žetona preko sistema upravljanja v DAO. Vlagatelji imajo ves čas popoln nadzor nad svojimi sredstvi. Vse transakcije se izvajajo preko pametnih pogodb, ki zagotavljajo decentraliziranost, transparentnost in varnost (Aave Protocol, brez datuma).

4.3 Compound

Compound je DeFi protokol, združljiv z EVM (angl. Ethereum Virtual Machine) in deluje na omrežju Ethereum. Osnovno sredstvo protokola je stabilni kovanec USDC. Uporabniki lahko protokol uporabljajo brez posrednika na dva načina. Prvi način je zastavljanje različnih kripto sredstev kot zavarovanje za izposojo osnovnega sredstva. Drugi način je depozit osnovnega sredstva v protokol, za kar prejmejo obresti, ki se obračunavajo v realnem času vsako sekundo. Obrestne mere za depozite in kredite so izračunane z algoritmičnim modelom in so funkcija stopnje izrabe osnovnega sredstva v likvidnostnem bazenu. Vsak model vključuje prelomno točko izrabe, nad katero se obrestna mera povečuje hitreje (Compound, brez datuma).

Na dan 2. 2. 2025 je skupna zaklenjena vrednost v Compound protokolu znašala 3,9 milijarde ameriških dolarjev. Protokol deluje na omrežjih Ethereum, Polygon, Base, Scroll, Optimism in Arbitrum (DefiLlama, brez datuma).

Compound je decentraliziran protokol, s katerim upravljajo lastniki žetona COMP. Sistem upravljanja omogoča skupnosti predlaganje, glasovanje in implementacijo sprememb preko pametnih pogodb protokola. Upravljanje Compound protokola je mogoče na različnih omrežjih, pogoj je le združljivost z EVM (Compound, brez datuma).

4.3.1 Poslovni model

Compound protokol ustvarja prihodke z razliko v obrestni meri za posojila in za depozite ter provizijami, ki se zaračunavajo za različne aktivnosti v protokolu. Vir prihodkov so tudi provizije ob likvidacijah, ki se zgodijo, ko posojilojemalci ne zagotovijo zadostne višine zavarovanja za posojilo in se njihova pozicija likvidira. Prihodki protokola se porabljajo za:

- nagrajevanje imetnikov COMP žetonov;
- razvoj in vzdrževanje protokola;
- vlagatelje, ki zagotavljajo likvidnost v protokolu;
- zakladnico DAO za nadaljnji razvoj (Compound, brez datuma).

Compound je imel leta 2024 72,7 milijonov ameriških dolarjev bruto prihodkov. Od tega je plačal 61,5 milijonov ameriških dolarjev obrestnih odhodkov varčevalcem, ki protokolu zagotovljajo likvidnost. Po plačilu varčevalcem je imel Compound 11,1 milijonov ameriških dolarjev neto prihodkov.

Tabela 4 na levi strani prikazuje bruto prihodke, obrestne odhodke, ki jih prejmejo vlagatelji ter neto prihodke, ki so izračunani med bruto prihodki in obrestnimi odhodki. Podatki so predstavljeni v ameriških dolarjih za štiriletno obdobje od 2021 do 2024.

Tabela 4: Letni prikaz prihodkov in obrestnih odhodkov Compound protokola za obdobje 2021–2024 (v USD)

Prihodki	**2024**	**2023**	**2022**	**2021**
Bruto prihodki	72.743.476	40.898.940	69.241.170	352.614.424
Obrestni odhodki	61.596.185	35.218.886	61.398.415	312.153.433
Neto prihodki	11.147.289	5.680.054	7.842.755	40.460.991

Vir: prirejeno po Token Terminal (brez datuma).

4.3.2 Analiza možnosti donosa za depozit

Na Compound protokolu lahko vlagatelji zaslužijo preko depozita osnovnega sredstva USDC v protokol. Za to prejmejo variabilne obresti, ki so odvisne od stanja na trgu in se dinamično prilagajajo glede na povpraševanje po izposoji v protokolu. Ko je povpraševanje po izposoji večje, so tudi obresti za varčevalce višje, kar spodbuja več uporabnikov k depozitu sredstev v protokol. Nasprotno, ko je povpraševanje po izposoji manjše, se obresti znižajo. Ves čas trajanja depozita imajo popoln nadzor nad svojimi sredstvi ter imajo kadarkoli možnost takojšnjega dviga sredstev. Vse transakcije se zgodijo s pomočjo pametnih pogodb in so vidne na verigi blokov (Compound, brez datuma).

5 EMPIRIČNA RAZISKAVA

V tem poglavju je predstavljena empirična raziskava, ki je bila izvedena z namenom preverjanja zastavljenega raziskovalnega vprašanja. Podrobno so opisani zasnova raziskave, metodologija ter postopek zbiranja in analize podatkov.

5.1 Zasnova, namen in cilja raziskave

V empiričnem delu magistrskega dela sem raziskal področje tehnologij DeFi z namenom ugotoviti, ali lahko depoziti na DeFi protokolih služijo kot alternativa tradicionalnim bančnim depozitom. Raziskava se osredotoča predvsem na uporabniško izkušnjo, regulatorni okvir, varnostne vidike in možnosti vključitve tehnologij DeFi v tradicionalno bančno okolje.

V nadaljevanju bom opredelil namen raziskave, cilja raziskave in raziskovalno vprašanje na katero naj bi empirična raziskava o alternativah DeFi tehnologij za bančne depozite odgovorila. Opisal bom metodologijo pridobivanja podatkov in pojasnil razlog za izbiro te metode. Na koncu bom še povzel odgovore intervjuvancev in jih umestil v teorijo.

V obdobju tehnološkega napredka na vseh področjih življenja in v času vzpenjanja tehnologije veriženja blokov ter kriptovalut vedno bolj pomembno vlogo dobiva tudi DeFi. Ključno vlogo pri vprašanju, ali bomo v prihodnosti hranili depozite na DeFi namesto na bankah, imajo regulatorji, centralne banke in poslovne banke. Prva dva bosta določala regulatorne okvire, zadnji pa oblikoval DeFi produkte za stranke, ki bodo skladni z regulacijo in tržno zanimivi. V teoretičnem delu sem preučil tradicionalni finančni sistem, tehnologijo veriženja blokov in DeFi. Potem sem za lažje razumevanje analize predstavil največje in najbolj uveljavljene DeFi protokole, ki imajo možnost donosa na depozit. To mi je pomagalo pri analizi ter bilo v pomoč pri doseganju ciljev raziskave in pri odgovoru na raziskovalno vprašanje.

Namen raziskave je ugotoviti trenutno stanje DeFi tehnologij ter preučiti, ali lahko depoziti na DeFi služijo kot alternativa bančnim depozitom. Raziskava se osredotoča predvsem na uporabniško izkušnjo, varnost in tveganja, regulatorni okvir ter možnosti integracije DeFi v tradicionalno bančno okolje. Osnovno raziskovalno vprašanje se glasi: »Ali znotraj protokolov DeFi obstaja tehnološka možnost za alternativo bančnim depozitom?«.

Da bi odgovoril na to vprašanje, sem si v raziskavi kot cilja zastavil:

- analizirati tehnološko ustreznost DeFi depozitov glede na regulatorne zahteve, uporabniško izkušnjo, varnost, donosnost in povezana tveganja;
- analizirati prednosti in slabosti DeFi depozitov v primerjavi s klasičnimi bančnimi depoziti.

Empirični del bo dopolnil teoretičen del magistrskega dela, kjer sem obravnaval tradicionalni finančni sistem, tehnologijo veriženja blokov, DeFi in glavne DeFi protokole. Temeljil bo na kvalitativnem pridobivanju podatkov s pomočjo delno strukturiranih intervjujev. To je tudi najpogostejša oblika pridobivanja kvalitativnih podatkov. Vprašanja bodo odprtega tipa in bodo lahko sledila predhodnemu zastavljenemu okviru ali pa bodo zastavljena popolnoma prosto. Spisek vprašanj za izpraševanca si bom pripravil vnaprej, izvedba pa bo prilagojena situaciji in toku pogovora. Za takšen tip intervjuja sem se odločil zaradi velike prilagodljivosti in možnosti poglobljenega izpraševanja o preučevani tematiki. To mi je pomagalo pri izvedbi analize, doseganju raziskovalnih ciljev in odgovoru na zastavljeno raziskovalno vprašanje (Kordeš in Smrdu, 2015).

