UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKA NALOGA

ANALIZA TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV IN ALTERNATIVNIH UPORAB NA PODROČJU DENARNIH TRANSAKCIJ

Ljubljana, januar 2019 GREGOR RAJŠP

IZJAVA O AVTORSTVU

Podpisani Gregor Rajšp, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza tehnologije veriženja podatkovnih blokov in alternativnih uporab na področju denarnih transakcij, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Matejem Marinčem

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

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

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

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

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

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

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

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

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

V Ljubljani, dne 27.01.2020 Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

ang. - angleško
ACH - (ang. Automated Clearing House); Automatizirana klirinška hiša
ASIC - (ang. Application-specific integrated circuit); Specifični integrirano vezje
BFT - (ang. Byzantine faul tolerance); Bizantinska toleranca napak
CCL - (ang. Cardano computation layer); Cardano sloj računanja
CSL - (ang. Cardano settlement layer); Caradno sloj poravnave
DPoS - (ang. Delegated proof of stake); Podrejeni dokaz o deležu
DDOS - (ang. Distributed denial-of-service); Porazdeljeno zavrnitev storitve
EBA - (ang. European Banking Authority); Evropski bančni organ
ECB - (ang. European Central Bank); Evropska centralna Banka
EU - (ang. European Union); Evropska Unija
FED - (ang. Federal Reserve System)
Gpi - (ang. Global Payment Initiative); Globalna plačilna pobuda
IBM - (ang. International Business Machines Corporation)
JPM - (ang. JP Morgan Chase Corporation)
KWh - (ang. Kilowatt hour); Kilovatna ura
MB - (ang. Megabyte); Megabajt
NACHA - (ang. National Automated Clearing House Association)
pBFT - (ang. Practical Byzantine Fault Tolerance); Praktična bizantinska toleranca napak
PoS - (ang. Proof of Stake); Dokaz o deležu
PoW - (ang. Proof of Work); Dokaz o delu
RPCA - (ang. Ripple Protocol Consensus Algorithm); Algoritem soglasja Ripple
RPoW - (ang. Reusable proof of work); Dokaz o delu za večkratno uporabo
RSA - Rivest Shamir Adleman
RTGS - (ang. Real-time gross settlement); Sistem bruto poravnave v realnem času
SCP - (ang. Stellar Consensus Protocol); Protokol soglasja Stellar
SCT - (ang. SEPA Credit Transfer); Kreditni prenos SEPA
SDD - (ang. SEPA Direct Debit); SEPA direktna bremenitev
SEC - (ang. Securities and Exchange Commission); Komisija za vrednostne papirje in borze
SEPA - (ang. Single Euro Payments Area); Enotno območje plačil v eurih
SWIFT - (ang. Society for Worldwide Interbank Financial Telecommunication)
TWh - (ang. Terawatt hour); Teravatna ura
USD - (ang. United States dollar); Ameriški dolar
ZDA - Združene države amerike

UVOD

Medtem ko so v preteklosti podjetja iskala inovacije na številnih področjih, predvsem na področjih, kot so marketing, prodaja, management in zgradbe organizacije, danes največjo priložnost za doseganje konkurenčne prednosti nudi tehnološki razvoj. Trg podjetja prisili konstantno vlagati v razvoj in nadgrajevanje tehnologij za podporo poslovanja ali iskanja novih rešitev za prodajo na trgu. Danes podjetja vlagajo številne vire v razvoj še bolj specializiranih načinov za tehnološko podporo poslovanja (aplikacije, spletno poslovanje, algoritmi, podatkovne baze, strojno učenje itd.). Finančni sektor pri tem seveda ni izjema, pravzaprav bi ga lahko uvrstili v sam vrh pri hitrosti sprejemanja in uvedbe nove tehnologije v poslovanje z namenom, dosegati konkurenčne prednosti. Uporaba interneta je modernizirala sisteme za izvajanje plačil in prenosov denarja ter revolucionirala trgovanje na delniških trgih in omogočila instantno trgovanje na vseh borzah po svetu. Tudi moderne banke se vse bolj osredotočajo na spletno in mobilno bančništvo oz. na spletno podporo obstoječemu poslovnemu modelu. V preteklosti so bile prisiljene velik del svojih virov investirati v odpiranje novih branž, poslovalnic in mreže bankomatov, danes pa je mogoče opraviti praktično vse bančne storitve preko spleta, trend pa nakazuje, da se bo to nadaljevalo. To je za banke in druge finančne ustanove tudi velik izziv, predvsem z vidika spletne varnosti in varovanja podatkov, po drugi strani pa tudi velika priložnost za digitalizacijo poslovanja, ki bo finančni sektor približala mlajšim, tehnološko bolj podkovanim generacijam. Velike investicije v razvoj novih tehnologij močno nakazujejo na spreminjanje poslovnih modelov bank in vse bolj obširno uporabo najmodernejših tehnologij, med njimi tudi tehnologije veriženja podatkovnih blokov.

Tehnologija porazdeljenih podatkovnih baz in veriženja podatkovnih blokov lahko v relativno preprosti terminologiji opišemo kot digitalizirano in porazdeljeno podatkovno bazo, ki vsebuje zgodovino vseh transakcij (Bashir, 2018, str. 5). Je ključni del delovanja tako imenovanih kripto valut, saj predstavlja podatkovno strukturo, ki omogoča kreacijo in porazdelitev digitalnih podatkovnih baz preko omrežja povezanih računalnikov, zavarovanih z naprednimi oblikami kriptografije (Nakamoto, 2009a). Kot avtorja tehnologije lahko navedemo osebo (ali skupino oseb) s psevdonimom Satoshi Nakamoto, ki je opisal delovanje kripto valute bitcoin, saj je želel ustvariti digitalni denarni sistem brez komponente zaupanja. Izrecno je navedel, da je razlog za vzpostavitev tega digitalnega denarnega sistema odstranitev posrednikov in tretjih oseb, ki so tradicionalno potrebni za izvajanje denarnih transakcij. Posredniki imajo določene stroške za izvajanje teh storitev, ti stroški pa se nato prenesejo na končne uporabnike in lahko vodijo do neučinkovitosti sistema in omejujejo dostop do finančnih storitev. Banke in drugi posredniki imajo razvit svoj sistem denarnih transakcij in uporabnikom nalagajo veliko provizij, izogibanje tem posrednikom pa je bil eden izmed dejavnikov za ustvarjanje kripto valute bitcoin (Nakamoto, 2009a). Kljub obljubam o zamenjavi obstoječega finančnega sistema pa se da zdi, da bo tehnologija veriženja podatkovnih blokov ta sistem optimizirala in omogočila številne nadgradnje.

Tehnologija bi lahko v prihodnosti popolnoma spremenila način opravljanja temeljnih funkcij bank in finančnih ustanov, saj omogoča uvedbo sistemov, ki bodo finančni sistem, vsaj v teoriji, naredili bolj transparenten, hitrejši in cenovno ugodnejši. Kot temeljna področja financ, ki se lahko spremenijo zaradi tehnologije, velja izpostaviti sistem denarnih transakcij, saj v teoriji namreč omogoča vzpostavitev učinkovitega sistema, ki bo nudil hitre in cenovno ugodne transakcije 24 ur na dan, 7 dni v tednu, 365 dni v letu. Poleg tega uporaba tehnologije nudi popolno sledljivost transakciji, kar omogoča večjo varnost in zanesljivost. Tehnologija ponuja tudi rešitve na področju pametnih pogodb, digitalizacije sredstev, vrednostnih papirjev, procesa poznavanja strank itd. Porazdeljene podatkovne baze in veriženje podatkovnih blokov omogočajo poleg uporabe v finančnem sektorju tudi številne druge rešitve na praktično vsakem področju elektronskega poslovanja. Podjetja z uvedbo tehnologije laže dostopajo do vseh podatkov, kar znatno zmanjša stroške nadzora in potrjevanja. Zmožnost zanesljivega shranjevanja podatkov omogoča uvedbo na vseh področjih, ki trenutno zahtevajo ogromno količino birokracije in papirnih dokazov. Tehnologija omogoča celotno digitalizacijo javnih registrov in javno dostopnih informacij, te pa bi bile nadgrajene in potrjene instantno. Tehnologija ima številne možne aplikacije na finančnem in bančnem področju že danes, potencial pa je opaziti predvsem v obsegu storitev, ki jih lahko spremeni v prihodnosti. Cilj magistrskega dela je proučitev in podroben opis tehnologije porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, tehnologije, ki omogoča njeno delovanje, prednosti in slabosti ter možnosti aplikacij na področju denarnih transakcij. V magistrskem delu ne bom analiziral tržne vrednosti kripto valut in razlogov za njihovo gibanje, ampak želim preveriti možnosti zamenjave trenutnega sistema denarnih transakcij ali uporabo veriženja kot izboljšavo in dopolnitev za doseganje višje stopnje učinkovitosti in lažjega dostopa do finančnega sistema. Opisati želim praktične primere uporabe, njihove prednosti, slabosti in možnosti integracije v trenutne sisteme. Temeljna raziskovalna vprašanja tega magistrskega dela:

- **Raziskovalno vprašanje 1:** Trenutni sistem denarnih transakcij je zaradi uporabe številnih posrednikov počasen, drag in neučinkovit.
- **Raziskovalno vprašanje 2:** Tehnologija porazdeljenih podatkovnih baz in veriženja podatkovnih blokov lahko zaradi svojih temeljnih lastnosti popolnoma zamenja obstoječi sistem, saj z eliminacijo posrednikov nudi hitrejši, cenejši in bolj učinkovit transakcijski sistem.
- **Raziskovalno vprašanje 3:** Tehnologija veriženja podatkovnih blokov ima številne možne aplikacije, predvsem v finančnem in bančnem sektorju.

V prvem delu so natančno predstavljeni tradicionalni plačilni sistemi, ki se uporabljajo trenutno, s poudarkom na sistemih v Evropski uniji. Opisal sem njihove ključne lastnosti, prednosti in tudi slabosti. Predvsem me je zanimalo delovanje sistemov, količina transakcij, ki jih obdelajo, hitrost obdelave teh transakcij, provizije in razširljivost. Najprej sem opisal lokalne sisteme, ki deluje na državni ravni oz., v primeru Evropske unije, na vseevropski ravni. Te sisteme sem razdelil na sisteme za plačila z večjimi vrednostmi, ki se delijo na

sisteme bruto poravnave v realnem času in sisteme neto poravnave. Nato sem analiziral sisteme za obdelavo večjega števila potrošniških plačil manjših vrednosti. Te sisteme je možno razdeliti na sisteme za kartična plačila in sisteme za medbančna nakazila, ki jih primarno obdelujejo razne avtomatizirane klirinške hiše. Nato sem analiziral še sisteme za mednarodne transakcije. V tretjem poglavju sem opisal tehnologijo porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, na kratko povzel zgodovino in ključne korake pri njenem razvoju. Opisal sem vrste sistemov na podlagi veriženja podatkovnih baz. V četrtem poglavju sem nadaljeval s tehničnim segmentom tehnologije, saj sem predstavil štiri ključne sklope lastnosti, ki temeljijo na med seboj povezanih že obstoječih vrstah tehnologij v obliki porazdeljene narave podatkovnih baz in peer-to-peer tehnologije, kriptografije, podatkovnih struktur ter algoritmov za soglasje. V petem poglavju sem podrobno proučil najbolj popularno uporabno tehnologijo porazdeljenih podatkovnih baz in veriženja, podatkovnih blokov, kripto valute. Na kratko sem opisal najbolj popularne kripto valute in jih na koncu primerjal glede na ključne parametre za njihovo uporabo. Nadaljeval sem z analizo uporabe veriženja podatkovnih blokov, predvsem na področju denarnih transakcij. Primarno sem se osredotočil na primere uporabe tehnologije v finančnih institucijah, ki ponujajo rešitev za realne probleme. Ker gre večinoma za zgolj teoretične primere uporabe, samih tehničnih vidikov nisem analiziral, saj so v splošnem isti kot tisti, ki so opisani v začetnih poglavjih tega dela. Nato sem podrobno opisal prednosti tehnologije, predvsem pa slabosti. V zaključku sem povzel vsebino magistrskega dela in ovrgel dva raziskovalna vprašanja, enega pa potrdil. Primerjal sem obstoječi sistem s sistemom, ki bi ga lahko omogočila tehnologija veriženja podatkovnih blokov, in ugotovil, da je težko govoriti o potencialni nadomestitvi tradicionalnih sistemov, obstajajo pa možnosti za nadgradnjo. Ker gre za relativno novo temo, o njej ni na voljo več tradicionalnega gradiva, kot so knjige in učbeniki. Ko je bilo možno, sem navajal vire iz knjig in učbenikov, kljub temu pa sem za vire primarno uporabljal avtorske članke v strokovnih revijah in poročila strokovnjakov. Uporabil sem tudi teoretična avtorska dela inovatorjev, znana kot beli papir, članke na spletnih straneh, analize in poročila, ki so jih pripravila razna svetovalna podjetja in podjetja, ki se ukvarjajo s praktično uporabo veriženja podatkovnih blokov.

1 TRADICIONALNI PLAČILNI SISTEMI

Plačilni sistem je kateri koli sistem, ki se uporablja za poravnavo finančnih transakcij s prenosom denarne vrednosti in vključuje institucije, instrumente, ljudi, pravila, postopke, standarde in tehnologije, ki omogočajo takšno izmenjavo (Bossone & Cirasino, 2001, str. 7). So vrsta procesov in tehnologij, ki prenašajo denarno vrednost od enega subjekta k drugemu, ki se običajno izvedejo v zameno za dobavo blaga, storitev ali za izpolnitev pravnih obveznosti. Plačilni sistemi naj bi bili varni in stroškovno učinkoviti, zmožni obdelati velike količine in rasti te količine, omogočajo izjemno nizko stopnjo zlorab in delujejo z nizkimi stroški (Bank for International Settlements, 2018, str. 91). Kljub temu širitev uporabe sistema ne sme voditi do sorazmernega povečanja stroškov, saj je bistvena značilnost vsakega uspešnega denarnega in plačilnega sistema množična uporaba. Uporabniki ne

potrebujejo le zaupanja v sam denar, ampak morajo tudi zaupati, da bo plačilo potekalo takoj in gladko.

Plačilni sistemi so ponavadi razvrščeni na plačilne sisteme velike vrednosti in potrošniške plačilne sisteme, odvisno od vrste transakcij, ki jih obdelujejo (Nakajima, 2017, str. 2). Potrošnika plačila so običajno nizkocenovne transakcije, ustvarjene v velikih količinah, na primer za nakup blaga in storitve in plačila med posamezniki. Plačila velike vrednosti se običajno izmenjujejo med finančnimi institucijami v okviru dejavnosti finančnega trga. Na splošno vključujejo velike količine in zahtevajo hitro, nepreklicno in pravočasno poravnavo. Iz teh razlogov je izredno pomembna lastnost končnost plačila (ang. finality of payment) in s tem povezana zmožnost izpodbijanja transakcij, ki so bile morda nepravilno izvršene (Bank for International Settlements, 2018, str. 93). Nanaša se na trenutek, ko je plačilo opravljeno in ima prejemna institucija nepreklicen dostop do denarja. Končnost plačila zahteva, da je sistem v veliki meri brez goljufij in operativnih tveganj na ravni posameznih transakcij in sistema kot celote. Dodatna pomembna lastnost je odpornost, ki opisuje sposobnost sistema, da preživi učinek prekinitve delovanja in obnovi svoje dejavnosti, da bi še naprej zagotavljal minimalne storitve. Obstoječi sistemi tipično dokazujejo visoke stopnje odpornosti, saj nudijo visoko raven storitev, brez daljših prekinitev. Poleg odpornosti je eden izmed dejavnikov, ki merijo samo delovanje sistemov, tudi razširljivost (ang. scalability) in je atribut, ki opisuje zmožnost sistema za rast in upravljanje povečanega povpraševanja (Investopedia, 2019a). Sistem, ki je opisan kot razširljiv, ima prednost, ker se bolj prilagaja spreminjajočim se potrebam ali zahtevam uporabnikov. Razširljivost je pogosto znak stabilnosti in konkurenčnosti, saj pomeni, da je sistem pripravljen na obvladovanje dotoka povpraševanja, povečane produktivnosti, trendov, spreminjajočih se potreb in celo novih konkurentov. Obstoječi plačilni sistemi tipično dokazujejo izjemno visoke stopnje razširljivosti, predvsem na področju plačil manjših vrednosti. Plačilne sisteme je mogoče primerjati s številnimi dejavniki, kot so cenovna ugodnost, hitrost, odpornost in razširljivost (Association for Financial Professionals, 2015, str. 3). Cenovna ugodnost plačilnega sistema se tipično izrazi v obliki transakcijske provizije, ki jo morata poravnati plačnik in/ali prejemnik za izvedbo transakcije. Poleg provizij za specifično transakcijo je velikokrat treba poravnati vstopni strošek oz. strošek uporabe sistema. Hitrost plačilnih sistemov se nanaša na čas, ki je povezan z izvedbo transakcije oz. s tem, kako dolgo mora prejemnik plačila čakati, da prejme plačilo.

1.1 Sistemi za prenose velike vrednosti

Sistemi za prenose velikih vrednosti (ang. large value payment systems) prenašajo transakcije, ki se izmenjujejo med finančnimi institucijami v okviru dejavnosti finančnih trgov in običajno vključujejo velike zneske, ki zahtevajo nujno, nepreklicno in pravočasno poravnavo (Tompkins & Olivares, 2016, str. 13). Obdelava prenosov velikih vrednosti vključuje dva ključna elementa: obračun (ang. clearing) in poravnavo (ang. settlement). Obračun oz. kliring je prenos in potrditev informacij med plačnikom in prejemnikom plačila

(Lai, 2018, str. 284). Poravnava je dejanski prenos sredstev med finančno institucijo plačnika in finančno institucijo prejemnika plačila. Končnost plačila in pravila teh sistemov tipično urejata pristojni regulator in veljavna zakonodaja. Sisteme za prenos velikih vrednosti običajno delimo na dve vrsti (Tompkins & Olivares, 2016, str. 12). Ko so bili uvedeni elektronski plačilni sistemi, so bili v mnogih državah najprej oblikovani na principu neto poravnave z odloženim oz. določenim časom. Končna poravnava neto pozicij se zgodi na koncu dneva. V novejših sistemih bruto poravnave v realnem času se poravnava izvede na bruto osnovi.

1.1.1 Sistemi bruto poravnave v realnem času

V zadnjih dveh desetletjih so bili sistemi za plačilo velikih vrednosti v mnogih državah preoblikovani tako, da so plačila, ki jih obdelujejo, poravnana na podlagi bruto poravnave v realnem času (Nakajima, 2017, str. 3). Sistem bruto poravnave v realnem času (ang. real-time gross settlement, v nadaljevanju RTGS) se običajno uporablja med bankami. Pošiljatelj banki naroči prenos sredstev prejemniku. Banka pošiljatelja uporabi svoj neposredni dostop do sistema plačil visoke vrednosti in naroči banki prejemnika, da bremeni svoj račun pri centralni banki in prejemniku odobri plačilo. Pomembna lastnost teh sistemov je, da je centralna banka porok za obe banki. Ta element sistemov RTGS znatno prispeva k stroškom in predstavlja veliko razliko med konvencionalnimi plačili. Sistem RTGS je boljši v zmanjšanju poravnalnega tveganja v primerjavi s sistemom neto poravnave. Tveganje poravnave je tveganje, da bo imel udeleženec plačilnega sistema težave z likvidnostjo in/ali izgubo, ker druga stranka ni izvedla plačil, kot je bilo pričakovano. Tipično so sistemi za prenose večjih vrednosti manj razširljivi od sistemov za prenose manjših vrednosti, saj delujejo v realnem času na bruto osnovi preko lokalnih centralnih bank. V tabeli 1 je prikazana primerjava treh sistemov za prenose visokih vrednosti glede na transakcijske provizije, čas ter volumen in vrednost transakcij.

Tabela 1: Primerjava sistemov za plačila večjih vrednosti

	Transakcijska provizija	**Transakcijski čas**	**Število transakcij na dan 2018**	**Število transakcij na leto 2018**	**Vrednost transakcij 2018**
TARGET2	0,8 – 0,125 EUR	< 1 minuta	346.008	88 milijonov	433 trilijonov EUR
EURO1	0,32 – 0,04 EUR	1 sek. – 30 min	198.054	50 milijonov	49 trilijonov EUR
Fedwire	0,82 – 0,03 USD	1 sek. – 1 dan	631.198	158 milijonov	716 trilijonov USD

Vir: European Central Bank (2018a); Federal Reserve Banks (brez datuma); EBA Clearing (2018).

1.1.1.1 TARGET2

Sistem TARGET2 je sistem bruto poravnave v realnem času, ki ga Eurosistem upravlja z denarjem centralne banke (European Central Bank, 2018b, str. 6). Ker račun prejemne institucije nikoli ni knjižen v dobro, preden je račun institucije, ki pošilja, obremenjen, je

institucija prejemnica vedno prepričana, da so prejeta sredstva brezpogojna in nepreklicna. Institucija prejemnica torej zaradi takih plačil ni izpostavljena kreditnemu ali likvidnostnemu tveganju. Cenovna shema za storitev TARGET2 ponuja dve možnosti za zaračunavanje provizij za obdelavo transakcij (European Central Bank, 2018a, str. 4–5):

- **možnost A:** mesečna naročnina v višini 150 EUR in fiksna provizija za transakcijo v višini 0,80 EUR na transakcijo;
- **možnost B**: mesečna provizija v višini 1,875 EUR in provizije za transakcije na podlagi obsega v razponu od 0,60 EUR do 0,125 EUR na transakcijo.

Leta 2018 je bilo 100 % plačil, poravnanih na plačilnem modulu sistema TARGET2, obdelanih v manj kot petih minutah (European Central Bank, 2018b, str. 39). Delež TARGET2 v celotnem prometnem sistemu velikega plačilnega prometa v evrih je 91-odstoten v vrednosti in 61-odstoten glede na obseg, povprečna vrednost transakcije na sistemu pa je približno 5 milijonov EUR.

1.1.1.2 Fedwire

Fedwire je sistem za prenos bruto sredstev v realnem času, ki finančnim institucijam omogoča elektronsko prenašanje sredstev, upravljajo pa ga ameriške centralne banke (Federal Reserve Banks, brez datuma). Prenose lahko sproži le pošiljateljeva banka, ko prejme ustrezno bančno navodilo. Ko so navodila prejeta in obdelana, centralna banka bremeni sredstva na rezervnem računu pošiljateljeve banke in kreditira račun banke prejemnice. Elektronski prenosi, poslani preko sistema Fedwire, so običajno zaključeni v istem dnevu, nekateri pa tudi takoj. Za vsako transakcijo se bankam zaračuna bruto transferna provizija v višini 0,82 USD, vendar je na voljo tristopenjski diskontni razpored, ki povzroči dejanske transakcijske stroške, ti pa stanejo 0,034–0,82 USD na transakcijo, odvisno od obsega transakcij (Federal Reserve Bank, 2019). Povprečna vrednost transakcije na sistemu Fedwire je približno 4,5 milijona EUR.

1.1.2 Sistemi neto poravnave

V sistemu neto poravnave z odloženim časom se neto pozicija vsake sodelujoče finančne institucije izračuna kot vsota vseh prenosov, ki jih je udeleženec prejel do določenega trenutka, minus vrednost vseh poslanih prenosov (Nakajima, 2017, str. 2). Glavna prednost je zmanjšanje zahtev za takojšnjo likvidnost za izpolnitev plačilnih obveznosti. Če medsebojna poravnava poteka med dvema udeležencema neposredno, se imenuje dvostranski sistem neto poravnave. Kadar poravnava poteka preko klirinške hiše ob odloženem času, se imenuje večstranski neto poravnalni sistem. V dvostranskem sistemu neto poravnave se izračuna končni znesek, ki ga vsak uporabnik dolguje drugemu. Večstranski sistem neto poravnave članom omogoča, da svoje plačilne obveznosti poravnajo preko centralne klirinške hiše.

Sistem EURO1 je sistem neto poravnave v evrih, ki je v lasti zasebnih bank (EBA Clearing, 2018). Je drugi največji plačilni sistem velike vrednosti, ki deluje v evrih. Sistem na koncu dneva poravna končna stanja svojih udeležencev preko sistema TARGET2. EURO1 obdeluje kreditne in debetne prenose. 95 % transakcij EURO1 se poravna v realnem času in več kot 99 % v 30 minutah (EBA Clearing, brez datuma). EURO1 je edinstven sistem neto poravnave in je ekvivalenten sistemom RTGS. Enkratno nadomestilo v višini 30.000 EUR se plača ob priključitvi na sistem. Provizije za transakcije se izračunajo na podlagi števila transakcij v razponu 0,32 EUR do 0,04 EUR.

1.2 Plačilni sistemi manjših vrednosti

Sistem plačil majhnih vrednosti se uporablja za obdelavo transakcij, ki niso nujne, nizkih vrednosti in se običajno izvaja v velikih količinah (Tompkins & Olivares, 2016, str. 9). Trg potrošniških plačil v evrih je veliko manj integriran kot segment plačil velikih vrednosti. Potrošniška plačila tipično temeljijo na nacionalnih plačilnih instrumentih in sistemih.

1.2.1 Plačilne kartice

Plačilne kartice so del plačilnega sistema in jih svojim strankam izdajo finančne institucije, ki lastnikom kartic omogočajo dostop do sredstev na bančnih računih ali do kreditnih računov, plačevanje preko elektronskih prenosov sredstev in dostop do bankomatov (European Central Bank, 2014, str. 5). V tabeli 2 je prikazana primerjava dveh največjih kartičnih sistemov glede na transakcijske provizije, čas ter volumen in vrednost transakcij.

Tabela 2: Primerjava plačilnih kartic

	Provizija (%)	**Transakcijski čas**	**Teoretično število transakcij na sekundo**	**Dejansko število transakcij na sekundo**	**Število transakcij na leto 2018**	**Vrednost transakcij na leto 2018 v USD**
VISA	0,2 – 1,75	< 1 sekunda	24.000	3.941	124 milijard	10.2 trilijona
Mastercard	0,2 – 2,2	< 1 sekunda	44.000	2.486	78 milijard	5.9 trilijona

Vir: VISA (2018); Mastercard (2018).

Kreditna kartica se izda za kreditno linijo, ki jo zagotavlja finančna institucija, debetna kartica pa se izda na depozitni račun, ki ga ima odprtega podjetje ali potrošnik. Kartična plačila vključujejo številne subjekte (European Central Bank, 2014, str. 21). Najpomembnejši so lastnik kartice in prejemnik plačila. Imetnik kartice pridobi kartico od izdajatelja[1] kartice, ki je pogosto banka, prejemnik plačila pa sklene pogodbo s prevzemnikom[2] kartic. Kartične sheme običajno uporabljajo tako imenovane provizije za

[1] Ponudnik plačilnih storitev, ki je član kartične sheme in vstopi v pogodbeno razmerje z imetnikom kartice.
[2] Ponudnik plačilnih storitev, ki vstopi v pogodbeno razmerje s prejemnikom plačila in izdajateljem kartice preko sheme plačil za namene sprejemanja in obdelave kartičnih transakcij.

izmenjavo (ang. interchange fee). Provizija se zaračuna za prenos sredstev z ene strani trga na drugo (običajno od prevzemnika na izdajatelja kartice) vsakič, ko se opravi plačilo s kartico. Običajno je večstranska in jo v osnovi omeji regulatorni organ za vse izdajatelje in prevzemnike kartic. Marca 2015 je Evropski parlament izglasoval omejitev provizij za izmenjavo na 0,3 % za kreditne kartice in 0,2 % za debetne kartice (European Commission, 2016). Poleg medbančnih provizij se v kartični shemi običajno uporablja več dodatnih provizij. Prevzemnik kartice zaračuna prejemniku plačila nadomestila za vse storitve, ki jih je ponudil, in za povračilo medbančne provizije, ki jo je treba plačati izdajatelju kartice (ang. merchant service charge). Izdajatelji kartic lahko zaračunajo provizije za imetnike kartic (ang. cardholder fees), na primer pristojbine za izdajo kartice, periodične pristojbine, pristojbine na transakcijo ter pristojbine za izpisek računa in informacije za obračun. Za uporabo plačilnih kartic je ključnega pomena sposobnost obdelave velikega števila transakcij v izjemno hitrem času. Kot referenčna točka hitrosti kartičnih shem se ponavadi uporablja število transakcij na sekundo, ki jih lahko obdela največji ponudnik plačilnih kartic VISA. Ta na dan obdela povprečno 350 milijonov transakcij ali približno 3.900 transakcij na sekundo, z najvišjo dnevno stopnjo 4.000 transakcij na sekundo (VISA, 2018, str. 3). Hkrati ima najvišjo teoretično zmogljivost okoli 24.000 transakcij na sekundo, vendar nikoli dejansko ne doseže več kot približno tretjino teoretične zmogljivosti, celo v času največjih nakupovalnih obdobij. Mastercard na dan obdela okoli 220 milijonov transakcij, z največjo teoretično zmogljivostjo okoli 44.000 transakcij na sekundo (Mastercard, 2018, str. 21). Visa in Mastercard vzdržujeta 99,9-odstotno razpoložljivost v omrežju, s povprečnim odzivnim časom okoli 150 milisekund..

1.2.2 Avtomatizirane klirinške hiše

Plačilna mreža avtomatiziranih klirinških hiš je poleg plačil s karticami še en sistem plačil manjših vrednosti, ki omogoča prenos sredstev neposredno med lokalnimi bankami. Avtomatizirane klirinške hiše (ang. automated clearing house, v nadaljevanju ACH) so centralizirani sistemi za plačila manjših vrednosti, ki se uporabljajo za izračun dvostranskih ali večstranskih pozicij udeležencev (Tompkins & Olivares, 2016, str. 13). Plačilna omrežja ACH so zasnovana samo za paketno obdelavo in so načeloma cenejša od kartičnih omrežij. So sistemi neto poravnave, zato je poravnava lahko odložena in obstaja likvidnostno tveganje. ACH so poleg plačilnih kartic najbolj prevladujoča oblika plačilnega sistema za plačila manjših vrednosti, saj večina držav uporablja vsaj en sistem kot del svojih osrednjih plačilnih sistemov. Vendar ACH tako kot sistemi za plačila večjih vrednosti delujejo le v delovnih dneh, in ker obdelujejo transakcije v serijah, lahko izvedba transakcij traja več dni, zlasti čez vikende in državne praznike. V tabeli 3 je prikazana primerjava dveh največjih avtomatiziranih klirinških hiš v EU in ZDA in funkcij, ki delujejo v njunem okviru, glede na transakcijske provizije, čas ter volumen in vrednost transakcij.

Tabela 3: Primerjava avtomatiziranih klirinških hiš

	Transakcijska provizija	Transakcijski čas	Število transakcij na dan 2018	Število transakcij na leto 2018	Vrednost transakcij na leto 2018
STEP2 SCT	0,001–0,002 EUR	1 delovni dan	18.2 milijona	4.43 milijarde	12 trilijonov EUR
STEP2 SDD Core	0,001–0,002 EUR	1 delovni dan	25.4 milijona	6.57 milijarde	1,2 trilijona EUR
STEP2 B2B SDD	0,001–0,002 EUR	1 delovni dan	324.765	85.21 milijona	723 milijard EUR
RT1 (SCT Inst)	/	3 sekunde	116.822	635 milijonov	6 milijard EUR
ACH Network	0,00185 USD	1–2 delovna dneva	100 milijonov	23 milijard	51.2 trilijona USD

Vir: EBA Clearing (2018); NACHA (2019).

