UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VPLIV RAZVOJA TEHNOLOGIJE PODATKOVNIH VERIG IN KRIPTOVALUT NA RAČUNOVODSTVO

Ljubljana, avgust 2017 TOMAŽ KOKELJ

IZJAVA O AVTORSTVU

Podpisani Tomaž Kokelj, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Vpliv razvoja tehnologije podatkovnih verig in kriptovalut na računovodstvo, pripravljenega v sodelovanju s svetovalko prof. dr. Sergejo Slapničar

IZJAVLJAM

1. da sem predloženo delo pripravil/-a 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/-a, 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/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;

7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a 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 _____ Podpis študenta:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Tehnologija veriženja podatkovnih blokov je bila predstavljena leta 2008 skupaj z digitalno valuto bitcoin. Vsak blok v verigi je sestavljen iz različnih kod, ki vsebujejo podatke. Vsak blok je povezan z drugimi bloki s šifriranjem, kar zagotavlja varnost. Tehnologijo veriženja podatkovnih blokov je mogoče primerjati z računovodstvom, saj gre za zapise transakcij, vendar v mreži. Ta mreža je sinhronizirana z različnimi uporabniki po svetu. Princip mreže je v tem, da gre za centralno skladišče vseh transakcij, ki so vidne v vsakem trenutku vsem uporabnikom v mreži (BLLiZ Consultancy, 2017).

Trenutna digitalna ekonomija je osnovana na zanašanju na zaupanja vrednega posrednika. Dejstvo je, da negotovo živimo v digitalnem svetu, ki se sklicuje na tretje osebe, ki zagotavljajo varnost in zasebnost naših digitalnih sredstev. Problem je, da je možno vire teh tretjih oseb manipulirati, ogrožati in tudi vdreti vanje (Crosby, Nachiappan, Patanayak, Venna, & Kalynaraman, 2016).

Namen magistrskega dela je predstaviti in razumeti tehnologijo podatkovnih verig in z njo povezane kriptovalute ter njihov vpliv na področje računovodstva z vidika stroke, sprememb pri poročanju finančnih izkazov in njihovo revidiranje.

Cilji magistrskega dela so pregledati relevantno literaturo ter obstoječe raziskave iz zgoraj omenjenega področja, opredeliti nastanek in pomen tehnologije podatkovnih verig, ugotoviti potencialne uporabnosti tehnologije po različnih industrijah, prikazati razliko med obstoječimi računovodskimi sistemi in sistemom, ki temelji na tehnologiji podatkovnih verig, ter predstaviti potencialne spremembe v računovodski stroki.

Magistrsko delo je teoretične narave, zato je zelo pomemba predpostavka, da so viri verodostojni in dovolj obsežni. V nalogi predpostavljam, da bodo subjekti v poslovnem in finančnem okolju nadaljevali z razvojem in adaptacijo tehnologije. Šele ob predpostavki, da bo tehnologija v prihodnosti dosegla kritično maso sprejetja, lahko dejansko pride do ugotovljenih transformacij in posledic, tudi v računovodstvu.

Največja omejitev tega dela je, da je tehnologija podatkovnih verig šele v razvojni fazi, kar pomeni, da so napovedi njene uporabe in posledic zgolj špekulativne narave. S podrobno predstavitvijo tehnologije na podlagi obstoječih raziskav in mnenj bom poskusil čim bolj natančno predstaviti možne spremembe v računovodski stroki.

Magistersko delo je sestavljeno zgolj iz teoretičnega dela, ki je sestavljen iz treh delov. Prvi del opredeljuje delovanje tehnologije podatkovnih verig, njene lastnosti, koristi in tveganja ter na koncu njeno potencialno uporabo. V drugem delu sledi opredelitev kriptovalut, njihovih lastnosti, koristi in tveganj ter opis trenutno najbolj razširjene kriptovalute, bitcoin. Tretji del aplicira teorijo prvega in drugega dela v računovodstvu.

1 TEHNOLOGIJA PODATKOVNIH VERIG

Tehnologija podatkovnih verig (angl. *blockchain technology*; v nadaljevanju blockchain) je tehnologija, ki je znana predvsem po podpori delovanju digitalne valute bitcoin, vendar pa vse bolj postaja tudi orodje za zagotavljanje varnosti podatkov, prenos digitalnih sredstev in obvladovanje velikih decentraliziranih sistemov. Zaradi številnih optimizacijskih učinkov se tehnologija uporablja že v nekaterih industrijah (predvsem finančni), saj ni potrebnega dragega centralnega nadzora (Koražija, 2017).

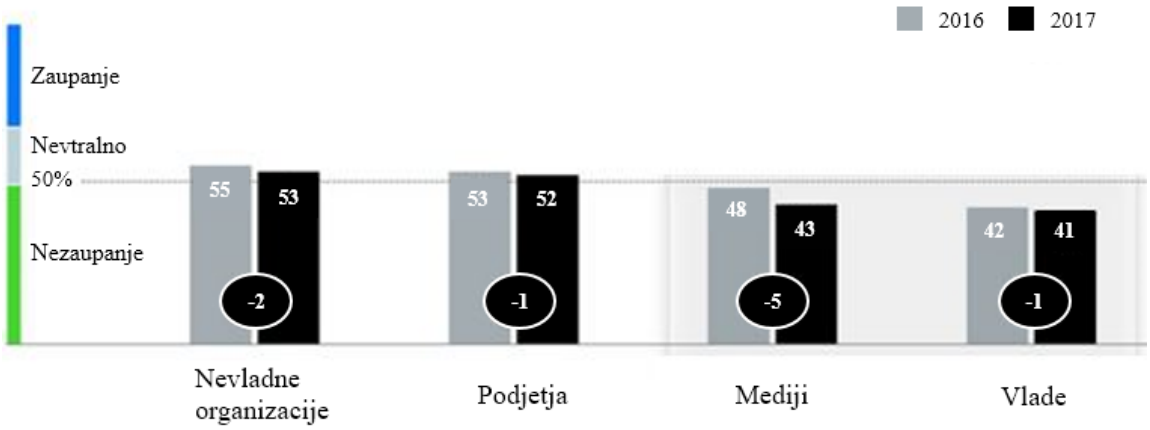
V okviru poglavja o tehnologiji veriženja podatkovnih blokov so opredeljeni razlogi za razvoj tehnologije veriženja blokov, njena opredelitev in kako deluje, katere so njene lastnosti, koristi in nevarnosti uporabe, kakšna je njena potencialna uporaba ter razvoj.