5.2 Metodologija

Empirični del magistrskega dela temelji na kvalitativnem pristopu. Zbiranje primarnih podatkov je bilo izvedeno s poglobljenima delno strukturiranima intervjujema, za katera sem predhodno pripravil sklop izhodiščnih vprašanj. Za to metodo sem se odločil, ker omogoča poglobljen vpogled v mnenja, izkušnje in opažanja strokovnjakov ter fleksibilno raziskovanje obravnavane problematike. Vprašanja, ki so pokrivala več področij raziskovanja, so vidna v prilogi 1. Služila so kot okvir, vendar sta intervjuja potekala po

drugačnem vrstnem redu s podvprašanji in diskusijo. Vprašanja so pokrivala bistvene razlike med bančnimi in DeFi depoziti, uporabniško izkušnjo, vpliv regulative, varnost in tveganja, poslovni model ter priložnosti za integracijo tehnologij DeFi depozitov v bančne depozite. Pred samim intervjujem sem izhodiščna vprašanja tudi delil z intervjuvancema. Kot pravijo Bregar in drugi (2005) to omogoča bolj poglobljeno pripravo na intervju, boljšo kakovost odgovorov in bolj sproščen potek intervjuja. Odgovore sem analiziral s kvalitativno vsebinsko analizo in jih primerjal z ugotovitvami teoretičnega dela magistrskega dela. S tem sem uspešno umestil empirično analizo alternativnih tehnologij DeFi v obstoječo teorijo in oblikoval odgovor na raziskovalno vprašanje.

5.2.1 Določitev in predstavitev intervjuvancev

Ključno merilo pri izboru intervjuvancev je bilo njuno strokovno poznavanje tako tradicionalnega bančnega sistema kot tudi DeFi. Tako sem lahko pridobil čim bolj realno stanje preučevane tematike. Odločil sem se, da bom intervjuval predstavnika poslovne banke, ki dela v blockchain hub oddelku ter predstavnika kripto podjetja, ki se ukvarja z implementacijo DeFi tehnologij v tradicionalne finance.

5.2.2 Potek in izvedba intervjujev

Intervjuvanca sta pred intervjujem prejela izhodiščna vprašanja, da sta se na intervju lahko ustrezno pripravila. V obdobju med 15. aprilom 2025 in 5. majem 2025 sem izvedel intervjuja. Oba intervjuja sta bila izvedena z video klicem preko aplikacije Google Meet. Intervju s predstavnikom poslovne banke je trajal 35 minut, intervju s strokovnjakom iz kripto podjetja pa 32 minut. Pri obeh sem uporabil snemalnik zvoka.

5.3 Analiza podatkov in predstavitev rezultatov raziskave

Vprašalnik je bil sestavljen iz več sklopov vprašanj, ki vključujejo uporabniško izkušnjo, regulacijo in pravno zaščito, varnost in tveganja, poslovni model tradicionalnega bančništva in DeFi ter možnosti integracije tehnologij DeFi v bančno okolje.

V nadaljevanju so predstavljeni rezultati po teh tematskih sklopih, pri čemer povzemam in primerjam stališča obeh intervjuvancev. Analizo odgovorov sem izvedel z uporabo kvalitativne vsebinske analize, kjer sem analiziral podatke v odgovorih intervjuvancev in jih združil v več vsebinskih kategorij.

5.3.1 Uporabniška izkušnja

Za začetek sem oba intervjuvanca vprašal o glavni razliki med bančnimi depoziti in DeFi depoziti z vidika povprečnega varčevalca. Oba sta poudarila, da je pri bančnih depozitih uporabniška izkušnja enostavnejša in prijaznejša kot pri DeFi depozitih. Intervjuvanec iz

kripto podjetja je izpostavil, da je uporabniška izkušnja pri bančnih depozitih bolj prijazna in podprta s strani osebja, medtem ko mora biti pri DeFi depozitih varčevalec bolj samostojen in tehnično izobražen. Dodal je še, da je v banki preprosto odpreti račun, bančni svetovalec pri tem pomaga in zadeva je hitro zaključena. V DeFi pa mora biti varčevalec veliko bolj tehnično usposobljen, saj potrebuje svojo digitalno denarnico, ki jo mora ustvariti sam. Zaključil je, da so DeFi depoziti zasnovani za samostojno uporabo, saj mora varčevalec sam upravljati s svojimi zasebnimi ključi, izbrati ustrezen protokol in razumeti delovanje decentralizirane platforme. Intervjuvanec iz poslovne banke meni, da je trenutno DeFi depozit precej manj dostopen za povprečnega varčevalca. V zadnjih letih se je uporabniška izkušnja izboljšala, vendar še ni dovolj dobra za množično uporabo. Prav tako je dodal, da morajo biti uporabniki še vedno tehnično dobro podkovani. Posebej je poudaril pomanjkanje zaupanja varčevalcev do DeFi tehnologij, saj gre za osebne prihranke. Oblika varčevanja v DeFi ni nekaj, kar ponuja banka, in tu še posebej, ko gre za depozite, mora biti 100-odstotno zaupanje v institucijo. Banke kot institucije uživajo tradicionalno zaupanje, ki ga DeFi (brez centralnega nosilca odgovornosti) še nima.

V nadaljevanju me je zanimalo, kaj najbolj ovira širšo uporabo DeFi depozitov med varčevalci. Oba sogovornika sta se strinjala, da sta glavni oviri slaba uporabniška izkušnja, na primer kompleksnost uporabe za varčevalce in tveganje pri uporabi DeFi platform. Strokovnjak iz kripto podjetja je izpostavil, da je izboljšanje uporabniške izkušnje trenutno največji izziv razvijalcev DeFi. Pravi, da mora biti prijetna za vse varčevalce, ne samo za tehnološke navdušence. Po njegovem mnenju je DeFi okolje zaradi velikega števila protokolov, ki delujejo na podlagi različnih poslovnih modelov, nepregledno in pogosto odvrne povprečnega varčevalca. Bančni strokovnjak pa je kot ključen razlog navedel nizko stopnjo zaupanja v DeFi, predvsem zaradi vseh izgub in propadov projektov iz preteklosti. Drugi razlog je strah pred napakami pri uporabi DeFi. Meni, da se povprečni varčevalec boji, da bi zaradi lastne neizkušenosti napravil nepopravljivo napako (npr. izgubil zasebni ključ ali poslal sredstva na napačen naslov), pri banki pa za varnost in pravilno izvedbo transakcij lahko poskrbi banka.

Nato sem ju vprašal, kaj bi lahko bile rešitve za prej omenjene izzive pri DeFi depozitih. Oba menita, da bi lahko hibridni DeFi depoziti na bankah varčevalcem olajšali dostop do DeFi depozitov. Omogočili bi, da banka za komitenta hrani njegova digitalna sredstva in skrbi za zasebne ključe ter varčevalcem preko prijaznega vmesnika nudi storitve DeFi. S tem bi varčevalci pridobili izkušnjo, podobno klasičnim bančnim depozitom, medtem ko bi v ozadju dejansko delovala tehnologija DeFi. Takšne rešitve bi lahko omogočile varno uporabo tehnologij, ki sicer zahtevajo popoln nadzor s strani posameznika. Oba tudi menita, da bi takšne rešitve lahko povečale varnost in zaupanje pri varčevalcih ter zmanjšale potrebo po tehničnem znanju, kar bi lahko omogočilo širšo uporabo DeFi depozitov v prihodnosti. Kljub temu pa opozarjata, da mora biti pri hibridnih produktih jasno urejeno tudi upravljanje tveganj. Mnogo varčevalcev namreč ne razume tveganj, kot so razlike med različnimi vrstami stabilnih kovancev, možnost prevar (npr. lažne spletne strani, angl. phishing) ali

vdora v pametno pogodbo in pomen skrbnega ravnanja z zasebnimi ključi. Brez osnovnega razumevanja teh konceptov je vstop neizkušenega varčevalca v DeFi lahko tvegano, kar upočasnjuje uporabo med varčevalci. Oba strokovnjaka sta zaključila, da DeFi depoziti v sedanji obliki še niso primerni za množično uporabo povprečnih varčevalcev, opažata pa trend izboljšav. Razvoj varčevalcu prijaznejših produktov in vključevanje tradicionalnih finančnih posrednikov kot povezavo do DeFi nakazujeta, da se bo dostopnost DeFi depozitov v prihodnosti povečala.