1.2.2.1 STEP2

STEP2 je vseevropska avtomatizirana klirinška hiša (ang. pan-European automated clearing house), ki jo upravlja podjetje EBA Clearing (EBA Clearing, 2018, str. 4). STEP2 od ustanovitve enotnega območja plačil v evrih (ang. Single euro payments area, v nadaljevanju SEPA) leta 2008 ponuja storitve obdelave kreditnih plačil v vseh državah EU. SEPA je iniciativa Evropske unije za plačilno integracijo in poenostavitev bančnih transferjev v evrih. V okviru sheme SEPA nudi sistem STEP2 naslednje storitve:

- **Kreditni prenos SEPA (ang. credit transfer) oz. SCT**: Omogoča prenos sredstev z enega bančnega računa na drugega. Pravila obračunavanja SEPA zahtevajo, da se plačila, opravljena pred obračunskih časom na delovni dan, knjižijo na račun prejemnika v enem delovnem dnevu.
- **Direktna bremenitev SEPA (ang. direct debit) oz. SDD**: Osnovna shema Core SDD se je začela izvajati 2. novembra 2009 in je namenjena predvsem potrošnikom, shema B2B SDD pa je namenjena poslovnim uporabnikom.

Poleg storitev v okviru STEP2 upravlja EBA Clearing tudi sistem RT1, ki omogoča takojšna kreditna plačila (EBA Clearing, 2018, str. 6). Takojšnje kreditno plačilo SEPA (ang. instant credit transfer) oz. SCT Inst. zagotavlja takojšen prenos sredstev do prejemnikovih plačil in lahko transakcije z majhno vrednostjo v evrih (do 15.000 EUR), trenutno pa je na voljo v 16 državah v EU.

1.2.2.2 ACH Network

ACH Network je elektronski sistem za prenos sredstev, ki ga upravlja Nacionalna zveza avtomatiziranih klirinških hiš (ang. National Automated Clearing House Association, v nadaljevanju NACHA) od leta 1974 (NACHA, 2019). Ta plačilni sistem se ukvarja s procesiranjem plačilnih list, direktnimi bremenitvami, vračili davkov, potrošniškimi računi itd. v ZDA. ACH združuje finančne transakcije in jih obdeluje v določenih časovnih

presledkih ves dan. Pravila NACHA navajajo, da se povprečne debetne transakcije ACH poravnajo v enem delovnem dnevu, kreditni posli pa v enem do dveh delovnih dneh.

1.3 Mednarodni plačilni sistemi

Mednarodno plačilo je izraz, ki se nanaša na posle, ki vključujejo posameznike, družbe, banke ali poravnalne institucije, delujoče v vsaj dveh različnih državah (Association for Financial Professionals, 2015, str. 4). Prva oblika mednarodnega plačilega sistema je sistem korespondenčnega bančništva preko omrežja SWIFT, ki vključuje vse mednarodne transakcije, izvedene med dvema bankama. Druga vključuje alternativne upravitelje plačilnih sistemov, ki uporabnikom omogočajo izvajanje transakcij izven bančnih kanalov. Današnje mednarodne plačilne sisteme preplavljajo številni posredniki v več regijah, vsak s svojimi pravili, predpisi in praksami. Zaradi tega so čezmejna plačila in transakcije drage, zamudne, zapletene in omejevalne. Stroški, povezani s transakcijami manjše vrednosti, v povprečju predstavljajo približno 1% letnega bruto domačega proizvoda v evropskih državah (European Commission, 2019, str. 57). Tabela 4 prikazuje primerjavo mednarodnih transakcij v omrežju SWIFT in dveh največjih alternativnih sistemih glede na transakcijske provizije, čas ter volumen in vrednost transakcij v letu 2018.

Tabela 4: Primerjava mednarodnih plačilnih sistemov

	Transakcijska provizija	**Transakcijski čas**	**Število transakcij na dan 2018**	**Število transakcij na leto 2018**	**Vrednost transakcij na leto 2018**
Medbančne transakcije (SWIFT)	6,6 – 180 EUR	1- 2 delovni dan	28 milijonov	7.1 milijarde	/
Western Union	3,9 – 190 EUR	1 minuta – več delovnih dni	2 milijona	275.8 milijona	81 milijard USD
Paypal	0,99 – 4,99 USD	< 1 sec	24 milijonov	9.9 milijarde	578 milijard USD

Vir: SWIFT (2018); Western Union (2018); Paypal (2018); NLB (2019); Bank of America (2019).

1.3.1 Medbančne transakcije (SWIFT)

Večina mednarodnih medbančnih prenosov se izvaja preko družbe Society for Worldwide Interbank Financial Telecommunication oz. SWIFT (Investopedia, 2019c). Gre za omrežje, ki ga finančne institucije uporabljajo za varno posredovanje informacij in navodil o plačilih z uporabo standardiziranega sistema kod. Sistem SWIFT ne omogoča prenosa sredstev, ampak samo pošilja plačilne naloge, ki jih morajo banke poravnati na sistemu korespondenčnih oz. posredniških bank (Investopedia, 2019b). Korespondenčna banka je banka, ki opravlja storitve v imenu druge, enakopravne ali neenakopravne finančne institucije. Lokalne banke najpogosteje uporabljajo korespondenčne banke za opravljanje transakcij, ki izvirajo iz tujih držav ali so tam dokončane, korespondenčne banke pa v tujini nastopajo kot njihovi zastopniki. Če banki nimata sklenjenega sporazuma, mora korespondenčna banka delovati kot posrednik. Vključevanje več posrednikov ustvarja

zapleteno mrežo postopkov, ki ovirajo preglednost čezmejnih plačil od začetka do konca, kar pogosto povzroči nepravilne transakcije, ki jih je treba pozneje uskladiti. Mednarodni bančni prenosi so relativno dragi, saj so provizije povprečno 8–10 % vrednosti prenosa (World Bank Group, 2019). Poleg relativno visoke cene prenosov so ti tudi zelo počasni, sploh pri manjših zneskih, saj se ti običajno obdelajo v lokalnih sistemih plačil majhnih vrednosti. Kljub relativni počasnosti in visokim stroškom v primerjavi z nacionalnimi pa SWIFT trenutno uvaja rešitev, ki bo omogočala hitrejše pošiljanje plačilnih nalogov in bo pospešila mednarodne medbančne prenose (SWIFT, 2018). Prizadevanja SWIFT-a, da pospeši plačila, so na voljo zaradi nove pobude SWIFT Global Payments Innovation oz. Gpi. Glavni namen pobude SWIFT Gpi je zagotoviti preglednejše provizije in sledenje plačil. V okviru gpi so banke članice zdaj dolžne zagotoviti izplačila v 24 urah ali hitreje in skoraj 50 % plačil v tem sistemu se zaključi v manj kot 30 minutah.

1.3.2 Ponudniki plačilnih storitev

V korespondenčnem bančništvu se tako plačnik kot prejemnik ukvarjata neposredno s svojimi bankami (Payoneer, 2015, str. 13–15). Ponudniki plačilnih storitev zagotavljajo alternativne storitve za obravnavanje čezmejnih plačil. Te storitve vplivajo na plačilno transakcijo za eno končno stranko ali tudi obe preko lastnih sistemov in omrežij. Ponudniki plačilnih storitev poravnajo transakcije, izvedene v njihovih omrežjih, s korespondenčnimi bankami na neto osnovi.

Najbolj razširjeni ponudniki plačilnih storitev so operaterji prenosa denarja (ang. money transfer operators) in ponudniki e-denarnic. Operaterji prenosa denarja so večja mednarodna podjetja, kot je Western Union, ki omogočajo storitev mednarodnih transakcij preko lastnih omrežij in sistemov. Vanje so vključene svetovna mreža agentov, bankomatov in elektronskih kanalov ter številne manjše ustanove, ki so specializirane za pošiljanje sredstev preko določenih migracijskih koridorjev (Payoneer, 2015, str. 15). Prednost uporabe teh plačilnih sistemov je predvsem v omogočanju izvajanja mednarodnih transakcij ljudem brez bančnih računov. Zaradi tega je uporaba teh sistemov priljubljena v državah v razvoju. E-denarnica je digitalno orodje (programska oprema ali aplikacija), ki potrošnikom omogoča shranjevanje načinov plačevanja. V njem so shranjeni podatki debetnih in kreditnih kartic in drugih načinov plačila.

E-denarnica omogoča posamezniku, da opravi elektronske transakcije z izboljšano izkušnjo plačila v primerjavi z vnosom vseh plačilnih poverilnic vsakič, ko se opravi nakup (Payoneer, 2015, str. 17). Denarnice lahko delujejo v spletnih in fizičnih trgovinah. Ponudniki e-denarnic so PayPal, Alipay, WeChat Pay, Apple Pay, Samsung Pay, Android Pay, Masterpass, Paylib, Amazon Pay, SEQR itd.

2 ANALIZA TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV

2.1 Zgodovina tehnologije

Koncept decentraliziranih digitalnih valut in drugih alternativnih možnosti, kot so digitalni nepremičninski registri, je prisoten že desetletja. Anonimni e-cash protokoli iz devetdesetih let prejšnjega stoletja, ki so temeljili na kriptografskem konceptu, znanem kot slepi podpis (ang. blind signature), so zagotovili valuto z visoko stopnjo zasebnosti, vendar pa večinoma niso zmogli pridobiti popularnosti zaradi svoje odvisnosti od centraliziranega posrednika (Chaum, 1983, str. 199–203). Struktura, ki je bila podobna današnji obliki tehnologije veriženja podatkovnih blokov, je bila prvič omenjena v raziskovalnem delu z naslovom *How to Time-Stamp a Digital Document* (Haber & Stornetta, 1991, str. 99–111). V članku je opisana tehnologija pošiljanja dokumenta na strežnik za časovni žig. Strežnik naj bi ta dokument podpisal s trenutnim časovnim žigom, poleg tega pa naj bi ga povezal s prejšnjim dokumentom z zapisom, ki se imenuje pokazatelj. Pokazatelji kažejo na lastnosti dokumenta in ne na lokacijo. Avtorja sta pri tem izpostavila dve ključni lastnosti za delovanje tehnologije. Prva je vzpostavitev avtomatskega sistema za časovno žigosanje ne glede na obliko dokumenta, kar bi preprečilo vsako spremembo dokumenta, ne da bi bila ta sprememba očitna. Druga lastnost je vzpostavitev sistema, ki onemogoča časovno žigosanje dokumenta s časom in datumom, ki je drugačen od dejanskega. Naslednja stopnja v razvoju je bil sistem dokaz o delu (ang. proof of work), ki sta ga predstavila Cynthia Dwork in Moni Naor v svojem delu *Pricing via Processing or Combatting Junk Mail* (Dwork & Naor, 1993, str. 139–147). Sistem opisujeta kot ukrep za preprečevanje napak pri storitvah in drugih zlorab, kot je vsiljiva vsebina v omrežju, tako da od naročnika storitve zahteva nekaj dela. Nadgradnjo sistema je sistemom Hashcash predlagal Adam Black (1997). Hashcash je algoritem za doseganje soglasja na podlagi dokaza o delu, ki zahteva specifično količino dokazila. Dokazilo je treba izračunati, vendar ga je mogoče učinkovito preveriti. Za uporabo e-pošte se v glavi sporočila dodaja tekstovno kodiranje žiga, ki dokazuje, da je pošiljatelj za izračun žiga pred pošiljanjem e-pošte porabil skromno količino računalniške procesorske moči. Z drugimi besedami: ker si je pošiljatelj vzel določen čas za ustvarjanje žiga in pošiljanje e-pošte, je malo verjetno, da pošilja nezaželeno pošto. Leta 1998 je kitajski računalniški inženir Wei Dai s svojim konceptom *b-money* predstavil idejo o ustvarjanju denarja z reševanjem računalniških ugank in decentralizirano komponento, vendar koncept ni bil dovolj dodelan in podroben in ideja kljub poskusom uporabe ni zaživela (Dai, 1998). Velik napredek v razvoju pomeni leta 2005. Tedaj je Nick Szabo po večletnem teoretiziranju predstavil teoretično podlago za protokol, s katerim bi na spletu lahko ustvarili unikatne digitalne delce (ki jih ni mogoče podvojiti) z minimalno odvisnostjo od zaupanja vrednih tretjih oseb in jih nato varno shranili (Szabo, 2005). Szabo je te digitalne delce poimenoval

bitgold oz. digitalno zlato. Predlog za BitGold temelji na izračunu niza bitov[3] iz niza izzivnih bitov (ang. challenge bits) z uporabo funkcije, ki se imenuje funkcija dokaza o delu (ang. proof of work function). Hal Finney, računalniški znanstvenik iz ZDA, je dodatno nadgradil sistem dokaza o delu in razvil tako imenovani sistem dokaza o delu za večkratno uporabo (ang. reusable proof of work, v nadaljevanju RpoW) za večkratno uporabo žetonov (Finney, 2004). Temeljni razlog za Finneyjevo delo je bila uporaba sistema RpoW kot žetonskega (ang. token) denarja, ki je temeljil na logiki vrednosti zlatih kovancev. Tako kot njihova vrednost temelji na vrednosti surovega zlata, potrebnega za izdelavo kovancev, vrednost žetona RpoW izhaja iz vrednosti virov, potrebnih za izdelavo teh digitalnih žetonov.

Vinay Gupta (2017) v članku za Harvard Business Review kot najpomembnejši korak izpostavlja razvoj tako imenovanega »eksperimenta digitalnih valut«, bolj znanega pod imenom bitcoin. Oseba ali skupina oseb pod psevdonimom Satoshi Nakamoto (Nakamoto, 2009b) je leta 2008 bitcoin definirala kot digitalno, decentralizirano, delno anonimno valuto, ki je ne podpira nobena svetovna vlada ali katera koli druga pravna entiteta in je ni mogoče zamenjati za zlato ali druge dobrine. Zanaša se na vrstniško (ang. peer-to-peer) omrežje in kriptografijo za ohranjanje integritete. Domena bitcoin.org je bila registrirana 18. avgusta 2008, oktobra istega leta pa je bil objavljen članek *Bitcoin: A Peer-to-Peer Electronic Cash System*. Drugi večji korak v predstavlja inovacija tehnologije veriženja podatkovnih blokov oz. ločitev te tehnologije od kripto valute bitcoin. To bi lahko opredelili tudi kot spoznanje, da je tehnologijo veriženja podatkovnih blokov možno uporabiti na številnih drugih področjih, ne le na primeru kripto valut.

2.2 Analiza veriženja podatkovnih blokov

Leta 2008 je Satoshi Nakamoto predlagal nov pristop digitalnega prenosa sredstev na porazdeljen vrstniški (ang. peer-to-peer) način s pomočjo valute, imenovane bitcoin (Nakamoto, 2009b). Osnovna tehnologija za bitcoin je bila imenovana veriženje podatkovnih blokov (ang. blockchain) in se nanaša na specifičen način organiziranja in shranjevanja informacij in transakcij (Natarajan, Krause & Gradstein, 2017, str. 4). Pozneje so bili razviti drugi načini za organiziranje informacij in transakcij za prenos sredstev v vrstniškem načinu, kar je vodilo do izraza tehnologija porazdeljenih podatkovnih baz (ang. distributed ledger technology), ki se nanaša na širšo kategorijo tehnologij.

2.2.1 Tehnologija porazdeljenih podatkovnih baz

Tehnološki izziv v digitalni izmenjavi sredstev na peer-to-peer osnovi je tako imenovani problem dvojne porabe, saj se lahko vsaka digitalna oblika sredstev in denarja zlahka podvoji

[3] En bit je tipično definiran kot informacijska entropija binarne naključne spremenljivke, ki je 0 ali 1 z enako verjetnostjo.

in goljufivo porabi več kot enkrat (Singhal, Dhameja & Panda, 2018, str. 4). Pri digitalnem denarju zahteva reševanje problema dvojne porabe vsaj to, da nekdo vodi evidenco o vseh transakcijah. Pred uvedbo porazdeljenih podatkovnih baz (ang. distributed ledger technology) je bila edina rešitev, da je to storil centralni subjekt, ki je preveril vse transakcije. Porazdeljenost podatkovnih baz pa se nanaša na pristop k beleženju in izmenjavi podatkov v več podatkovnih bazah (ang. ledger), ki imajo enak zapis podatkov in se skupaj vzdržujejo in nadzirajo preko porazdeljenega omrežja uporabnikov oz. računalniških strežnikov, ki se imenujejo vozlišča (ang. node). To je baza podvojenih, skupnih in sinhroniziranih digitalnih podatkov, ki so geografsko razdeljeni na več mest v omrežju (Natarajan, Krause & Gradstein, 2017 str. 4). Vsak uporabnik omrežja shrani najnovejšo kopijo celotne podatkovne baze, s tem pa je izmenjava digitalnih denarnih sredstev izvedljiva, saj lahko vsak uporabnik v svoji kopiji neposredno preveri, ali je prišlo do prenosa oz. ni bilo nobenega poskusa dvojnega zapravljanja.

Razlikujemo med dvema razredoma porazdeljenih podatkovnih baz, ki se bistveno razlikujeta v operativni postavitvi (Singhal, Dhameja & Panda, 2018, str. 7). En razred temelji na porazdeljenih podatkovnih bazah s potrebo po dovoljenju (ang. permissioned). Tovrstni sistemi so podobni konvencionalnim plačilnim mehanizmom, saj lahko za preprečitev zlorab podatkovno bazo posodobijo le zaupanja vredni udeleženci. Ta vozlišča izbere osrednji organ, ki deluje kot lastnik ali administrator, na primer podjetje, ki je omrežje razvilo in ga tudi nadzoruje. Ti sistemi se od konvencionalnih razlikujejo v smislu shranjevanja evidenc o transakcijah, skupna pa jim je odvisnost od določenih institucij kot končnega vira zaupanja. Možna je identifikaciji uporabnikov in dodelitev pravnega lastništva omrežja. Istočasno pa ta funkcija znatno zmanjša eno glavnih prednosti tehnologije veriženja podatkovnih blokov, to je namreč sposobnost eliminacije potrebe po zaupanju in delovanje brez centralne entitete. Kljub temu tudi v omrežjih z dovoljenji načeloma ni potrebe po aktivnem delovanju administratorja za izvajanje transakcij.

Drugi razred porazdeljenih podatkovnih baz je povsem decentraliziran in deluje brez potrebe po dovoljenju (ang. permissionless) (Bank for International Settlements, 2018). Sodeluje lahko kdor koli, nihče nima posebnega dovoljenja za vnos transakcij v podatkovno bazo. V odprtih sistemih ni potrebe po zaupanju med uporabniki, ker sistem uporablja kompleksne algoritme za doseganje soglasja o stanju podatkovnih baz, pri katerih uporabniki porabljajo lastne viri z reševanjem matematičnih ugank ali pa zastavijo lastna sredstva, da bi lahko podatke o transakcijah dodali na porazdeljene podatkovne baze. Ti algoritmi aktivno spodbujajo uporabnike k poštenemu vedenju, kar eliminira potrebo po zaupanju med posameznimi uporabniki. Omrežja Bitcoin in Ethereum sta najbolj znana primera popolnoma odprtih sistemov, ki se jim lahko uporabniki po želji pridružijo in jih zapustijo, brez potrebe po odobritvi centralne entitete. Vse kar uporabnik potrebuje za pridružitev omrežju, je pravilna programska oprema, nato pa si lahko prenese svojo različico podatkovne baze in začne opravljati transakcije v omrežju.

2.2.2 Veriženje podatkovnih blokov

Koncept veriženja podatkovnih blokov oz. podatkovnih verig je bil razvit za omrežje Bitcoin, ko je Nakamoto predlagal valuto na podlagi posebne vrste porazdeljene podatkovne baze, imenovane podatkovna veriga. Podatkovna veriga je posebna vrsta tehnologije porazdeljenih podatkovnih baz, ki uporablja kriptografske in algoritemske metode za ustvarjanje in preverjanje nenehno naraščajoče podatkovne strukture v obliki verige podatkovnih blokov, ki vsebujejo specifične podatke (Natarajan, Krause & Gradstein, 2017, str. 7). Javno dostopna porazdeljena podatkovna baza se posodablja v obliki paketov transakcij, ki se imenujejo bloki (Bashir, 2018, str. 21). Bloki se nato zaporedoma vežejo med seboj in tako tvorijo podatkovne verige. Vsak blok je majhna datoteka, ki vsebuje podatke o več transakcijah, v njih pa so navedeni znesek, plačnik in prejemnik plačila ter provizija za transakcijo. Prvotni protokol Bitcoin je omejil vsak blok na največjo velikost datoteke 1 MB, kar v praksi pomeni, da je v vsak blok mogoče vključiti približno 2.000 transakcij (Nakamoto, 2009b). V blok se sprejemajo samo transakcije z veljavnim digitalnim podpisom, ki je povezan s prenesenimi sredstvi. V omrežju Bitcoin se nov blok doda blokovni verigi le enkrat vsakih 10 minut, pri drugih omrežjih pa je ta čas odvisen od pravil, ki so jih opredelili razvijalci. Dodajanje bloka v obstoječo verigo zahteva veljavno dokazilo o delu, veljavno dokazilo o deležu ali drugo vrsto dokazila, odvisnega od algoritma za soglasje, ki se uporablja v omrežju. Za izvajanje transakcij na teh omrežjih se tipično uporabljajo za omrežje specifične valute.

Omrežja, ki temeljijo na konceptu porazdeljenih podatkovnih baz oz. podatkovnih verig, imajo dve skupini udeležencev (Norton, 2017, str. 18). Prvi se imenujejo rudarji in delujejo kot knjigovodje, drugi pa so uporabniki, ki želijo v tem omrežju opravljati transakcije. Nove dodatke k bazi podatkov sproži rudar, ki ustvari nov podatkovni blok. Podatki o novem bloku se nato delijo po celotnem omrežju in vsebujejo šifrirane podatke o transakciji in vsi udeleženci skupaj določijo veljavnost bloka v skladu z vnaprej določeno metodo algoritemskega doseganja soglasja. Šele po potrditvi vsi udeleženci dodajo novi blok v svoja podatkovna skladišča. S tem mehanizmom se vsaka sprememba na podatkovni bazi posnema po celotnem omrežju, vsak član mreže pa ima polno in identično kopijo celotne podatkovne baze v vsakem trenutku.

Ta pristop se lahko uporablja za beleženje transakcij z vsemi sredstvi, ki jih je mogoče predstaviti v digitalni obliki. Kljub temu da so vsa vozlišča enaka, lahko prevzamejo različne vloge (rudarji, polna vozlišča, itd.). Pri polnem vozlišču (ang. full node) se celotna veriga kopira na eno samo napravo, ki je povezana z omrežjem. To pomeni, da shranjenih informacij ni mogoče izgubiti ali uničiti, ker bi to pomenilo, da bi morali uničiti vsako polno vozlišče v omrežju. Temeljna lastnost tehnologije je zagotavljanje popolnoma zaupanja vredne storitve med uporabniki, ki si med seboj ne zaupajo popolnoma (Cachin & Vukolic, 2017, str. 2). S tem ko se odločanje porazdeli po celotnem omrežju in ne na eni centralni entiteti, lahko dosežemo izjemno visoko raven zaupanja v samo omrežje.

2.2.3 Transakcije na podatkovni verigi

Zamisel, na kateri temeljijo ta omrežja, je, da namesto banke, ki centralno beleži transakcije, knjigo posodablja rudar in posodobitev nato shranijo vsi uporabnik. Transakcije na podatkovnih verigah običajno potekajo na naslednji način (Singhal, Dhameja & Panda, 2018, str. 127):

1. Programska oprema plačnika se posvetuje z omrežjem oz. podatkovno verigo, da pridobi podatke o preteklih transakcijah in dejanskem stanju sredstev plačnika. Plačnik oz. njegov anonimni kriptografski digitalni podpis nato javno objavi plačilno transakcijo, tudi prejemnika plačila, plačani znesek in transakcijsko provizijo, ki jo je plačnik pripravljen plačati rudarju.
2. Rudarji izberejo nepredelane transakcije, prihodki od njih pa se bodo maksimirali zaradi provizij in jih vključijo v računalniške izračune, dokler prvi rudar ne najde veljavnega dokazila o delu. Če podatkovna veriga uporablja drugačen algoritem za doseganje soglasja, kot je dokazilu o deležu, rudarjem ni treba opraviti računalniških izračunov.
3. Uspešno dokazilo omogoča, da rudar doda blok transakcij podatkovni verigi in nato pobere provizije za vključene transakcije in nagrado za dodani blok.
4. Vsak računalnik v omrežju preveri transakcijo v skladu z pravili za potrjevanje, ki jih postavijo ustvarjalci določenega omrežja.. Potrjene transakcije so shranjene v blok in so zapečatene z zgoščevalno funkcijo.Če se bo novi blok pojavil kot pravilna in sprejeta različica, ga bo večina rudarjev še naprej dopolnjevala z novimi bloki.

Singhal, Dhameja in Panda (2018, str. 129) kot ključno dejstvo izpostavljajo, da mora biti vsak lastnik zmožen porabiti svoja sredstva, vendar le enkrat. Kriptografski digitalni podpisi se uporabljajo za preverjanje plačilnih transakcij (na primer A plača 1 B-ju), saj dokazujejo, da je plačilo odobril tisti, ki nadzira porabljeno sredstvo. Kljub temu ostaja problem dvojne porabe, ki bi se lahko pojavila, če bi na primer A hkrati oddajal plačilna navodila B-ju in hkrati C-ju za isto sredstvo. Ker A uporablja pravilen digitalni podpis za podpisovanje obeh plačilnih sporočil, sta obe veljavni. Del rešitve je, da prejemniki preverijo javno podatkovno verigo in ugotovijo, ali so njihove nasprotne stranke dejansko lastnice zneska sredstev, za katerega (tj. znesek) trdijo, da ga (tj. znesek) prenašajo.

Drugi ključni aspekt je algoritem za doseganje soglasja, ki rudarje spodbuja, naj dodajo le pravilne posodobitve podatkovne verige. Tveganje je, da bi slabonamerni uporabniki večkrat porabili sredstva in hkrati razširili lažne različice v upanju, da bodo prejemniki sprejeli lažne različice. Zato mora biti posodobitev verige dovolj draga, da odvrne lažne poskuse posodabljanja. Vendar če je posodobitev draga, mora obstajati tudi nagrada za spodbujanje resničnih posodobitev. Protokol bitcoin rešuje to z rudarji, ki posodabljajo podatkovno verigo in v zameno prejemajo nagrade in transakcijske provizije, ko dodajo pakete veljavnih transakcij bloku.

2.3 Vrste porazdeljenih podatkovnih baz

Čeprav imata tehnologija porazdeljenih podatkovnih baz in veriženje podatkovnih blokov enako konceptualno poreklo in namen, da ustvarita porazdeljeno bazo podatkov, nista povsem enaki. Vsak od teh konceptov zahteva porazdeljenost in soglasje med vozlišči. Toda tehnologija veriženja podatkovnih blokov organizira podatke v blokih in posodablja vnose s strukturo, ki vsebuje samo nov dodatek. Raziskovalci Svetovne banke (Natarajan, Krause & Gradstein, 2017, str. 11) menijo, da v praksi ne gre za binarno kategorizacijo, ampak za stopnjo odprtosti in decentralizacije sistemov. Sisteme, kot so Bitcoin, je mogoče uvrsti na en spekter s popolnoma odprtim javnim sistemom. Na drugi strani spektra so privatna omrežja s potrebo po dovoljenju za njihovo uporabo. V tabeli 5 je prikazana primerjava ključnih lastnosti sistemov brez dovoljenja, kot sta Bitcoin in Ethereum, ki tipično temeljijo na veriženju podatkovnih blokov, in sistemih z dovoljenjem, kot so Libra, Corda in IBM Worldwide.

Tabela 5: Primerjava vrst sistemov

	Sistemi brez dovoljenja (podatkovne verige)	**Sistemi z dovoljenjem (porazdeljene podatkovne baze)**
Centralna entiteta	Brez potrebe po lastniku oz. administratorju	Centralna entiteta ima določeno stopnjo nadzora
Dostop	Prost za vse	Pridružijo se lahko le izbrani uporabniki
Stopnja zaupanja	Brez potrebe po zaupanju med posameznimi uporabniki	Visoka stopnja potrebe po zaupanju med uporabniki
Odprtost	Podatkovna baza je odprta in transparentna, se deli med vse uporabnike	Različne stopnje odprtosti in transparentnosti
Varnost	Se dosega z distribucijo med vse uporabnike in večjim obsegom omrežja	Se dosega z omejitvami dostopa in manjšim obsegom omrežja
Identiteta	Uporabniki so anonimni oz. uporabljajo psevdonime	Potreba po verifikaciji identiteta uporabnika
Hitrost	Počasna obdelava omejuje hitrost	Hitrejša obdelava
Soglasje	Dokaz o delu, eventualno dokaz o deležu	Številne oblike algoritmov, ki so manj zahtevni
Sredstva	Tipično se uporabljajo za omrežje specifične kripto valute, možna uporaba žetonov, ki predstavljajo vsako sredstvo	Vsa sredstva
Pravno lastništvo	Ni pravnega lastništva omrežja	Lastnik/administrator je pravna entiteta
Primer	Bitcoin, Ethereum	Corda(R3), IBM Worldwide, Libra

Vir: Natarajan, Krause & Gradstein (2017).

Po drugi razdelitvi se porazdeljene podatkovne baze delijo na javne, zasebne in konzorcijske (Buterin, 2017). Pri javnih sistemih lahko vsak dostopa do podatkov v podatkovni bazi, izvaja transakcije in v bazi vidi svoje transakcije. Možno je tudi, da vsakdo potrdi podatkovne bloke ali pa sodeluje v postopku odločanja. Ta vrsta sistemov je v praksi identična sistemom brez dovoljenja, saj ni enega centralnega lastnika, ampak je sistem popolnoma decentraliziran. Primer javnih sistemov sta omrežji Bitcoin in Ethereum. Sisteme s potrebo po dovoljenju lahko ločimo na konzorcijske in zasebne. V konzorcijskih sistemih je identiteta udeležencev znana, proces soglasja pa nadzorovan s predhodno izbranimi vozlišči. Konzorcijski sistemi so običajno omejeni na subjekte (ponavadi gre za različna

podjetja), ki sodelujejo v določenem poslovnem scenariju ali delu tega scenarija. Ti sistemi tako za delovanje potrebujejo dovoljenja in se običajno štejejo za delno decentralizirane zaradi manjšega števila vozlišč v primerjavi z javnimi sistemi. Ta vozlišča imajo med seboj hierarhičen odnos, saj imajo lahko podjetja različen odnos do deljenja podatkov s širšo javnostjo. Pravice za dostop do podatkov je tako mogoče omejiti le na člane konzorcija. Ker ni potrebe po visoki stopnji varnosti kot pri javnih sistemih, pri konzorcijskih sistemih ni potrebe po uporabi algoritmov za soglasje med udeleženci, ki si med seboj ne zaupajo, ampak uporabljajo algoritme, ki temeljijo na zaupanju znanim uporabnikom. Zaradi pravnih potreb so ti sistemi primerni za uporabo na področju financ, bančništva, nepremičnin itd.