1.1 Razlogi za razvoj tehnologije podatkovnih verig

Tehnologija podatkovnih verig ali blockchain tehnologija se je začela razvijati zaradi dveh temeljnih problemov: problema nezaupanja in problema koncentracije moči.

Problem nezaupanja izhaja iz dejstva, da trenutna infrastruktura interneta ne omogoča dovolj visoke ravni varnosti in zasebnosti. Vrzel so zapolnili posredniki, ki so prevzeli vlogo zagotavljanja varnosti in zasebnosti (Tapscott & Tapscott, 2016). Tovrsten sistem ni popoln in, kot omenjeno, predstavlja svojevrstne omejitve, ki bodo podrobneje predstavljene v nadaljevanju.

Slika 1: Stopnja zaupanja v štiri vrste institucij v letih 2016–2017



Vir: Edelman, 2017 Edelman trust Barometer, 2017.

Podjetje Edelman, ki že veliko let izvaja raziskave o stopnji zaupanja, je v svoji zadnji raziskavi »2017 Edelman Trust Barometer« ugotovilo, da je v letu 2017 prišlo do zgodovinsko največjega padca zaupanja v vse institucije – vlade, podjetja, medije in nevladne organizacije. Stopnjo zaupanja v posamezno vrsto institucije prikazuje Slika 1. Padec splošnega zaupanja je tesno povezan s posledicami globalne finančne krize iz leta 2008 ter globalizacijo in tehnološkim razvojem. Korupcija, imigracije, globalizacija, slabšanje socialnih vrednot in stopnja inovacij so ključni faktorji, ki so prispevali k omenjenemu padcu. Posledica tega je tudi zmanjšanje zaupanja v sistem, katerega spremljajo občutek nepravičnosti, pomanjkanje upanja in samozavesti ter želje po spremembah (Edelman, 2017).

Ponovna vzpostavitev zaupanja je deljena odgovornost med institucijami in prebivalstvom. Institucije se morajo zavezati k dolgoročnemu izboljšanju ekonomskih in socialnih pogojev (Harrington, 2017). Zaupanje je ključnega pomena za družbo in njeno delovanje (Twenge, Campbell, & Carter 2014). Tapscott in Ticoll (2003) definirata zaupanje kot pričakovanje, da bo nasprotna stran ravnala po štirih principih integritete:

- odkritost v pomenu komuniciranja iskrenih, točnih in celovitih informacij s strani organizacij je pomemben faktor v vzpostavljanju zaupanja organizacije s svojimi zaposlenimi, partnerji, kupci, javnostjo in drugimi deležniki.
- upoštevanje v poslovnem svetu pomeni pošteno izmenjavo koristi. Zaupanje in zmožnost sodelovanja v dobri veri med dvema partnerjema zahteva spoštovanje in upoštevanje medsebojnih interesov, želja in občutkov.
- odgovornost zahteva jasne obveze do interesnih skupin in njihovo spoštovanje. Posamezniki in institucije morajo deležnikom ali neodvisnim zunanjim strokovnjakom dokazati, da so spoštovali njihove zaveze in nosili odgovornost pri nespoštovanju.
- transparentnost nalaga aktivno in odprto podajanje informacij interesnim skupinam, ki imajo pravico do teh informacij.

Integriteta sistema je potrebna, da izpolni pričakovanja uporabnikov in okrepi njihovo zaupanje v sistem. V nasprotnem primeru bodo uporabniki zapustili sistem. Doseganje in ohranjanje integritete temelji na številnih faktorjih, najpomembnejša med njimi sta poznavanje števila uporabnikov in poznavanje zanesljivosti uporabnikov. Integriteto je torej najtežje doseči v popolnoma odprtih sistemih, kjer sta ta dva faktorja relativno nepoznana (Drescher, 2017, str. 30). Tehnične okvare in zlonamerni uporabniki sta dve pomembni grožnji pri doseganju integritete. Glavni izziv, ki ga blockchain torej poskuša rešiti, je, kako doseči integriteto in zaupanje v popolnoma distribuiranem vrstniškem omrežju (angl. *peer-to-peer network,* v nadaljevanju P2P omrežje). Število uporabnikov v omrežju je nepoznano, prav tako je nemogoče opredeliti zanesljivost njihovega delovanja. Ta problem je v računalništvu dobro poznan, in sicer kot Byzantinov problem generalov ali tudi problem soglasja (angl. *Byzantine Generals problem*) (Lamport, Shostak, & Pease, 1982).