Na koncu prvega sklopa vprašanj sem ju vprašal še o prednostih, ki jih DeFi depoziti ponujajo v primerjavi z bančnimi. Bančni strokovnjak je kot prednost omenil predvsem lažje in hitrejše premikanje sredstev med različnimi DeFi protokoli. Varčevalci lahko relativno hitro umaknejo svoj depozit iz enega protokola in ga prenesejo v drugega, ki ponuja višji donos, kar omogoča modularna zasnova DeFi. Pri bančnih depozitih takšne fleksibilnosti ni, saj je zamenjava banke dolgotrajen proces, pogajalska moč varčevalca glede donosa na depozit pa zelo omejena. Predstavnik kripto podjetja meni, da so višje obrestne mere ena glavnih prednosti DeFi depozitov. Zaradi večje tržne konkurence in manj operativnih stroškov DeFi protokoli ponujajo višje obresti na depozite kot banke. Kot primer je izpostavil, da banke v Sloveniji trenutno ponujajo skoraj nične obrestne mere na depozite, medtem ko lahko v DeFi varčevalci dosegajo višje donose na depozite. Če bi kateri DeFi protokol ponujal podobno nizke obresti kot banke, bi lahko v kratkem času izgubil vse varčevalce, saj bi ti svoje depozite prenesli drugam. DeFi varčevalcem nudi večjo izbiro in konkurenčnejše pogoje. Poleg tega dodaja, da DeFi omogoča tudi izposojo sredstev s kripto zavarovanjem, česar banka po navadi ne ponuja komitentom. Na primer, v DeFi lahko varčevalec zastavi poleg stabilnega kovanca tudi Bitcoin ali Ethereum kot zavarovanje in si izposodi stabilni kovanec.

5.3.2 Regulacija in pravna zaščita uporabnikov

Pri naslednjem sklopu vprašanj sem se osredotočil na regulatorne vidike in pravno zaščito uporabnikov pri DeFi depozitih. Poglavje sem odprl z vprašanjem o trenutnem stanju regulacije na področju DeFi, zlasti v luči nedavno sprejete evropske regulative MiCAR. Bančni strokovnjak je povedal, da je trenutno pravni okvir za DeFi še zelo nejasen in neustrezen za DeFi. V MiCAR so namreč iz neposredne regulacije izvzeti DeFi in DAO. Razlog za to naj bi bil, da je področje DeFi po ocenah regulatorjev še relativno majhno po obsegu sredstev. Poleg tega regulatorji ne vedo koga regulirati, saj pri številnih DeFi protokolih ni centralizirane pravne entitete ali odgovorne osebe. Dejal je, da si predstavlja prihodnjo regulacijo DeFi tako, da bi regulatorji regulirali posamezne storitve, ki jih DeFi protokoli nudijo, podobno kot urejajo bančne storitve. Če npr. obstaja depozitna ali posojilna storitev za stabilne kovance, naj bo regulirana enako, kot so zdaj regulirane banke pri depozitih ali kreditih. Ker intervjuvanec dela v poslovni banki se zaveda, da je izvajanje takšnega nadzora zelo zahtevno. DeFi deluje preko interneta, je globalen in deluje brez fizične prisotnosti na določenem območju. Meni, da bo uveljavljanje učinkovite regulacije

težavno, saj ni jasno, kako kaznovati kršitelje ali kako prisiliti k skladnosti platformo, ki deluje anonimno na spletu. Dodal je, da smo verjetno še več let oddaljeni od učinkovite regulative DeFi, čeprav se bo pritisk s strani regulatorjev s povečevanjem obsega sredstev v DeFi stopnjeval. Zaključil je, da MiCAR, ki je v veljavi, sedaj določa bolj jasno opredelitev kripto sredstev. Tudi tradicionalne finančne institucije bodo v prihodnosti zaradi bolj predvidljive regulacije lažje vključevale DeFi v svoje produkte. Strokovnjak iz kripto industrije je na začetku izpostavil, da je reguliranje DeFi zahtevno. Po njegovem mnenju bo sčasoma prišlo do regulacije DeFi in DAO, morda že v okviru naslednje dopolnitve MiCAR regulacije. Ta naj bi določala pravila tudi za decentralizirane platforme. Ocenjuje, da bi lahko regulator izbral posreden način regulacije. Namesto da se regulira sam decentraliziran protokol ali DAO (kar je pravno in praktično izredno težko), bi lahko regulirali sredstva in upravljalske žetone, s katerimi se upravlja protokol. S tem bi dosegli, da DAO, ki želi delovati na določenem trgu (npr. v Evropski Uniji), izpolnjuje določene pogoje glede svojih upravljalskih žetonov in s tem posredno spoštuje regulacijo. Kljub temu poudarja, da ostajajo odprta vprašanja glede izvrševanja takšne regulacije.

V drugem delu tega sklopa sem sogovornika intervjuval o pravni zaščiti varčevalcev v DeFi v primerjavi z varčevanjem na banki. Intervjuvanec iz poslovne banke pravi, da pravne zaščite pri DeFi depozitih skorajda ni. Pri bančnih depozitih so varčevalci zaščiteni s strogo regulacijo bank, nadzorom centralnih bank ter s sistemskim jamstvom za vloge, kjer so bančni depoziti zavarovani do 100.000 EUR. Za depozite v DeFi takšnih mehanizmov ni. Kripto strokovnjak je odgovoril, da v primeru DeFi ni določene pravno odgovorne entitete, zato odgovornosti za morebitno oškodovanje varčevalcev ne nosi nihče. V primeru propada protokola, prevar, hekerskih vdorov ali slabih odločitev decentraliziranega upravljanja varčevalci niso zaščiteni. Prav tako je omenil, da pri nekaterih zavarovalnicah že obstajajo produkti za zavarovanje DeFi depozitov. Delno to sedaj regulira tudi MiCAR regulacija, ki izdajateljem centraliziranih stabilnih kovancev nalaga zahteve o ustrezni kapitalski ustreznosti. Odgovor je zaključil, da formalne pravne zaščite v DeFi še ni.

Kot zadnje v tem sklopu sem sogovornika vprašal, kakšna bi po njunem mnenju morala biti regulacija DeFi. Bančni strokovnjak zagovarja stališče, da če DeFi protokol opravlja enako storitev kot banka (npr. hranjenje depozitov), potem naj zanjo veljajo enaka pravila kot pri bankah. Torej meni, da se bi moralo regulirati posamezne storitve ali produkte, ki so na voljo uporabnikom. DeFi protokoli bi morali zaprositi za pridobitev licenc in biti nadzorovani, tako kot druge finančne institucije. Obenem pa je dodal, da bo težko najti način za vzpostavitev takšne regulacije in spremljanje njenega izvrševanja. Strokovnjak iz kripto podjetja si želi regulacijo, ki bo uravnotežena, ne bo ovirala inovacij, a hkrati dala uporabnikom več varnosti. Zaključuje, da mora biti tudi jasno definirana.