Konzorcijske sisteme je možno enačiti s sistemi s potrebo po dovoljenju, saj imajo zelo podobne lastnosti. Zasebni sistemi so zelo podobni konzorcijskim sistemom, vendar je njihov uporabnik samo ena organizacija. Zaradi tega je težko opredeliti vrednost teh sistemov, saj je v teh primerih možna uporaba navadne baze podatkov, saj si vsi uporabniki med seboj zaupajo in lahko med seboj delijo informacije.

3 TEHNIČNI VIDIKI TEHNOLOGIJE

Veriženje podatkovnih blokov ni samo tehnologija, temveč je povezano s poslovnimi funkcijami in primeri uporabe ter se prepleta z ekonomskimi načeli za doseganje soglasja med uporabniki (Singhal, Dhameja & Panda, 2018, str. 32). Tradicionalni način beleženja transakcij temelji na centraliziranem subjektu, ki ohranja samo eno zgodovino transakcij, s čimer izvaja nadzor nad celotno bazo podatkov in vnaša zaupanje v sistem. Težava s tako centraliziranim sistemom izhaja iz potrebe po zaupanju in povečanju stroškov. Tehnologija veriženja podatkovnih blokov rešuje ta vprašanja z uporabo kriptografije, algoritmov za doseganje soglasja in računalniških podatkovnih struktur. Ne glede na primer uporabe so transakcije zavarovane s kriptografijo, zato je mogoče zagotoviti, da le veljavni uporabnik sproži transakcijo in je nihče ne more ponarediti. Edini način preprečevanja dvojne porabe je, da mora vsako vozlišče vzdrževati bazo transakcij, zato je izredno pomembno, da se vsa vozlišča dogovorijo o skupnem stanju baze podatkov.

Pri večini takšnih težav je zaradi poznavanja in upoštevanja problema bizantinskih generalov opisano, kako lahko sistem ostane imun za situacije, ko eno ali več računskih vozlišč poskuša namerno podreti sistem in vnesti ponarejeno stanje baze podatkov. Področje algoritmov za soglasje z uporabo ekonomskih iniciativ ponuja pristop za določitev, kako se bo sistem obnašal in zagotavljal integriteto. Ne predvidevajo, ali je vozlišče pošteno, nezlonamerno in etično, ter predvidevajo, da udeleženci delujejo v skladu z ekonomskimi iniciativami, ne po moralnih vrednotah (Singhal, Dhameja & Panda, 2018, str. 37). Ker obstajajo različne vrste poslovnih težav in situacij z različnimi stopnjami zapletenosti, so v uporabi različni algoritmi, vendar je splošno načelo vzdrževanja dosledne baze preverjenih transakcij enako. Tehnike računalništva nato združijo kriptografijo in algoritme za soglasje v uporabno obliko,

ki omogoča decentralizirano in porazdeljeno interakcijo med vozlišči s strukturo podatkov za izgradnjo podatkovnih verig.

3.1 Porazdeljena narava podatkovnih baz

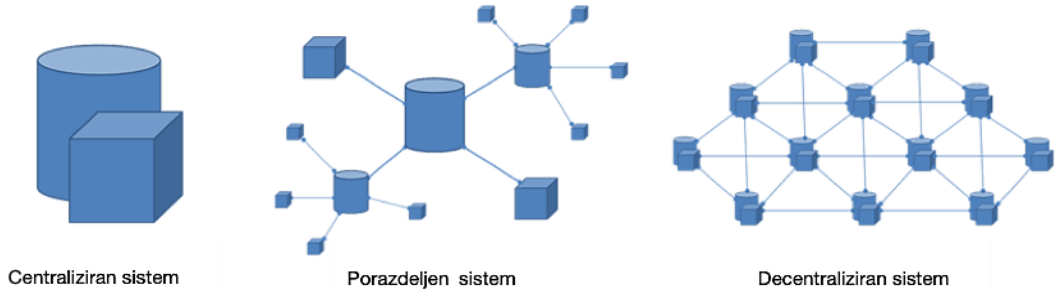
Porazdeljeni sistemi so računalniška paradigma, pri kateri dve ali več vozlišč usklajeno delujeta, da bi dosegli skupni rezultat (Bashir, 2018, str. 50). Oblikovana so tako, da jih končni uporabniki vidijo kot enotno logično platformo. Vozlišče lahko definiramo kot posameznega igralca v porazdeljenem sistemu. Vsa vozlišča so sposobna pošiljati in sprejemati sporočila med seboj in drug od drugega. Vozlišča so lahko poštena, napaka ali zlonamerna in imajo pomnilnik in procesor. Programske sisteme lahko oblikujemo na več načinov, vendar pa se ena od temeljnih odločitev nanaša na arhitekturo in način, kako so komponente organizirane in povezane (Drescher, 2017, str. 40). Tipično lahko programske sisteme razdelimo glede na stopnjo centralizacije/decentralizacije in distribucije. Centralizacija se nanašata na raven nadzora. V centraliziranem sistemu nadzor izvaja samo en subjekt, v decentraliziranem sistemu pa ni enotnega kontrolnega subjekta, saj se nadzor deli med več neodvisnimi subjekti. Pri centraliziranih programskih sistemih so komponente nameščene okrog in povezane z eno osrednjo komponento. Ko govorimo o centralizaciji programskih sistemov, obstajajo tri ločene vrste centralizacije (Buterin, 2017):

- **Arhitekturna centralizacija.** Koliko fizičnih računalnikov sestavlja sistem? Koliko teh računalnikov lahko preneha delovati v enem samem trenutku? Ta vidik decentralizacije je tisto, kar določa, kako porazdeljeno je omrežje.
- **Politična centralizacija.** Koliko posameznikov ali organizacij na koncu nadzoruje računalnike, iz katerih je sestavljen sistem? Ta vidik decentralizacije določa vidik zaupanja omrežja.
- **Logična centralizacija.** Ali so podatkovne strukture, ki jih sistem predstavlja in vzdržuje, bolj podobne enemu objektu ali so bolj ali manj enakomerno porazdeljene? Pomeni, da obstaja eno splošno dogovorjeno stanje in sistem se obnaša kot en sam računalnik.

Na sliki 1 je prikazano grafično razlikovanje med centraliziranimi, porazdeljenimi in decentraliziranimi sistemi. Porazdeljenost se namreč nanaša na razlike v lokaciji delov sistema oz. subjektov, vključenih v programske sisteme (Singhal, Dhameja & Panda, 2018, str. 12). V neporazdeljenem sistemu so vsi deli sistema na isti fizični lokaciji. V porazdeljenem sistemu obstajajo deli sistema na ločenih lokacijah. Porazdeljeni sistem je model, v katerem komponente, ki so na omrežnih računalnikih, komunicirajo in usklajujejo svoja dejanja s posredovanjem sporočil (Furbush, 2018). Na sliki 1 je porazdeljeni sistem grafično prikazan v sredini. Porazdeljeni sistem vsebuje več vozlišč, ki so fizično ločena, vendar povezana z omrežjem. Vsako vozlišče vsebuje majhen del programske opreme porazdeljenega sistema. Takšne sisteme je težko oblikovati, vzdrževati, upravljati ali uvajati zaupanje, vendar pa ne trpijo zaradi omejitev konvencionalnih centraliziranih sistemov.

Imajo več prednosti, kot so večja računalniška moč, nižji stroški, večja stopnja zanesljivosti in večja sposobnost naravno rasti. Centralizirani porazdeljeni sistem je tisti, v katerem je glavno vozlišče, ki je odgovorno za razbijanje nalog ali podatkov in distribucijo obremenitve po vozliščih (Singhal, Dhameja & Panda, 2018, str. 14). Po drugi strani pa je decentralizirani porazdeljeni sistem tisti, pri katerem ni glavnega vozlišča, vendar pa se računanje porazdeli; na sliki 1 je prikazan na desni strani.

Slika 1: Razlikovanje med različnimi vrstami sistemov



Vir: Ahsan (2018).

V praksi se vozlišča v porazdeljenih sistemih lahko razvrstijo v obliki sistemov klient/strežnik (centralizirani sistem) ali peer-to-peer sistemov (decentralizirani sistem). V sistemih klient/strežnik klient zahteva vir, strežnik pa ta vir nudi, kar pomeni, da nadzoruje omrežje. Strežnik lahko vire nudi več klientom hkrati, medtem ko je klient v stiku samo z enim strežnikom. Peer-to-peer sistemi vsebujejo vozlišča, ki so enakovredni udeleženci pri izmenjavi podatkov in vse naloge so enako razdeljene med vsa vozlišča. Sestavljeni so iz posameznih vozlišč, ki omogočajo, da so njihovi računalniški viri neposredno dostopni vsem drugim članom omrežja, ne da bi imeli osrednjo točko koordinacije (Vu, Lupu & Ooi, 2009, str. 11). Vozlišča v omrežju so enakovredna glede njihovih pravic in vlog v sistemu. Po drugih definicijah so peer-to-peer omrežja opisana preprosto kot nasprotje arhitektur klient/strežnik (Singh, 2001). To je popolnoma drugačna struktura kot pri omrežjih klient/strežnik, pri katerih deluje vozlišče izključno kot strežnik ali klient, ne more pa izvajati obeh dejavnosti. Podatkovne verige brez dovoljenja so politično decentralizirane (nihče jih ne nadzira) in arhitekturno decentralizirane (brez osrednje točke neuspeha), vendar so logično centralizirane (eno skupno dogovorjeno stanje) (Buterin, 2017). Omrežja s potrebo po dovoljenju večinoma nadzoruje en subjekt, zato lahko govorimo, da so arhitekturno decentralizirana, vendar politično centralizirana. Tako kot omrežja brez dovoljenja so tudi omrežja z dovoljenjem logično centralizirana. Ker so procesna moč in vse naloge v omrežju enakomerno porazdeljene med vozlišča v omrežju, tako pri omrežjih brez dovoljenja kot pri omrežji z dovoljenem govorimo o vrsti peer-to-peer sistemov (Bashir, 2018, str. 22). Veriženje podatkovnih blokov se lahko obravnava kot orodje za doseganje in ohranjanje integritete v porazdeljenih peer-to-peer sistemih. Ti lahko uporabljajo veriženje podatkovnih blokov, da dosežejo in ohranijo celovitost in integriteto sistema, saj je omrežje splet enakopravnih povezanih vozlišč (Singhal, Dhameja & Panda, 2018, str. 40). Ta vozlišča med

seboj komunicirajo, da potrjujejo nove transakcije in dodajo nove bloke v podatkovno verigo. Nobena centralna entiteta nima vpliva pri tem, ali je transakcija sprejeta ali se blokira. Ker se ti sistemi zanašajo na soglasje med mnogimi enakopravnimi vozlišči v omrežju, da bi spremenili verigo z novimi dodatki, so podatkovne verige sistemi peer-to-peer.

3.2 Kriptografija

Kriptografija je področje računalništva in matematike, ki se osredotoča na tehnike za varno komuniciranje (Boneh & Shoup, 2017). Definirana je kot oblika zagotavljanja varnosti s kodiranjem sporočila, tako da to postane neberljivo, in obratno. Je metoda za zaščito informacij in komunikacij z uporabo kod, tako da lahko informacije berejo in obdelujejo le tisti, na katere so naslovljene. Kriptografija pa ne omogoča samo zaščite podatkov pred krajo in spremembo podatkov. Eden ključnih aspektov kriptografije je avtentikacija uporabnikov. Koncept se nanaša na varne komunikacijske tehnike, ki izhajajo iz matematičnih konceptov in izračunov, ki jih je težko razvozlati. Boneh in Shoup (2017, str. 18) izpostavljata pet glavnih funkcij kriptografije:

- **zaupnost:** zaupni kriptografski sistemi imajo definiran niz pravil, ki omejujejo celoten ali delen dostop do določenih informacij;
- **integriteta podatkov:** pomeni skrb za natančnost in točnost podatkov v celotnem ciklu kriptografskega sistema;
- **avtentikacija:** omogoča potrjevanje resničnosti nekega atributa neke tretje entitete;
- **nepovratnost:** mehanizem za dokazovanje, da je pošiljatelj to sporočilo res poslal;
- **izmenjava ključev:** metoda, po kateri se ključi delijo med pošiljateljem in prejemnikom.

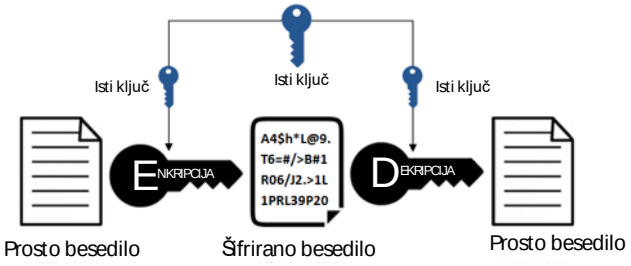
Postopki in protokoli, ki izpolnjujejo navedene kriterije, so znani kot kriptosistemi (Menezes, Oorschot & Vanstone, 2001, str. 15). Kriptosistemi uporabljajo niz protokolov, znanih kot kriptografski algoritmi za šifriranje in dešifriranje sporočil, ki omogočajo komunikacijo med računalniškimi sistemi in napravami. Šifrirni paket (ang. cipher suite) uporablja prvi algoritem za šifriranje, drugega za preverjanje pristnosti sporočil in tretjega za izmenjavo ključev. Ta proces, vgrajen v protokolih in napisan v programski opremi, ki deluje na operacijskih sistemih in omrežnih računalniških sistemih, vključuje generiranje javnih in zasebnih ključev za šifriranje/dešifriranje podatkov, digitalno podpisovanje in preverjanje pristnosti sporočil ter izmenjavo ključev.

Vse informacije v obliki besedilnega sporočila, številskih podatkov ali računalniškega programa lahko imenujemo prosto besedilo (ang. plaintext) (Singhal, Dhameja & Panda, 2018, str. 35). Ideja je šifriranje besedila z uporabo algoritma za šifriranje in ključa, ki izdela šifrirano besedilo. Šifrirano besedilo se lahko nato prenese na predvidenega prejemnika, ki ga dešifrira z algoritmom za dešifriranje in ključem, da dobi odprto besedilo. Moderna kriptografija je razdeljena na dve vrsti shem, kriptografijo s simetričnim ključem in kriptografijo z asimetričnim ključem (Menezes, Oorschot & Vanstone, 2001, str. 15).

3.2.1 Kriptografija s simetričnim ključem

Šifrirni algoritmi z enim oz. simetričnim ključem ustvarijo fiksno dolžino bitov s tajnim ključem, ki ga pošiljatelj uporablja za šifriranje podatkov, sprejemnik pa za dešifriranje podatkov. Ključni aspekt teh shem je varna zamenjava ključev pred začetkom komunikacije in nato uporaba tega istega ključa, kar je prikazano na sliki 2 (Barakat, Eder & Hanke, 2018, str. 5–11). Kriptografija s simetričnimi ključi se pogosto uporablja. Simetrični kriptosistemi so običajno hitrejši in uporabnejši, če je velikost podatkov velika.

Slika 2: Simetrične kriptografije za šifriranje besedila



Vir: ssl2buy (2019).

Simetrična kriptografija obstaja v dveh različicah, kot pretočne šifre (ang. stream cyphers) in blokovne šifre (ang. block cipers) (Menezes, Oorschot & Vanstone, 2001, str. 22). Algoritmi pretočne šifre in blokovne šifre se razlikujejo po načinu kodiranja in dekodiranja.

Pretočne šifre pretvarjajo en simbol odprtega besedila v en simbol šifriranega besedila. To pomeni, da se šifriranje izvede za en bit odprtega besedila naenkrat. Blokovne šifre temeljijo na zamisli o razdelitvi odprtega besedila v sorazmerno večje bloke skupin fiksne dolžine bitov in nadaljnje kodiranje vsakega bloka ločeno z istim ključem. Običajne velikosti vsakega bloka so 64 bitov, 128 bitov in 256 bitov.

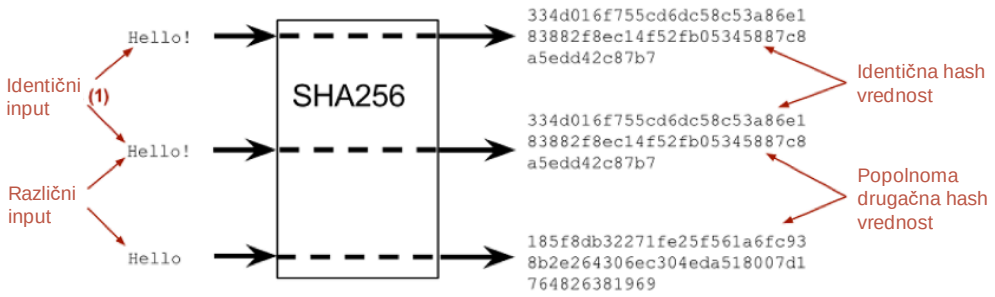
Pri simetrični ključni kriptografiji obstajajo nekatere omejitve (Singhal, Dhameja & Panda, 2018, str. 52):

- Pošiljatelj in sprejemnik si morata pred vsakim sporočilom deliti ključ. To zahteva vzpostavljen zanesljiv mehanizem ustvarjanja in izmenjave ključa.
- Pošiljatelj in sprejemnik morata zaupati drug drugemu, saj uporabljata isti simetrični ključ. Če je sprejemnik kompromitiran od napadalca ali če si je sprejemnik namerno delil ključ z nekom drugim, je sistem ogrožen.
- Priporočljivo je, da spreminjata ključ za vsako komunikacijsko sejo.
- Za učinkovito upravljanje ključev je pogosto potrebna zaupanja vredna tretja oseba.

3.2.2 Kriptografske zgoščevalne funkcije

Zgoščevalna (ang. hash) funkcija je vsaka funkcija, ki lahko prilagodi podatke poljubne velikosti na podatke fiksne velikosti (Menezes, Oorschot & Vanstone, 2001, str. 33). Je matematični problem, ki ga je težko rešiti, vendar je rezultat zelo enostavno preveriti (Natarajan, Krause & Gradstein, 2017, str. 9). Zgoščevalna funkcija vzame vhodni niz številk in črk in ga spremeni v nov x-mestni niz, ki obstaja iz naključnih črk in številk. Ta x-mestni niz je izhodna oz. zgoščevalna vrednost. Slika 3 prikazuje delovanje kriptogafske zgoščevalne funkcije, kje vidimo, da če se spremeni katera koli številka ali črka v vhodnem nizu, se bo spremenila tudi izhodna vrednost.

Slika 3: Kriptografska zgoščevalna funkcija SHA256.



Vir: Manning Publications (2017).

Pri veriženju podatkovnih blokov se informacije o transakcijah uporabljajo kot vhodni podatki, ki jih nato algoritem zgoščevalne funkcije transformira v izhodne podatke fiksne dolžine (Menezes, Oorschot & Vanstone, 2001, str. 201). A le če zgoščevalna funkcija izpolnjuje nekaj dodatnih pogojev, se lahko uporabi za kriptografske aplikacije. Kriptografske zgoščevalne funkcije so posebna vrsta zgoščevalnih funkcij, primernih za uporabo v kriptografiji, saj predstavljajo programski algoritem, ki prilagodi poljubno veliko bazo podatkov na niz bitov s fiksno velikostjo. Ključna lastnost kriptografskih zgoščevalnih funkcij je enosmerna funkcija, ki jim omogoča, da je edini način, da odkrijemo podatke, vnesene v zgoščevalno funkcijo, iskanje vseh možnih kombinacij, da bi lahko odkrili pravilno. Enosmerne funkcije je enostavno izračunati, vendar je zelo težko izračunati njihove inverzne funkcije (Thomsen, 2009, str. 3). Če imamo vnosni podatek *x*, lahko enostavno izračunamo funkcijo *f(x)*, toda če poznamo vrednost *f(x)*, je izredno težko izračunati vrednost *x*. Vnosni podatek je lahko kateri koli niz katere koli velikosti, vendar je izhodna vrednost fiksne dolžine, na primer 256-bitni izhod ali 512-bitni izhod. Če se uporabi algoritem SHA-256, ki ga uporablja omrežje Bitcoin, bo ustvarjena 256-bitna zgoščevalna vrednost. Ta protokol deluje s podatki, razdeljenimi na kose 512 bitov (ali 64 bajtov). Algoritem kriptografsko šifrira in nato izda 256-bitno zgoščevalno vrednost. Algoritem vključuje relativno preprost šifrirni krog, ki se ponovi 64-krat. Kriptografska zgoščevalna funkcija, ki se uporablja v kriptografiji, mora izpolnjevati specifične lastnosti.

Thomsen (2009, str. 5) med najpomembnejše pogoje uvršča naslednje:

- **Determinističnost**. Pomeni, da bo zgoščevalna vrednost vedno enaka, ne glede na to, kolikokrat so vnosni podatki obdelani z algoritmom zgoščevalne funkcije. Ta lastnost je ključna takrat, ko imamo opravka z večjim številom podatkov in transakcij, saj nam omogoča, da si sistem zapomni le zgoščevalno vrednost in ne celotne dolžine inputa. Pomembna lastnost je tudi dejstvo, da vsaka majhna sprememba vnosnih podatkov popolnoma spremeni zgoščevalno vrednost.
- **Hitrost.** Zgoščevalna funkcija mora biti sposobna hitro in učinkovito obdelati vnosne podatke in vrniti zgoščevalno vrednost, saj v nasprotnem primeru celoten sistem deluje počasi in neučinkovito.
- **Odpornost proti trkom** (ang. collision resistance). Pomeni, da je težko najti dve vhodni vrednosti, ki dajeta isto zgoščevalno vrednost. Trk se zgodi, ko imata dve specifični sporočili isto zgoščevalno vrednost. Funkcija se šteje kot odporna na trke, če obstaja izjemno majhna verjetnost trka. V praksi to pomeni, da je izjemno težko poiskati par sporočil *x1* in *x2* z zgoščevalno vrednostjo *h*, kjer $x1 \neq x2$ *in* $h(x1) = h(x2)$.
- **Odpornost na predhodno sliko** (ang. preimage resistance). Glede na zgoščevalno vrednost nekega sporočila mora biti težko najti kakršno koli drugačno sporočilo s to enako zgoščevalno vrednostjo. Pomeni, da je za vsa vnaprej določena izhodna sporočila računsko neizvedljivo, da bi našli katera koli vhodna sporočila, ki imajo iste zgoščevalne vrednosti kot ta izhodna sporočila. Z zgoščevalno funkcijo *H* in dano zgoščevalno vrednostjo *h* je izjemno težko najti katero koli sporočilo *x* z lastnostjo $H(x) = h$.
- **Sekundarna odpornost na predhodno sliko** (ang. second preimage resistance). Glede na dano vrednost nekega sporočilo bi bilo težko najti drugačno sporočilo, ki ima isto zgoščevalno vrednost. Pomeni, da je za dano sporočilo *x1* težko najti drugo sporočilo $x2 \neq x1$ in lastnostjo $h(x1) = h(x2)$.

Narayanan, Bonneau, Felten, Miller in Goldfeder (2016, str. 155) dodajajo še dve ključni lastnosti kriptografskih funkcij hash funkcij:

- **Deterministično skrivanje** (ang. deterministic hiding). Lastnost skrivanje zgoščevalni funkciji omogoča, da skrijemo obseg prostora podatkov, ki jih vnašamo. Glede na zgoščevalno vrednost $H(x) = h$, ki jo generira zgoščevalna funkcija *H*, bi moral napadalec generirati zgoščevalno vrednost vsakega sporočila *x* v vnosnem prostoru naključno, če bi hotel poiskati sporočilo *x*, katerega zgoščevalna vrednost je *h*, kar onemogoča predvidevanje, katero vhodno sporočilo bo generiralo pravilno zgoščevalno vrednost. Na primer: če so vhodni podatki, ki jih zabeležimo, v obliki »A plača B« in »B plača E«, potem je vhodni prostor zlahka predvidljiv v obliki »1 plača 2«. To je nezaželena situacija, saj je izračunavanje vhodnih podatkov lažje. Najprej se ustvarijo vse zgoščevalne vrednosti obrazca H v obliki »1 plača 2«, kar proizvede pregledno tabelo vsakega vhodno-izhodnega para. Da kriptografska zgoščevalna funkcija pridobi lastnost skrivanja, moramo vnosnim podatkom vsakič dodati naključen niz podatkov s fiksno

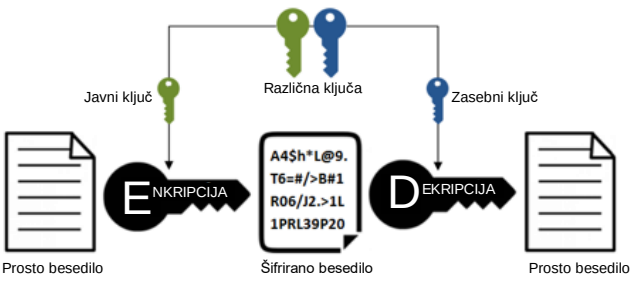
dolžino *r*, ki ga povežemo z vnosnimi podatki *x*. Zgoščevalna funkcija *H(x) = h* zdaj v praksi postane *H(x) = H(r||x) = h*, kjer simbol || označuje povezovanje.

– **Prijaznost za sestavljanke** (ang. puzzle friendliness). Pomeni, da je glede na del naključno izbrane vhodne vrednosti *k* in izhodne vrednosti, dolge *n-bitov*, praktično nemogoče poiskati vhodno vrednost *x*, kjer *je H (k || x) = h*. V preprostih pojmih pomeni, da če predpostavljamo izhodno vrednost *h* in izberemo naključno vrednost *k*, bo praktično nemogoče poiskati takšno vrednost *x*, da bo zgoščevalna vrednost povezanih vrednosti *x* in *k* enaka izhodni vrednosti *h*.

3.2.3 Kriptografija z asimetričnim ključem

Kriptografske sheme druge vrste so znane kot asimetrične kriptografske sheme oz. kot kriptografija javnega ključa (Menezes, Oorschot & Vanstone, 2001, str. 25). Te sheme so rezultat ideje o izmenjavi ključev iz leta 1976 (Diffie & Hellman, 1976, str. 644–654), pri katerih imajo vsi uporabniki tako zasebni kot javni ključ v obliki niza naključnih črk in številk. Deljenje javnega ključa omogoča šifrirano komunikacijo med uporabnikoma A in B, saj uporabniku B omogoča uporabo javnega ključa uporabnika A za sestavljanje šifriranega sporočila. S to tehniko so rešili problem distribucije ključev v simetričnem kriptografskem sistemu z uvedbo digitalnih podpisov. Koncept zasebnega ključa pa omogoča, da lahko samo uporabnik A dešifrira sporočilo uporabnika B. Vrste kriptografije javnega ključa vključujejo algoritem RSA, ki se pogosto uporablja na internetu, tj. algoritem digitalnega podpisa (ang. digital signature algorithm), sprejet kot zvezni standard za obdelavo informacij za digitalne podpise, in algoritem digitalnega podpisa eliptične krivulje (ang. elliptic curve digital signature algorithm), ki ga uporablja omrežje Bitcoin (Menezes, Oorschot & Vanstone, 2001, str. 45). Vsak udeleženec omrežja ima zasebni ključ, ki se uporablja za podpisovanje digitalnih sporočil in ga pozna le posamezni uporabnik, in javni ključ, ki je javno znan in se uporablja za preverjanje identitete pošiljatelja digitalnega sporočila (Menezes, Oorschot & Vanstone, 2001, str. 28). Slika 4 prikazuje proces uporabe asimetrične kriptografije za šifriranje besedila.

Slika 4: Asimetrične kriptografija za šifriranje besedila



Vir: ssl2buy (2018).

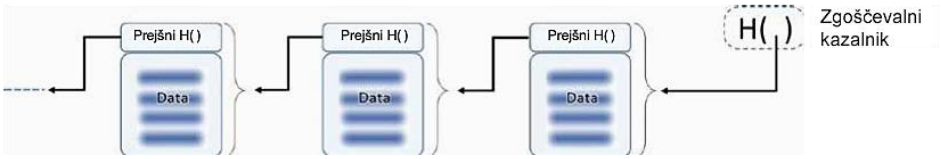
Ko se kriptografski ključi kombinirajo s peer-to-peer omrežjem, se pojavi zelo koristna oblika digitalnih interakcij (Singhal, Dhameja & Panda, 2018, str. 99). Postopek se začne,

ko pošiljatelj vzame svoj zasebni ključ in ustvari posebno obvestilo, v primeru kripto valute pošilja določeno vsoto kripto valute in jo veže na javni ključ prejemnika. Podatkovni blok, ki vsebuje digitalni podpis, časovni žig in ustrezne informacije, se nato predvaja v vsa vozlišča v omrežju in prejemnik postane lastnik poslane vsote. Bloki so podpisani z digitalnim podpisom, ki pošiljatelja povezuje z vsebino bloka, kar je podobno podpisu pogodbe, zato se pošiljatelju zmanjša količina kripto valute v lasti.

3.3 Podatkovna struktura

Podatkovne verige so strukturirane v obliki povezanega seznama blokov, ki vsebujejo podatke o transakcijah. Posamezno podatkovno verigo lahko shranimo kot datoteko ali v preprosto bazo podatkov (Antonopoulos, 2014, str. 163). Blok je podatkovna struktura, ki združuje podatke o transakcijah. Sestavljen je iz glave, ki vsebuje metapodatke, sledi pa ji dolg seznam transakcij, ki tvorijo večino njegove velikosti. Bloki so povezani nazaj, saj se vsak nanaša na prejšnji blok v verigi. Bloki v podatkovni verigi so identificirani z zgoščevalno vrednostjo, ki se ustvari s kriptografskim algoritmom v glavi bloka. Vsak blok se sklicuje na prejšnji blok, znan kot nadrejeni oz. starševski blok (ang. parent block) preko zgoščevalnega kazalnika (ang. hash pointer) v glavi bloka. Zgoščevalni kazalnik je zgoščevalna vrednost, ki kaže na podatkovni blok, kjer je zgoščevalni kazalnik zgoščevalna vrednost samega podatkovnega bloka, in kaže na prejšnji podatkovni blok ter zagotavlja način za preverjanje, ali so bili podatki spremenjeni. Rečemo lahko, da vsak blok vsebuje zgoščevalno vrednost svojega nadrejenega bloka v lastni glavi, zaporedje zgoščevalne vrednosti, ki povezuje vsak blok z njegovim nadrejenim, pa ustvarja verigo, ki sega vse do prvega bloka (Singhal, Dhameja & Panda, 2018, str. 115). Prvi ustvarjen blok se imenuje genezni blok (ang. genesis block). Čeprav ima blok samo en nadrejen blok, ima lahko začasno več otrok oz. podrejenih blokov (Antonopoulos, 2014, str. 164). Vsak podrejen blok se nanaša na isti blok kot njegov nadrejeni blok in vsebuje isto zgoščevalno vrednost. Podrejeni bloki se pojavijo med razmejitvami verige (ang. fork), začasnim stanjem, ki se pojavi, ko različne bloke skoraj istočasno odkrijejo različni rudarji. Na sliki 5 je prikazana struktura podatkovnih verig, kjer se bloki povezujejo z zgoščevalnimi kazalniki.