Ker pogosto ne vemo, kdo je stranka nasproti in ali ravna z integriteto, se moramo zanesti na tretjo osebo, ki jamči za stranko nasproti. Te tretje osebe so različni posredniki. Posredniki hkrati hranijo zapise transakcij in vzpostavljajo poslovno logiko, ki je vodilo spletnega poslovanja. Primeri teh posrednikov so banke, vlade, PayPal, Visa International Service Association, Uber, Apple, Google in druge organizacije (Tapscott & Tapscott, 2016, str. 11).

Drug problem je problem koncentracije moči, ki se nanaša na to, da velika podjetja in države izkoriščajo arhitekturo interneta za povečanje svoje moči in vpliva nad gospodarstvi in družbo. S tem gospodarska moč postaja vse bolj skoncentrirana in zakoreninjena. Namesto širokega in demokratskega dostopa do podatkov se ti kopičijo v določenem krogu organizacij, ki jih izkoriščajo za nadzor in moč (Tapscott & Tapscott, 2016, str. 12).

Trgi, ki izkazujejo mrežne učinke in ekonomije obsega, so bolj nagnjeni k višji koncentraciji, ceteris paribus (Van Gorp & Batura, 2015). Mrežni učinki pomenijo, da imajo uporabniki koristi od večjega omrežja oziroma od večjega števila uporabnikov znotraj omrežja (Rasch, 2017). To velja predvsem za digitalne storitve, kjer so podatki ključnega pomena. Veliki konglomerati, kot so Google, Amazon, Apple, Microsoft, Facebook in podobni, zbirajo ogromne količine podatkov o posameznikih in institucijah, tudi tiste, ki so ustvarjeni v privatne namene in s tem koristijo mrežne učinke. Baze podatkov so postale nov in v tem smislu pomemben razred sredstev. Podobno počnejo tudi vlade, ki lahko z zbiranjem podatkov nadzorujejo in manipulirajo s svojimi državljani, da krepijo svoje interese (Tapscott & Tapscott, 2016, str. 13).

Opisana problema sta bila poglavitna razloga za začetek razvoja tehnologije podatkovnih verig, saj se z razvojem te tehnologije zmanjšujeta nezaupanje in koncentracija moči.

1.2 Opredelitev tehnologije podatkovnih verig

Tehnologijo podatkovnih verig poznamo tudi pod izrazom »tehnologija veriženja podatkovnih blokov«. Po definiciji je blockchain distribuirana digitalna baza podatkov ali, z uporabo računovodske terminologije, glavna knjiga (Wunsche, 2016, str. 3). Prvič je bila predstavljena kot podporna arhitekturna tehnologija za digitalno valuto bitcoin leta 2008, ko jo je v svojem poročilu opisala oseba pod psevdonimom Satoshi Nakamoto (Byström, 2016, str. 3). Natančneje lahko tehnologijo podatkovnih verig definiramo kot digitalno, časovno posodobljeno, porazdeljeno in kriptografsko zapečateno bazo podatkov. Prenos podatkov poteka preko mreže različnih uporabnikov, med katerimi se delijo podatki. Baza vsebuje vse informacije v zvezi s podatki in hkrati omogoča, da identiteta sodelujočih ostane zaupna. Baza je vidna vsem sodelujočim, vendar pa se lahko posodobi samo ob potrditvi večine sodelujočih. Kar je pomembno, je, da ko so podatki enkrat zavedeni v bazi, se ne morejo več izbrisati (Deloitte, 2016a, str. 6).

Nastanek tehnologije izhaja iz ideje posedovanja digitalnega sredstva, ki ga je mogoče varno prenesi med dvema uporabnikoma brez posredovanja tretje osebe (Mazonka, 2016). Digitalna sredstva so lahko ustvarjena s strani omrežja (kriptovalute, digitalni vrednostni papirji, digitalni podatki, certifikati, finančna poročila, glasovi itd.) ali pa so digitalna reprezentacija fizičnega sredstva. Zadnje imenujemo tudi simbolična sredstva (angl. *tokenized assets*) (Financial Industry Regulatory Authority, 2017, str. 3). Tehnologija omogoča varen in učinkovit način prenosa lastniških pravic nad temi sredstvi ter vpliva na nastanek novih konceptov, kot so pametne pogodbe (angl. *smart contracts)*. Pametnim pogodbam se napoveduje močan vpliv na sklepanje poslov (Šutanovac, 2017).

Tretje osebe, kot so centralne institucije in drugi posredniki, vzpostavljajo zaupanje v sistem z zagotavljanjem njegove integritete. Odsotnost teh posrednikov povzroča dva osrednja problema (Friedlmaier, Tumasjan, & Welpe, 2016, str. 3):

- digitalna sredstva so lahko nerazločljivo in neskončno kopirana. Hkrati jih je mogoče istočasno uporabiti večkrat. Problem je poznan kot problem dvojne porabe, zato je potrebno zagotoviti, da nihče ne more istega digitalnega sredstva porabiti dvakrat (Swan, 2015, str. 2). Rešitev tega problema je kriptografsko časovno zaznamovanje transakcij.
- zanesljiv računalniški sistem mora biti sposoben obvladovati odpoved ali nepošteno ravnanje ene ali več komponent. Nezanesljivost predstavlja način delovanja, ki je pogosto spregledan (npr. pošiljanje konfliktnih informacij različnim delom sistema). Ta problem se imenuje Byzantinov generalov problem. Blockchain je oblikovan na podlagi Byzantinove tolerance odpovedi, saj pričakuje mogoče okvare in nepošteno ravnanje uporabnikov. Cilj tehnologije je odstraniti človeški faktor iz faze procesiranja ter ga nadomestiti z rigorozno definiranim in javno dostopnim protokolom, ki bi ga vsiljevalo omrežje neodvisnih računalnikov (BitFury Group & Garzik, 2015b, str. 15).