5.3.3 Varnost in tveganja

V tem sklopu sem strokovnjaka spraševal o varnostnih vidikih in tveganjih DeFi depozitov v primerjavi z bančnimi depoziti. Na vprašanje, kako varni so DeFi depoziti v primerjavi z bančnimi, sta intervjuvanca podala nekoliko različna mnenja in omenila nove vrste tveganj DeFi depozitov. Predstavnik poslovne banke je poudaril, da banke delujejo v strogo nadzorovanem okolju in posvečajo veliko pozornosti operativni odpornosti svojih sistemov. K odporni in varni infrastrukturi informacijske tehnologije jih od leta 2022 zavezuje še evropska regulativa DORA, ki bankam nalaga še dodatne standarde informacijske varnosti in odpornosti sistemov. Pri bankah je namreč ključno, da komitenti nikoli ne izgubijo dostopa do svojih sredstev, ker lahko to privede do bančnega zloma. Pravi, da so nasprotno DeFi veliko bolj odprt ekosistem, kjer so vstopne ovire za vstop na trg manjše. Neprimerljivo lažje kot banko, je ustvariti DeFi protokol in začeti sprejemati depozite varčevalcev. Nizka vstopna ovira je sicer dobra za inovacije, saj lahko vsakdo preizkusi svojo idejo. Po drugi strani pa to pomeni, da na trg vstopajo neizkušeni ali zlonamerni podjetniki. Za konec je dodal, da je v preteklosti že ogromno varčevalcev izgubilo sredstva, ker so bili žrtve prevar DeFi protokolov ali pa so kupili stabilen kovanec, ki je izgubil vrednost v primerjavi z ameriškim dolarjem. Zaradi teh dejavnikov se mu trenutno DeFi depozit še ne zdi varna izbira. Strokovnjak iz kripto podjetja je odgovoril, da so DeFi depoziti bolj tvegani, še posebej zaradi množice novih protokolov in pametnih pogodb, ki se pojavljajo. Vendar pa dodaja, da so se nekateri vodilni DeFi protokoli izkazali za zelo varne. Omenil je Aave in MakerDAO, ki spadata med največje DeFi protokole za depozite in imata že dolgo zgodovino delovanja brez večjih varnostnih incidentov. Za ta dva trdi, da sta tudi varnejša kot banke, saj sta z obsegom sredstev in skozi čas dokazala zanesljivost pametnih pogodb. Imata javno pregledano kodo, izvedene zunanje varnostne revizije in znane razvojne ekipe. Prav tako sta delovala tudi med največjimi pretresi na kripto trgu. Smiselno se mu zdi razlikovati med novimi protokoli, kjer je tveganje varnostnih lukenj ali prevar večje in uveljavljenimi protokoli, kjer je to tveganje bistveno nižje. V bankah te razlike med ponudniki iz uporabniškega vidika ni, ker regulacija zagotavlja vsaj minimalni standard varnosti pri vseh bankah, medtem ko mora DeFi varčevalec sam presoditi, kateremu protokolu zaupa svoj depozit.

V nadaljevanju me je zanimalo, katera so največja tveganja pri DeFi depozitih. Strokovnjak iz kripto podjetja je izpostavil tehnološko tveganje kode, tveganje stabilnih kovancev in tveganje pri uporabi. Prvo tveganje izvira iz kode pametnih pogodb, ki lahko imajo napake, ki jih hekerji izkoristijo in odtujijo depozite. Tudi domnevno varni protokoli so lahko tarča naprednih napadov, zato sta kakovost kode in varnostne revizije pametnih pogodb izrednega pomena. Stabilni kovanci predstavljajo drugo tveganje. So osnova za DeFi depozite. Intervjuvanec opozarja, da lahko stabilni kovanci izgubijo vrednost 1:1 proti svoji referenčni fiat valuti. Še posebej pri algoritmičnih stabilnih kovancih, kot je DAI, obstaja možnost, da ob izrednih tržnih šokih algoritmi ne zdržijo in kovanec izgubi vrednost. Na tveganje izgube vrednosti niso povsem imuni niti centralizirani stabilni kovanci, kot sta USDC in USDT. To

se zgodi med izrednimi nihanji na trgu kriptovalut, ko kratkotrajno izgubijo vezavo na referenčno fiat valuto. Pri tem je dodal, da so centralizirani stabilni kovanci podvrženi še tveganju centralizacije izdajatelja kovanca. Podjetje, ki izdaja centraliziran stabilni kovanec, lahko sredstva zamrzne in onemogoči varčevalcem razpolaganje z njimi. Tretje veliko tveganje pa so uporabniške prevare. Varčevalci so lahko žrtve spletne prevare, če na lažnih spletnih straneh vpišejo svoje privatne ključe. Zlonamerni posamezniki lahko v nekaj sekundah ukradejo sredstva. Strokovnjak iz poslovne banke ni našteval tehnoloških tveganj, je pa v svojem odgovoru na splošno opozoril na možnost prevar in propadov DeFi protokolov, kar dopolnjuje zgoraj navedeno. Izpostavil je, da odsotnost regulacije omogoča zlonamernežem, da zavedejo ljudi s prevarami, kot jih je že opisal njegov predhodnik. Prav tako je posredno opozoril na tveganja skladnosti, kot so neizpolnjevanje zahtev glede preprečevanja pranja denarja in financiranja terorizma, saj DeFi protokoli trenutno ne izvajajo postopkov preverjanja svojih varčevalcev in ne izvajajo procesov proti preprečevanju pranja denarja.

5.3.4 Poslovni model tradicionalnega bančništva in DeFi

V naslednjem sklopu smo govorili o poslovnem modelu bank v primerjavi z DeFi ter možnosti integracije DeFi tehnologij v bančne produkte. Intervjuvanca sem najprej vprašal, kako primerjata poslovni model bančnih depozitov z modelom DeFi depozitov.

Bančni strokovnjak je razložil, da banka hrani depozite varčevalcev in ta sredstva posoja naprej kreditojemalcem. Pri tem imajo banke vzpostavljene modele ocenjevanja tveganj, ki določajo komu in pod kakšnimi pogoji se lahko posodi denar. Zaslužek banke nastane iz razlike med obrestmi, ki jih banka plača varčevalcem in obrestmi, ki jih prejme od posojilojemalcev. Tudi DeFi protokol povezuje ponudbo varčevalcev in povpraševanje izposojevalcev. Sredstva varčevalcev posodi naprej kreditojemalcem. S sredstvi se ustvari likvidnost v posojilnih bazenih, za kar varčevalec dobi delež prihodka od obresti. Strokovnjak iz kripto podjetja je prav tako povedal, da razlike v poslovnem modelu ni. V obeh primerih gre za finančno posredovanje med varčevalci in posojilojemalci.

Oba pravita, da se razlike pojavijo v načinu izvedbe oziroma operativnem modelu. Kripto strokovnjak je povedal, da imajo DeFi protokoli bistveno drugačen operativni model kot banke. Slednje potrebujejo številčno ekipo zaposlenih na več področjih. Ukvarjati se morajo z ogromno administrativnimi postopki, da izpolnjujejo vse zahteve regulatorjev. DeFi pa uvajajo avtomatizacijo z algoritmi, ki nadomeščajo ljudi. Pametne pogodbe avtomatizirajo procese, kot so izračun obrestnih mer v realnem času glede na prej nastavljene parametre, določajo višino vrednosti zavarovanja za posojila, avtomatično lahko likvidirajo in poplačajo posojila, ko zavarovanje pade pod zahtevani prag. Takšno poslovanje zmanjšuje operativne stroške in pospeši procese, saj se transakcije in prilagoditve izvršujejo v realnem času. Bančni strokovnjak je še dodal, da je DeFi lahko bolj učinkovit zaradi odsotnosti posrednikov, kot so zaposleni v banki. Pametne pogodbe se namreč izvajajo ves čas.

Samodejno lahko izvajajo na tisoče operacij. Po drugi strani opozarja, da bo trajalo še precej časa, da se bodo v DeFi razvili tako dobri modeli tveganja, kot jih imajo banke. Slednje imajo desetletja zgodovinskih podatkov za prilagoditve modelov upravljanja tveganj, DeFi pa so na tem področju še na začetku. Sicer se strinja, da je nekaj največjih DeFi protokolov, kot sta MakerDAO in Aave, dokazalo, da lahko kljub vsem tržnim krizam delujejo nemoteno.