Slika 5: Podatkovni bloki, povezani z zgoščevalnimi kazalniki

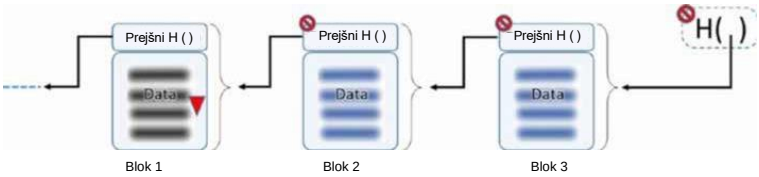


Vir: Singhal, Dhameja & Panda (2018).

Čeprav ima blok lahko več kot en podrejen blok, ima lahko samo en nadrejen blok, ker ima blok samo eno zgoščevalno vrednost prejšnjega bloka. Zgoščevalna vrednost nadrejenega bloka je v glavi in s tem vpliva na zgoščevalno vrednost trenutnega bloka (Antonopoulos,

2014, str. 165). Če se spremeni vrednost nadrejenega bloka, se spremeni vrednost podrejenega. Spremenjena zgoščevalna vrednost nadrejenega bloka zahteva spremembo zgoščevalnega kazalnika podrejenega bloka, kar pa povzroči spremembo zgoščevalne vrednosti podrejenega, to zahteva spremembo zgoščevalnega kazalnika sekundarno podrejenega bloka, ki nato spremeni zgoščevalno vrednost sekundarno podrejenega bloka in tako naprej. Ta nadaljevalni učinek zagotavlja, da bloka potem, ko vsebuje več generacij, ni mogoče spremeniti, ne da bi pri tem izsili ponovni izračun vseh blokov, ki mu sledijo v verigi. Ker bi tak preračun zahteval ogromno količino računalniške moči, obstoj dolge verige blokov povzroči, da je zgodovina verige nespremenljiva, kar je ključna značilnost varnosti. V omrežju Bitcoin se transakcije štejejo kot varne, kot se bloku doda šest novih blokov (Norton, 2017, str. 78). Slika 6 prikazuje poskus spremembe podatkovne verige. V primeru sovražnega na blok 3 na sliki 6 in poizkusu spremembe podatkov bo zaradi ključne lastnosti zgoščevalne funkcije rezultat vsake majhne spremembe podatkov dramatična sprememba zgoščevalne vrednosti preostalih blokov (Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016, str. 11–13). Vsaka majhna sprememba bloka 3 na sliki 6 bo tako spremenila podatke in zgoščevalna vrednost v bloku 2, kar bo spremenilo podatke in zgoščevalno vrednost v bloku 1 in tako dalje, vse do geneznega bloka. Struktura bloka (velikost, razdelitev podatkov in glave, število transakcij v bloku itd.) se določi pri oblikovanju same verige (Antonopoulos, 2014, str. 164).

Slika 6: Poskus spremembe podatkovne verige



Vir: Singhal, Dhameja & Panda (2018).

3.3.1 Razmejitev

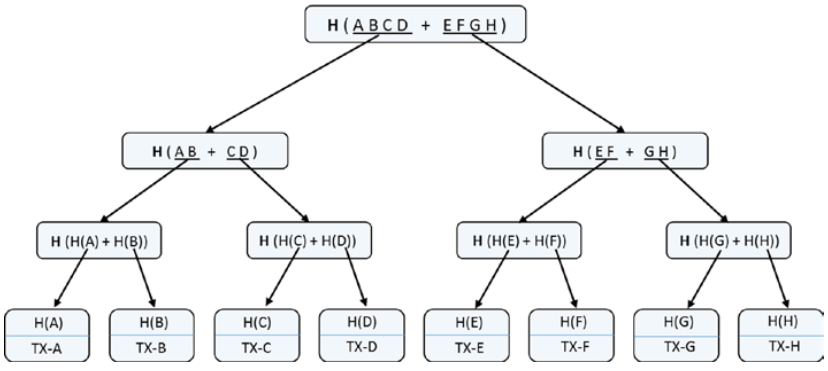
Kot že omenjeno, ima lahko posamezni blok več podrejenih blokov, kar se zgodi zaradi procesa, ki se imenuje razmejitev. Ta se pojavi, ko se podatkovna veriga v porazdeljeni podatkovni bazi razdeli na dve različni poti naprej, ki ju je potem treba razrešiti (Natarajan, Krause & Gradstein, 2017, str. 19). V mnogih primerih se razmejitve rešujejo avtomatizirano. Razmejitve se hitro razrešijo, ko se enemu izmed dodanih blokov doda nov blok, medtem ko drugi blok zapusti celotno omrežje. V drugih primerih lahko razmejitve, ki ostanejo nerešene, ustvarijo dve konkurenčni zgodovini podatkovne verige. Obstajajo tri vrste razmejitev (Bank for International Settlements, 2018, str. 103):

- **naključna razmejitev:** do naključne razmejitve lahko pride, če so posodobitve platforme nenamerno nezdružljive s prejšnjo kodo, kar pomeni, da vozlišča začnejo uporabljati dve različici programske opreme, dokler niso neskladnosti popravljene;
- **mehka razmejitev:** je združljiva nazaj, kar pomeni, da se bloki, ki jih obdelujejo vozlišča z nadgrajeno programsko opremo, štejejo za veljavna pri vozliščih, ki nimajo nadgrajene programske opreme, vendar obratno ne drži; to spodbuja vsa vozlišča, da nadgradijo svojo programsko opremo;
- **trda razmejitev:** ni združljiva nazaj, kar pomeni, da je nadgradnja programske opreme uvedla novo pravilo, ki se ne šteje za veljavno do nadgradnje vozlišča; če se člani skupnosti ne strinjajo z novimi pravili, se v tem primeru lahko odločijo, da ne nadgradijo novih pravil, pač pa nadaljujejo na prvotni verigi z uporabo stare programske opreme.

3.3.2 Merklova drevesa

Merklova drevesa so vrsta podatkovnih struktur za varno in učinkovito shranjevanje podatkov na bloke. Prvi jih je razvil in patentiral Ralph Merkle leta 1979 (Merkle, 1979, str. 12). Slika 7 prikazuje osnovno obliko Merkovega drevesa. So način produciranja zgoščevalnih vrednosti velikega števila posameznih kosov podatkov in si pri tem pomagajo pri razdeljevanju teh kosov na manjše sekcije (Buterin, 2015). Nato generira jo zgoščevalne vrednosti teh sekcij, nato pa postopek ponovijo in v sekcije razdelijo zgoščevalne vrednosti sekcij in generirajo njihove zgoščevalne vrednosti, dokler ne ostane ena sama zgoščevalna vrednost. Ta se imenuje koreninska zgoščevalna vrednosti (ang. root hash) in je na sliki 7 prikazana na vrhu. Najnižje zgoščevalne vrednosti v Merklovem drevesu se imenujejo listi (ang. leaves), vse zgoščevalne vrednosti v sredini pa veje (ang. branches).

Slika 7: Primer Merklovega drevesa

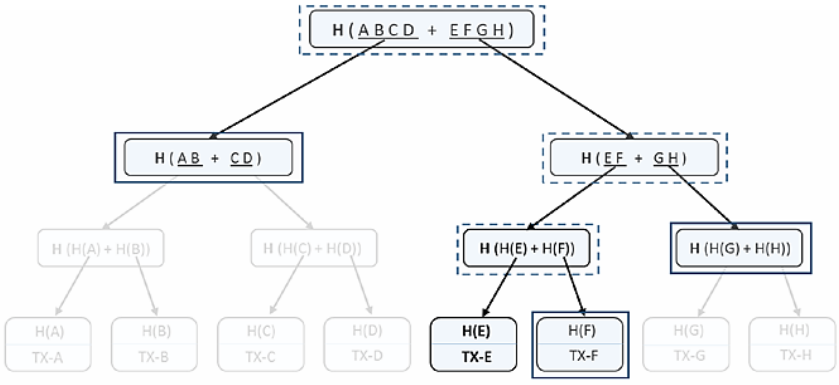


Vir: Singhal, Dhameja & Panda (2018).

Uporaba Merklovih dreves nam omogoča bolj učinkovit proces ugotavljanja, ali določena transakcija sodi v posamezni blok. Sprememba na kateri koli ravni se ne ujema z zgoščevalno vrednostjo, ki je shranjena na eni ravni navzgor, vse do koreninske vrednosti. Merklovo drevo je strukturirano na binarni način, zato mora biti na ravni listov vedno parno

število predmetov (transakcij). Vitalik Buterin (2015) kot ključni aspekt Merklovih dreves izpostavlja omogočanje koncepta, imenovanega Merklov dokaz (ang. Merkle proof), s katerim lahko učinkovito preverimo, ali so listi, veje in koreninske vrednosti na poti navzgor po drevesu sestavljeni iz istih zgoščevalnih vrednosti in so na pravem mestu. Ta lastnost pomeni, da nam ni treba pregledati vseh zgoščevalnih vrednosti, ampak samo pregledamo, ali je kos podatkov konsistenten s koreninsko vrednostjo s pregledovanjem manjše podsekcije vseh zgoščevalnih vrednosti. Če je korenska zgoščevalna vrednost javno dostopna, je v vsakem trenutku možno uporabiti Merklov dokaz za verifikacijo pozicije in integritete kosa podatkov v podatkovni bazi (Curran, 2018). Če je v Merklovem drevesu *n* transakcij (listov), potem preverjanje traja Log_n časa (Singhal, Dhameja & Panda, 2018, str. 122). Če želimo preveriti, ali transakcija resnično pripada Merklovemu drevesu, ni treba pregledati vseh predmetov in celotnega drevesa, ampak je potrebna samo pravilna podmnožica. Preverjanje začnemo z izbrano transakcijo in jo zaradi binarne narave drevesa preverimo skupaj z njenim parom, izračunamo njuno zgoščevalno vrednost ter preverimo, ali se ujema z nadrejeno zgoščevalno vrednostjo. Nato nadaljujemo z nadrejeno zgoščevalno vrednostjo in njenim parom na tej ravni, da dobimo njuno nadrejeno zgoščevalno vrednost. Na sliki 8 je prikazano preverjanje transakcije *H(E).* Na sliki so za preverjanje transakcije zahtevani le trdni pravokotniki, črtkani pravokotniki pa se lahko izračunajo. Ker obstaja osem transakcijskih elementov *(n = 8)*, bi bili za preverjanje potrebni le trije izračuni *(Log_2 (8) = 3).*

Slika 8: Preverjanje transakcij na Merklovem drevesu



Vir: Singhal, Dhameja & Panda (2018).

3.4 Algoritmi za soglasje

Soglasje lahko opredelimo kot splošno strinjanje ali strinjanje večine med večjim številom subjektov (Sarcevic, Palen, White, Starbird & Anderson, 2012, str. 47–50). Pri omrežjih, ki temeljijo na tehnologiji porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, je določanje, ali so podatki pravilni, izjemno kompleksen in zahteven izziv. Algoritmi soglasja se v tem primeru navezujejo na proces strinjanja vseh razdeljenih vozlišč o zgodovini in končnem stanju podatkov na zadnji verziji podatkovne baze. To končno stanje se imenuje

porazdeljeno soglasje (Bashir, 2018, str. 12). Vsak nov blok, ki se doda v verigo, mora doseči soglasje glede na postavljen mehanizem (Cachin & Vukolic, 2017, str. 4). Kljub temu se posamezna vozlišča lahko zrušijo, obnašajo zlonamerno in delujejo proti skupnemu cilju ali pa preprosto izgubijo komunikacijo z omrežjem. Da omrežje doseže stanje neprekinjenih storitev, vozlišča uporabljajo algoritme soglasja, ki so tolerantni za napake, da se zagotovi strinjanje glede stanja verige. Vsa vozlišča preverijo informacije, ki jih je treba dodati verigi, saj ta funkcija spodbuja zaupanje vseh vozlišč, da veriga kot celota deluje pravilno. Pravila v obliki algoritmov soglasja dosegajo, da vsi uporabniki izvajajo podvajanja z enakimi podatki in metodami, zato da bodo sčasoma ustvarili enake rezultate. Porazdeljena narava zahteva od udeležencev v omrežju, da dosežejo soglasje glede veljavnosti novih vnosov podatkov z upoštevanjem specifičnega niza pravil (Baliga, 2017, str. 5). To se doseže z uvedbo algoritma soglasja, ki je specificiran v oblikovanju tehnologije veriženja podatkovnih blokov in se lahko razlikuje glede na njegovo naravo, namen in sredstva v obravnavi (Natarajan, Krause & Gradstein, 2017). Algoritmi soglasja omogočajo posodabljanje verige podatkovnih blokov, poleg tega pa zagotavljajo, da so vsi bloki v verigi resnični in vsebujejo podatke o dejanskih transakcijah. Vsak algoritem soglasja je sestavljen iz specifičnega sklopa pravil, ki vozliščem diktira, kako lahko verificirajo podatkovni blok in ga dodajo verigi. Algoritmi za soglasje imajo tri ključne lastnosti, na podlagi katerih se lahko določi nivo uporabe in učinkovitosti (Baliga, 2017):

- **varnost:** algoritem soglasja je obravnavan kot varen, če vsi uporabniki pri podvajanju proizvedejo isti končni rezultat in če so ti rezultati v skladu s pravili mehanizma;
- **živost:** algoritem soglasja je živ, če vsi delujoči uporabniki omrežja eventualno proizvedejo neko vrednost;
- **toleranca napak:** algoritem soglasja nudi sprejemljivo toleranco napak, če si lahko opomore od odpovedi oz. nepoštenega delovanja enega ali več uporabnikov v omrežju.

3.4.1 Bizantinska toleranca napak

Problem bizantinskih generalov so prvič opredelili Lamport, Shostak in Pease (1982, str. 382–401) in opisuje scenarij, po katerem se mora več generalov dogovoriti o času napada na svojega skupnega sovražnika. Zaplet pri tem je, da je lahko nepošten en general ali več, kar pomeni, da lahko lažejo o svoji izbiri (na primer pravijo, da se strinjajo, da bodo napadli, a ne bodo). Da bi generali dosegli soglasje, se morajo vsi strinjati o isti odločitvi. Zgodbo je mogoče prenesti na področje računalniških sistemov, kjer so računalniki generali, njihovi digitalni sistemi komuniciranja pa so kurirji, ki dostavljajo sporočila med njimi. Problem komuniciranja in nezaupanja zaradi potencialnega nepoštenega vedenja imenujemo bizantinska napaka (ang. byzantine fault) in je napaka, ki različnim uporabnikom predstavi različna sporočila. Bizantinska toleranca napak (ang. byzantine fault tolerance, v nadaljevanju BFT) je kategorija algoritmov, katerih namen je rešiti problem doseganja soglasja, ko vozlišča lahko ustvarijo poljubne podatke (Bach, Mihaljević & Žagar, 2018, str. 1548). V okviru porazdeljenih sistemov je bizantinska toleranca napak zmožnost

porazdeljenega računalniškega omrežja, da pravilno doseže zadostno soglasje, čeprav nepoštene komponente sistema ne delujejo pravilno ali širijo nepravilne informacije drugim vozliščem. Bizantinska toleranca je definirana kot stopnja gotovosti, ki jo ima porazdeljeni računalniški sistem glede statusa vozlišča, ko ni popolne informacije o tem, ali je vozlišče pravilno ali ne. Cilj vsakega sistema je tolerantnost za bizantinske napake, ki omogoča obrambo pred bizantinskimi napakami. Pravilno uveden sistem, ki je toleranten za bizantinske napake, mora biti sposoben zagotavljati storitve, ob predpostavki, da je večina komponent poštenih. Zaradi decentralizirane narave verige podatkovnih blokov in same vrednosti podatkov, shranjenih v podatkovnih bazah, imajo nepošteni uporabniki velike ekonomske iniciative, da bi v sistemu povzročili bizantinske napake, kar povzroči nujno potrebo po vzpostavitvi sistema, tolerantnega za bizantinske napake. V odsotnosti tolerance za bizantinske napake lahko vsak nepošten uporabnik posreduje in potrdi lažne transakcije, kar izniči ključne prednosti tehnologije veriženja podatkovnih blokov. Sistem, ki je toleranten za bizantinske napake, zagotovi svojo varnost in živost, če v njegovi življenjski dobi ne bo napačnih oz. pokvarjenih več kot tretjina oz. $\lfloor (n-1) \div 3 \rfloor$ vozlišč (n je skupno število vozlišč v sistemu) (Bach, Mihaljević & Žagar, 2018, str. 1548). Prvi velik preboj pri rešitvah problema bizantinskih generalov je bila uvedba algoritma za soglasje, imenovanega praktična bizantinska toleranca napak (ang. practical byzantine fault tolerancev nadaljevanju pBFT), na področju veriženja podatkovnih blokov pa z algoritmom imenovanim, dokaz o delu (ang. proof of work, v nadaljevanju PoW) v sistemu Bitcoin (Nakamoto, 2009b). Kasneje so se razvili še številni drugi načini za vzpostavitev sistema, tolerantnega za bizantinske napake. V tabeli 6 je prikazana primerjava med najbolj popularnimi algoritmi za doseganje soglasja glede na vrsto omrežja tolerirano stopnjo nepoštenih uporabnikov v omrežju, hitrostjo transakcij, porabo električne energije in stopnjo razširljivosti.

Tabela 6: Primerjava pogosto uporabljenih algoritmov za soglasje

	PoW	**PoS**	**DPoS**	**pBFT**	**RPCA**	**SCP**
Vrsta omrežja	Brez dovoljenja	Brez dovoljenja	Brez dovoljenja	Potreba po dovoljenju	Brez dovoljenja	Brez dovoljenja
Tolerirana stopnja nepoštenih uporabnikov	< 25 % računalniške moči	< 51 % deleža	< 51 % vseh delegiranih validatorjev	< 33 % nepoštenih vozlišč	< 20 % nepoštenih vozlišč	< 33 % nepoštenih vozlišč
Hitrost transakcij	Počasna	Hitra	Hitra	Hitra	Hitra	Hitra
Poraba energije	Velika	Srednja	Srednja	Majhna	Majhna	Majhna
Stopnja razširljivosti	Nizka	Visoka	Visoka	Nizka	Visoka	Visoka
Primer	Bitcoin	Peercoin	Bitshares	Hyperledger	Ripple	Stellar

Vir: Zheng, Xie, Dai, Chen & Wang (2018).

3.4.2 Dokaz o delu

Dokaz o delu (ang. proof of work) je najbolj popularna metoda za doseganje soglasja na decentraliziranih omrežjih. Uporabniki, ki želijo potrditi podatkovni blok in ga dodati verigi,

morajo dokazati, da so porabili določeno količino procesorske moči, in to tako, da rešijo matematično uganko oz. najdejo pravilno zgoščevalno vrednost, ki je manjša kot določena stopnja težavnosti (Baliga, 2017, str. 6). Uporabniki v omrežju, ki se ukvarjajo s tem procesom, se imenujejo rudarji (Wang in drugi, 2018, str. 3). Matematični problem, s katerim se sooča vsak rudar, je, da najde zgoščevalno vrednost za podatke v svojem bloku, ki se začne z določenim številom zaporednih ničel. Ta zgoščevalna vrednost se imenuje podpis in ga potrebujejo, če želijo podatkovni blok dodati verigi. Število potrebnih zaporednih ničel določajo pravila vsake verige podatkovnih blokov in dodajanje novega bloka ni mogoče, če ta ne vsebuje zadostnega števila zaporednih ničel. Količina ničel, določena v pravilih podatkovne verige, se imenuje stopnja težavnosti in določa, kako zahtevno je reševanje ugank za dodajanje novih blokov. Stopnja težavnosti povzroča, da je ta uganka težje rešljiva in s tem bolj zamudna. Trenutno je stopnja težavnosti rudarjenja v omrežju Bitcoin približno 12.973.235.968.799, kar pomeni, da je verjetnost generiranja pravilne zgoščevalne vrednost 1 do približno 12 trilijonov (Bitinfocharts, 2019). Rudarji, ki najdejo ustrezen podpis, blok oddajo drugim rudarjem. Drugi rudarji zdaj preverijo legitimnost podpisa tako, da vzamejo niz podatkov oddajanega bloka in generirajo njegovo zgoščevalno vrednost, da bi videli, ali se dejansko ujema z zgoščevalno vrednostjo v podpisu. Če je veljavna, bodo drugi rudarji potrdili njeno veljavnost v skladu s pravili omrežja in se strinjali, da se blok lahko doda v verigo. Blok se lahko zdaj doda v verigo in se razširi na vsa druga vozlišča v omrežju. Druga vozlišča bodo blok sprejela in ga shranila v podatke o transakcijah. Ko je blok dodan v verigo, se vsak naslednji blok, dodan po tem, šteje kot potrditev za ta blok. Več potrditev kot jih ima transakcija oz. globlje kot je v verigi, težje jo je spremeniti. Ker je zgoščevalna vrednost, ki jo generira algoritem zgoščevalne funkcije, popolnoma naključna za vsako drugačno vneseno vrednost, rudarji s podatki podatkovnega bloka povežejo in konstantno spreminjajo naključni niz podatkov v podatkovnem bloku (Singhal, Dhameja & Panda, 2018, str. 60). Ta naključni niz podatkov se imenuje nonce. Vsakič ko rudar spremeni vrednost nonce, spremeni vnosno vrednost, kar spremeni izhodno vrednost zgoščevalne funkcije oz. zgoščevalno vrednost. Računalniška naprava ali več povezanih naprav producira zgoščevalne vrednosti s hitrostjo nekaj mega (MH/s), giga (GH/s) ali celo tera zgoščevalnih vrednosti na sekundo (TH/s), dokler ne najdejo zgoščevalne vrednosti, ki ustreza stopnji težavnosti. To število poskusov na sekundo se imenuje hitrost zgoščevalne funkcije (ang. hash rate) (Bai in drugi, 2018, str. 3). Ker rudarji za iskanje pravilne zgoščevalne vrednosti porabljajo lastno procesno moč in posledično elektriko, imajo ekonomsko iniciativo, da se njihov blok doda verigi, saj s tem prejmejo nagrado in si povrnejo stroške rudarjenja ter dodatno zaslužijo, s tem pa zagotovijo varnost v verigi. Za nagrado so rudarji nagrajeni z vnaprej specificirano kripto valuto in njeno količino.

Na primer: pri rudarjenju v omrežju Bitcoin je nagrada za bloke prepolovljena vsakih 210.000 blokov ali približno vsaka 4 leta. Leta 2009 je bila nagrada 50 bitcoinov, leta 2013 je bila 25 BTC, leta 2019 12,5 BTC, sredi leta 2020 pa se bo znova prepolovila na 6,25 BTC (Bitinfocharts, 2019). Ker se nagrade v obliki na novo izdane kripto valute, ki jo izda omrežje, konstantno zmanjšujejo, so rudarji lahko nagrajeni tudi s provizijami, ki jih plačajo

uporabniki. Toda rudarji ne obdelujejo transakcij naključno ali v časovnem zaporedju. Rudarji dejansko dobijo možnost, da izberejo, katere transakcije so vključene v vsak blok, in obstaja omejitev števila transakcij, ki so lahko vključene. Ker rudarji prejmejo tudi provizijo za transakcije, vključene v podatkovne bloke, ki jih dodajo, imajo prednost transakcije z višjimi provizijami nad tistimi s povprečnimi, nizkimi ali neobstoječimi pristojbinami. Zato se provizije za transakcije z bitcoinom uporabljajo za spodbujanje rudarjev k obdelavi in preverjanju transakcij. Mehanizem PoW, ki ga uporablja omrežje Bitcoin, je primeren za decentralizirano porazdeljeno omrežje, pri katerem ni potrebe po avtentikaciji uporabnikov, zato se lahko vsak pridruži omrežju kot rudar. Baliga (2017, str. 9) pa kljub temu mehanizem PoW opisuje kot ranljiv za tako imenovane napade z dokazom o delu (ang. proof of work attack) oz. kot napad 51 %, pri čemer slabonamerni uporabniki obvladujejo več kot 51 % omrežja. Poleg tega najnovejše raziskave potrjujejo, da lahko mehanizem PoW omogoča doseganje porazdeljenega soglasja le, če manj kot 25 % omrežja deluje nepošteno (Vukolic, 2016, str. 118–120), kar se razlikuje od nedavnih predvidevanj, da lahko mehanizmi PoW delujejo, če je nepoštenih manj kot 50 % omrežja.

Omrežje Ethereum je v svoji prejšnji verziji, imenovani Homestead, kot algoritem soglasja prav tako uporabljal mehanizem dokaz o delu, vendar v drugačni obliki (Baliga, 2017, str. 7). Ta se imenuje EthHash in omogoča hitro potrditev transakcij ter zagotavlja odpornost ASIC[4] za preprečevanje napadov 51 %. EthHash je bil zasnovan proti centralizaciji rudarjev, kar je bila slabost v Bitcoinu. Zaradi izjemne cenovne dostopnosti ASIC-jev je bilo mogoče doseči izvajanje rudarjenja na zelo visokih stopnjah, s čimer je precej presegal računalniško strojno opremo za splošne namene. To je izbranim subjektom, kot so velike korporacije ali skupine nepoštenih ali kriminalnih posameznikov, omogočilo, da ustvarijo rudarske bazene z zelo visoko hitrostjo rudarjenja in nadzorujejo velik del omrežja Bitcoin. S tem ko je mehanizem odporen na opremo ASIC, zagotovimo, da bazeni rudarjev ne morejo prevzeti nadzora nad rudarsko močjo v omrežju. Kljub temu pa ima Ethereum isto pomanjkljivost kot Bitcoin v primeru napada 51 %, saj lahko tudi v tem primeru napadalec, ki nadzoruje 51 % rudarske moči, poljubno generira nove veje podatkovnih blokov. Ker pa je mehanizem odporen na opremo ASIC, je tak napad manj verjeten. Omrežje Ethereum je mehanizem Homestead prenehalo uporabljati 16. oktobra 2017 in začelo uporabljati mehanizma Metropolis.

3.4.3 Dokaz o deležu

Dokaz o deležu (ang. proof of stake, v nadaljevanju PoS) algoritmi so zasnovani tako, da premostijo slabosti algoritmov PoW in veliko porabo električne energije v procesu rudarjenja (Baliga, 2017, str. 8). Algoritem PoS popolnoma nadomesti rudarjenje z

[4] Uporabi specifično integrirano vezje (ang. application-specific integrated circuit) je vezje, prilagojeno za določeno uporabo, ne za splošno uporabo.

alternativnim pristopom, ki vključuje uporabnikov delež ali lastništvo kripto valute v omrežju. Algoritem PoS naključno izbere validatorje za ustvarjanje podatkovnega bloka, s čimer se zagotovi, da noben validator ne more predvideti, kdaj bo lahko potrdil naslednji blok. Uporabniki v omrežju se lahko povežejo z omrežjem, tako da vplačajo varnostne depozite, višino katerih določi protokol omrežja. Ti uporabniki postanejo tako imenovani vezani validatorji in kažejo predanost za širjenje omrežja, s tem ko vplačajo depozite. Vsak validator je naključno izbran za izdelavo bloka iz seznama aktivnih validatorjev, pri čemer je verjetnost izbire linearno utežena z višino depozita. Če validator ni aktiven, je izbran drug validator in ta postopek se ponavlja, dokler algoritem ne najde aktivnega validatorja, ki pridobi pravico, da ustvari nov blok. Če validator ustvari blok, ki se vključi v verigo, prejme nagrado, če pa se blok ne vključi v verigo, protokol deluje tako, da validator izgubi del depozita, ki je enak nagradi za dodani blok. Algoritem PoS ima dve različici, verižno različico (ang. chain-based), in različico v slogu bizantinske tolerance za napake (ang. BFT-style) (Yang, 2019, str. 4). Verižni algoritem uporablja psevdonaključno izbiro validatorja, ki nato ustvari nov blok in ga doda v obstoječo verigo blokov. Pogostost izbire validatorja je nastavljena na neki vnaprej določen časovni interval. Algoritem v slogu BFT uporablja algoritem, odporen na bizantinske napake, za izbiro naslednjega veljavnega bloka. Tukaj imajo validatorji pravico, da naključno predlagajo naslednji blok. V primerjavi s PoW PoS prihrani več energije in je učinkovitejši. Številna omrežja na začetku uporabljajo PoW in ta se postopoma spreminja v PoS. Ethereum na primer načrtuje prehod iz Ethasha v Casper s prehodom na verzijo Serenity, ta pa bo uporabljala koncept varnostnih depozitov za doseganje soglasja (Prasad, 2019).

3.4.4 Podrejeni dokaz o deležu

Podrejeni dokaz o deležu (ang. delegated proof of stake, v nadaljevanju DPoS) je algoritem za soglasja, ki ohranja varen in nepokvarljiv dogovor o resničnem stanju omrežja, potrjuje transakcije in deluje v obliki digitalne demokracije (Bach, Mihaljević & Žagar, 2018, str. 1545). DPoS uporablja glasovanje v realnem času v kombinaciji s sistemom socialnega rangiranja za doseganje soglasja. Vsi uporabniki sistema glasujejo za tako imenovane aktivne delegate, glasovna moč pa se določi glede na količino deleža, ki ga ima uporabnik. Ker je pomembno, da omrežje deluje tekoče in varno, morajo delegati ponavadi del deleža položiti na varnostni račun kot depozit, da dokažejo predanost omrežju. Ta depozit se pri nepoštenem obnašanju zaseže. Aktivni delegati nimajo moči, s katerimi bi lahko spreminjali podrobnosti transakcij, lahko pa nekatere transakcije teoretično izključijo iz bloka. To v praksi nima večjega učinka, saj bi te transakcije v nov blok vključil drug delegat, potrditev transakcije pa bi prišla z majhno zamudo. Delegat, ki te transakcije ni dodal, bi bil iz omrežja izključen, njegov depozit pa zasežen. Uporaba DPoS kot algoritma soglasja narašča. Omrežja, ki trenutno uporabljajo DPoS, so BitShare, Lisk, EOS, Steem, Ark, Nano, Cardano in Tezos.

3.4.5 Praktična bizantinska toleranca napak

Praktična bizantinska toleranca napak (ang. Practical Byzantine Fault Tolerance, v nadaljevanju pBFT) je ena od optimizacij koncepta BFT, ki sta jo uvedla Miguel Castro in Barbara Liskov (2002, str. 398–461). Da bi model pBFT deloval, je predpostavka, da količina zlonamernih vozlišč v omrežju ne more istočasno biti enaka ali večja od n celotnih vozlišč v sistemu v danem oknu ranljivosti. Algoritem učinkovito zagotavlja tako živost kot tudi varnost, če je število nepoštenih vozlišč f v obsegu f $\leq$[(n+1)/3], kjer n predstavlja skupna vozlišča, hkrati zlonamernih ali napačnih. Model pBFT deluje v treh fazah in se osredotoča predvsem na zagotavljanje praktične replike bizantinskega stroja trenutnega stanja, ki dopušča bizantinske napake (nepoštena vozlišča) s predpostavko, da obstajajo neodvisne napake vozlišč in manipulirana sporočila, ki se širijo s specifičnimi, neodvisnimi vozlišči. Vsa vozlišča v sistemu komunicirajo med seboj, cilj pa je, da se vsa poštena vozlišča dogovorijo o stanju sistema in dokažejo, da so sporočila prišla iz določenega vozlišča ter preverijo, ali sporočilo med prenosom ni bilo spremenjeno. Dodajanje novega bloka se izvede v glasovalnem krogu. V vsakem krogu bo po nekaterih pravilih izbrano primarno vozlišče, ki je odgovorno za naročilo transakcije. Celoten postopek je razdeljen v tri faze: predpripravljena faza (ang. pre-prepared phase), pripravljena faza (ang. prepared phase) in izvršilna faza (ang. commited phase). V vsaki fazi bo vozlišče vstopilo v naslednjo fazo, če je prejelo glasove od več kot 2/3 vseh vozlišč. pBFT torej zahteva, da je omrežje poznano vsakemu vozlišču. Danes obstaja peščica platform, ki uporabljajo optimizirane ali hibridne različice algoritma pBFT kot svoj algoritem soglasja ali vsaj njegov del, v kombinaciji z drugim mehanizmom soglasja (Vukolic, 2016, str. 125).