V naslednjem poglavju bom z obrazložitvijo delovanja tehnologije podatkovnih verig predstavil doseganje rešitve teh problemov. Z uporabo deljenega omrežja in pametne kriptografije je Satoshi Nakamoto izdelal model soglasij, ki rešuje omenjene probleme brez vpletenosti tretje osebe (Tapscott & Tapscott, 2016, str. 5).

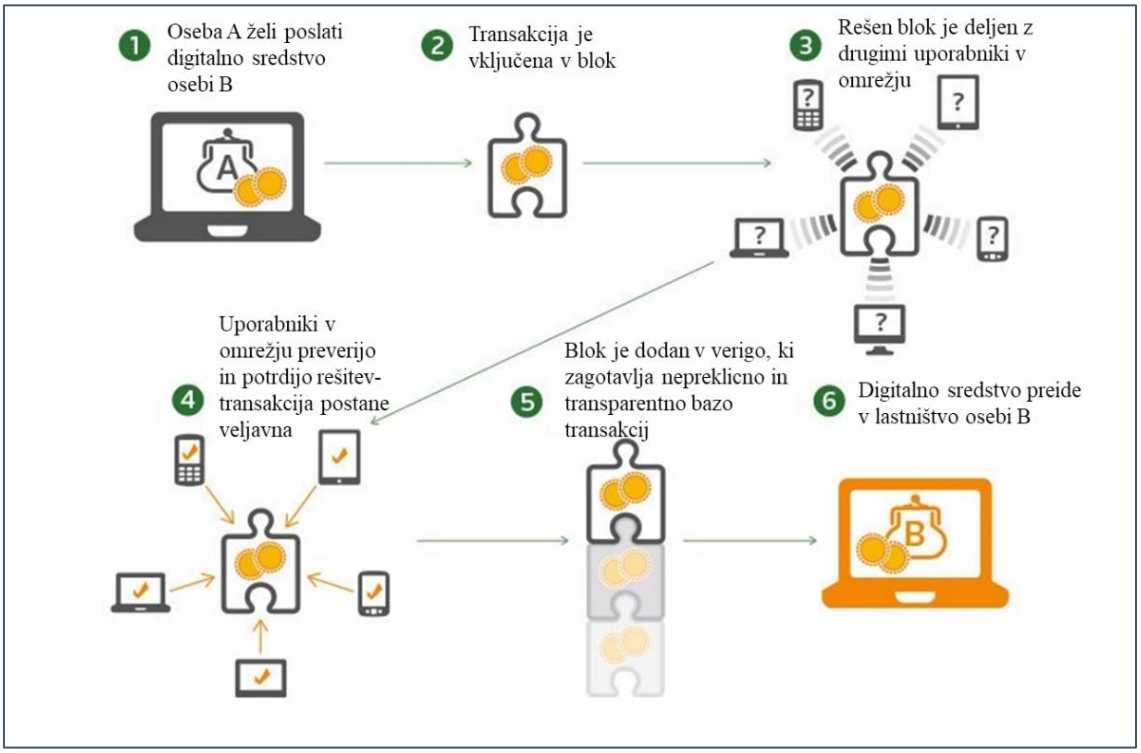
1.3 Delovanje tehnologije podatkovnih verig

V sklopu poglavja o delovanju tehnologije podatkovnih verig je opredeljen temeljni princip delovanja, rudarjenje in njegova ekonomska iniciativa, vrste razcepitev verig in modeli potrjevanja transakcij digitalnih sredstev.

1.3.1 Temeljni princip delovanja

Blockchain baza podatkov ima obliko verige, ki jo sestavljajo bloki. Bloki vsebujejo podatke o prenosu lastništev digitalnih sredstev. Veriga blokov je ustvarjena in vzdrževana preko P2P omrežja med seboj povezanih računalnikov oziroma uporabnikov (Financial Industry Regulatory Authority, 2017, str. 3). Uporabnik (angl. *node*) lahko zavzema različne vloge. Ločimo tri glavne funkcije: predlaganje, potrjevanje in preverjanje transakcij. Transakcije se izmenjujejo in beležijo v javnem sistemu (angl. *public ledger*) (Šutanovac, 2017). Slika 2 prikazuje osnovni proces delovanja tehnologije podatkovnih verig.

Slika 2: Osnovni proces prenosa digitalnih sredstev na podlagi tehnologije podatkovnih verig



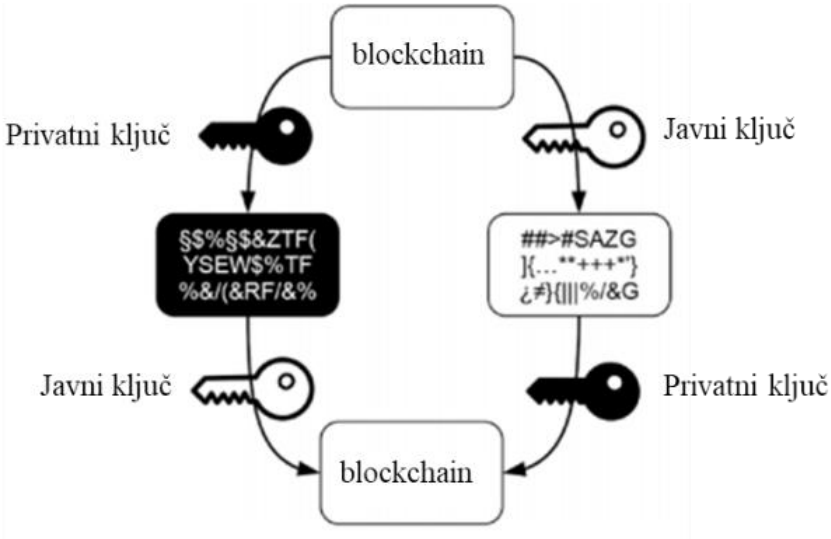
Vir: World Economic Forum, How will blockchain technology transform financial services?, 2015.