Nato me je zanimalo, katere inovacije oziroma lastnosti DeFi bi po mnenju sogovornikov lahko banke vključile v svoje produkte za varčevalce. Bančni strokovnjak vidi veliko potenciala predvsem v tehnologiji DeFi za izboljšanje več bančnih procesov. Pravi, da bi se lahko tokenizirani depoziti in stabilni kovanci uporabljali pri čezmejnih plačilih. Uporaba DeFi bi lahko povečala učinkovitost pri poravnavi vrednostnih papirjev, kot so tokenizirane delnice in obveznice ter pri deviznih poslih. Zgoraj našteto sicer presega ožji pojem depozitov, kaže pa na širši trend, da banke raziskujejo uporabo teh tehnologij za nadgradnjo različnih storitev. Zato sem mu zastavil podvprašanje, kako vidi integracijo DeFi specifično za depozite. Odgovoril je, da mu je privlačna možnost zelo hitrega prehajanja med različnimi DeFi protokoli za depozite in s tem lažje iskanje najboljše možne obrestne mere. Dodal je tudi možnost uporabe drugih kriptovalut in tokeniziranih sredstev kot hipoteko za posojila. Torej banke bodo v prihodnosti ponujale tudi zavarovana posojila s kripto portfeljem strank. Kripto intervjuvanec vidi največje prednosti DeFi ravno v višjih obrestnih merah in večji fleksibilnosti varčevalcev, kar bodo po njegovem mnenju tradicionalne banke primorane omogočiti v prihodnosti. Kot druga prednost DeFi je izpostavil večjo transparentnost. Varčevalci lahko v realnem času spremljajo, kaj se dogaja z likvidnostnim bazenom, kjer imajo depozite in tudi kakšno je stanje zavarovanja posojil, s katerimi so si posojilojemalci izposodili sredstva. Nasprotno pa v tradicionalnem bančništvu komitent zaupa banki, da hrani njegove depozite in neposrednega vpogleda v to, kaj banka dela z njimi, nima. Tudi bančni strokovnjak je omenil, da je pri bankah veliko stvari za uporabnika nevidnih, kar ima prednost v poenostavitvi uporabniške izkušnje, a morda slabost v pomanjkanju transparentnosti. Kljub temu banke zaradi regulative razkrivajo svoje bilance, kapitalsko ustreznost in druge kazalnike, kar to nadomešča.

5.3.5 Integracija tehnologij DeFi v bančni sektor

Na koncu smo govorili še o prihodnjem razvoju DeFi depozitov. Zanimalo me je, katere dejavnike vidita kot ključne, da bi DeFi depoziti lahko postali resna alternativa bančnim depozitom. Povedala sta mi tudi, kakšno je njuno mnenje o hibridnih produktih, ki bi združevali DeFi tehnologijo, sedanjo uporabniško izkušnjo in varnost bančnih depozitov ter skladnost z regulativo. Oba intervjuvanca prihodnost vidita v hibridnih produktih in ne v popolni zamenjavi DeFi z bankami. Strokovnjak iz kripto podjetja meni, da bo DeFi tehnologija postala zaledna tehnologija bančnega sistema. DeFi, kot ga poznamo zdaj, ne vidi v širši uporabi, ampak bodo banke uporabljale tehnologijo veriženja blokov in svoje stare tehnološke sisteme za izvrševanje transakcij zamenjale s pametnimi pogodbami. Torej

uporabniška izkušnja bo ista. Meni, da bodo banke še obstajale in da bodo zaposleni v bankah v podporo strankam kot do zdaj. Povprečen varčevalec verjetno sploh ne bo vedel, da v ozadju deluje DeFi. Izpostavil je še, da bodo banke zaradi DeFi tehnologije lahko ponudile hitrejše, cenejše in bolj inovativne produkte. Bančni strokovnjak je odgovoril, da je DeFi na določenih področjih učinkovitejši od trenutnih sistemov bank in to banke pozorno spremljajo. Meni, da bodo banke tehnologijo veriženja blokov preučile in uporabile, če bodo videle priložnosti za učinkovitost in varnost. Predstavil je nekatere aktualne razvojne projekte nekaterih bank, ki se že dogajajo ali se bodo kmalu. Trenutno nekatere banke predvsem še eksperimentirajo z implementacijo DeFi v bančne produkte. Navedel je zelo zanimiv primer francoske banke Société Générale, ki je izdala tokenizirano obveznico in jo uporabila kot zavarovanje v DeFi protokolu MakerDAO, da je proti njej najela posojilo v stabilnem kovancu. Za institucije, zato DeFi niso več zgolj tehnologija s potencialom, ampak tradicionalne finančne institucije aktivno raziskujejo, kako lahko povežejo svoje regulirano poslovanje z DeFi. Še vedno pa je regulacija omejitev pri hitrejšem povezovanju DeFi in bank. Banke morajo poznati svojo stranko, nadzirati transakcije zaradi preprečevanja pranja denarja in poročati regulatorju. Odprti in anonimni DeFi protokoli tega še ne omogočajo.

Na vprašanje, kako vidita hibridne produkte za depozite, sta intervjuvanca odgovorila v skladu s svojim pogledom na integracijo. Bančni strokovnjak je tu omenil vlogo skrbništva digitalnih sredstev s strani bank. Meni, da bo večina ljudi v prihodnosti uporabljala skrbniške digitalne denarnice, ki jih bodo ponudile banke, saj povprečen varčevalec ne želi sam nositi odgovornosti za varnost svojih privatnih ključev in depozitov. Banke bodo najprej morale zgraditi infrastrukturo za to skrbništvo digitalnih sredstev, kjer bi lahko varčevalci hranili depozite v stabilnih kovancih in druge kripto žetone. Tudi kripto sogovornik je bil enakega mnenja, čeprav je pristaš zasebnosti in samostojnega upravljanja s premoženjem, se strinja, da povprečen varčevalec ne bo želel popolnoma samostojno upravljati svojih finančnih sredstev. Tudi on vidi prihodnost v tem, da bodo banke ohranile svojo vlogo posrednika in integrirale DeFi v svoje zaledne tehnološke sisteme. Meni, da bodo banke bodo ponujale nove produkte, ki bodo za delovanje uporabljali pametne pogodbe.

Na koncu me je zanimalo, kdaj bi banke nove hibridne varčevalne produkte ponudile varčevalcem. Bančni strokovnjak ocenjuje, da se bodo v prihodnjih nekaj letih nadaljevali poizkusi in pilotni projekti. Prve bi lahko produkte na osnovi DeFi tehnologije ponudile manjše banke, nato pa bodo sledile tudi večje banke, ko bo delovanje že bolj preizkušeno. Pravi, da je veliko odvisno tudi od hitrosti regulatorjev, saj bi lahko z jasno regulativo banke hitreje razvile skladen produkt. Kripto strokovnjak je rekel, da je težko napovedati, vidi pa trend, da se tradicionalne finance in DeFi združujejo. Centralne banke z razvojem digitalnih valut centralnih bank in poslovne banke z raziskovanjem tokeniziranih depozitov pravzaprav že uvajajo nekatere principe decentraliziranih tehnologij v klasični sistem. Oba sogovornika menita, da bo končni uporabnik pri tem imel koristi v obliki boljše uporabniške izkušnje, hitrejših transakcij, višjih donosov na depozit in večje izbire, brez občutka povečane kompleksnosti in tveganosti.

6 DISKUSIJA

V tem poglavju so predstavljene ključne ugotovitve magistrskega dela, pridobljene na podlagi pregleda literature in izvedene kvalitativne raziskave. V diskusiji bom primerjal teoretična izhodišča z ugotovitvami intervjujev ter podal zaključke, ali so DeFi protokoli lahko izvedljiva alternativa bančnim depozitom. V nadaljevanju so sistematično obravnavane glavne raziskovalne teme in odgovor na raziskovalno vprašanje.

6.1 Ključne ugotovitve

V sklopu magistrskega dela sem želel ugotoviti, ali so lahko DeFi protokoli alternativa bančnim depozitom. Odgovoriti sem želel na raziskovalno vprašanje in preučiti:

- uporabniško izkušnjo,
- regulacijo in pravno zaščita uporabnikov,
- varnost in tveganja,
- poslovni model tradicionalnega bančništva in DeFi ter
- integracijo tehnologij DeFi v banke.

Na podlagi zbrane literature in virov ter rezultatov kvalitativne raziskave sem prišel do ugotovitev, ki so povzete v nadaljevanju.