3.4.6 Ripple Protocol Consensus Algorithm

Omrežje in istoimenska kripto valuta Ripple je prvi primer uporabe algoritma za soglasje v obliki federativnega bizantinskega sporazuma (ang. federated byzantine agreement, v nadaljevanju FBA) (Baliga, 2017, str. 10). V sistemih federativnega bizantinskega sporazuma ni potrebe po predčasni identifikaciji in preverjanju vsakega vozlišča, članstvo je odprto, nadzor pa decentraliziran. Vozlišča lahko izberejo, komu zaupajo. Kot pove že ime, je algoritem Ripple Protocol (RPCA) algoritem za soglasje, ki ga uporablja izključno Ripple in je bil razvit posebej za obravnavanje vprašanj počasnosti, ki so prisotna v drugih algoritmih (Ripple Labs Inc., brez datuma). Deluje z glasovalnim algoritmom, ki omogoča uporabnikom, znanim kot prehodi (ang. gateways), ki so predvsem banke in druge javne institucije, da glasujejo o verodostojnosti transakcij, ki jih predlagajo uporabniki. Prehodi preverjajo verodostojnost predlogov za transakcije, ki jih prejmejo od uporabnikov, in vse veljavne transakcije predložijo na glasovanje. Potem glasujejo o vseh transakcijah, ki jih odobri njihov edinstveni seznam vozlišč (ang. unique node list). Ta seznam je podmnožica vseh prehodov, ki jih izbere algoritem Ripple ali sami prehodi, da bi zmanjšali verjetnost, da člani te skupine izvedejo napad na sistem. Glasovanje se običajno izvede samodejno z uporabo algoritma, ki ga nadzoruje vsak prehod. Proces glasovanja poteka v več krogih, v

katerih so predlogi o transakcijah razdeljeni v omrežju, vse medsebojno nasprotne transakcije pa izločene. Transakcije, ki ne izpolnjujejo minimalne stopnje za odobritev, se zavržejo. Vse transakcije, ki jih je v zadnjem krogu odobrilo vsaj 80 % UNL, so dodane podatkovni bazi. Za vozlišče bo podatkovna baza ostala pravilna, dokler je delež okvarjenih vozlišč v UNL manjši od 20 %.

3.4.7 Stellar Consensus Protocol

Stellar je ta pristop še izpopolnil in sprejel prvi dokazljivo varen protokol FBA (Mazieres, 2016). Stellar Consensus Protocol (SCP) je decentraliziran algoritem za soglasje, pri katerem vozlišča v omrežju ne potrebujejo zaupanja v celotno omrežje, ampak imajo možnost izbire, katerim vozliščem zaupajo. Ta skupina vozlišč, ki si medsebojno zaupajo, se imenuje kvorumska rezina. Kvorum je sklop vozlišč, ki zadostuje za dosego dogovora, medtem ko je rezina podmnožica kvoruma, ki prepriča eno določeno vozlišče. SCP se začne z nominacijskim protokolom, tako da predlaga nove transakcije oz. vrednosti za dogovor. Vsako vozlišče, ki prejme te vrednosti, bo med njimi glasovalo za eno samo vrednost, kar na koncu pripelje do ene vrednosti, ki bo dobila večino glasov. Po uspešno izvedenem nominacijskem protokolu se uporabi protokol glasovanja. Med to fazo vozlišča sprožijo glasovanje o tem, ali naj se prevzamejo ali zavrnejo vrednosti, ki so bile izbrane med prejšnjo fazo.

4 UPORABA TEHNOLOGIJE NA PODROČJU DENARNIH TRANSAKCIJ

Inovativna tehnologija veriženja podatkovnih blokov je vsaj v teoriji zmožna preoblikovati infrastrukturo finančnih storitev (Perkins, 2018, str. 7). Finančne storitve, ki temeljijo na veriženju podatkovnih blokov, bodo odprle nove možnosti za inovacije na razvitih trgih in pripomogle k širšemu dostopu, preglednosti in likvidnosti za nekatera bolj nepregledna območja, ki ostajajo na kapitalskih trgih (Miller in drugi, 2019, str. 9). Na eni strani je tehnologija, ki ponuja možnost preoblikovanja ekonomskih modelov in omogoča razvoj trgov in izdelkov, ki prej niso bili na voljo ali niso donosni. Najpopularnejši primer teh novih rešitev so kripto valute, vedno bolj razširjena pa je tudi uporaba digitalnih kriptografskih žetonov in digitalizacije realnih sredstev.

Na drugi strani velike svetovne banke in finančne institucije tesno sodelujejo s podjetji, ki razvijajo tehnologijo, da bi raziskali primere uporabe, ki so pomembni za njihovo poslovanje, in izvedeli, kako lahko nova tehnologija vpliva na njihove stare sisteme in infrastrukturo (Forbes.com, 2019a). Večina korporativnih pobud je doslej dobila obliko konzorcijskih ali zasebnih omrežij, saj poskušajo podjetja upravljati kompromis med izkoriščanjem nove, še nepreverjene tehnologije in ohranjanjem integritete obstoječih poslov.

4.1 Kripto valute

Podobno kot tehnologija veriženja podatkovnih blokov se tudi izraz kripto valute redno uporablja. Izraz se nanaša na širok spekter tehnološkega razvoja, ki uporablja več vrst različnih tehnologij (Houben & Snyers, 2018, str. 20). Valuta je običajno vezana na specifično omrežje, na kateri se uporablja. Ker se tehnologija veriženja podatkovnih blokov gradi na kriptografiji, se takšna valuta običajno imenuje kripto valuta. Primarni primer je bitcoin, ki je domača valuta omrežja Bitcoin. Drugi primer je ethter, ki je domača valuta omrežja Ethereum (Buterin, 2013). Tako kot Bitcoin tudi Ethereum omogoča uporabnikom shranjevanje in prenos ethrov v omrežju na porazdeljen peer-to-peer način. Čeprav sta bitcoin in ether daleč najbolj popularni kripto valuti, danes na trgu obstaja več kot 1500 različnih kripto valut (CoinMarketCap, 2019). Kripto valute običajno niso podprte z realnimi sredstvi in razen električne energije, porabljene za doseganje soglasja, nimajo intrinzične vrednosti, zaradi česar so podvržene veliki volatilnosti (Singhal, Dhameja & Panda, 2018, str. 156). Zaradi tega se je v zadnjem času na trgu pojavila specifična podkategorija, imenovana stabilni kovanci (ang. stablecoins), katerih vrednost je vezana na realna sredstva, ponavadi na fiat valuto. Večina kripto valut je v glavnem klon prve in največje kripto valute bitcoin in preprosto uporablja drugačne parametre, kot so različni časi dodajanja blokov, dobava valute in shema izdajanja (Hileman & Rauchs, 2018, str. 20). Te kripto valute niso pretirano inovativne, pogosto jih imenujejo alternativni kovanci (ang. altcoins) in jih je mogoče uvrstiti v prvo generacijo kripto valut. Medtem pa so se pojavile kripto valute, ki so si sposodile določene koncepte od bitcoina, ob tem pa ponudile nove inovativne funkcije, zato lahko govorimo o kripto valutah druge in tretje generacije. Te nove funkcije se nanašajo predvsem na uporabo novih mehanizmov soglasja (na primer dokazilo o vložku) in decentraliziranih računalniških platform, imenovanih pametne pogodbe, ki zagotavljajo bistveno drugačno funkcionalnost in omogočajo uporabo izven transakcij in denarnih funkcij.

4.1.1 Definicija kripto valut

Evropska centralna banka je kripto valute klasificirala kot podmnožico virtualnih valut in jih opredelila kot obliko nereguliranega digitalnega denarja, ki ga običajno izdajajo in nadzirajo njegovi razvijalci, uporabljajo in sprejemajo pa člani določene virtualne skupnosti (European Central Bank, 2012, str. 13). Poleg tega je dodatno pojasnila, da je mogoče razlikovati tri vrste virtualnih valut glede na interakcijo s tradicionalnimi valutami in gospodarstvom:

- virtualne valute, ki se lahko uporabljajo samo v zaprtem virtualnem sistemu, običajno v spletnih igrah;
- virtualne valute, ki so enostransko povezane z realnim gospodarstvom, saj obstaja menjalno razmerje za nakup valute (s tradicionalnim denarjem), kupljena valuta pa se lahko kasneje uporabi za nakup virtualnih izdelkov in storitev;

– virtualne valute, ki so dvostransko povezane z realnim gospodarstvo, saj obstajajo menjalni tečaji tako za nakup kot za prodajo virtualne valute.

Kripto valute spadajo v zadnjo vrsto, saj jih lahko kupimo in prodamo s tradicionalnim denarjem ter uporabimo za nakup digitalnih in realnih izdelkov in storitev. V novejšem poročilu je ECB predložila posodobljeno opredelitev virtualnih valut: opredeljene so kot digitalna predstavitev vrednosti, ki je ne izda centralna banka, kreditna institucija ali institucija za elektronski denar in ki se v nekaterih okoliščinah lahko uporablja kot alternativa denarju (European Central Bank, 2015, str. 7). Tako kot ECB je tudi Mednarodni denarni sklad razvrstil kripto valute kot podmnožico virtualnih valut. Opredeljuje jih kot digitalne predstavitve vrednosti, ki jih izdajo zasebni razvijalci in so denominirane v njihovi lastni obračunski enoti (International Monetary Fund, 2016, str. 7). Odbor za plačilne in tržne infrastrukture, organ Banke za mednarodne poravnave, je kripto valute kvalificiral kot digitalne valute ali sheme digitalnih valut (Committee on Payments and Market Infrastructures, 2015, str. 4). Te sheme naj bi imele naslednje ključne značilnosti: so sredstva, katerih vrednost je odvisna od ponudbe in povpraševanja, podobna blagu, kot je zlato, vendar z ničelno intrinzično vrednostjo; uporabljajo tehnologijo podatkovnih baz, ki omogoča oddaljeno izmenjavo elektronske vrednosti z enakovrednimi medsebojnimi komunikacijami v odsotnosti zaupanja med strankami in brez potrebe po posrednikih, ne upravlja jih noben posameznik ali institucija. Evropski bančni organ je predlagal, da se izraz kripto valute sklicuje na izraz virtualne valute. Te opredeljuje kot digitalne predstavitve vrednosti, ki jih ne izdaja niti centralna banka niti javni organ, niso nujno povezane s fiat valuto, ampak jih uporabljajo fizične ali pravne osebe kot sredstvo izmenjave in jih je mogoče prenesti, shraniti ali z njimi elektronsko trgovati (Enria, 2018, str. 3). Svetovna banka je klasificirala kripto valute kot podmnožico digitalnih valut. Opredeljuje jih kot digitalne predstavitve vrednosti, izražene v njihovi lastni obračunski enoti in različne od e-denarja, ki je preprosto digitalni plačilni mehanizem, izražen v fiat denarju. V nasprotju z večino drugih oblikovalcev politik je Svetovna banka sama definirala kripto valute kot digitalne valute, ki se zanašajo na kriptografske tehnike za doseganje soglasja (Natarajan, Krause & Gradstein, 2017 str. 5). Glede na navedene definicije je jasno, da v regulativnem prostoru ni splošno sprejete opredelitve pojma kripto valut, večina oblikovalcev politike pa se je vzdržala določitve izraza v celoti. Houben in Snyers (2018, str. 23) definicije kripto valut povzameta kot digitalno predstavitev vrednosti, namenjeno temu, da predstavlja peer-to-peer alternativo zakonitim plačilnim sredstev, ki jih izda vlada, je zavarovana z mehanizmom, imenovanim kriptografija, in se lahko pretvori v zakonito plačilno sredstvo ter se uporablja kot sredstvo za izmenjavo.

4.1.2 Omrežja in kripto valute prve generacije

Vsa omrežja in valute, uporabljene v teh omrežjih, so napisane v programskem jeziku C ++ in kot osnovo uporabljajo izvorno kodo omrežja Bitcoin z decentralizirano valuto, ki ne potrebuje zaupanja vredne tretje osebe (Abhishek, Pronaya, Arunendra & Atul, 2019, str. 3).

Prva generacija kot algoritem za soglasje uporablja dokaz o delu, kar dela ta omrežja relativno počasna, neučinkovita in draga, saj rudarstvo zahteva veliko količino električne energije. Zdi se, da Satoshi Nakamoto ni resno razmišljal o možni širši uporabi podatkovnih blokov, zato omrežje Bitcoin nima nekaterih pomembnih značilnosti omrežij druge in tretje generacije ter ima omejeno funkcionalnost (Investopedia.com, 2019d).

4.1.2.1 Bitcoin (BTC)

Omrežje Bitcoin je plačilno omrežje, ki deluje na podlagi kriptografskih protokolov, opisanih v prejšnjih poglavjih. Uporabniki pošiljajo in prejemajo monetarne enote, imenovane bitcoin, z oddajanjem digitalno podpisanih sporočil v omrežje z uporabo kriptografskih digitalnih denarnic. Transakcije se zabeležijo v porazdeljeno javno bazo podatkov z algoritmom soglasja, imenovanim dokaz o delu (Grinberg, 2011, str. 194). Kot omenjeno v poglavjih o delovanju podatkovnih verig, vsebujejo bloki podatke o transakcijah v omrežju. Kapaciteta obdelave transakcij v omrežju Bitcoin je omejena s povprečnim časom ustvarjanja novega bloka 10 minut in omejitvijo velikosti bloka na 1 megabajt. To omejujejo hitrost omrežja in sposobnost obdelave velike količine transakcij. Skupno število bitcoinov, ki jih je mogoče ustvariti z rudarjenjem, je omejeno, saj je sistem programiran tako, da bodo rudarji čez čas nagrajeni z vedno manj bitcoini in da v nobenem trenutku ne bo v obtoku več kot 21 milijonov bitcoinov (Nakamoto, 2009a). Ker je ustvarjanje in povečanje vrednosti avtomatizirano in omejeno s samim sistemom, pomeni, da ni potrebe po posredovanju centralnega subjekta za izdajo. Omejeno število bitcoinov skupaj z dejstvom, da so menjalni tečaji odvisni od ponudbe in povpraševanja, ne da bi vladni organ lahko posredoval, povzroča veliko nihanje vrednosti. Najvišja cena je bila 17. decembra 2017, ko je bil en bitcoin vreden 19.270 USD, v času pisanja tega dela pa je bila cena 7.232 USD (Bitinfocharts, 2019). Bitcoin je tipičen primer odprtega sistema brez dovoljenja (Natarajan, Krause & Gradstein, 2017, str. 8). Vsak se javnemu omrežju lahko pridruži ali ga zapusti po lastni volji, ne da bi to moral odobriti kateri koli subjekt. Vse, kar je potrebno, da se pridružimo omrežju Bitcoin in dodamo transakcije v knjigo, je računalnik, na katerem je bila nameščena ustrezna programska oprema.

4.1.2.2 Transakcije v omrežju Bitcoin

Kljub visoki stopnji volatilnosti cene ene enote bitcoin je število dnevnih transakcij v omrežju relativno stabilno in se je v času pisanja približevalo rekordnim ravnem s konca leta 2017, ko je bilo na dan opravljenih približno 400 tisoč transakcij (Bitinfocharts, 2019). V času pisanja je bilo na dan opravljenih približno 280 tisoč transakcij, v letu 2018 pa je bilo na dan povprečno približno 267 tisoč transakcij. Vse skupaj je bilo v letu 2018 opravljenih približno 81 milijonov transakcij v skupni vrednosti približno 2,2 trilijona USD. Kot omenjeno, je število transakcij, ki jih omrežje Bitcoin lahko procesira, omejeno tako s časom dodajanja novega bloka kot z velikostjo samega bloka, ki je bila v času pisanja 1 MB. Preprosta transakcija z enim inputom in enim outputom v omrežju Bitcoin predstavlja

velikost približno 192 bajtov (Tradeblock, 2015). Če predvidevamo polno zasedenost omrežja in povprečen čas nastanka novega bloka približno 10 minut, lahko izračunamo, da lahko omrežje na sekundo teoretično obdela maksimalno približno 8,7 transakcije. Ker pa omrežje Bitcoin pozna več različnih tipov transakcij, je bila v času pisanja povprečna velikost transakcij v omrežju 466 bajtov, kar se je odrazilo v teoretični sposobnosti obdelave maksimalno 3,6 transakcije na sekundo (Bitinfocharts, 2019). Transakcijske provizije so vključene v transakcijo, da bi transakcijo obdelal rudar in jo potrdilo omrežje (Singhal, Dhameja & Panda, 2018, str. 212). Ker je prostor, ki je na voljo za transakcije, v bloku trenutno umetno omejen, to pomeni, da je treba za hitro obdelavo transakcije ponuditi višjo transakcijsko provizijo kot drugi uporabniki. Uporabniki lahko sami določijo provizije, ki so jo pripravljeni plačati za izvedbo transakcije, seveda pa bodo rudarji tipično izbrali transakcije z višjimi provizijami. Večina sodobnih denarnic za bitcoin bo pregledala raven aktivnosti v verigi in samodejno zagotovila priporočeno provizijo. Provizije so neodvisne od višine zneska transakcije. Kot referenčna mera se tipično uporabljajo provizije, ki so potrebne, da se transakcija doda v prvem, tretjem in šestem bloku po izvedeni transakciji. V času pisanja so bile transakcijske provizije v omrežju Bitcoin naslednje (Bitcoinfees.info, brez datuma):

- pristojbina za oddajo transakcije v naslednjem bloku (10 minut): 0,290 USD,
- pristojbina za oddajo transakcije v treh blokih (30 minut): 0, 295 USD,
- pristojbina za oddajo transakcije v šestih blokih (60 minut): 0,113 USD.

Pri tehnologiji veriženja podatkovnih blokov so potrditve merilo, koliko novih blokov je bilo dodanih bloku s transakcijo. Več kot je potrditev, bolj varna je transakcija. V omrežju Bitcoin je za transakcije običajno potrebnih od 2 do 6 potrditev, da je transakcija veljavna (Coincentral.com, 2018). Ko je transakcija vključena v blok in tako pridobi prvo potrditev, je treba počakati približno 10 minut za vsako dodatno potrditev, po prvi potrditvi pa je čakalna doba za vsako dodatno potrditev popolnoma neodvisna od plačane transakcijske provizije. Zaradi potrebe po 6 potrditvah se transakcije v omrežju Bitcoin štejejo kot opravljene šele po 60 minutah. Ceno transakcijske provizije za bitcoin na koncu določata raven aktivnosti v verigi in hitrost, s katero naj bi se po uporabnikovi želji transakcija obdelovala. Če je omrežje preobremenjeno, bodo uporabniki morali za transakcijo plačati višjo provizijo.

4.1.2.3 SegWit

Segregated Witness oz. skrajšano na SegWit je predlagana posodobitev programske opreme omrežja Bitcoin, ki je namenjena odpravljanju določenih pomanjkljivosti v omrežju (Coindesk, 2018b). Namen je preprečiti transakcijske deformacije, omogočiti neobvezni prenos podatkov in obiti določene omejitve protokolov, kot je omejitev velikosti bloka z mehko razmejitvijo. Transakcijska deformacija (ang. transaction malleability) je postopek spreminjanja edinstvenega identifikatorja transakcije tako, da se najprej spremeni digitalni

podpis, uporabljen za njegovo izdelavo. SegWit to doseže z lajšanjem problema omejevanja velikosti bloka, ki zmanjšuje hitrost transakcij tako, da transakcijo razdeli na dva segmenta, pri čemer podatke o podpisu oz. podatke o priči (ang. witness data) odstrani iz izvirnega prvotnega segmenta in jih doda kot ločeno strukturo na koncu. Izvirni segment bi še naprej vseboval podatke o pošiljatelju in prejemniku, nova struktura (podatki o priči) pa bi vsebovala skripte in podpise. Podatki o podpisu bi bili ločeni od zapisa na Merklovem drevesu o tem, kdo pošilja ali sprejema bitcoine. To omogoča povečanje dovoljene velikosti bloka na maksimalno 4 MB. Posodobitev Segregated Witness je bila aktivirana 23. avgusta 2017 in v času pisanja se je približno 40 % vseh transakcij v omrežju obdelalo na vozliščih, ki podpirajo posodobitev (Bitinfocharts, 2019). Velikost transakcij se je po posodobitvi povečala na 328 bajtov za najbolj preprosto transakcijo in 570 bajtov za povprečno transakcijo. To po predvidevanju polne zasedenosti omrežja in velikosti bloka 4 MB omogoča obdelavo maksimalno 20,3 do 11,7 transakcij na sekundo.

4.1.2.4 Bitcoin Lightning Network

Mreža Lightning je izrecno zasnovana tako, da pomaga pri reševanju problema visokih provizij za majhna plačila, poleg tega pa povečuje celoten pretok transakcij. Je decentraliziran sistem za takojšnje velike količine mikroplačil in odpravlja tveganje prenosa skrbništva na zaupanja vredne tretje osebe (Poon & Dryja, 2016). Predstavlja plačilni protokol druge stopnje, ki omogoča hitre transakcije med sodelujočimi vozlišči in je na voljo kot rešitev problema razširljivosti omrežij, kot je Bitcoin. V njem je sistem peer-to-peer za obdelavo mikroplačil preko omrežja dvosmernih plačilnih kanalov brez prenosa skrbništva sredstev. Običajna uporaba mreže Lightning se nanaša na odprtje plačilnega kanala, tako da se primarna transakcija financiranja (ang. funding transaction) dodeli ustreznemu osnovnemu bloku, nato pa se izvede poljubno število tranksakcij na mreži Lightning, ki posodabljajo predhodno porazdelitev sredstev, ne da bi se predvajali celotni verigi. Nato sledi zaprtje plačilnega kanala z oddajanjem končne različice transakcije za distribucijo sredstev kanala. Plačilni kanali omogočajo udeležencem, da prenašajo denar drug drugemu, ne da bi morali vse svoje transakcije objavljati na podatkovni verigi.

4.1.2.5 Bitcoin Cash (BCH)

Bitcoin Cash predstavlja obliko trde razmejitve podatkovne verige (Houben & Snyers, 2018, str. 36). Je rezultat dveh različnih vizij o prihodnosti omrežja Bitcoin. Nekateri rudarji so želeli dvigniti omejitev velikosti bloka z 1 MB na 8 MB, da bi zmanjšali stroške transakcij, izboljšali potrditvene čase in povečali stopnjo razširljivosti. Ker skupnost ni mogla doseči soglasja, je nastalo novo omrežje Bitcoin Cash. Tako kot Bitcoin tudi Bitcoin Cash uporablja mehanizem PoW, kar pomeni, da je v njem mogoče rudariti. Posebnost omrežja Bitcoin Cash in neposredna posledica trde razmejitve je dejstvo, da je vsak uporabnik, ki je imel znesek kripto valute bitcoin v času razmejitve (1. avgust 2017, 13:16 UTC), prav tako postal lastnik istega zneska kripto valute bitcoin cash. Načeloma trda razmejitev ne spreminja narave

podatkovne verige, kar pomeni, da omrežje Bitcoin Cash deluje na odprti verigi tako kot omrežje Bitcoin. Zaradi dviga velikosti bloka na 8 MB se lastnosti omrežja izboljšajo v primerjavi z omrežjem Bitcoin, kar je razvidno v tabeli 6. Kljub temu pa se omrežje Bitcoin Cash ne more primerjati s tradicionalnimi plačanimi metodami. Kljub dvigu velikosti bloka se ta dejansko ni povečala, saj je dnevno povprečje velikosti blokov v omrežju Bitcoin Cash le 171 kB (Bitinfocharts, 2019). To tipično kaže na nizko stopnjo sprejetja in uporabe omrežja. Dodatna pomanjkljivost je centralizacija, ki je v nasprotju s splošnim načelom javnih podatkovnih verig, saj samo štiri rudarske skupine nadzorujejo približno 50 % celotnega omrežja, kar lahko vodi do prevzema omrežja z napadom 51 %.

4.1.2.6 Litecoin (LTC)

Kot Bitcoin je tudi Litecoin odprtokodna decentralizirana vrstniška kripto valuta, ki deluje na istoimenskem omrežju (Houben & Snyers, 2018, str. 37). Ustvarjena je bila oktobra 2011 in se od omrežja Bitcoin razlikuje na dva načina. Prvič, uporablja algoritem za soglasje, imenovan Scrypt, ki sicer temelji na osnovi PoW, vendar je zasnovan tako, da je specializacija strojne opreme bolj zapletena. Ker rudarstvo zahteva uporabo računalniškega pomnilnika, specializirana strojna oprema za rudarjenje ne deluje. To je pomembno, ker lahko teoretično pomaga decentralizirati omrežje, kar večjemu številu uporabnikov omogoča, da so v procesu rudarjenja konkurenčni. Čas, potreben za ustvarjanje bloka v omrežju Bitcoin, je približno 10 minut, medtem ko je povprečni čas izdelave bloka v omrežju Litecoin približno 2,5 minute (Hileman & Rauchs, 2018, str. 17). Zato je potrditev hitrejša in transakcije so cenejše, zaradi hitrejše obdelave transakcij pa je omrežje manj dovzetno za napad dvojne porabe. Drugič, skupna omejitev dobave kripto valute v omrežju Litecoin je s 84 milijoni kovancev kar precej višja od 21 milijonov omejitve dobave v omrežju Bitcoin. Omrežje Litecoin ima podobne slabosti kot druga omrežja, zgrajena na podlagi omrežja Bitcoin, saj je rudarjenje izrazito centralizirano. Samo trije rudarski bazeni namreč nadzirajo približno 50 % omrežja, zaradi česar je omrežje ranljivo za napad 51 %. Kljub temu da je omrežje manj dovzetno za dvojno porabo, pa zaradi kratkih časov med novimi bloki ni tako varno kot druga omrežja.

4.1.2.7 Ripple (XRP)

Ripple je ime plačilne mreže in plačilnega protokola, ki so ga ustvarili Arthur Britto, David Schwartz in Ryan Fugger (Houben & Snyers, 2018, str. 38). Leta 2012 ga je razvila in izdala družba z istim imenom, da bi omogočila varne, takojšnje in skoraj brezplačne globalne finančne transakcije. Za razliko od omrežja Bitcoin je izvorna koda tehnologije Ripple v zasebni lasti podjetja, kar pomeni, da je ne more preveriti noben zunanji uporabnik. Za razliko od mnogih drugih omrežij Ripple ni decentraliziran in je centralno nadzorovan kot del podjetja Ripple Labs Inc. To je zato, ker Ripple Labs Inc. določa, kdo lahko deluje kot validator transakcij v njegovem omrežju. Ripple je zelo priljubljena mreža, saj jo mnoge banke po vsem svetu uporabljajo kot osnovo za lastno infrastrukturo za poravnavo, njena

domača valuta XRP pa je v zadnjih petih letih stalno prisotna med prvimi petimi kripto valutami s tržno kapitalizacijo. Gre za digitalni valutni sistem, v katerem se transakcije preverjajo s konsenzom med člani mreže, ne pa z rudarskim procesom (Ripple Labs Inc., brez datuma). Nova različica sistema je bila zasnovana zato, da bi odpravili zanašanje omrežja Bitcoin na centralizirane borze, porabili manj energije in transakcije opravljali hitreje in ceneje. Sama veriga se šteje za javno, saj jo lahko uporablja kdor koli. Ripple prav tako ne temelji na tehnologiji veriženja podatkovnih blokov, ampak je samo oblika porazdeljenega podatkovnega skladišča, katere posebnosti javnosti niso znane. XRP za preverjanje transakcij uporablja svoj specifični konsenzni protokol, imenovan RPCA. Temelji na izboljšanju zakasnitve (ang. latencty), ki jo povzroča zahteva po sinhronizirani komunikaciji omrežnih vozlišč na javnih omrežjih, kot je Bitcoin. Ripple lahko obdela transakcije v 4 sekundah, v času pisanja je bila cena ene enote XRP 0,26 USD, število edinstvenih naslovov oz. uporabnikov pa zaradi zasebne narave podatkovne verige ni znano (Bitinfocharts, 2019). V letu 2018 je omrežje Ripple obdelalo približno 229 milijonov transakcij v skupni vrednosti približno 279 milijard USD. Iz tega lahko sklepamo, da je omrežje dejansko obdelalo le približno 7 transakcij na sekundo, kar je občutno manj, kot je teoretična zmožnost predelave 1500 transakcij, ki jo zagovarjajo razvijalci. Omrežje Ripple je znano po nizkih provizijah; v času pisanja je bila provizija okoli 0,0002 USD za transakcijo (Bitinfocharts, 2019).

4.1.3 Omrežja in kripto valute druge generacije

S premikom proti decentralizaciji omejene zmogljivosti omrežij prve generacije niso bile sposobne zadostiti potrebam splošne uporabe (Investopedia.com, 2019d). Leta 2013 je bilo razvito omrežje Ethereum, ki je podatkovna veriga z vgrajenim, Turing popolnim[5] programskim jezikom, ki podpira vse vrste transakcij, vključno z zankami. Zagotavlja virtualno abstrakcijo in vsak lahko ustvari lastna navodila za lastništvo in obliko transakcij ter določi funkcijo prehoda stanja. Ethereum je tako utrl pot pametnim pogodbam, majhnim računalniškim programom, ki živijo in se izvajajo v podatkovni verigi (Abhishek, Pronaya, Arunendra & Atul, 2019, str. 5).

4.1.3.1 Ethereum (ETH)

Ethereum je decentralizirana platforma, ki izvaja tako imenovane pametne pogodbe. Pametne pogodbe so pogodbe z lastnim izvajanjem ali aplikacije, ki se izvajajo natančno tako, kot je programirano, brez možnosti izpadov, cenzure, goljufije ali motnje tretjih oseb (European Commission, 2019, str. 56). Z uvedbo virtualnega stroja Ethereum (ang.

[5] V računalniški teoriji se pravi, da je sistem za manipulacijo podatkov Turing popoln, če ga lahko uporabimo za simulacijo katerega koli Turingovega stroja.

Ethereum virtual machine) in njegovega popolnega programskega jezika Solidity je Buterin razvijalcem ponudil možnost programiranja aplikacij, ki omogočajo pisanje prilagodljivih transakcij preko omrežja. Tako kot Bitcoin je Ethereum primer odprte verige in rudarji ustvarijo veljavne bloke, tako da porabijo električno energijo za iskanje rešitev za matematično uganko. Ethereumov algoritem za soglasje PoW, imenovan Ethash, se nekoliko razlikuje od tistega, ki ga uporablja omrežje Bitcoin. Omrežje načrtuje prehod na energijsko učinkovitejši protokol na PoS, imenovan Casper, v prihodnji izdaji programske opreme Ethereum, imenovane Serenity. Tehnično gledano, platforma Ethereum sama po sebi ni kripto valuta (Houben & Snyers, 2018, str. 33). Vendar pa Ethereum tako kot druge odprte verige zahteva obliko vrednosti za spodbujanje validacije transakcij v omrežju. Kripto valuta ether ne omogoča le, da se pametne pogodbe gradijo na platformi Ethereum, ampak deluje tudi kot sredstvo za izmenjavo. Velik del ethra so predhodno ustvarili oz. narudarili (ang. pre-mined) njegovi izumitelji in ga prodali, da bi plačali stroške razvoja. V času pisanja je bila cena ene enote ethra 189 USD, število pa za razliko od kripto valute bitcoin ni omejeno (Bitinfocharts, 2019).