Dva uporabnika, ki si želita izmenjati digitalno sredstvo, to storita z uporabo asimetrične kriptografije (angl. *public-key cryptography*) in soglasnega sistema potrjevanja (Brito & Castillo, 2013, str. 5).

Asimetrična kriptografija je temelj za identificiranje uporabnikov in zaščito njihovih sredstev pred dostopom nepooblaščenih oseb. S pomočjo le-te se zaščiti premoženje, ki je vezano na račune oziroma lastnike. Medtem ko se pri simetrični kriptografiji uporabi isti ključ tako za šifriranje kot dešifriranje, se pri asimetrični kriptografiji ključa razlikujeta. Ta dva ključa tvorita par medsebojno ustreznih ključev. V predstavljenem procesu ključa

imenujemo privatni in javni ključ (Drescher, 2017, str. 94–98). Javni ključi predstavljajo »naslov« uporabnika v omrežju (številke računov), na katere lahko uporabniki prenašajo pravice do lastništev sredstev (so znani celotnemu omrežju). Poleg identifikacije računov so javni ključi uporabljeni tudi za avtorizacijo transakcij. Dostop do računov je na drugi strani omejen le na tiste, ki imajo v lasti privatni ključ do tega računa (znani le posameznemu uporabniku) (Financial Industry Regulatory Authority, 2017, str. 3). Oba sta sicer lahko uporabljena za obe metodi – šifriranje in dešifriranje. Slika 3 predstavlja prikaz postopka asimetrične kriptografije, v katerem s črnim ključem (privatni ključ) uporabnik šifrira podatke. Slednji so lahko dešifrirani le z belim ključem (javni ključ) ali obratno (Van Tilborg & Jajodia, 2014).

Slika 3: Prikaz asimetrične kriptografije (uporaba javnega in privatnega ključa za šifriranje in dešifriranje)

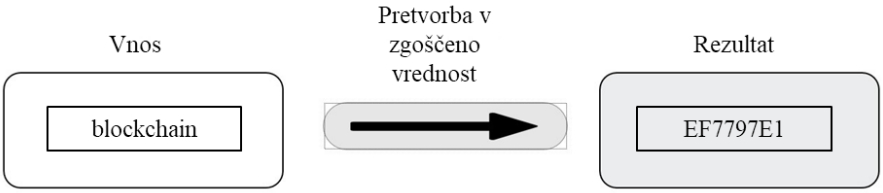


Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

Obstajajo številni modeli potrjevanja transakcij. Najbolj pogosto uporabljen model je »dokazilo o delu« in je zaradi svoje razširjenosti tudi podrobneje predstavljen v nadaljevanju (poglavje 1.3.4).

V prvem koraku se z metodo zgoščevalne funkcije (angl. *hashing*) nizu podatkov sredstva aplicira zapleteno matematično formulo z namenom šifrirati podatke v zgoščeno vrednost (v nadaljevanju angl. *hash*) ali digitalen niz naključnih številk in črk (Mazonka, 2016, str. 1). Ker gre za uporabo asimetrične kriptografije (SHA-256), je povratna pretvorba nemogoča brez ustreznega ključa (Financial Industry Regulatory Authority, 2017, str. 21). Za posamezno sredstvo se torej generira edinstven hash, kot to prikazuje Slika 4.

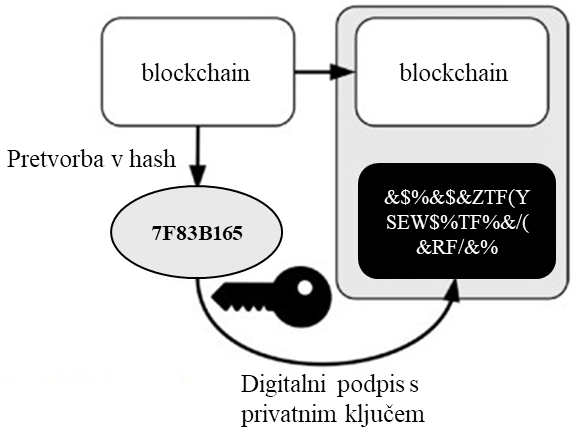
Slika 4: Postopek generiranja zgoščene vrednosti iz podatkov



Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

Pošiljatelj sredstva z metodo asimetrične kriptografije nato digitalno podpiše hash sredstva, ki ga želi prenesti (Mazonka, 2016, str. 2). Digitalni podpis deluje tako, da originalne podatke (na Sliki 5 »blockchain« predstavlja originalni podatek) najprej pretvorimo v hash. V naslednjem koraku hash podatkov šifriramo s privatnim ključem uporabnika. Šifriran hash podatkov je torej digitalni podpis podatka. Podatek in digitalni podpis sta skupaj objavljena v omrežju. (Drescher, 2017, str. 105). Digitalni podpis je unikaten za vsako transakcijo.