Intervjuja z bančnim in kripto strokovnjakom sta pokazala, da so DeFi depoziti v času pisanja magistrskega dela še bistveno manj primerni za varčevalce in zaupanja vredni kot pa klasični bančni depoziti. Uporabniška izkušnja pri bančnih depozitih je preprostejša, saj so postopki jasni, vodijo jih usposobljeni bančni uslužbenci, medtem ko mora biti varčevalec pri DeFi tehnično nadpovprečno izobražen in samostojen pri upravljanju svojih sredstev. Drugi dejavnik je tudi zaupanje, saj banke kot institucije tradicionalno uživajo zaupanje med varčevalci, ki ga DeFi še niso vzpostavile. Glavni oviri za širšo uporabo DeFi depozitov sta zahtevna uporaba ter visoko tveganje pri uporabi DeFi platform. Povprečnega varčevalca odvračajo upravljanje digitalne denarnice, varovanje zasebnih ključev in strah pred nepopravljivimi napakami pri uporabi, kot je izguba zasebnega ključa in nakazan denar na napačen naslov. K nizki stopnji zaupanja prispevajo tudi številni pretekli primeri izgub sredstev in propadlih projektov v kripto industriji. Za omenjene ovire bi lahko bili rešitev hibridni DeFi produkti za bančne depozite. Banke bi za varčevalce hranile digitalna sredstva in zasebne ključe. S tem bi lahko bil dostop do DeFi depozitov lažji in bolj varen. Uporabniška izkušnja bi bila podobna kot pri klasičnih bančnih depozitih, po drugi strani bi se zmanjšala potreba po tehničnem znanju in za varčevalce bi odgovornost za upravljanje depozitov in skladnost z regulativo prevzela banka.

Prednosti DeFi depozitov so višji donosi in večja fleksibilnost za varčevalce v primerjavi z bančnimi depoziti. Zaradi visoke konkurence in bolj stroškovno učinkovitega delovanja so obrestne mere višje kot pri bančnih depozitih. Varčevalci lahko sredstva tudi razmeroma

hitro prestavijo iz enega DeFi protokola v drugega v iskanju boljše obrestne mere za depozite. Po drugi strani je zamenjava banke počasna, pogajalska moč komitenta pri obrestnih merah pa omejena. DeFi omogočajo tudi nove finančne storitve, kot so posojila s kripto zavarovanjem, ki pri bankah zaenkrat niso mogoča. Po drugi strani se v DeFi še razvijajo modeli upravljanja tveganj, ki jih imajo banke že bolj razvite zaradi dolgoletnih izkušenj in podatkov.

Na področju regulative in pravne zaščite varčevalcev je med DeFi depoziti in bančnimi depoziti velika razlika. Trenutnega pravnega okvira za DeFi depozite ni, evropska uredba MiCAR izključuje decentralizirane protokole in DAO iz neposrednega nadzora. Posledično varčevalci DeFi depozitov nimajo nobene pravne zaščite, ki jo varčevalci na bankah imajo. DeFi depoziti prinašajo nova tveganja, ki v bančništvu niso prisotna. To so tehnološko tveganje kode in tveganje stabilnih kovancev, za kar varčevalci nimajo nobene pravne zaščite. Tveganje kode lahko varčevalci zmanjšajo z uporabo protokolov, ki že vrsto let obratujejo brez večjih varnostnih incidentov. Imajo pregledno odprtokodno kodo in redne zunanje varnostne revizije. Bistvena razlika pa je, da v DeFi uporabnik sam nosi odgovornost za izbiro varnega protokola, medtem ko v bančnem sistemu regulatorni nadzor pri vseh bankah zagotavlja vsaj minimalne varnostne standarde.

V prihodnosti bi lahko bila namesto popolne zamenjave bank z DeFi, verjetna združitev tehnologij DeFi s tradicionalnim bančništvom. Kot že omenjeno imajo hibridni produkti velik potenical, saj bodo združevali DeFi tehnologijo z obstoječo bančno infrastrukturo, regulativo, varnostjo in uporabniško izkušnjo. Tehnologija DeFi bo postala zaledna tehnologija bančnega sistema. Torej banke bi lahko transakcije izvajale s pametnimi pogodbami, medtem ko bo uporabniška izkušnja za stranke ostala enaka kot doslej. Povprečni varčevalec tako morda sploh ne bo vedel, da v ozadju deluje DeFi. Banke bodo hranile digitalna sredstva in zasebne ključe varčevalcev. Veliko bo odvisno od hitrosti regulatorjev. Jasna regulacija bi bankam omogočila hitrejši razvoj skladnih DeFi produktov. Varčevalci bomo imeli od tega koristi v obliki hitrejših transakcij, višjih obrestnih merah za depozite in večje konkurenčnosti trga, brez povečanja kompleksnosti in tveganj.

Odgovor na glavno raziskovalno vprašanje: »Ali znotraj protokolov DeFi obstaja tehnološka možnost za alternativo bančnim depozitom?« je zaradi zgoraj naštetih dejavnikov in rezultatov raziskave negativen.

6.2 Omejitve in priporočila za nadaljnje raziskovanje

Pri pisanju magistrskega dela sem se tako v teoretičnem kot tudi v empiričnem delu soočal z določenimi omejitvami, ki vplivajo na končne ugotovitve. Ena od omejitev teoretičnega dela je pomanjkanje znanstvene literature, saj je področje DeFi, zlasti z vidika uporabe za bančne depozite, razmeroma novo in še neraziskano. Na tem področju še vedno primanjkuje empiričnih znanstvenih raziskav. Prav tako je razvoj tehnologije bistveno hitrejši od njenega

znanstvenega in zakonodajnega razvoja, kar lahko vpliva na aktualnost določenih ugotovitev.

Empirični del raziskave je temeljil na delno strukturiranih intervjujih z dvema strokovnjakoma, kar predstavlja relativno omejen vzorec za raziskavo. Ker je bila uporabljena kvalitativna metoda, so pridobljeni podatki subjektivne narave in odražajo osebna stališča intervjuvancev. Oba sogovornika sta strokovnjaka s področja tehnologij DeFi, vendar sem si v okviru raziskave prizadeval pridobiti tudi mnenje regulatorja, da bi zagotovil bolj uravnotežen in celovit vpogled v obravnavano problematiko. V ta namen sem želel izvesti intervju z viceguvernerjem Banke Slovenije, dr. Markom Pahorjem, vendar z njim žal nisem uspel vzpostaviti kontakta. Kljub temu sem z intervjujem s predstavnikom poslovne banke pridobil širšo perspektivo institucij do obravnavanega področja. Omejitev raziskave predstavlja tudi dejstvo, da so bile zaradi obsežnosti tematike in omejene dolžine magistrskega dela posamezne vsebine obravnavane zgolj okvirno, brez možnosti poglobljene analize.

Za prihodnje raziskave bi bilo smiselno razširiti vzorec sogovornikov ter vključiti še predstavnike centralne banke in regulatorjev. S tem bi se zagotovil širši nabor podatkov ter bolj uravnotežena in primerljiva analiza. Priporočljivo je tudi vključevanje metodološke triangulacije, na primer s kombinacijo intervjujev, anket in fokusnih skupin, saj bi to pripomoglo k večji zanesljivosti rezultatov. Za nadaljnje raziskave priporočam raziskovanje v smeri razvoja hibridnih DeFi produktov za bančne depozite.

7 SKLEP

Z razvojem družbe in napredka tehnologij, ki pomembno izboljšujejo produktivnost na vseh ravneh življenja, morajo tudi banke stopiti v korak s časom. Ključno je, da preučujejo nove tehnologije in prilagajajo delovanje svojih procesov.

Skozi pretekla leta je popularnost trga kriptovalut povzročila veliko zanimanje za DeFi. Danes imajo večjo veljavo predvsem zaradi svojega tehnološkega potenciala, kot pa zaradi špekulacije po hitrem zaslužku s kripto žetoni. DeFi predstavljajo pomemben razvoj na področju digitalizacije in avtomatizacije finančnega sistema. S celovito analizo DeFi je očitno, da ima pravilen nadaljnji razvoj tehnologije veriženja blokov skupaj z razvojem ustrezne regulative potencial za napredek tradicionalnih financ in v okviru tega tudi bančnih depozitov. Ta tehnologija bi lahko ob povezavi s skrbništvom in varnostjo bank, izboljšala trenutno stanje trga in omogočila hitrejše izvajanje finančnih transakcij. Večja konkurenca med bankami in zagotavljanje stalne razpoložljivosti finančnih storitev brez geografske ali institucionalne omejitve je po mojem mnenju ključni doprinos DeFi za varčevalce.