4.1.3.2 Transakcije v omrežju Ethereum

V času pisanja je bilo v omrežju Ethereum na dan opravljenih približno 628 tisoč transakcij, v letu 2018 pa je bilo povprečno število transakcij na dan približno 688 tisoč (Bitinfocharts, 2019). Vse skupaj je bilo v letu 2018 opravljenih približno 251 milijonov transakcij v skupni vrednosti približno 428 milijard USD. V omrežju Ethereum je čas med bloki približno 15 sekund, velikost bloka pa temelji na kompleksnosti pogodb, znani kot omejitev plina (ang. gas limit) (Blockgeeks, 2018). Za vsako transakcijo ali pametno pogodbo, sklenjeno v omrežju, je potreben plin (ang. gas). Plin se uporablja v pogodbi za plačilo rudarjem, ki obdelujejo to transakcijo. Trenutno je največja velikost bloka okoli 7.999.992 plina, osnovne transakcije ali plačila z enega računa na drugega pa imajo kompleksnost 21.000 plinov, tako da lahko rudarji v blok vključijo približno 380 transakcij (Blockgeeks, 2018). S povprečnim časom dodajanja blokov okoli 15 sekund lahko omrežje obdela maksimalno približno 25 transakcij na sekundo, dejansko pa obdela le približno 7 transakcij na sekundo, saj vsi bloki niso popolnoma zapolnjeni. V skladu z belo knjigo Ethereuma bi moralo biti 7 novih dodanih blokov dovolj za potrditev transakcije (približno 2 minuti), ena največjih kripto borz Coinbase pa zahteva 50 potrditev, preden obravnava dokončanje transakcije (približno 12 minut). V času pisanja je bila povprečna transakcijska provizija okoli 0,14 USD (Bitinfocharts, 2019).

4.1.3.3 Pametne pogodbe

Pametna pogodba je niz obljub, določenih v digitalni obliki, s programom, ki uveljavlja pogodbo, vgrajeno v kodo. Pametne pogodbe se izvajajo na podlagi tehnologije veriženja podatkovnih blokov. Pametna pogodba je izvršljiva koda, ki se izvaja v podatkovni verigi za uveljavitev sporazuma med dvema ali več strankami (Natarajan, Krause & Gradstein,

2017 str. 29). Vsak ukaz, ki ga lahko izvede računalnik, lahko teoretično izpelje pametna pogodba. Transakcije ali podatki, zabeleženi na porazdeljenem podatkovnem skladišču, sprožijo pametno pogodbo, ukazi, ki jih izvedejo, pa so nato zapisani v porazdeljenem podatkovnem skladišču. Pametna pogodba je mehanizem, ki vključuje digitalna sredstva in dve ali več strank, pri katerih so nekatere ali vse stranke postavile sredstva, ki se samodejno prerazporedijo mednje v skladu s formulo, temelječo na nekaterih podatkih, ki v času, ko se začne pogodba, niso znani (Eze, 2018, str. 4). Pogodbe morajo biti preverljive za vsako vozlišče v omrežju, kar pomeni, da morajo vsa vozlišča v omrežju videti iste podatke. Pametne pogodbe pomagajo pri izmenjavi denarja, premoženja ali drugih sredstev na pregleden način, pri čemer se izogibajo storitvam posrednika, kot je banka, odvetnik ali notar. Ključna značilnost pametnih pogodb je, da ni mogoče manipulirati z njihovo vsebino in da njihovega izvajanja ni mogoče preprečiti. Pametna pogodba zmanjšuje razlike, ki se običajno pojavijo pri tradicionalni obdelavi pogodb, kar lahko privede do dragih tožb. Zaradi preglednosti, varnosti in učinkovitosti je to še posebej dobra izbira za preoblikovanje poslovanja, saj pogodbe ponujajo večjo komercialno učinkovitost, nižje transakcijske in pravne stroške, lahko odpravijo človeško pristranskost in zmanjšajo potrebo po odvetnikih. Pametne pogodbe pa niso imune na napake, saj tehnologija še ni popolnoma razvita, kar pomeni, da spekter možnih aplikacij ni v celoti raziskan.

4.1.3.4 Stellar (XLM)

Podobno kot Ripple je Stellar porazdeljena infrastruktura za izvajanje plačil, ki sta jo v začetku leta 2014 ustanovila dva od ustanoviteljev omrežja Ripple (Stellar Development Foundation, brez datuma). Omrežje ponuja izjemno hitre transakcije z zanemarljivimi provizijami in možnostjo neposredne izmenjave med različnimi valutami, rodilo pa se je kot trda razmejitev (ang. hard fork) protokola Ripple (Adams, 2018). Stellar je decentralizirano omrežje, Ripple pa centralizirano, ravno zato pa uporabniki, h katerim stremita obe omrežji (banke in druge finančne institucije), preferirajo Ripple.

Prvotno se je valuta, ki se uporablja v omrežju, imenovala stellar (STR), nato pa je bila preimenovana v lumens (XLM). Transakcije v omrežju Stellar imajo izredno majhno provizijo – v višini 0,00001 XLM, kar je okoli 0,000003 USD (Mazieres, 2016). Ta provizija deluje predvsem kot ukrep, da se prepreči, da bi uporabniki omrežje preplavili s transakcijami. Omrežje tipično velja za veliko bolj razširljivo, saj lahko v teoriji obdela več kot 1.000 transakcij na sekundo. To skupaj z zanemarljivimi provizijami pomeni, da je veliko primernejše za splošno uveljavljanje v svetu. Omrežje ne uporablja algoritmov za soglasje na podlagi PoW ali PoS, temveč uporablja lastni algoritem, imenovan Stellar Consensus Protocol. Stellar se lahko uporablja tudi za izgradnjo pametnih pogodb, omogoča pa tudi transakcije med valutami, kar pomeni, da lahko uporabnik pošilja plačila v želeni valuti, prejemnik plačila pa jih prejme v svoji želeni valuti.

4.1.4 Omrežja in kripto valute tretje generacije

Ker se uporaba pametnih pogodb vsak dan povečuje, tehnologija ne more podpreti takšnega obsega mikrotransakcij (Abhishek, Pronaya, Arunendra & Atul, 2019, str. 5). Čeprav je Ethereum izboljšal hitrost transakcij, za podporo današnjemu gospodarstvu še vedno ni dovolj učinkovit. Tretja generacija omrežij si prizadeva združiti najboljše vidike prve in druge generacije ter zagotoviti infrastrukturo, ki obravnava razširljivost, združljivost in trajnost. Glavne značilnosti so širša funkcionalnost in boljša zasnova, ki omogoča izogibanje težavam, kot je slaba razširljivost. Tipično ne uporabljajo algoritmov za soglasje PoW, ampak sodobnejše oblike, kot sta PoS in DPoS (Investopedia.com, 2019d).

4.1.4.1 EOS.IO

EOS.IO je omrežje, ki uporablja domačo kripto valuto EOS in poseduje večino atributov resničnega računalnika, vključno s strojno opremo z računalniškimi viri, ki so enakomerno porazdeljeni med nosilci kripto valut EOS (Block.one, 2018). Namen platforme je zagotoviti decentralizirano gostovanje aplikacij, ustvarjanje pametnih pogodb in decentralizirano shranjevanje poslovnih rešitev, ki rešujejo vprašanja razširljivosti ter odpravljajo vse provizije za uporabnike zaradi modela lastništva, po katerem je uporabnik upravičen do uporabe sredstev v omrežju, ki so enakovredna njegovemu deležu, brez potrebe po plačilu za vsako transakcijo. Omrežje to doseže tako, da lahko deluje na več računalniških jedrih, pa tudi z algoritmom za soglasje DPoS. Kripto valuta EOS zagotavlja pasovno širino (ang. bandwith) in shranjevanje v podatkovnih verigi v sorazmerju s celotnim vložkom (lastnik 1 % žetonov EOS dostopa do 1 % skupne razpoložljive pasovne širine). Žetoni EOS omogočajo lastniku, da glasuje in sodeluje pri upravljanju omrežja, ponovno v sorazmerju z lastniškim deležem. Kljub vsem omenjenimi značilnostim in prednostim pa omrežje ni brez pomanjkljivosti (CryptoRunner, brez datuma). Ker je bil EOS.IO zasnovan tako, da se zanaša na samo 21 proizvajalcev blokov, ki potrjujejo vse transakcije, lahko govorimo o zelo centraliziranem omrežju. Koncentracija proizvajalcev blokov omogoča, da EOS doseže visoko stopnjo obdelave transakcij, kar je mogoče, ker se morajo informacije o blokih širiti le skozi 21 vozlišč in ne skozi 18.000 vozlišč kot v omrežju Ethereum. Zelo majhno število proizvajalcev blokov in možnost majhne volilne udeležbe predstavljata veliko slabost omrežja, saj to ni decentralizirano in demokratično.

4.1.4.2 Cardano (ADA)

Cardano je pametna pogodbena platforma, ki jo razvija podjetje Input Output Hong Kong. Omrežje deli svoj protokol na dve plasti (Bhutoria, 2018, str. 3). Prva plast je Cardano settlement layer (CSL), kjer kot enota za štetje deluje kripto valuta ADA, druga pa Cardano computation layer (CCL) za izvajanje pametnih pogodb. Cardano je podobno kot Ethereum zasnovan in se še naprej razvija kot platforma, na kateri se lahko izvajajo pametne pogodbe in decentralizirane aplikacije (Houben & Snyers, 2018, str. 28). Poleg možnosti pošiljanja

vrednosti so imetniki kvalificiranega zneska kripto valute ADA upravičeni do izvolitve za vodjo v protokolu Ouroboros DPoS. Ouroboros je akademsko pregledan protokol, ki čas deli na epohe. Delegati, znani kot vodje, so izbrani za vsako epoho in vsak vodja je dodeljen delu epohe. Kdor ima kvalificirano količino kovancev ADA, je upravičen do izvolitve za vodjo. Izbirni postopek naključno izbere vrsto kovancev v dobavi kovancev in njihov lastnik je izbran za vodjo. Zato velja, da več kot je kovancev, večja je verjetnost, da bodo imeli zmagovalne kovance. Dokazilo o vložku Ouroboros preprečuje centralizacijo rudarjenja, saj odpravlja potrebo po kopičenju velikih količin računalniške moči za uspešno odstranjevanje blokov in izbiro voditeljev na podlagi sistema loterije. Cardano uporablja programsko kodo visoke stopnje zanesljivosti (ang. high assurance code) za izgradnjo platforme, da uporabniku omogoči uporabo zanesljive varnostne kode za izgradnjo pametnih pogodb na platformi, ki je podvržena formalnemu preverjanju, s čimer se zagotovi, da ne bo propadla, ko bo izvedena (Bhutoria, 2018, str. 5). Večina tveganj in izzivov izhaja iz dejstva, da je Cardano še vedno v procesu razvijanja (Bhutoria, 2018, str. 6). Razširljivost, združljivost in trajnost so še vedno daleč in se verjetno ne bodo uveljavile do leta 2019 ali 2020. Druga omrežja, kot je Ethereum, pa delajo na lastnem nizu izboljšav in učinkovitosti in imajo podoben časovni okvir. Če Cardano in Ethereum istočasno uvedeta izboljšave na področju razširljivost in zmogljivost, Cardano ne bo nujno bolj konkurenčna platforma.

4.1.5 Stabilni kovanci

Stabilni kovanci so oblika kripto valut, ki so stabilizirani glede na ceno (Berentsen & Schär, 2019, str. 65). To pogosto dosežejo z vezanjem na drugo realno sredstvo ali referenčno vrednost, kot je ameriški dolar. Ne izda jih centralna banka in uporabljajo različne mehanizme, ki zagotavljajo nizko volatilnost. Stabilni kovanci tipično uporabljajo programsko kodo in lastnosti obstoječih omrežji. Namen stabilnih kovancev je ublažiti in rešiti volatilnost, medtem pa kljub temu obdržati druge značilnosti kripto valut. Volatilnost je odvrnila kupce, vlagatelje in trgovce od tega, da sprejmejo kripto valute, saj predstavlja negotovo hrambo vrednosti in preveč niha, da bi bila uporabna kot obračunska enota. Zaradi visoke stopnje stabilnosti predstavljajo ti kovanci učinkovito in priročno sredstvo izmenjave in varčevanja. Nekateri strokovnjaki menijo, da so lahko dobra alternativa v državah z nestabilnimi gospodarstvi. Večja podjetja zdaj vidijo vrednost stabilnih kovancev in razvijajo svoja lastna omrežja in kripto valute (Reuters, 2019). Facebook je s partnerskimi podjetji razvil obliko stabilne kripto valute, imenovane libra, ki bo uporabnikom omogočala prenos denarja preko aplikacije Whatsapp. Globalna investicijska banka JP Morgan pa je izdala prvi bančni digitalni žeton, imenovan JPM Coin, ki bo uporabljen za takojšnjo poravnavo transakcij med strankami v njihovem veleprodajnem bančnem poslovanju.

4.1.5.1 Stabilni kovanci, zavarovani s fiat valutami

Prva razvrstitev stabilnih kovancev je bila zavarovana (ang. collateralized) oz. podprta s fiat valutami (Berentsen & Schär, 2019, str. 68). Zavarovanje se nanaša na zastavo določenega

sredstva s strani izdajalca, ki posamezniku za eno enoto USD (ali druge fiat valute) proda eno enoto zavarovanega stabilnega kovanca in obljublja, da drži rezervo v obliki fiat valute v vrednosti izdanih žetonov. V to kategorijo spadajo omrežja, kot so Tether, TrueUSD, Paxos, Stable in Circle. Ti projekti izhajajo iz obljube, da se vsak žeton izda na podlagi 1 : 1 z ustrezno valuto v rezervi. Centralizirana struktura zahteva določeno stopnjo zaupanja pri preverjanju in potrjevanju, da se rezerve v celoti ujemajo s količino žetonov. Prednosti so predvsem lahko razumljiva in enostavna struktura (Blockchain.com, 2018, str. 22). Fiat valute so stabilno sredstvo, saj jih (pravno) podpirata vlada in gospodarstvo države, kar zagotavlja, da osnovne cene ne bodo veliko nihale. Slabosti so predvsem centraliziranost, ki vodi k pojavu različnih slabosti in tveganj, kot so enotna točka neuspeha, stečaj centralnega subjekta in pojav moralnega tveganja (ang. moral hazard). Poleg tega je za popolno delovanje sistema treba zaupati osrednjemu subjektu, kar je v nasprotju z načelom kripto valut. V centraliziranem sistemu rezerv, ko posamezniki izgubijo zaupanje v centraliziran subjekt, bodo verjetno likvidirali svoja sredstva.

4.1.5.2 Stabilni kovanci, zavarovani s kripto valutami

So stabilni kovanci, ki so zavarovani z drugimi kripto valutami, ponavadi s tistimi, ki imajo visoko stopnjo tržne kapitalizacije, kot so bitcoin ali ethereum (Berentsen & Schär, 2019, str. 69). Značilno je, da so podprti z mešanico kripto valut, ne samo ene kripto valute, kar omogoča boljšo porazdelitev tveganja, saj je tveganje volatilnosti za posamezno kripto valuto precej višje kot tveganja za kombinirano skupino kripto valut. Najpogostejša oblika te vrste stabilnih kovancev zahteva od uporabnikov, da vložijo in zaklenejo določeno količino kripto valut v pametno pogodbo, ki nato uravnava razmerje med stabilnimi kovanci in kripto valutami. Tako kot tradicionalne kripto valute imajo decentralizirano strukturo, ki ne temelji na podlagi zaupanja in je pregledna ter varna. Je učinkovita, saj se pretvorba kripto valut v stabilne kovance zgodi hitro, ker se transakcija izvede na podatkovni verigi. Ker je vsaka transakcija zabeležena v javni verigi, omogoča popolno preglednost in odgovornost. Slabost je primarno predvsem sama volatilnost; ker je osnovno sredstvo samo kripto valuta, je po naravi veliko bolj volatilna od drugih sredstev, kot so blago ali fiat denar.

4.1.5.3 Algoritemski stabilni kovanci

So edina kategorija stabilnih kovancev, ki niso zavarovani z nobenim sredstvom, saj uporabljajo algoritemsko voden pristop k širitvi in krčenju dobave denarja iz kovancev, tako kot centralna banka s tiskanjem denarja (Blockchain.com, 2018, str. 14). Ko se skupno povpraševanje po kovancih povečuje, se ustvari nova ponudba stabilnih kovancev za znižanje cene na stabilne ravni. Glavni cilj je, da se cena kovanca čim bolj približa 1 USD. Ker so vse prilagoditve narejene na podatkovni verigi, so vsi podatki shranjeni v zaupljivi, pregledni in varni podatkovni bazi. Ker se vrednost samodejno prilagodi glede na tržno povpraševanje in ponudbo, bodo cene ostale stabilne.

4.1.6 Primerjava kripto valut

Razlike med valutami so velike v vseh dimenzijah. Medtem ko so transakcijske provizije in povprečni transakcijski časi kazalniki, ki vplivajo na zadovoljstvo strank, je zmogljivost omrežja, da obdela veliko število transakcij, pomemben kazalnik sposobnosti kripto valute za razširljivost. V tabeli 7 je prikazana primerjava najbolj razširjenih kripto valut glede na transakcijsko provizijo, povprečni transakcijski čas, teoretično in dejansko število transakcij na sekundo, volumen transakcij v letu 2018 in algoritem soglasja, ki ga omrežje uporablja. Stabilni kovanci načeloma delujejo z uporabo omrežja že obstoječe kripto valute in imajo tako praktično identične lastnosti, prednosti in slabosti. Iz tabele 7 je prav tako razvidno, da je največja kripto valuta, bitcoin, stalno razvrščena med valute z najslabšimi lastnostmi. Pomemben razlog za to je lahko, da je bil bitcoin pionir in njegovi nasledniki so lahko svoje valute ustvarili po analizi moči in slabostih bitcoina.

Tabela 7: Primerjava kripto valut

	Povprečna Provizija (v USD)[6]	**Povprečni transakcijski čas**	**Teoretično število transakcij na sekundo**	**Dejansko število transakcij na sekundo v letu 2018**	**Število transakcij v 2018**	**Vrednost transakcij v 2018 (v USD)**	**Algoritem soglasja**
Bitcoin	0,797	60 minut	8,7	2,5	81 milijonov	2,2 trilijona	PoW
Ethereum	0,173	6 minut	25	7,69	251 milijonov	815 milijard	PoW
Bitcoin Cash	0,003	60 minut	116	0,71	22 milijonov	215 milijard	PoW
Ripple	0,0002	4 sekunde	1500	7,29	229 milijonov	279 milijard	RPCA
Litecoin	0,025	30 minut	56	0,4	12 milijonov	129 milijard	PoW
Stellar	0,0000025	5 sekund	1000	0,02	563 tisoč	321 milijonov	SCP
EOS	Brez	1,5 sekunde	3996	26	825 milijonov	25 milijard	DPoS
Cardano	0,0074	5 minut	250	0,02	650 tisoč	137 milijard	PoS

Vir: Bitinfocharts(brez datuma); Coinmetrics (brez datuma); Lastni izračuni.

4.2 Digitalni žetoni

Z izrazom tokenizacija (ang. tokenization) je mišljen proces prenosa pravic, povezanih z realnimi sredstvi, v digitalno obliko teh sredstev v obliki žetonov (ang. token) v podatkovno verigo (Chen, 2018, str. 61). Žetoni v podatkovni verigi lahko predstavljajo široko paleto omejenih sredstev, kot so valute, vrednostni papirji, nepremičnine, točke zvestobe itd. Imajo običajno fiksno ponudbo ali sledijo preglednemu načrtu dobave, zaradi česar so protiinflacijski. Poleg tega jih je mogoče prenašati brez vključitve osrednjega subjekta in je

[6] Drseče 90-dnevno povprečje v obdobju 5.9.-5.12.2019

z njimi mogoče trgovati na digitalnih borzah (Jafery, 2018). Tipično se postopek tokenizacije začne na specializiranih platformah za izdajanje žetonov, kot je Polymath, ki zagotavlja tehnične in pravne rešitve za listinjenje (ang. securitization) delnic, obveznic ali drugih sredstev na podatkovni verigi in ima industrijska partnerstva s sekundarnimi trgi, kot je tZero, kar zagotovi likvidnost za vrednostne žetone, ki so bili izdani v verigi Polymath. Likvidnost nato omogočajo platforme za trgovanje oz. sekundarni trgi (European Commission, 2019, str. 58). Trenutno sta največji taki platformi tZero in Sharespot. Poleg startup podjetij pa se za vstop na področje tokenizacije odločajo tudi uveljavljena podjetja na finančnem področju. Nasdaq, druga največja borza na svetu, namreč razvija platformo za izdajanje vrednostnih žetonov in trgovanje z njimi (Brawenewcoin, 2018). V nasprotju z valuto vrednostni žeton ni vezan na podatkovno verigo, ampak je ustvarjen na vrhu verige in urejen s pametno pogodbo.

4.2.1 Storitveni žetoni (ang. utility tokens)

Uporabniku omogočajo dostop do izdelka ali storitve, uporabljajo se samo za delovanje znotraj zaprtega ekosistema in niso zasnovani kot naložbe (Smith, 2019, str. 7). Uporabnostni žetoni se lahko obravnavajo kot inačica kuponov ali drugih sredstev, s katerimi lahko vlagatelji dostopajo do blaga in storitev. Čeprav se ti žetoni lahko izdajo kot del postopka zbiranja kapitala, sami žetoni njihovim imetnikom ne dajejo nobenih možnosti, da bi dobili pravico do deleža dobička ali kakršne koli besede o tem, kako bo organizacija upravljana. Storitvene žetone lastniki unovčijo za dostop do blaga in storitev organizacije, ki bi jih sicer plačali v gotovini. Žeton daje uporabniku dostop ali privilegije notranjega omrežja, skupaj s katerim koli izdelkom ali storitvami, ki jih omrežje ponuja. Premoženjski žetoni pridobijo svojo vrednost iz vrednosti sredstva, storitveni žetoni pa pridobijo vrednost iz vrednosti izdelka, ki ga zagotavlja njegova zaprta mreža.

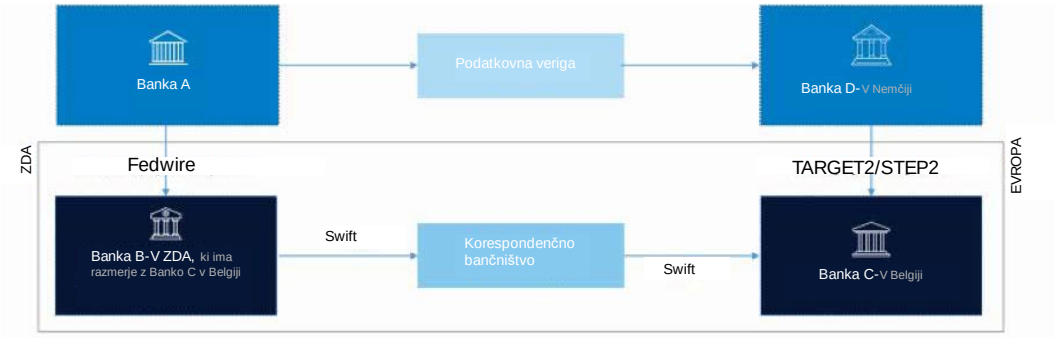
4.2.2 Premoženjski žetoni (ang. security token)

Predstavlja dejansko lastništvo sredstva in se lahko uporablja kot gospodarska enota za poslovanje, ki poteka v omrežju, vlagatelji pa lahko od njih pričakujejo dobiček (Smith, 2019, str. 9). V bistvu so enakovredni izdajanju lastniških deležev po postopku uvrstitve delnic v prvo kotacijo. Nanje lahko gledamo kot na obliko lastniških papirjev, saj je lastnik oz. vlagatelj upravičen bodisi do deleža dobička organizacije bodisi lahko upravičeno pričakuje, da bo izvajal neko stopnjo upravljavskega nadzora. Izdajatelji v zadnjem času premoženjske žetone raje kot po nereguliranem postopku prve izdaje žetonov izdajajo s specializiranim postopkom, imenovanim ponudba vrednostnih žetonov (ang. security token offering). Ti se pojavljajo kot bolj legitimna možnost, kot sheme prve izdaje žetonov, saj je za sheme ponudbe vrednostnih žetonov obvezno, da jih odobri Komisija za vrednostne papirje (SEC), kar pomeni, da so značilno bolj varni pred goljufijami (U.S. Securities and exchange commission, brez datuma).

4.3 Plačilni sistemi

Tehnologija veriženja podatkovnih blokov omogoča finančnim institucijam, da ustvarjajo neposredne povezave in se izogibajo korespondenčnemu bančništvu (Miller in drugi, 2019, str. 43). Z vzpostavitvijo porazdeljenega omrežja za mednarodno poravnavo lahko veriženje podatkovnih blokov odstrani neučinkovitost sedanjega sistema in ponuja možnosti za znatno znižanje stroškov, zlasti na čezmejnem medbančnem delu transakcije. Z znižanjem stroškov poravnave in povečanjem učinkovitosti medbančnih in čezmejnih prenosov bi lahko tehnologija še pomembneje pripomogla k optimizaciji procesa obdelave in poravnave plačil. Proces je prikazan na sliki 9: tehnologija porazdeljenih podatkovnih baz podpira vse transakcije, brez potrebe po centralni entiteti. To pomeni, da bi lahko transakcije poravnali neposredno med banko pošiljatelja in prejemnika, in to z uporabo porazdeljenih podatkovnih baz, kar bi pomagalo znižati stroške vzdrževanja mreže korespondenčnih bank, pri tem pa se nam ne bi bilo treba zanašati na mrežo skrbniških storitev in korespondenčnih bank.

Slika 9: Sistem plačil preko podatkovnih verig



Vir: Infosys (2018).

Aprila 2018 je Banco Santander postala prva mednarodna banka, ki je zagotavljala čezmejna plačila s protokolom, ki ga je razvil Ripple, temu so sledile številne druge mednarodne finančne institucije (European Commission, 2019, str. 59). SWIFT, se je na to odzval s povečanjem hitrosti in učinkovitosti sistema in široko različno testiral integracijo tehnologije v svoje sisteme. Med letoma 2017 in 2018 je SWIFT izvedel obsežen test uporabe tehnologije in dokaza koncepta (ang. proof of concept), rezultati takšnih testov, ki jih je izvedlo 34 bank, pa kažejo učinkovite koristi z uporabo tehnologije v realnem času, posebej povezane s poročanjem in upravljanjem likvidnosti, popolno sledljivost transakcij in poenostavljeno usklajevanje po računih.

4.3.1 Ripple

Podjetje Ripple je najpomembnejši igralec, ki poskuša zamenjati sistem korespondenčnega bančništva in uporabo omrežja SWIFT (Zhang, Qiu & Gao, 2019, str. 432). Najbolj poznano je po svoji kripto valuti XRP in ločeno od bančnih produktov. Je istočasno sistem bruto

poravnave v realnem času, menjalnica valut in mreža za izvajanje čezmejnih nakazil. Ripple je najbolj znan kot orodje, ki lahko odpravi bančne neučinkovitosti, saj služi kot porazdeljeni plačilni protokol, ki temelji na podatkovni verigi, kar omogoča takojšnje in poceni transakcije med različnimi bankami in finančnimi institucijami. RippleNet je globalna mreža bank in finančnih institucij, ki lahko pošiljajo in prejemajo plačila z uporabo porazdeljene finančne tehnologije (Ripple Labs Inc., 2017). Zasnovan je tako, da zagotavlja plačila v realnem času z nizkimi stroški, saj služi kot enotna decentralizirana globalna mreža. Z odstranitvijo razdrobljenosti pri obdelavi plačil lahko nudi učinkovito obdelavo brez točk trenja. xCurrent je programska rešitev podjetja Ripple, ki omogoča bankam, da takoj poravnajo čezmejna plačila s sledenjem od začetka do konca (Ripple Labs Inc., 2017). S pomočjo xCurrent se banke v realnem času medsebojno obveščajo, da potrdijo podatke o plačilu pred začetkom transakcije in potrdijo poravnavo. xCurrent temelji na odprtem in nevtralnem protokolu Interledger, ki omogoča medsebojno delovanje med različnimi podatkovnimi bazami in omrežji. Ponuja kriptografsko varen plačilni tok s prenosljivostjo transakcij in minimizacijo potrebnih informacij. Zasnovan je tako, da je v skladu z zahtevami banke glede tveganj, zasebnosti in skladnosti in se prilega obstoječi infrastrukturi banke, kar povzroči minimalne stroške integracije in motnje v poslovanju.

4.3.2 Libra

Libra je svetovna digitalna valuta in finančna infrastruktura, ki jo je v sodelovanju s številnimi globalnimi vodilnimi podjetji razvilo globalno podjetje Facebook in naj bi se začela uporabljati leta 2020 (Libra Association, brez datuma). Zgrajena je na odprtokodni istoimenski podatkovni verigi, katere cilj je, da služi kot trdna osnova za finančne storitve, vključno z novo svetovno valuto, ki lahko zadovolji dnevne finančne potrebe milijard ljudi. Upravljanje projekta, valute in transakcij bo kriptografsko zaupano združenju Libra (ang. Libra Association), članski organizaciji, ki so jo ustanovili hčerinska družba podjetja Facebook, Calibra in 27 drugih vodilnih podjetij na področju plačil, tehnologije, telekomunikacij, spletnega trga, tveganega kapitala in neprofitnih organizacij. Trije ključni dejavniki pri zasnovi podatkovne verige Libra so oblikovanje in uporaba programskega jezika Move, uporaba lastnega algoritma za soglasje, odpornega na bizantinske tolerance napak LibraBFT, ter sprejemanje in podvajanje široko sprejetih podatkovnih struktur v obliki Merklovih dreves (CNET, 2019). Načrt je, da se istoimenski digitalni žeton podpre z realnimi finančnimi sredstvi, kot so košarica valut in ameriški zakladniški vrednostni papirji, da bi se izognili volatilnosti, zato bo vsak izmed začetnih partnerjev in članov združenja Libra vložil začetnih 10 milijonov ameriških dolarjev. Partnerji bodo v okviru združenja ustvarili nove enote valute na podlagi povpraševanja, enote valute pa bodo uničene, ko bodo unovčene za običajno valuto. Ker gre za konzorcijsko podatkovno verigo, se Libra ne bo zanašala na rudarjenje kripto valut, transakcije bodo lahko obdelali in potrdili samo člani združenja tehtnic. Združenje upa, da bo v petih letih začelo prehod na PoS, čeprav priznavajo, da ne obstaja rešitev, ki bi lahko zagotovila obseg, stabilnost in varnost, potrebno za podporo milijardam ljudi in transakcijam po vsem svetu. Začetna uskladitev transakcij bo

opravljena pri vsakem partnerju, za usklajevanje pa bo uporabljena tehnologija porazdeljenih digitalnih skladišč. V nasprotju s kripto valutami, kot je bitcoin, ki uporabljajo algoritme za soglasje, Libra ni decentralizirana, saj se zanaša na zaupanje v združenje kot dejansko centralno banko (BBC, 2019). Projekt se je soočil s kritikami in nasprotovanjem regulatorjev in centralnih bank, saj strokovnjaki dvomijo o tem, ali bo Libra svojim uporabnikom zagotavljala dovolj visoko stopnjo zasebnosti (Bloomberg, 2019a). Večina kritik se nanaša zlasti na pomanjkanje regulatornega okvira za kripto valute in podatkovne verige ter na škandale podjetja Facebook pri upravljanju zasebnih podatkov uporabnikov. Jerome Powell, predsednik FED, je pred kongresom povedal, da ima FED resne pomisleke o tem, kako bi se Libra spoprijela s »pranjem denarja, zaščito potrošnikov in finančno stabilnostjo« (New York Times, 2019).