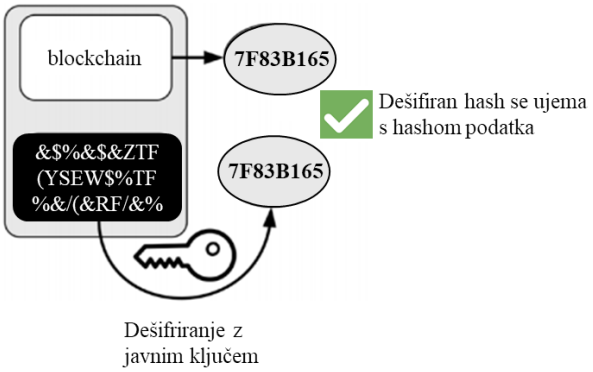
Slika 5: Prikaz digitalnega podpisa



Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

Zunanji uporabnik lahko preveri verodostojnost transakcije tako, da z javnim ključem prejšnjega lastnika dešifrira njegov digitalni podpis. V kolikor se rezultat ujema s hashem sredstva, potem to služi kot dokaz, da je oseba resnično podpisala prenos. Če v vmesni fazi pride do spremembe podatkov, se hash podatkov ne ujema z dešifriranim hashem (Mazonka, 2016, str. 2). Preverbo veredostojnosti digitalnega podpisa prikazuje Slika 6.

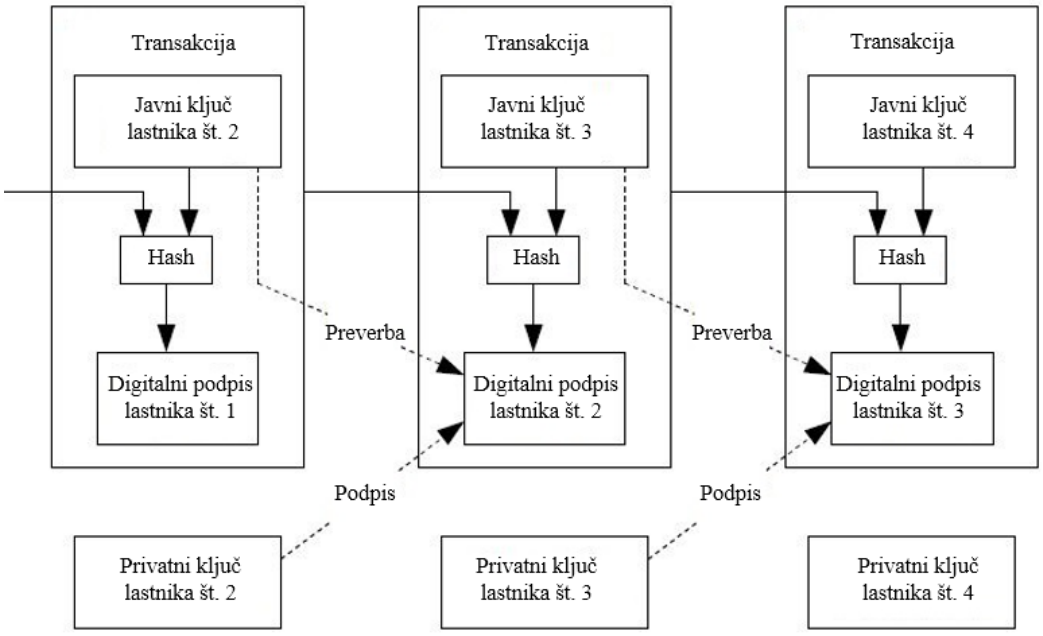
Slika 6: Ilustracija preverbe verodostojnosti digitalnega podpisa



Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

Slika 7 prikazuje, da vsaka transakcija vključuje hash sredstva, javni ključ lastnika sredstva in digitalni podpis prejšnjega lastnika. Podpis dokazuje, da je prejšnji lastnik potrdil prenos.

Slika 7: Zaporedje večkratnega prenosa sredstva



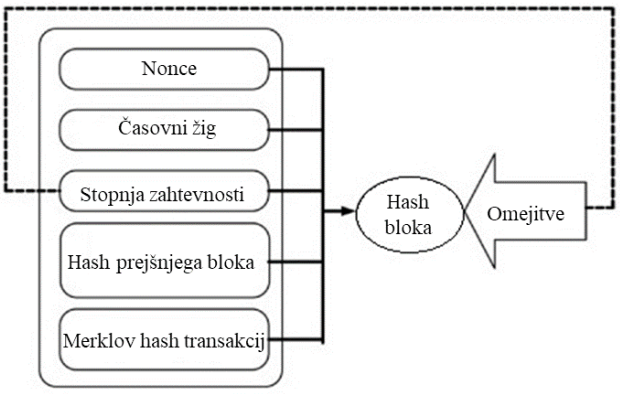
Vir: S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

Vse transakcije so javno objavljene v omrežju. V naslednjem koraku uporabniki združijo določeno število transakcij v blok. Transakcije znotraj bloka so združene v Merklovem drevesu in se na koncu agregirajo v enoten hash transakcij (Merkle, 1998). Blok je sestavljen iz dveh polj, glave in telesa. Telo vsebuje Merklovo drevo transakcij (podatke), glava pa ključne informacije. Ključne informacije so sledeče (Kuo Chuen, 2015, str. 49):

- zgoščena vrednost (hash) prejšnjega bloka, na katerega se povezuje blok (n-1);
- merklov hash vseh vsebovanih hashev transakcij;
- časovni žig, ki kreiranje bloka časovno zaznamuje do sekunde natančno;
- bitno polje, ki predstavlja zahtevnost matematične uganke. Zahtevnost uganke je izražena skozi omejitve oziroma določeno število začetnih ničel, ki jih mora končni hash vsebovati. Večje kot je število ničel, težja je uganka, saj zmanjšuje razpon potencialnih rešitev (Drescher, 2017, str. 91);
- naključna vrednost (angl. *nonce*), ki predstavlja matematično uganko. Rudarji iščejo pravi hash bloka s spreminjanjem te poljubne vrednosti, dokler ta ne ustreza omejitvam v prejšnji postavki – določenemu številu ničelnih bitov. Ko pridejo do prave vrednosti nonca, rudarji delijo to vrednost z drugimi uporabniki, ki lahko preverijo to rešitev.