Skozi magistrsko delo sem prikazal tako negativne kot pozitivne lastnosti DeFi za bančne depozite, jih analiziral, dosegel cilja in oblikoval ključne ugotovitve. Delo s tem prispeva k razumevanju, kako se lahko bančništvo preoblikuje z uvajanjem tehnologij DeFi. Izpostavil

sem, da bodo varčevalci imeli pozitivne koristi te tehnologije, le če bo razvoj potekal v smeri varnih, reguliranih in uporabniku prijaznih produktov za depozite.

DeFi so v trenutni obliki možna alternativa bančnim depozitom, predvsem za manjšino tehnoloških navdušencev, ki lahko riziko in vso odgovornost za svoja dejanja nosijo sami. Menim, da bodo tradicionalne banke in DeFi v prihodnosti vedno manj direktni konkurenti, temveč bodo vse bolj povezani v novi obliki finančnih hibridnih produktov za depozite. Tako bodo DeFi tehnologije služile kot avtomatski program za izvrševanje transakcij in oblikovanje novih produktov za varčevanje, banke pa kot most med inovativno tehnologijo in varčevalci. Magistrsko delo potrjuje, da DeFi lahko v prihodnosti izboljšajo produkt bančnih depozitov, predvsem z vidika avtomatizacije, donosnosti, fleksibilnosti in dostopnosti, medtem ko trenutno še niso ustrezna alternativa z vidika uporabniške izkušnje, regulative in varnosti za varčevalce.

SEZNAM KLJUČNE LITERATURE

1. Axelsen, H., Jensen, J. R. in Ross, O. (2022). When is a DAO Decentralized? *Complex Systems Informatics and Modeling Quarterly*, *31*, 51–75. https://doi.org/10.7250/csimq.2022-31.04
2. Busayatananphon, C. in Boonchieng, E. (2022). Financial Technology DeFi Protocol: A Review. *7th International Conference on Digital Arts, Media and Technology, DAMT 2022 and 5th ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering, NCON 2022*, 267–272. https://doi.org/10.1109/ECTIDAMTNCON53731.2022.9720373
3. Buterin, V., Illum, J., Nadler, M., Schär, F. in Soleimani, A. (2024). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Blockchain: Research and Applications*, *5*(1), 100–176. https://doi.org/10.1016/J.BCRA.2023.100176
4. Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Review, Federal Reserve Bank of St. Louis Review*, *103*(2), 153–174. https://doi.org/10.20955/r.103.153-74
5. Weingärtner, T., Fasser, F., Reis Sá da Costa, P. in Farkas, W. (2023). Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management 2023, 16*(10), 454. https://doi.org/10.3390/jrfm16100454

LITERATURA IN VIRI

1. Aave Protocol. (brez datuma). *Aave Documentation.* https://aave.com/docs
2. Acharya, V., Philippon, T., Richardson, M. in Roubini, N. (2009). The financial crisis of 2007-2009: Causes and remedies. *Financial Markets, Institutions and Instruments*, *18*(2), 89–137. https://doi.org/10.1111/J.1468-0416.2009.00147_2.X

3. Adwani, R. in Sudhakar Rao, V. (2025). Decentralized Finance (DeFi): Reshaping Traditional Banking Systems. *European Economic Letters, 15*(1). https://doi.org/10.52783/EEL.V15I1.2432
4. Ammous, S. (2022). *Bitcoin standard : decentralizirana alternativa centralnemu bančništvu*. Orcabay.
5. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. in Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014
6. Antonopoulos, A. M. in Wood, G. (2018). *Mastering Ethereum : Building Smart Contracts and DApps*. O'Reilly.
7. Aramonte, S., Huang, W. in Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*. https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
8. Artemis. (brez datuma). *Maker - A Deep Dive Into The World's First Unbiased Global Financial System*. https://www.artemis.xyz/research/maker---a-deep-dive-into-the-worlds-first-unbiased-global-financial-system
9. ATVP. (brez datuma). *Drugi finančni produkti | Vlagatelji ATVP*. https://vlagatelj.atvp.si/financni-produkti/drugi-financni-produkti
10. Bach, C., Bhaskar, N. D., Birch, D. G. W., Buchanan, A., Choo, K.-K. R., Chuen, D. L. K., Cruysheer, A., De Filippi, P., Haili, L., Jaag, C., JinCheng, Z., Killeen, A., Kristof, A., Lee, T. M., Levin, R. B., Li, G., Lim, J. W., Mas, I., McKinney, R. E., … Zuberi, M. M. (2024). *Handbook of Digital Currency (Second Edition)*. Academic Press. https://doi.org/10.1016/B978-0-323-98973-2.01002-9
11. Balkovec, J. (2000). Izobraževanje za upravljanje osebnega premoženja. *Andragoška spoznanja*, *6*(1), 49–62. https://doi.org/10.4312/AS.6.1.49-62
12. Banka Slovenije. (brez datuma). *Enotni sklad za reševanje*. https://www.bsi.si/financna-stabilnost/resevanje-bank/enotni-sklad-za-resevanje
13. Bashir, I. (2018). *Mastering Blockchain - Second Edition*. Packt Publishing Ltd.
14. Bashir, I. (2023). *Mastering Blockchain - Fourth Edition*. Packt Publishing Ltd.
15. Benediktsdottir, S., Danielsson, J. in Zoega, G. (2011). Lessons from a collapse of a financial system. *Economic Policy*, *26*(66), 183–235. https://doi.org/10.1111/J.1468-0327.2011.00260.X
16. Borgersen, T. A. (2017). The optimal LTV-ratio, mortgage market variability and monetary policy regimes: A demand-side perspective. *Journal of Financial Economic Policy*, *9*(2), 225–239. https://doi.org/10.1108/JFEP-06-2016-0044/FULL/XML
17. Bregar, L., Ograjenšek, I. in Bavdaž, M. (2005). *Metode raziskovalnega dela za ekonomiste: izbrane teme.* Ekonomska fakulteta Univerze v Ljubljani.
18. Burton, M. in Brown, B. (2014). *The Financial System and the Economy: Principles of Money and Banking* (Fifth). Routledge.
19. Buterin, V. (2014). A next generation smart contract in decentralized application platform. *Ethereum White Paper*, *37*.

20. Cecchetti, S. G. in Schoenholtz, K. L. (2015). *Money, banking, and financial markets*. McGraw-Hill Education.
21. Chainalysis Team. (2024, 24. januar). C*rypto-hacking-stolen-funds-2024* [objava na blogu]. Pridobljeno 4. januarja 2025 s https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/
22. Chainlink. (brez datuma). *What Is a Blockchain Oracle?* https://chain.link/education/blockchain-oracles#types-of-blockchain-oracles
23. Chen, Y. in Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, *13*. https://doi.org/10.1016/J.JBVI.2019.E00151
24. Compound. (brez datuma). *Compound III*. https://docs.compound.finance/
25. DefiLlama. (brez datuma). *Total Value Locked in DeFi*. https://defillama.com
26. Delphidigital. (brez datuma). *Aave: A Review Of The Fundamentals.* https://members.delphidigital.io/reports/a-look-back-at-aaves-2022-fundamentals
27. Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress. https://doi.org/10.1007/978-1-4842-2604-9
28. Dune. (brez datuma). *Sky – Financial Reporting*. https://dune.com/steakhouse/makerdao
29. Elrom, E. (2019). *The Blockchain Developer*. Apress. https://doi.org/10.1007/978-1-4842-4847-8
30. Evropska komisija. (2021, 25. maj). *European Financial Stability and Integration Review 2021*. https://finance.ec.europa.eu/system/files/2021-05/european-financial-stability-and-integration-review-2021_en.pdf
31. Feige, G. (2024). *Modelling and Simulation of Cryptocurrency Lending* (magistrsko delo). Harvard University. https://dash.harvard.edu/handle/1/37378521
32. Github. (brez datuma). *MakerDao.* https://github.com/makerdao/developerguides/blob/master/dai/dsr-integration-guide/dsr-integration-guide.md
33. Gogel, D. (2021). DeFi Beyond the Hype – The Emerging World of Decentralized Finance. *Wharton Blockchain and Digital Asset Project*, 1–20. https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
34. Gürünlü, M., Dayi, F., Erdem, S., Altun, D., Adhami, S., Giudici, G., Son-Turan, S., Gümüş Gülüzar, K., Gümüş, Y., Çimen, A. in Serkan, C. (2019). *Blockchain Economics and Financial Market Innovation*. Springer International Publishing. https://doi.org/10.1007/978-3-030-25275-5
35. Harvey, C. R. , Ramachandran, A. in Santoro, J. (2021). *DeFi and the Future of Finance* (First.). John Wiley and Sons.
36. Hassan, S. in De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, *10*(2), 1–10. https://doi.org/10.14763/2021.2.1556
37. Joker.si. (brez datuma). *Proof-of-work in proof-of-stake: V čem je razlika?* https://www.joker.si/proof-of-work-in-proof-of-stake-v-cem-je-razlika/