4.3.3 IBM World Wire

V letu 2019 je IBM ustvaril globalno plačilno omrežje v realnem času za podporo čezmejnim transakcijam in deviznemu poslovanju v več kot 50 državah z uporabo digitalnih sredstev v obliki stabilnih kovancev (Forbes, 2019b). IBM Blockchain World Wire bo pomagal finančnim institucijam izboljšati storitve, ki jih zagotavljajo svojim potrošnikom z optimizacijo in pospeševanjem transakcij, čezmejnih plačil in nakazil. Omrežje World Wire trenutno deluje z uporabo kripto valute v omrežju Stellar, imenovane lumens (XLM), in lastnega stabilnega kovanca, vezanega na ameriški dolar (IBM, 2018). World Wire služi kot omrežni ponudnik za mednarodna plačila, kar omogoča direktni prenos, ne pa zapletenosti običajnega korespondenčnega bančništva. World Wire trenutno omogoča plačila v 72 državah z 48 valutami, šest mednarodnih bank, tudi Bank Busan in Rizal Commercial Banking Corporation, pa je že podpisalo pisma o nameri za izdajo svojih stabilnih kovancev na platformi. Po regulatorni odobritvi bo platforma World Wire dodala stabilne kovance, vezane na evro, indonezijski rupij, filipinski peso, korejski von in brazilski real. Protokol zagotavlja razširljivost, potrebno za podporo v obsegu tisoč transakcij na sekundo.

4.3.4 JPM Coin

JP Morgan Chase, globalna bančna in finančna služba je napovedala razvoj novega stabilnega kovanca JPM Coin, ki je vezan na ameriški dolar in načrtuje uvajanje v plačilne poravnave v tem letu (Bloomberg, 2019b). JPM Coin bo zgrajen na zasebni podatkovni verigi Quorum, ki je zasebna oblika omrežja Ethereum. JPM Coin naj bi bil sprva usmerjen v obdelavo velikih mednarodnih poravnav, izvajanje transakcij z vrednostnimi papirji in zamenjavo uporabe dolarjev v operacijah zakladniških storitev podjetja (JPMorgan Chase, 2019). Zanašal se bo na depozitni sistem, v katerem bodo žetoni dostopni šele, ko bo banka položila depozit. Na tej točki lahko stranke uporabijo žetone za plačila, ki temeljijo na veriženju podatkovnih blokov. Podjetje bo uničilo potrebno količino žetonov, ko bodo stranke izplačale svoje kovance. Projekt JPM je veliko bolj evolucijski kot revolucionaren.

Glavna prednost kovanca JPM Coin je dejstvo, da je njegova vrednost vezana na dolar, zaradi česar je stabilen medij za izmenjavo.

4.3.5 R3 Corda

Konzorcij R3 želi postaviti nov operativni sistem za finančne trge (Coindesk, 2018a). Rezultat razvoja konzorcija je odprtokodna platforma na podlagi tehnologije porazdeljenih podatkovnih baz, imenovane Corda, namenjene finančnemu svetu, ki obravnava zapletenejše transakcije in omejuje dostop do podatkov o transakcijah. Cilj Corde je zagotoviti platformo s skupnimi storitvami, da se zagotovi, da so vse storitve združljive med udeleženci omrežja, še vedno pa spodbujajo inovativnost in hitrejši čas obdelave, saj bi osnovno infrastrukturo sprejela in razumela obstoječa podjetja. SWIFT je napovedal, da načrtuje povezavo Corde s svojim razvojnim okvirom Global Payments Innovation. Povezava bo omogočala uporabnikom SWIFT, da lahko poravnajo čezmejna plačila preko tehnologije porazdeljenih podatkovnih baz.

5 PREDNOSTI IN SLABOSTI TEHNOLOGIJE

Sistemi, ki temeljijo na tehnologiji porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, imajo pred tradicionalnimi centraliziranimi podatkovnimi strukturami številne prednosti (Golosova & Romanovs, 2018, str. 2). Zaradi raznolikosti in specifičnosti posameznih sistemov je težavno doseči visoko stopnjo generalizacije prednosti tehnologije. Poleg večje decentraliziranost in transparentnosti omogoča tehnologija veriženja eliminacijo potrebe po centralni avtoriteti in zaupanju med uporabniki v omrežju (Bashir, 2018, str. 36). Lastnost decentraliziranosti, eliminacije potrebe po centralni avtoriteti in predvsem anonimnosti pa težko apliciramo na finančni sektor zaradi visoke stopnje potreb po identifikaciji, regulaciji in ustreznosti. Kljub določenim lastnostnim, ki jih je možno obravnavati kot prednosti, imajo omrežja, ki uporabljajo tehnologijo porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, še vedno številne slabosti.

5.1 Prednosti tehnologije

5.1.1 Decentralizacija

Tehnologija omogoča neposreden prenos sredstev med dvema nasprotnima strankama in decentralizirano vodenje evidenc, s čimer se odpravi potreba po posredniku ali osrednjem organu, ki nadzoruje podatkovno bazo (Natarajan, Krause & Gradstein, 2017, str. 14). To v teoriji pomeni nižje stroške, večjo varnost in hitrejši čas obdelave podatkov. Vsi uporabniki, ki se pridružijo omrežju, brez potrebe po dovoljenju, lahko sodelujejo pri overjanju podatkov in oblikujejo porazdeljen sistem potrjevanja transakcij. Za razliko od centraliziranega sistema imajo vozlišča v porazdeljenem peer-to-peer sistemu enako omrežno moč in v okolju

med njimi ni bistvene razlike, saj imajo enake pravice in obveznosti. Vsako vozlišče mora upoštevati enaka pravila, da lahko skupaj vzdržujejo zapise podatkov v celotnem omrežju. Poleg teh prednosti, velja izpostaviti še povečano učinkovitost in hitrost z odstranjevanjem trenja, ki nastaja pri izvajanju transakcij ali pri postopkih obračuna in poravnav, saj se odstranijo posredniki, postopek pa se avtomatizira. Veriženje podatkovnih blokov je tudi stroškovno učinkovito, saj ima velik potencial pri znižanju stroškov, ker odpravi potrebo po spravi in usklajevanju. Podatki, ki so v verigi, predstavljajo absolutno resnico, zato jih ni treba usklajevati. Potencialni prihranki so možni tudi zaradi nižjih stroškov vzdrževanja infrastrukture, človeških delovnih ur in preprečevanja goljufij.

5.1.2 Transparentnost

Tehnologija omogoča visoko stopnjo transparentnosti zaradi dejstva, da imajo vsi uporabniki v lasti kopijo podatkovne baze (Schneider in drugi, 2016, str. 9). Do sprememb lahko pride le, ko se doseže soglasje v skladu s pravili omrežja, spremembe pa so nato posredovane celotnemu omrežju. Spremembe podatkovnih baz se v obliki blokov dodajo v podatkovno verigo, podatki v blokih pa morajo biti identični za vse uporabnike, kar v praksi pomeni, da lahko številni različni udeleženci v omrežju dostopajo do istih podatkov. To pomembno poveča stopnjo transparentnosti v primerjavi z obstoječimi sistemi, pri katerih lahko administrator omeji dostop do celotnega ali določenega dela podatkov. Vsak lahko pregleduje podatke o podatkovni verigi in razvija aplikacije preko skupnega vmesnika. Take stopnje preglednosti v finančnih sistemih doslej še ni bilo, zlasti v zvezi z velikimi podjetji. Dodaja se stopnja odgovornosti, ki je doslej prav tako še ni bilo. Viri podatkov in upravljanje pripadajo vsem vozliščem, ki se pridružujejo sistemu oz. omrežju, subjekti zunaj sistema pa so blokirani. Kot pri tehnologiji porazdeljenih podatkovnih baz so vsi zapisi podatkov in operacije v sistemu pregledni za vsa vozlišča v omrežju (Lin & Liao, 2017, str. 654). Tehnologija veriženja podatkovnih blokov zagotavlja visoko stopnjo preglednosti podatkov s kombinacijo asimetričnega šifriranja in zgoščevalnih funkcij. Postopki, pravila in metode dostopa do omrežja so javni, kar zagotavlja, da so vsa vozlišča sposobna pregledati podatke, zabeležene v podatkovni verigi, in jim slediti. Eden od primerov, ki ga najpogosteje uporabljajo, je upravljanje dobavnih verig (ang. supply chain management). Tehnologija lahko omogoča neprekinjeno sledenje v celotni dobavni verigi. To pomeni, da lahko potrošniki natančno vedo, kaj vsebuje njihova hrana, ali gre za ekološko in pošteno trgovino, ali je njihovo blago pristno, ali je pridelano v skladu s pravicami delavcev. To ni koristno samo za potrošnika, saj so lahko popolnoma prepričani, od kod prihajajo izdelki in kaj vsebujejo, temveč tudi za podjetje, ki proizvaja izdelke. Takšna preglednost pomaga ohraniti integriteto podjetja z zmanjšanjem škandalov v proizvodnji.

5.1.3 Eliminacija potrebe po zaupanju

Ker se tehnologija veriženja podatkovnih blokov izvaja v decentraliziranem sistemu, za prenos podatkov med vozlišči v omrežju ni potrebno vzajemno zaupanje med udeleženci

(Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016, str. 6). Podatkovna veriga temelji na načelih porazdeljenih peer-to-peer sistemov in kriptografije z uporabo decentraliziranih struktur, ki tvorijo zaupanja vreden odnos med vozlišči in porazdeljenimi sistemskimi strukturami, brez potrebe po zaupanju posameznemu vozlišču. Algoritmi za doseganje soglasja omogočajo, da se soglasno in varno dogovori o tem, kaj je treba dodati v porazdeljeno podatkovno bazo, hkrati pa zagotavljajo njeno integriteto. Ker ti algoritmi predstavljajo osnovo za zaupanje, omogoča odstranitev centralne avtoritete in posrednikov ter posledično znižanje skupnih stroškov transakcije.

5.1.4 Nepokvarljivost in preverljivost

Veriženje podatkovnih blokov v teoriji zagotavlja nepokvarljivo in preverljivo sled transakcij katerega koli digitalnega ali fizičnega sredstva, ki jo je mogoče zlahka revizijsko preveriti (Natarajan, Krause & Gradstein, 2017, str. 15). Tehnologija veriženja podatkovnih blokov uporablja specifične podatke in časovne žige v blokih za identifikacijo in beleženje vsake transakcije, kar vozlišču omogoča, da vodi vrstni red transakcij in omogoča sledljivost podatkov. Časovni žig ne zagotavlja samo izvirnosti podatkov, ampak tudi zmanjšuje stroške sledljivosti transakcij (Lin & Liao, 2017, str. 655). Hkrati okrepi nepovratne spremembe podatkov ali informacij. Transakcije mora pregledati večina vozlišč sistema, preden jih je mogoče dodati. Tudi če ima napadalec zmogljive računalniške zmogljivosti, je zapis izjemno težko spremeniti; do tega lahko pride le, če napadalec nadzoruje 51 % ali več celotnega omrežja. Ta funkcija zagotavlja, da je sistem stabilen in zanesljiv, ter reši težave z dvojno porabo.

5.2 Slabosti tehnologije

Zaradi relativne novosti in nezrelosti tehnologije veriženja podatkovnih blokov so z uporabo povezani številni izzivi in tveganja, ki jih bo v prihodnosti treba odpraviti. Kljub številnim potencialnim aplikacijam na raznovrstnih področjih je trenutno še nejasno, ali bo veriženje podatkovnih blokov sposobno zagotoviti prednosti pred obstoječo tehnologijo in kako znatne bodo te prednosti.

5.2.1 Primernost

Podjetja iz različnih sektorjev so navdušena nad tehnologijo in njenim potencialom za poganjanje digitalne transformacije ob reševanju problemov iz resničnega življenja (Umeh, 2016, str. 59). Kljub temu pa napovedi, ki predvidevajo uporabo tehnologije v skoraj vsakem projektu, ne razumejo temeljnih razlogov za uporabo, zlasti z vidika upravljanja podatkov. Če ni potrebe po shranjevanju podatkov, tehnologija ne bo dodala nobene vrednosti že uveljavljenim tehničnim rešitvam (Casino, Dasaklisb & Patsakisa, 2019, str. 68). Če je v določenem sistemu predviden le ena entiteta, ki dodaja podatke, ta tehnologija tudi ne bo

zagotovila dodatnih jamstev v primerjavi z navadno bazo podatkov, saj bi bila ta najverjetneje primernejša izbira, zlasti z vidika hitrosti transakcij. Tehnologija je primerna, kadar se pokaže potreba po transakcijah med nezaupljivimi uporabniki ali po stalnem zgodovinskem zapisu. Na primer: če obstaja potreba, da sodeluje več subjektov, ki si med seboj ne zaupajo ter spreminjajo stanje sistema in vplivajo nanj, je lahko veriženje podatkovnih blokov primerna rešitev.

5.2.2 Razširljivost

Razširljivost zadeva sposobnost obdelave velikega števila transakcij v katerem koli omrežju. Za množično uporabo podatkovnih verig morajo te biti sposobne obravnavati scenarij, v katerem je v omrežju na milijone uporabnikov. Stopnja razširljivosti je pomembna, ker narekuje morebitno zmogljivost vsakega omrežja, saj zagotavlja hitro delovanje aplikacije in podpira velik obseg transakcij (Casino, Dasaklisb & Patsakisa, 2019, str. 69). Poleg tega bodo hitro rastoča omrežja zahtevala hiter mehanizem soglasja, da bi potrdila več transakcij in hkrati zagotovila hitrost potrjevanja. Bitcoin se ne uporablja kot zamenjava za fiat valute primarno zaradi razširljivosti, saj lahko zaradi omejitev velikosti blokov in neučinkovitih algoritmov za soglasje obdela le 3 do 7 transakcij na sekundo, kar je precej manj, kot jih lahko obdelajo tradicionalni plačilni sistemi, kot sta Visa in Mastercard. Drugi aspekt razširljivosti se nanaša na velikost podatkovnih verig (Zheng, Xie, Dai, Chen & Wang, 2018, str. 15). Omrežja zahtevajo od vsakega uporabnika, da prenese in preveri zgodovino vseh transakcij, ki so bile izvedene, vključno s plačanim zneskom, plačnikom, prejemnikom plačila in drugimi podrobnostmi. Ko vsaka transakcija dodaja nekaj sto bajtov, se podatkovna veriga bistveno povečuje. V času pisanja je podatkovna veriga omrežja Bitcoin naraščala z okoli 50 gigabajti na leto in je znašala približno 218 gigabajtov (Bitinfocharts, 2019). Da bi ohranili velikost porazdeljenih baz in čas, ki je potreben za preverjanje obvladljivih transakcij, imajo omrežja omejitve pretoka transakcij. Naslednji vidik vprašanja razširljivosti je, da je posodobitev odvisna od zastojev (Bank for International Settlements, 2018, str. 99). V javnih omrežjih, ki temeljijo na veriženju podatkovnih blokov, da bi omejili število transakcij v danem trenutku, se lahko novi bloki dodajo samo v vnaprej določenih intervalih. Ko je število dohodnih transakcij takšno, da so na novo dodani bloki že na največji dovoljeni velikosti protokola, se sistem ustavi in številne transakcije gredo v čakalno vrsto. Z omejitvijo zmogljivosti se provizije povečajo, kadar povpraševanje po transakcijah doseže omejitev zmogljivosti. Transakcije so včasih lahko v vrsti nekaj ur, kar omejuje uporabnost za vsakodnevne transakcije in plačila na debelo.

5.2.3 Energijska neučinkovitost

Uporaba algoritmov za soglasje PoW in posledično dodajanje podatkovnih blokov na podatkovno verigo v obliki rudarjenja porabi ogromno energije (Economist, 2018). Ta energija je praktično zapravljena in ne opravlja nobene praktične naloge. Čeprav rudarska strojna oprema hitro postaja energijsko učinkovitejša, skupna raven porabe energije, ki jo

zahteva PoW, še naprej narašča. Pravzaprav je težava pri zgoščevalni vrednosti, ki je za vsak blok prilagojena računalniški moči omrežja, tako da je vedno potrebnih približno 10 minut za dodajanje novega bloka. Pod temi pogoji povečanje učinkovitosti samo povečuje konkurenco in vodi k višji stopnji nadgradnje strojne opreme, vendar ne zmanjšujejo celotne ravni porabe energije. Trenutno omrežje Bitcoin porabi 73 TWh električne energije na leto, kar je približno toliko kot celotna Avstrija ali Kolumbija, posamezna transakcija pa 607 KWh (Digiconomist, brez datuma-a). Drugo največje omrežje Ethereum porabi 7,01 TWh električne energije na leto kar je približno tolikot kot celotni Honduras ali Angola, posamezna transakcija pa 27 KWh (Digiconomist, brez datuma-b). Edina razlika je v tem, da je povprečna cena za KWh za rudarje bitcoina ocenjena na približno 5 centov na KWh, za Ethereum pa se domneva, da v povprečju plačajo 10 centov na KWh, kar je posledica dejstva, da je Ethereum ASIC odporen.

5.2.4 Varnost in nespremenljivost

V večini literature je tehnologija veriženja podatkovnih blokov opisana kot varna in nespremenljiva, kar pa ni povsem res (Casino, Dasaklisb & Patsakisa, 2019, str. 71). V tradicionalnih plačilnih sistemih posameznega plačila ni mogoče preklicati, ko se obdela. V nasprotju s tem pa javna omrežja, ki uporabljajo tehnologijo veriženja podatkovnih blokov, ne morejo zagotavljati absolutne končnosti posameznih plačil. Kljub temu da je tehnologija odporna na nedovoljene posege (ang. tamper resistant), jih ne moremo obravnavati kot popolnoma nespremenljive, saj obstajajo situacije, ko se lahko podatkovne verige spremenijo. Pri nekaterih podatkovnih verigah se zadnji objavljeni bloki zamenjajo z daljšo alternativno verigo z različnimi zadnjimi bloki, ko dva rudarja istočasno dodata nov blok. Večina omrežij uporablja strategijo sprejemanja najdaljše verige kot stanje resnice, kadar obstaja več konkurenčnih verig. Če verigi tekmujeta, vendar vsaka vključuje svoje lastno edinstveno zaporedje zadnjih blokov, se sprejme daljša veriga. Vendar to ne pomeni, da so transakcije v nadomeščenih blokih izgubljene, temveč so morda vključene v drug blok ali vrnjene v čakalno vrsto transakcij. Ta stopnja šibke nespremenljivosti za zadnje bloke je razlog, da večina uporabnikov omrežja počaka na več novih dodanih blokov, preden menijo, da je transakcija veljavna. Za omrežja brez dovoljenj je lahko sprejem daljše nadomestne verige blokov posledica napada, znanega kot napad 51 % (Yaga, Mell, Roby & Scarfone, 2018, str. 36). V ta namen napadalec preprosto pridobi dovolj sredstev, da prehiti hitrost ustvarjanja blokov v preostalem omrežju (ima več kot 51 % sredstev, uporabljenih za izdelavo novih blokov). Ta napad ni tehnično težaven, saj se samo ponavlja normalen postopek uvedbe tehnologije veriženja podatkovnih blokov, toda z izbranimi transakcijami, bodisi vključenimi ali izpuščenimi, in s hitrejšim tempom. Toda nedavne raziskave kažejo, da so celo vozlišča z manj kot 51-odstotno močjo še vedno nevarna. Eyal in Sirer (2013) sta pokazala, da je omrežje ranljivo, tudi če se za goljufijo porabi le majhen del moči. Pri sebični rudarski strategiji (ang. selfish mining) sebični rudarji ohranijo svoje bloke brez oddajanja, zasebna veriga pa je javnosti razkrita le, če so izpolnjene nekatere zahteve. Ker je zasebna veriga daljša od sedanje javne verige, jo bodo sprejeli vsi rudarji. Racionalni rudarji bodo

povabljeni, da se pridružijo novi verigi, in sebični rudarji lahko hitro presežejo 51 % moči. Poznamo še več vrst napadov v omrežja, ki temeljijo na veriženju podatkovnih blokov (Viswanathan & Shah., 2018):

- **napad Sybil:** subjekt bi lahko v omrežju oblikoval veliko število identitet, da bi učinkovito nadzoroval pomemben delež v lastništvu in/ali odločanju omrežja;
- **napad z zapravljanjem manjše vrednosti** (ang. peny spend attack): subjekt preplavi omrežje s transakcijami z nizko vrednostjo, da prepreči zagon omrežja;
- **napad DDoS** (ang. distributed denial of service attack): pojavi se, ko obstaja namen prekiniti promet v omrežju s poplavljanjem omrežja z zlonamernimi transakcijami;
- **napad dogovarjanja:** eden ali več subjektov (ali vozlišč) se odloči, da se bodo medsebojno dogovorili za izvedbo nekaterih zlonamernih operacij v omrežju.

Za omrežja s potrebo po dovoljenju lahko ta napad preprečimo, saj lastnik ali konzorcij dovoli vozliščem, da se pridružijo omrežju in iz njega odstranijo vozlišča, kar jim omogoča nadzor. Manj je verjetnosti, da bodo nastale konkurenčne verige, saj lahko lastnik vozlišča prisili v pošteno sodelovanje, saj lahko nesodelujoča vozlišča odstrani.

5.2.5 Zasebnost in anonimnost

Porazdeljeni vidik podatkovne verige pomeni, da ima vsako polno vozlišče, ki obdeluje transakcije, dostop do podatkov. (Andrew & Douglas, 2018, str. 2). V javnem omrežju, to pomeni, da je podatkovna veriga javno dostopna in mogoče je slediti vsaki transakciji. Omrežja brez dovoljenja so tipično psevdoanonimna, kar pomeni, da podatki o transakcijah niso neposredno povezani z določenim posameznikom, je pa mogoče skupaj povezati več pojav istega posameznika. Ta problem poslabša tudi teoretično nespremenljiva narava zapisov v podatkovni verigi, saj pomeni, da ko bo posameznik identificiran na kakršen koli način, bo življenjska doba transakcij trajno povezana s to osebo. Eden od načinov identifikacije je nadziranje komunikacije med vozlišči in uporaba programske opreme, ki lahko povezujejo transakcije in naslove internetnih protokolov. Identifikacija je problematična predvsem zaradi možnosti napada na posameznika in poskus pridobitve zasebnega ključa. Zaradi decentralizirane narave ni osrednjega organa, ki bi preprečeval delovanje nepoštenih uporabnikov, zato lažne transakcije, ki jo je omogočil heker, ki ima uporabnikov zasebni ključ, ni mogoče ustaviti ali naknadno razveljaviti. Napadi, pri katerih so ukradeni zasebni ključi, so podobni vdorom v spletne bančne račune. Največja tatvina, ki je obsegala krajo kripto valute Bitcoin v vrednosti 450 milijonov USD, se je zgodila leta 2014, ko so v obdobju enega meseca napadalci infiltrirali do tedaj največjo borzo kripto valut, imenovano Mt. Gox (Bloomberg, 2014).

5.2.6 Pravne in regulatorne slabosti

Pri sistemih za denarne transakcije predstavlja izziv določanje končne točke transakcije in ali je to transakcijo možno spremeniti ob odsotnosti centralne entitete (Natarajan, Krause &

Gradstein, 2017, str. 20). Drugi izziv je sodna pristojnost glede podatkov in nadzora transakcij pri globalnih omrežjih, na katerih se izvajajo čezmejne transakcije. Regulacija takih omrežij je izjemno težavna, saj nobena pravna entiteta ni lastnik porazdeljene podatkovne baze (Fulmer, 2019, str. 172). Pri konzorcijskih in zasebnih omrežjih je ta izziv rešen, saj obstaja pravni lastnik oz. administrator omrežja. Za uporabo na finančnem področju bodo morala omrežja, ki uporabljajo tehnologijo veriženja podatkovnih blokov, sprejeti standarde o poznavanju strank in skrbnih pregledih strank pri regulacijah glede preprečevanja pranja denarja in financiranja terorizma. Ker javna omrežja zakrijejo identiteto uporabnikov z uporabo sistema enkripcije z javnim ključem, je tem regulacijam nemogoče zadostiti. Konzorcijska in zasebna omrežja to rešijo s potrebo po identifikaciji pred uporabo omrežja. Ker je nepokvarljivost in nespremenljivost ena ključnih lastnosti tehnologije veriženja podatkovnih blokov, se pojavljajo vprašanja o načinu reševanja sporov glede transakcij, predvsem pa glede izbrisa napačnih transakcij (Fulmer, 2019, str. 187).

SKLEP

V tem magistrskem delu sem podal podlago za analizo tehnologije porazdeljenih podatkovnih baz in veriženja podatkovnih blokov v primerjavi s tradicionalnimi transakcijskimi sistemi, kako tehnologija deluje, kakšne vrste poznamo, kako se lahko uporablja kot učinkovit način za pomoč pri reševanju vprašanj glede širokega spektra problemov, primarno na področju denarnih transakcij. V prvem poglavju sem analiziral obstoječe sisteme za izvajanje denarnih transakcij. Ti se razlikujejo glede na tip transakcije, saj je odvisno, ali gre za lokalno ali za mednarodno transakcijo. Pri lokalnih transakcijah sisteme ločimo glede na višino plačila in nujnost. Če gre za nujne transakcije višje vrednosti, jih banke načeloma poravnajo v sistemu za prenose velikih vrednosti, ki jih upravlja centralna banka ali pa je za ta namen ustanovljena družba. Te sisteme definira manjši volumen transakcij, ker pa gre za medbančne transakcije, je njihova vrednost na izjemno visoki ravni. Gre za sisteme, pri katerih lahko sodelujejo le finančne institucije, zato imajo ti sistemi tipično visoke vstopne stroške, stroški samih transakcij pa so relativno nizki. Ker je ključni aspekt sistemov varnost in obdelava, ki jo opravi centralna banka, je čas transakcij relativno dolg. V primeru plačil manjših vrednosti se tipično uporabljajo kartična omrežja in avtomatske klirinške hiše, ki so zasnovane za obdelavo velikih količin plačil z nizko vrednostjo. Po analizi kartičnih omrežji in avtomatiziranih klirinških hiš lahko sklepamo, da obdelajo veliko število transakcij in dokazujejo visoke stopnje razširljivosti, provizije pa so relativno nizke in stabilne. Pri mednarodnih prenosih banke uporabljajo sistem SWIFT in sistem korespondenčnih bank; slednje služijo kot posredniki med lokalnimi bankami, ki med seboj nimajo vzpostavljenih odnosov. Transakcije preko teh sistemov so kljub napredkom v zadnjem času še vedno počasne in drage. Glavno konkurenco sistemu medbančnih prenosov še vedno predstavljajo alternativni ponudniki plačilnih storitev, ki v večji meri opravljajo prenose manjše vrednosti. Ti omogočajo transakcije izven bančnih kanalov z nižjimi provizijami. Po analizi obstoječih sistemov lahko ovržem raziskovalno vprašanje 1. Obstoječi sistemi, predvsem lokalni, nudijo uporabnikom hitre in cenovno ugodne storitve,

predvsem pa zagotavljajo visoko stopnjo razširljivosti, kar dokazujeta tako visoka stopnja transakcij kot volumen samih transakcij.

V nadaljevanju sem podrobno analiziral tehnologijo porazdeljenih podatkovnih baz in veriženja podatkovnih blokov. Tehnologija se nanaša na pristop k beleženju in izmenjavi podatkov v več podatkovnih bazah, ki so geografsko razdeljeni na več mest v omrežju, zato govorimo, da je sistem porazdeljen. Vsak uporabnik shrani najnovejšo kopijo celotne podatkovne baze, s tem pa je izmenjava digitalnih sredstev izvedljiva, saj lahko vsak uporabnik v svoji kopiji neposredno preveri, ali je prišlo do prenosa oz. ni bilo nobenega poskusa dvojnega zapravljanja. Razlikujemo med dvema razredoma porazdeljenih podatkovnih bazah, ki se razlikujeta v operativni postavitvi. En razred temelji na porazdeljenih podatkovnih bazah s potrebo po dovoljenju, drugi razred pa je povsem decentraliziran in deluje brez potrebe po dovoljenju. Podatkovna veriga je posebna vrsta tehnologije porazdeljenih podatkovnih baz, ki uporablja kriptografske in algoritemske metode za ustvarjanje podatkovne strukture v obliki verige podatkovnih blokov. Javno dostopna porazdeljena podatkovna baza se posodablja v obliki paketov transakcij. Vsaka posodobitev se imenuje blok in ti bloki vsebujejo podatke o novih transakcijah, skupaj z zgodovino vseh transakcij. Bloki se nato zaporedoma vežejo in tako tvorijo podatkovne verige. Za preprečevanje delovanja nepoštenih uporabnikov v omrežju uporabljajo algoritme za doseganje skupnega soglasja o stanju podatkov v podatkovni verigi. Omrežja s potrebo po dovoljenju tipično uporabljajo specifične in bolj učinkovite algoritme za doseganje soglasja, saj obstaja oblika centralne avtoritete, ki uporabo dovoljuje samo zaupanja vrednim uporabnikom. Omrežja brez potrebe po dovoljenju pa uporabljajo algoritme, temelječe na ekonomskih iniciativah, ki uporabnike odvračajo od nepoštenega ravnanja.