Osebe, ki so odgovorne za združevanje transakcij in oblikovanje blokov ter njihovo dodajanje v verige, se imenujejo rudarji (angl. *miners*). Njihova naloga je, da bloku določijo zgoščeno vrednost bloka. Zgoščena vrednost bloka je dobljena iz kombinacije sestavin glave bloka (Mazonka, 2016). To storijo tako, da namenjajo računalniške zmogljivosti in energijo za tekmovanje v reševanju matematične uganke (algoritmi) oziroma iščejo pravo vrednost naključne vrednosti. Proces reševanja zato imenujemo rudarjenje (angl. *mining*) (Nakamoto, 2008, str. 3). Hash uganke so lahko rešene z metodo preizkušanja in napak. Metoda zahteva ugibanje prave vrednosti naključne številke in iskanje hasha, ki zadovoljuje dane omejitve. Slika 8 prikazuje proces pridobitve hasha novega bloka.

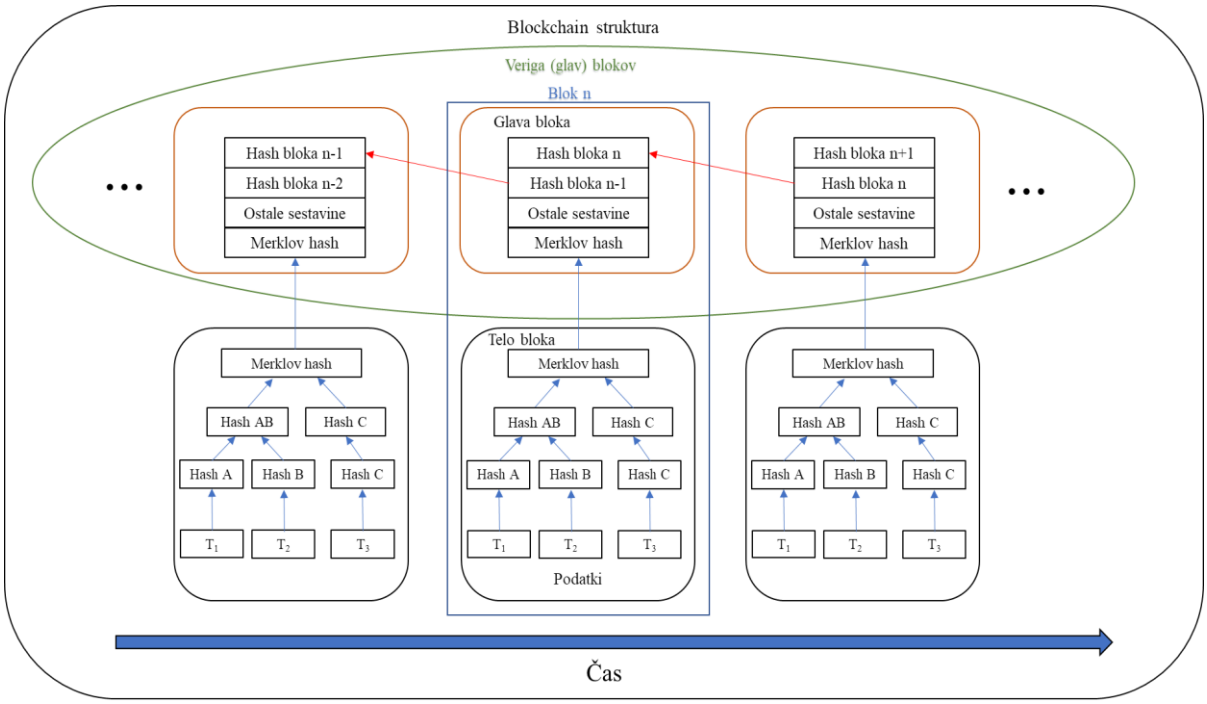
Slika 8: Shema pridobitve zgoščene vrednosti novega bloka



Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

Zgoščena vrednost bloka deluje kot kriptografski prstni odtis, ki omogoča, da so vse transakcije preverljive. V principu je podobno iskanju zmagovalnih loto številk. Večjo možnost imajo tisti, ki posedujejo moderno računalniško opremo in se hkrati povezujejo z drugimi rudarji. Glavni faktorji so torej sreča, procesorska moč in velikost delovne skupine.

Slika 9: Struktura blockchain verige



Povzeto in prirejeno po R. C. Merkle, A digital signature based on a conventional encryption function, 1998; O. Mazonka, Blockchain: Simple Explanation, 2016; S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008; D. Drescher, Blockchain basics: A non-technical introduction, 2017.

Slika 9 povzema v tem poglavju opisane korake v končno strukturo blockchain verige. Tovrsten proces potrjevanja transakcij se nanaša na model »dokazilo o delu«. Rešitev se nato deli z drugimi uporabniki v omrežju. Slednji preverijo rešitev in jo v primeru ujemanja potrdijo. S tem se ustvari konsenz, blok se doda obstoječi verigi in transakcije znotraj bloka se izvedejo (Tapscott & Tapscott, 2016, str. 240–241).