38. Kitzler, S., Victor, F., Saggese, P. in Haslhofer, B. (2023). Disentangling Decentralized Finance (DeFi) Compositions. *ACM Transactions on the Web*, *17*(2). https://doi.org/10.1145/3532857/ASSET/6BDB2754-FDE8-441D-B992-CF401E68DC51/ASSETS/GRAPHIC/TWEB-21-0092-F10.JPG
39. Kordeš, U. in Smrdu, M. (2015). *Osnove kvalitativnega raziskovanja* (1. izd.). Založba Univerze na Primorskem.
40. Lamport, L., Shostak, R. in Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401.
41. MakerDAO. (brez datuma). *MakerDAO Technical Docs*. https://docs.makerdao.com/
42. Malcolm, C. (2024, 28. februar). *DeFi Regulation: Practical Next Steps to Make the Industry Safer* [objava na blogu]. Pridobljeno 8. januarja 2025 s . https://www.chainalysis.com/blog/defi-regulation-practical-next-steps-to-make-the-industry-safer/
43. Markowitz, H. (1952). Portfolio Selection. *The Journal of Finance*, *7*(1), 77. https://doi.org/10.2307/2975974
44. Mishkin, F. S. (2016). *The Economics of Money, Banking and Financial Markets, Global Edition.* Pearson Addison Wesley.
45. Mishkin, F. S. in Eakins, S. (2023). *Financial Markets and Institutions, Global Edition* (Tenth). Pearson Higher Ed.
46. Muske, G. in Winter, M. (2004). Personal Financial Management Education: An Alternative Paradigm. *Journal of Financial Counseling and Planning*, *15*(2), 79–88. https://doi.org/10.1177/1077727X8701600101
47. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf
48. Paxos. (2024, 22. maj). *Understanding the Different Blockchain Types* [objava na blogu]. Pridobljeno 15. januarja 2025 s https://www.paxos.com/blog/understanding-the-different-blockchain-types
49. Qin, K., Zhou, L., Gamito, P., Jovanovic, P. in Gervais, A. (2021). An empirical study of DeFi liquidations: Incentives, risks, and instabilities. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 336–350. https://doi.org/10.1145/3487552.3487811
50. Ribnikar, I. (2003). *Monetarna ekonomija II. Mednarodni denarni sistem* (2. izdaja). Ekonomska fakulteta Univerze v Ljubljani.
51. Robertson, D. (2015). *Managing Operational Risk*. Palgrave Macmillan. https://doi.org/10.1007/978-1-137-44217-8
52. Schiller, J. (2022). *Essays on Monetary Policy* (doktorska disertacija). University of Bayreuth, Faculty of Law, Business and Economics.
53. Shah, K., Lathiya, D., Lukhi, N., Parmar, K. in Sanghvi, H. (2023). A systematic review of decentralized finance protocols. *International Journal of Intelligent Networks*, *4*, 171–181. https://doi.org/10.1016/J.IJIN.2023.07.002
54. Sky Protocol. (brez datuma). *Crypto (General).* https://sky.money/faq

55. StandICT. (2022). *Decentralised Finance (DeFi) report 2022.* The European Union Blockchain Observatory & Forum. standict.eu/sites/default/files/2022-06/DeFi Report EUBOF - Final_0.pdf#page=5.19
56. Sun, X., Stasinakis, C. in Sermpinis, G. (2024). Decentralization illusion in Decentralized Finance: Evidence from tokenized voting in MakerDAO polls. *Journal of Financial Stability*, *73*. https://doi.org/10.1016/J.JFS.2024.101286
57. Szabo, N. (1994). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/FM.V2I9.548
58. Token Terminal. (brez datuma). *Market overview.* https://tokenterminal.com/explorer
59. Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D. in Knottenbelt, W. J. (2021). *SoK: Decentralized Finance (DeFi)*. https://doi.org/http://dx.doi.org/10.48550/arXiv.2101.08778
60. Yaga, D., Mell, P., Roby, N. in Scarfone, K. (2018). Blockchain Technology Overview. *National Institute of Standards and Technology Internal Report*. https://doi.org/10.6028/NIST.IR.8202
61. Zetzsche, D. A., Arner, D. W. in Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/JFR/FJAA010
62. Zheng, Z., Xie, S., Dai, H., Chen, X. in Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data,* 557–564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85
63. Zveza potrošnikov Slovenije. (brez datuma). *Depoziti – katera banka ponuja najvišje obresti*. https://www.zps.si/novice/depoziti-katera-banka-ponuja-najvisje-obresti-2024-01-19

PRILOGA

Priloga 1: Vprašalnik o alternativnih tehnologijah DeFi za bančne depozite

Splošna primerjava in uporabniška izkušnja

- Kako bi primerjali bančni depozit in depozit v DeFi z vidika povprečnega varčevalca?

- Kako ocenjujete uporabniško izkušnjo za depozit v DeFi, v primerjavi z bančnim depozitom?

- Kaj menite, da ovira večjo uporabo DeFi depozitov med povprečnimi uporabniki?

- Katere prednosti, ki jih bančni depoziti nimajo, ponujajo DeFi depoziti?

Regulacija in pravna zaščita varčevalcev

- Glede na to da MiCAR regulacija določa pravila za centralizirane ponudnike kripto storitev in centralizirane izdajatelje kripto sredstev, ne pa za DAO, ki upravljajo DeFi protokole - kako naj bi bili po vašem mnenju slednji regulirani?

- Na kakšen način bi lahko regulatorni organi sodelovali z razvijalci DeFi za vzpostavitev regulacije, ki ne bi zavirala inovacij?

- Kakšna je trenutna pravna zaščita uporabnikov DeFi?

- Zavarovanje depozitnih vlog na bankah in DeFi je drugačno. V Evropski Uniji so depoziti na banki vključeni v jamstvo za vloge pri centralnih bankah do 100.000 €, kako je s tem pri DeFi depozitu?

- Kako bi lahko zagotovili zaščito uporabnikov na primeru DAO, kjer ni določene pravno odgovorne entitete?

Varnost in tveganja

- Kako ocenjujete varnost depozitov v DeFi v primerjavi z varnostjo depozitov na bankah?

- Katera so po vašem mnenju najpomembnejša tveganja pri DeFi depozitih?

- Kako bi ocenili razmerje med donosom in tveganjem pri DeFi depozitih v primerjavi z bančnimi depoziti, mogoče tudi tveganje ki ga z Defi depozitom sprejmeš?

- Kakšna tveganja predstavljajo izdajatelji stabilnih kovancev pri DeFi depozitu?

Poslovni model tradicionalnega bančništva in DeFi

- Kakšne so razlike v poslovnem modelu ustvarjanja donosa na depozit pri bančnih depozitih in DeFi depozitih?

- Katere inovacije oziroma lastnosti DeFi depozitov bi po vašem mnenju lahko banke integrirale v svoje depozitne produkte?

- Kako vidite prihodnost hibridnih produktov za depozit, ki bi združevali skladnost z regulacijo bank in tehnološke inovacije DeFi?

Integracija DeFi v bančni sektor

- Kateri dejavniki na področjih regulacije, tehnologije, ekonomskega modela ali drugje, so potrebni, da bi DeFi depoziti lahko postali alternativa tradicionalnim bančnim depozitom?

- Na katerih področjih DeFi depoziti že zdaj presegajo bančne depozite?