Tehnologija pa ni brez slabosti in izzivov. Primarni izziv je pomanjkanje razširljivosti, predvsem pri omrežjih, ki bodo soglasje dosegala z uporabo algoritma za soglasje, imenovanega dokazilo o delu. Ta algoritem se je pri največjem in najbolj razširjenem omrežju Bitcoin izkazal kot zelo neučinkovit in precej omejuje razširljivost tako omrežja Bitcoin kot tudi drugega največjega omrežja Ethereum. Zaradi omejitve velikosti podatkovnih blokov in hitrosti dodajanja blokov na podatkovno verigo je teoretična stopnja obdelave omrežja le približno 7 transakcij na sekundo, dejanska pa le približno 3 transakcije na sekundo. Ta omejitev velikosti bloka na 1 megabajt in hitrosti dodajanja novih blokov na 10 minut povzroči nastanek zastojev, saj rudarji ne morejo dovolj hitro dodajati transakcij v podatkovno verigo. Dodatno slabost predstavlja potreba po dodatnih potrditvah zadnjega bloka. V omrežju Bitcoin se tako transakcija šteje za varno šele, ko se bloku doda šest novih. To pomeni, da tudi če uporabnik izbere dovolj visoko provizijo, da je njegova transakcija takoj vključena v prvi nov blok, bo za končnost transakcije čakal eno uro. Zaradi lastnosti omrežja, da lahko uporabniki sami določijo provizije, se te dvignejo, zaradi želje, da bi rudarji transakcije čim prej dodali v bloke. Ta situacija ob visoki stopnji uporabe omrežja pripelje do izredno visokih provizij, kar še dodatno onemogoča uporabo kripto valut za vsakdanje transakcije. Druga omrežja so poskušala ta problem rešiti na različne načine,

predvsem s spremembami ključnih parametrov, kot so velikost bloka pri uporabi algoritma za soglasje PoW oz. uporabo alternativnih algoritmov za soglasje. Kljub temu ugotavljam, da jim v tem pogledu v veliki meri ni uspelo. Za uporabo kripto valut se problematično zdi področje plačil majhnih vrednosti, kot se to v večji meri izvaja na kartičnih omrežjih. Novejša omrežja, kot so Ripple, EOS in Stellar, ki z modernimi algoritmi za soglasje vsaj v teoriji nudijo boljše lastnosti in omogočajo višjo stopnjo razširljivosti, kljub temu pa je večina njihovih prednosti trenutno teoretičnih in podanih od njihovih razvijalcev. Uporaba kripto valut ima trenutno edino smiselno aplikacijo na področju čezmejnih plačil, pri čemer pa so plačila manjših vrednosti še vedno zelo počasna in draga. Pomanjkljivosti so vidne tudi na področjih varnosti, kjer lahko zaradi zasnove tehnologije pride do situacije, da nepošteni uporabniki s pomočjo različnih napadov prevzamejo nadzor nad omrežjem. Tudi nadzor in regulacija plačilnih omrežij, kripto valut in drugih oblik tehnologije veriženja podatkovnih blokov, kot so digitalna sredstva in pametne pogodbe, sta trenutno še vedno relativno nerazvita, pri določenih omrežjih pa sta zaradi uporabe naprednih kriptografskih postopkov tudi nemogoča. Določanje lastništva in odgovornosti je pri javnih omrežjih izjemno težko, saj ni centralnega subjekta, ki bi deloval kot administrator omrežja. Iz teh ugotovitev lahko popolnoma ovržem raziskovalno vprašanje 2, saj menim, da je tehnologija v trenutni fazi še daleč od možnost zamenjave obstoječega sistema denarnih transakcij.

Kljub tem, pa lahko tehnologija v prihodnosti nadgradi sisteme, uporabljene na finančnem področju. Namesto da bi se zanašali na centralizirane organizacije, in uporabljali številne posrednike, bodo lahko transakcije v prihodnosti potekale na konzorcijskih omrežij in bodo tako hitrejše in cenejše. Rešitve, ki jih ponujajo podjetja Facebook in partnerji z omrežjem Libra, Ripple s svojima produktoma RippleNet in xCurrent, R3 z razvojnim okvirjem Corda in IBM ter SWIFT z omrežjem World Wide, predstavljajo aplikacije tehnologije, ki lahko v prihodnosti eliminirajo posrednike in niso omejene na delovne ure bank. JPM Coin, ki ga bo v prihodnosti uporabljala ena izmed največjih globalnih bank JP Morgan, dodatno nakazuje, da bodo obstoječe finančne institucije uvedle to tehnologijo, da bi optimizirale poslovanje in svojim strankam zagotavljale višjo raven storitev. Poleg kripto valut je temeljna uporaba tehnologije veriženja podatkovnih blokov predvsem v integraciji obstoječih sistemov in tehnologije na področjih kot so tokenizacija, digitalna sredstva in digitalizacija javnih registrov. Zaradi teh ugotovitev lahko potrdim raziskovalno vprašanje 3.

Moje magistrsko delo prispeva k širšemu in globljemu razumevanju tehnologije porazdeljenih podatkovnih baz in veriženja podatkovnih blokov, tako s tehničnega vidika delovanja tehnologije kot tudi uporabe na realnih primerih. Gre za zanimiv razvoj tehnologije, ki je bila primarno razvita kot alternativa obstoječemu finančnemu sistemu, vendar ima zaradi svojih ključnih lastnosti omejeno uporabo. Konstantne inovacije ter razvoj tehnologije in digitalizacije sodobne družbe bodo privedli do sprejetja širokega nabora različnih rešitev, ki bodo precej spremenile tako vsakdanje življenje kot poslovanje. Med inovacijami je tudi tehnologija porazdeljenih podatkovnih baz in veriženja podatkovnih blokov in njene različne izpeljanke.

LITERATURA IN VIRI

1. Abhishek, S., Pronaya, B., Arunendra, S. & Atul, M. (2019). A Systematic Review on Evolution of Blockchain Generations. *ITEE Journal, 7*(6), 1–8.
2. Adams, C. (2018, 8. marec). *Stellar Lumens Vs Ripple.* Pridobljeno 4. februarja 2019 iz https://www.investinblockchain.com/stellar-lumens-vs-ripple/
3. Ahsan, J. (2018, 18. julij). *Centralization vs. Decentralization: The Best (and worst) of Both Worlds.* Pridobljeno 5. marca 2019 iz https://hackernoon.com/centralization-vs-decentralization-the-best-and-worst-of-both-worlds-7bfdd628ad09
4. Andrew, L. & Douglas, A. (2018). Bitcoin Investigations: Evolving Methodologies and Case Studies. *Journal of Forensic Research, 9*(3), 1–7.
5. Antonopoulos, A. M. (2014). *Mastering Bitcoin.* Sebastopol: O'Reilly.
6. Association for Financial Professionals. (2015). *Benchmarking Survey Payments Cost.* Pridobljeno 16. novembra 2019 iz https://www.afponline.org/survey-research-economic-data/2015-afp-payments-cost-benchmarking-survey
7. Bach, L. M., Mihaljević, B. & Žagar, M. (2018). Comparative Analysis of Blockchain Consensus Algorithms. *International Convention on Information and Communication Technology, Electronics and Microelectronics, 41,* 1545–1550.
8. Bai, Q., Zhou, X., Wang, X., Xu, Y., Wang, X. & Kong, Q. (2018). A Deep Dive into Blockchain Selfish Mining. *IEEE International Conference on Communications,* 1–7.
9. Baliga, D. A. (2017). *Understanding consensus models.* Pridobljeno 4. julija 2019 iz https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf
10. Bank for International Settlements. (2018). *Annual Economic Report.* Pridobljeno 4. julija 2019 iz https://www.bis.org/publ/arpdf/ar2018e.pdf
11. Bank of America Corporation. (brez datuma). *International Wire transfers.* Pridobljeno 6. novembra 2019 iz https://www.bankofamerica.com/wire-transfer.go
12. Barakat, M., Eder, C. & Hanke, T. (2018). *An Introduction to Cryptography*. University of Kaiserslautern.
13. Bashir, I. (2018). *Mastering Blockchain* (2 izd.). Birmingham: Packt Publishing.
14. BBC. (2019, 18. junij). *Facebook's Libra pitches to be the future of money.* Pridobljeno 2. avgusta 2019 iz https://www.bbc.com/news/technology-48667525
15. Berentsen, A. & Schär, F. (2019). *Stablecoins: The quest for a low- volatility cryptocurrency.* University of Basel: Centre for Economic Policy Research.
16. Bhutoria, M. (2018). *Cardano (ADA).* Pridobljeno 6. julija 2019 iz https://www.circle.com/marketing/pdfs/research/circle-research-cardano.pdf
17. Bitcoinfees.info. (brez datuma). *Bitcoin Transaction Fees.* Pridobljeno 5. decembra 2019 iz https://bitcoinfees.info/
18. Bitinfocharts. (2019). *Cryptocurrency statistics.* Pridobljeno 5. decembra 2019 iz https://bitinfocharts.com/statistic
19. Black, A. (1997). *Hashcash.* Pridobljeno 9. februarja 2019 iz http://www.hashcash.org/papers/announce.txt

20. Block.one. (2018, 16. marec). *Technical White Paper v2*. Pridobljeno 4. aprila 2019 iz https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
21. Blockchain.com. (2018). *The state of stablecoin.* Pridobljeno 7. julija 2019 iz https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf
22. Blockgeeks. (2018). *What is Ethereum Gas?* Pridobljeno 1. maja 2019 iz https://blockgeeks.com/guides/ethereum-gas/
23. Bloomberg. (2014, 28. februar). *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss.* Pridobljeno 3. marca 2019 iz https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy
24. Bloomberg. (2019a, 18. junij). *Facebook Token Runs Into Instant Political Opposition* Pridobljeno 3. avgusta 2019 iz https://www.bloomberg.com/news/articles/2019-06-18/france-calls-for-central-bank-review-of-facebook-cryptocurrency
25. Bloomberg. (2019b, 14. februar). *JPMorgan's Crypto Coin Puts Ripple's Relevance in Question.* Pridobljeno 16. avgusta 2019 iz https://www.bloomberg.com/news/articles/2019-02-14/jpmorgan-s-crypto-experiment-raises-ripple-relevance-question
26. Boneh, D. & Shoup, V. (2017, 30. september). *A Graduate Course in Applied Cryptography: Version 0.4.* Pridobljeno 4. februarja 2019 iz https://crypto.stanford.edu/~dabo/cryptobook/
27. Bossone, B. & Cirasino, M. (2001). *The Oversight of the Payments Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies.* Washington: World Bank Group.
28. Brawenewcoin. (2018, 20. oktober). *Nasdaq planning a tokenized securities platform*. Pridobljeno 10. marca 2019 iz https://bravenewcoin.com/insights/nasdaq-planning-a-tokenized-securities-platform
29. Buterin, V. (2013). *Ethereum White Paper: A next-generation smart contract and decentralized application platform* Pridobljeno 12. februarja 2019 iz https://github.com/ethereum/wiki/wiki/White-Paper
30. Buterin, V. (2015, 15. november). *Merkling in Ethereum* [objava na blogu]. Pridobljeno 7. februarja 2019 iz https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/
31. Buterin, V. (2017, 6. februar). *The Meaning of Decentralization* [objava na blogu]. Pridobljeno 26. februarja 2019 iz https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
32. Cachin, C. & Vukolic, M. (2017). *Blockchain Consensus Protocols in the Wild*. Zurich: IBM Research .
33. Casino, F., Dasaklisb, T. K. & Patsakisa, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81.
34. Castro, M. & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems, 20*(4), 398–461.
35. Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings*, 199–203.

36. Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons, 61*(4), 567–575.
37. CNET. (2019, 15. julij). *Everything you need to know about Facebook's Libra cryptocurrency*. Pridobljeno 2. avgusta 2019 iz https://www.cnet.com/news/everything-you-need-to-know-about-facebooks-libra-cryptocurrency/
38. Coincentral.com. (2018, 1. oktober). *What Are Blockchain Confirmations and Why Do They Matter?* Pridobljeno 8. maja 2019 iz https://coincentral.com/blockchain-confirmations/
39. Coindesk. (2018a, 13. april). *Beyond Banking: R3's Expanding Vision for Global Blockchain.* Pridobljeno 15. maja 2019 iz https://www.coindesk.com/beyond-banking-r3-expanding-vision-global-blockchain
40. Coindesk. (2018b, 22. februar). *What is SegWit?* Pridobljeno 2. maja 2019 iz https://www.coindesk.com/information/what-is-segwit
41. CoinMarketCap. (2019). *All Cryptocurrencies.* Pridobljeno 12. septembra 2019 iz https://coinmarketcap.com/all/views/all/
42. Coinmetrics. (brez datuma). *Community Network Data*. Pridobljeno 5. decembra 2019 iz https://coinmetrics.io/community-network-data/
43. Committee on Payments and Market Infrastructures. (2015). *Digital currencies.* Pridobljeno 6. oktobra 2019 iz https://www.bis.org/cpmi/publ/d137.pdf
44. CryptoRunner. (brez datuma). *A Complete Comparison with All Pros/Cons of NEO vs EOS.* Pridobljeno 3. julija 2019 iz https://cryptorunner.com/neo-vs-eos/
45. Curran, B. (2018, 9. julij). *What is a Merkle Tree? Beginner's Guide.* Pridobljeno 2. marca 2019 iz https://blockonomi.com/merkle-tree/
46. Dai, W. (1998). *bmoney.* Pridobljeno 3. februarja 2019 iz http://www.weidai.com/bmoney.txt
47. Diffie, W. & Hellman, M. (1976). New Directions in Cryptography. *IEEE transactions on information theory, 22*, 644–654.
48. Digiconomist. (brez datuma-a). *Bitcoin Energy Consumption Index.* Pridobljeno 11. avgusta 2019 iz https://digiconomist.net/bitcoin-energy-consumption
49. Digiconomist. (brez datuma-b). *Ethereum Energy Consumption Index*. Pridobljeno 11. februarja 2019 iz https://digiconomist.net/ethereum-energy-consumption
50. Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* New York: Apress.
51. Dwork, C. & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. *CRYPTO 92: Lecture Notes in Computer Science, 740,* 139–147.
52. EBA Clearing. (2018). *Annual Report 2018. EBA Clearing.* Pridobljeno 6. septembra 2019 iz www.ebaclearing.eu/media/azure/production/eba-clearing-annual-report-2018
53. EBA Clearing. (brez datuma). *A unique RTGS-equivalent net settlement system.* Pridobljeno 13. aprila 2019 iz https://www.ebaclearing.eu/services/euro1/overview/
54. Economist. (2018, 9. junij). *Why bitcoin uses so much energy*. Pridobljeno 16. marca 2019 iz https://www.economist.com/2018/07/09/why-bitcoin-uses-so-much-energy

55. Enria, A. (2018). *Designing a Regulatory and Supervisory Roadmap for FinTech*. Pridobljeno 2. septembra 2019 iz https://eba.europa.eu/sites/default/documents/files/documents/10180/2151635
56. European Central Bank. (2012). *Virtual currency schemes*. Pridobljeno 6. septembra 2019 iz https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en
57. European Central Bank. (2014). *Card payments in Europe.* Pridobljeno 2. septembra 2019 iz https://www.ecb.europa.eu/pub/other/cardpaymineu_renfoconsepaforcards2014
58. European Central Bank. (2015). *Virtual currency schemes–a further analysis.* Pridobljeno 5. septembra 2019 iz https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen
59. European Central Bank. (2018a). *TARGET2 Pricing Guide Version 6.0.* Pridobljeno 6. septembra 2019 iz https://www.ecb.europa.eu/paym/target/target2/fees/shared/pdf/TARGET2_Pricing_Guide
60. European Central Bank. (2018b). *TARGET2 Annual Report 2018.* European Central Bank. Pridobljeno 3. septembra 2019 iz https://www.ecb.europa.eu/pub/pdf/targetar/ecb.targetar2018.en.pdf
61. European Commission. (2016, 19. junij). *Antitrust: Regulation on Interchange Fees.* Pridobljeno 21. novembra 2019 iz https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2162
62. European Commission. (2019). *Blockchain Now And Tomorrow.* Pridobljeno 2. novembra 2019 iz https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow
63. Eyal, I. & Sirer, E. G. (2013). *Majority is not Enough: Bitcoin Mining is Vulnerable.* Cornell University: Department of Computer Science.
64. Eze, K. (2018). Smart Contracts: A Primer. *Journal of Scientific and Engineering Research, 5*(5), 538–541.
65. Federal Reserve Bank. (2019). *Fedwire Funds Service 2019 Fee Schedules.* Pridobljeno 1. maja 2019 iz https://www.frbservices.org/resources/fees/wires-2019.html
66. Federal Reserve Banks. (brez datuma). *Fedwire Funds Service.* Pridobljeno 1. maja 2019 iz https://www.frbservices.org/financial-services/wires/index.html
67. Finney, H. (2004, 15. avgust). *RPOW - Reusable Proofs of Work.* Pridobljeno 2. septembra 2019 iz https://nakamotoinstitute.org/rpow/
68. Forbes. (2019b, 18. marec). *IBM Launches A Blockchain-Based Global Payments Network Using Stellar's Cryptocurrency.* Pridobljeno 18. marca 2019 iz https://www.forbes.com/sites/rachelwolfson/2019/03/18/ibm-launches-a-blockchain-based-global-payments-network-using-stellars-cryptocurrency/
69. Forbes.com. (2019a, 7. marec). *Forget Cryptocurrencies. How Can Financial Institutions Make Use Of Blockchain?* Pridobljeno 27. marca 2019 iz https://www.forbes.com/sites/darrynpollock/2019/03/07/forget-cryptocurrencies-how-can-financial-institutions-make-use-of-blockchain/2/#3fb652c852eb
70. Fulmer, N. (2019). Exploring the Legal Issues of Blockchain Applications. *Akron Law Review, 52*(1), 162–191.

71. Furbush, J. (2018, 6. december). *Distributed systems: A quick and simple definition*. Pridobljeno 11. maja 2019 iz https://www.oreilly.com/ideas/distributed-systems-a-quick-and-simple-definition
72. Golosova, J. & Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. *IEEE Workshop on Advances in Information, Electronic and Electrical Engineering, 6*, 1–6.
73. Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal, 4*, 160–210.
74. Gupta, V. (2017, 28. februar). *A Brief History of Blockchain.* Pridobljeno 20. decembra 2018 iz hbr.org/2017/02/a-brief-history-of-blockchain
75. Haber, S. & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology, 3*(2), 99–111.
76. Hileman, G. & Rauchs, M. (2018). *2nd global cryptoassets benchmarking study*. Pridobljeno 1. septembra 2019 iz https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf
77. Houben, P. D. & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for crime, money laundering and tax evasion.* European Parliament.
78. IBM. (2018). *Introducing IBM Blockchain World Wire – the new global financial rail.* Pridobljeno 7. maja 2019 iz https://www.ibm.com/downloads/cas/JLDYADKJ
79. Infosys. (2018). *Blockchain technology and financial services.* Pridobljeno 6. novembra 2019 iz https://www.infosys.com/consulting/Documents/blockchain-technology
80. International Monetary Fund. (2016). *Virtual Currencies and Beyond.* Pridobljeno 29. decembra 2018 iz https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
81. Investopedia. (2019a, 9. april). *Scalability.* Pridobljeno 1. maja 2019 iz https://www.investopedia.com/terms/s/scalability.asp
82. Investopedia. (2019b, 7. februar). *Correspondent Bank.* Pridobljeno 14. marca 2019 iz https://www.investopedia.com/terms/c/correspondent-bank.asp
83. Investopedia. (2019c, 10. februar). *How the SWIFT System Works.* Pridobljeno 18. marca 2019 iz https://www.investopedia.com/personal-finance/050515/swift-system.asp
84. Investopedia.com. (2019d, 25. junij). *Blockchain Technology's Three Generations*. Pridobljeno 1. julija 2019 iz https://www.investopedia.com/tech/blockchain-technologys-three-generations/
85. Jafery, R. (2018, 27. september). *Intro to Tokenized Assets and Security Tokens.* Pridobljeno 3. marca 2019 iz https://hackernoon.com/tokenized-assets-security-tokens-and-stos-ae72dc0e275e
86. JPMorgan Chase. (2019, 14. februar). *J.P. Morgan Creates Digital Coin.* Pridobljeno 4. maja 2019 iz https://www.jpmorgan.com/news/digital-coin-payments
87. Lai, R. (2018). Understanding Interbank Real-Time Retail Payment Systems. *Handbook of Blockchain, Digital Finance, and Inclusion, 1*, 283–310.
88. Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382–401.

89. Libra Association. (brez datuma). *The Libra Blockchain.* Pridobljeno 2. avgusta 2019 iz https://developers.libra.org/docs/the-libra-blockchain-paper
90. Lin, I.-C. & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security, 19*(5), 653–659.
91. Manning Publications. (brez datuma). *Cryptographic Hashes and Bitcoin.* Pridobljeno 5. novembra 2019 iz https://freecontent.manning.com/cryptographic-hashes-and-bitcoin/
92. Mastercard. (2018). *Annual Report 2018.* Pridobljeno 6. julija 2019 iz https://investor.mastercard.com/investor-relations/financials-and-sec-filings
93. Mazieres, D. (2016, 25. februar). *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensusstellar.org.* Pridobljeno 8. marca 2019 iz https://www.stellar.org/papers/stellar-consensus-protocol.pdf
94. Menezes, A., Oorschot, P. & Vanstone, S. (2001). *Handbook of Applied Cryptography* (5 izd.). Boca Raton: CRC Press.
95. Merkle, R. (1979). *Secrecy, authentication, and public key systems.* Stanford University: Stanford Electronics Laboratories.
96. Miller, D., Mockel, P., Myers, G., Niforos, M., Ramachandran, V., Rehermann, T. & Salmon, J. (2019). *Blockchain: Opportunities for Private Enterprises in Emerging Markets.* Washington: World Bank Group.
97. NACHA. (2019, 14. februar). *Network Statistics.* Pridobljeno 10. maja 2019 iz https://www.nacha.org/content/network-statistics
98. Nakajima, M. (2017). *Analysis on World Trends of Payment Systems.* Kashiwa: Reitaku University, Faculty of Economics and Business Administration.
99. Nakamoto, S. (2009a, 24. maj). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Pridobljeno 21. decembra 2018 iz https://bitcoin.org/bitcoin.pdf
100. Nakamoto, S. (200ba, 2. november). *Bitcoin open source implementation of P2P currency.* Pridobljeno 22. decembra 2018 iz https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/#selection-9.0-9.50
101. Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University.
102. Natarajan, H., Krause, S. & Gradstein, H. (2017). *Distributed Ledger Technology (DLT) and Blockchain.* Washington: World Bank Group.
103. New York Times. (2019, 10. junij). *Fed Chair Raises 'Serious Concerns' About Facebook's Cryptocurrency Project.* Pridobljeno 4. avgusta 2019 iz www.nytimes.com/2019/07/10/technology/fed-chair-facebook-libra.html
104. NLB d. d. (2019). *NLB Tarifa za prebivalstvo.* Pridobljeno 12. oktobra 2019 iz https://www.nlb.si/tarifa-za-prebivalstvo
105. Norton, C. (2017). *Blockchain: Everything You Need to Know About the Technology Behind Bitcoin.* New York: Pronoun.
106. Payoneer. (2015). *Navigating the world of cross border payments.* Pridobljeno 2. marca 2019 iz http://www.iqpc.com/media/1003982/57107.pdf

107. PayPal Pte. Ltd. (2019, 1. oktober). *User Agreement for PayPal Service.* Pridobljeno 14. novembra 2019 iz https://www.paypal.com/gi/webapps/mpp/ua/useragreement
108. Perkins, D. W. (2018). *Cryptocurrency: The Economics of Money and Selected Policy Issues.* Washington: Congressional Research Service.
109. Poon, J. & Dryja, T. (2016, 14. januar). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.* Pridobljeno 24. februarja 2019 iz https://lightning.network/lightning-network-paper.pdf
110. Prasad, R. (2019, 19. april). *Tackling Ethereum's Blockchain Trilemma via Serenity, Ethereum 2.0.* Pridobljeno 10. maja 2019 iz https://hackernoon.com/tackling-ethereums-blockchain-trilemma-via-serenity-ethereum-2-0-1fb423a6b184
111. Reuters. (2019, 18. junij). *Explainer: 'Stablecoins' in the spotlight as Facebook unveils Libra cryptocurrency.* Pridobljeno 2. julija 2019 iz https://www.reuters.com/article/us-crypto-currencies-explainer/explainer-stablecoins-in-the-spotlight-as-facebook-unveils-libra-cryptocurrency-idUSKCN1TJ1T6
112. Ripple Labs Inc. (2017). *Product Overview: A technical overview of xCurrent.* Pridobljeno 2. januarja 2019 iz https://ripple.com/files/ripple_product_overview.pdf
113. Ripple Labs Inc. (brez datuma). *XRP Overview*. Pridobljeno 3. marca 2019 iz https://ripple.com/xrp/
114. Sarcevic, A., Palen, L., White, J., Starbird, K. & Anderson, M. B. (2012). Beacons of hope in decentralized coordination: Learning from on-the-ground. *CSCW '12 Computer Supported Cooperative Work*, 47–56.
115. Schneider, J., Blostein, A., Lee, B., Kent, S., Groer, I. & Beardsley, E. (2016). *Profiles in innovation blockchain: Putting Theory into Practice.* New York: Goldman Sachs Inc.
116. Singh, M. P. (2001). Peering at Peer-to-Peer Computing. *IEEE Internet Computing, 4*(5), 4–5.
117. Singhal, B., Dhameja, G. & Panda, P. S. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions.* New York: Apress.
118. Smith, S. S. (2019). Blockchain, Tokenization, and Implications for Financial Services Practitioners. *International Journal of Accounting and Financial Reporting, 9*(1), 1–14.
119. ssl2buy. (brez datuma). *Symmetric vs. Asymmetric Encryption – What are differences?* Pridobljeno 3. septembra 2019 iz https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
120. Stellar Development Foundation. (brez datuma). *Get started with the basics of the Stellar network.* Pridobljeno 2. julija 2019 iz https://www.stellar.org/how-it-works/stellar-basics/
121. SWIFT. (2018). *SWIFT Annual Review 2018.* Pridobljeno 11. septembra 2019 iz https://www.swift.com/about-us/financials
122. Szabo, N. (2005, 29. december). *Bit Gold.* Pridobljeno 29. januarja 2019 iz https://nakamotoinstitute.org/bit-gold/

123. Thomsen, S. S. (2009). *Cryptographic Hash Functions.* Lyngby: Technical University of Denmark.
124. Tompkins, M. & Olivares, A. (2016). Clearing and Settlement Systems from Around the World: A Qualitative Analysis. *Payments Canada Discussion Paper, 5*, 6–44.
125. Tradeblock. (2015, 15. oktober). *Analysis of Bitcoin Transaction Size Trends.* Pridobljeno 7. maja 2019 iz https://tradeblock.com//analysis-of-bitcoin-transaction-size
126. U.S. Securities and exchange commission. (brez datuma). *Spotlight on Initial Coin Offerings (ICOs).* Pridobljeno 8. januarja 2019 iz https://www.sec.gov/ICO
127. Umeh, J. (2016). Blockchain Double Bubble or Trouble? *ITNOW, 58*, 58–61.
128. VISA. (2018). *Annual Report 2018.* Visa. Pridobljeno 29. decembra 2018 iz https://s1.q4cdn.com/0506/files/financials/annual/2018/Visa-2018-Annual-Report
129. Viswanathan, S. & Shah., A. (2018, 20. Oktober). *The Scalability Trilemma in Blockchain* [objava na blogu]. Pridobljeno 8. maja 2019 iz https://medium.com/@aakash/the-scalability-trilemma-in-blockchain-75fb57f646df
130. Vu, Q., Lupu, M. & Ooi, B. (2009). *Architecture of Peer-to-Peer System.* New York: Springer.
131. Vukolic, M. (2016). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. Zurich: IBM Research .
132. Wang, W., Hoang, T., Hu, P., Niyato, D., Wang, P. & Wen, Y. (2018). A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks. *IEEE, 7*, 22328–22370.
133. Western Union, Inc. (brez datuma). *Transfer fees.* Pridobljeno 6. novembra 2019 iz https://www.westernunion.com/content/wucom/base/ru/en/transfer-fees.html
134. World Bank Group. (2019). *Migration and Remittances : Recent Developments and Outlook.* Pridobljeno 5. julija 2019 iz hhttp://documents.worldbank.org/curated/en/80516/Special-topic-transit-migration
135. Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018). *Blockchain Technology Overview*. Washington: National Institute of Standards and Technology.
136. Yang, L. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration, 15*, 80–90.
137. Zhang, R., Qiu, T. & Gao, Y. (2019). Ripple vs. SWIFT: Transforming Cross Border Remittance Using Blockchain Technology Remittance Using Blockchain Technology. *Procedia Computer Science: International Conference on Identification, Information and Knowledge in the Internet of Things, 147,* 428–434.
138. Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services, 14*(4), 352–373.

PRILOGA

Priloga 1: Slovar angleških izrazov

Altcoins - Alternativni kovanci
Automated clearing house - Avtomatizirana klirinška hiša
Bandwith - Pasovna širina
Block cipers - Blokovne šifre
Blockchain - Tehnologija veirženja podatkovnih blokov
Branches - Vse zgoščevalne vrednosti v sredini (veje)
Byzantine fault - Bizantinska napaka
Cardholder fees - Provizije za imetnike kartic
Challenge bits - Izzivni biti
Cipher suite - Šifrirni paket
Clearing - Obračun
Collateralization - Zavarovanost
Collision resistance - Odpornost proti trkom
Commited phase - Izvršilna faza
Delegated proof of stake – Podrejen dokaz o deležu
Deterministic hiding - Deterministično skrivanje
Digital signature algorithm - Algoritem digitalnega podpisa
Distributed ledger technology - Tehnologija porazdeljenih podatkovnih baz
Elliptic curve digital signature algorithm - Algoritem digitalnega podpisa eliptične krivulje
Finality of payment - Končnost plačila
Fork - Razmejitev verige
Full node - Polno vozlišče
Funding transaction - Transakcija financiranja
Gas - Plin
Gas limit - Omejitev plina
Gateways - Prehodi
Genesis block - Prvi ustvarjen blok
Hard fork - Trda razmejitev
Hash function - Zgoščevalna funkcija
Hash pointer - Zgoščevalni kazalnik
Hash rate - Hitrost zgoščevalne funkcije
High assurance code - Programska koda visoke stopnje zanesljivosti
Initial coin offering - Začetna ponudba kovancev
Interchange fee - Provizije za izmenjavo
Large value payment systems - Sistemi za prenose velikih vrednosti
Latencty - Zakasnitev
Leaves - Najnižje zgoščevalne vrednosti v merklovem drevesu (listi)
Ledger - Podatkovna baza
Libra association - Združenje Libra
Merchant service charge - Medbančne provizije

Merkle proof - Merklov dokaz
Money transfer operators - Operaterji prenosa denarja
Moral hazard - Moralno tveganje
Node - Vozlišče
Pan-european automated clearing house - Vseevropska avtomatizirana klirinška hiša
Parent block - Nadrejeni oz. Starševski blok
Peer-to-peer - Vrstniško
Peny spend attack - Napad z zapravljanjem manjše vrednosti
Permissioned – S potrebo po dovoljenju
Permissionless - Brez potrebe po dovoljenju
Plaintext - Prosto besedilo
Preimage resistance - Odpornost na predhodno sliko
Pre-mine - Predhodno ustvariti oz. pred-rudariti
Prepared phase - Pripravljena faza
Pre-prepared phase- Predpripravljena faza
Proof of concept-Dokaz o delovanju
Proof of work - Dokaz o delu
Proof of work function - Funkcija dokaza o delu
Puzzle friendliness - Prijaznost za sestavljanke
Real-time gross settlement - Poravnava na bruto osnovi v realnem času
Reusable Proof of Work – Dokaz o delu za večkratno uporabo
Root hash value - Koreninska zgoščevalna vrednosti
Scalability - Razširljivost
Second preimage resistance - Sekundarna odpornost na predhodno sliko
Securitization - Listinjenje
Security token - Premoženjski žeton
Security token offering - Ponudba vrednostnih žetonov
Selfish mining strategy - Sebična rudarska strategiji
Settlement - Poravnava
Stablecoins - Stabilni kovanci
Stream cyphers - Pretočne šifre
Supply chain management - Upravljanje dobavnih verig
Tamper resistantance - Odpornost na nedovoljene posege
Token - Žeton
Tokenization - Tokenizacija
Transaction malleability - Transakcijska deformacija
Unique node list - Edinstveni seznam vozlišč
Utility tokens – Storitveni žetoni
Whitepaper - Beli papir
Witness data - Podatki o podpisu oz. priči