Pomembnost rudarjenja je v nadaljevanju opredeljena preko njihove ekonomske iniciative in razcepitve verig.

1.3.2 Ekonomska iniciativa rudarjev

V popolnoma odprtem P2P omrežju lahko vsak uporabnik potrdi blok. V zaprtih sistemih je število potrjevalcev omejeno. Podrobna opredelitev razlike med obema sistemoma sledi v poglavju »Odprti in zaprti blockchain sistemi«. Rudarji tekmujejo v reševanju matematičnih ugank in dodajanju blokov s ciljem, da pridejo do nagrade. Spodbuda je nagrada v obliki vgrajenega žetona (angl. *token*), ki nosi vrednost. Lahko gre za enoto kriptovalute ali transakcijske provizije. Na tovrsten način so kriptovalute tipično povezane s tehnologijo podatkovnih verig. S tem se ustvarja spodbuda za ohranjanje in vzdrževanje decentraliziranega odprtega sistema. Z večjim številom uporabnikov se poveča vrednost

žetonov, ker kriptovaluta postane bolj uporabna. To posledično privlači več rudarjev, kar ultimativno poveča varnost omrežja (Catalini & Gans, 2016, str. 8–9).

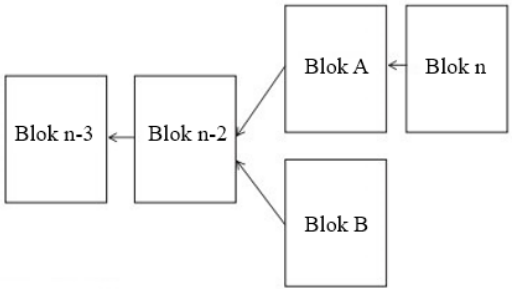
Po besedah The Economist (2015) rudar, ki najde rešitev, prejme 25 bitcoinov kot nagrado, ampak šele potem, ko je dodanih naslednjih 99 blokov v verigo. Prvotno so bili rudarji za vsak uspešen blok nagrajeni s 50 bitcoini. Nagrada se sicer razpolovi na vsakih 210.000 potrditev ali na okoli 4 leta. Dodatno rudarji zaslužijo tudi s transakcijskimi provizijami (Kuo Chuen, 2015, str. 50). To je spodbuda rudarjem za sodelovanje in potrjevanje transakcij v bitcoin sistemu. Celotna vrednost prihodkov rudarjev, izražena v ameriških dolarjih, v bitcoin sistemu se je v obdobju december 2016–junij 2017 gibala med 1,2 milijonov $ in 7,2 milijonov $ (Blockchain Luxembourg, 2017a). Podrobnejši dejavniki visoke fluktuacije prihodkov in tržne vrednosti bitcoina so opredeljeni v poglavju 2.4.

1.3.3 Razcepitev verige

Obstaja možnost, da rudarji istočasno pridejo do rešitve, kar pomeni, da sta dva, ali več, bloka dodana verigi v istem trenutku. To povzroči začasno razcepitev verige. Obstajata dve vrsti razcepitve: mehka in trda razcepitev.

Kadar gre le za razcepitev verige brez sprememb v protokolu, to imenujemo mehka razcepitev (Sikorski, Haugton, & Kraft, 2017, str. 3). Tudi po razcepitvi rudarji nadaljujejo s potrjevanjem blokov. Tista veja verige, ki prva dobi nov blok, postane najdaljša in hkrati tudi edina veljavna. Kot prikazuje Slika 10, bodo v takšnem primeru rudarji v naslednji fazi nadaljevali z verigo A. Blok B postane osamljen blok (Kuo Chuen, 2015, str. 51). Najdaljša veriga namreč v primeru modela »dokazila o delu« predstavlja največ kumulativnega vloženega računalniškega dela. Slednje onemogoča tudi razcepitev verige v preteklosti, saj bi nova veja potrebovala dovolj veliko procesorske moči, da bi dohitela in prehitela obstoječo najdaljšo verigo. Za to bi oseba ali skupina potrebovala vsaj 51 % procesorske zmogljivosti celotnega omrežja (Poon & Dryja, 2016).

Slika 10: Razcepitev verige



Vir: D. L. Kuo Chuen, Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Data, 2015.

Osamljeni bloki, ki so izločeni iz glavne verige, ne prispevajo k prenosu lastništev sredstev. Transakcije, vsebovane v teh blokih, so vrnjene med nepotrjene transakcije in so ponovno vključene v glavno verigo z naslednjim veljavnim blokom. Podobno kot transakcije tudi nagrade za osamele bloke postanejo neveljavne (Drescher, 2017, str. 174–175).

Do sedaj se je najdaljša razcepitev bitcoin blockchain verige zgodila leta 2013, ko je zaradi hrošča v protokolu nastalo 24 blokov v vzporedni verigi. Statistično je malo verjetno, da bi razdvojitev verige trajala več kot nekaj blokov. V povprečju so najdaljše razcepljene verige dolge do 6 blokov. To pomeni, da ko bloku sledi več kot 6 blokov, lahko z veliko gotovostjo transakcijo smatramo kot dokončno (BitFury Group & Garzik, 2015b, str. 6).

Trda razcepitev na drugi strani pomeni, da se v infrastrukturi sistema (koda protokola) zgodi pomembna sprememba (novi algoritmi, pravila, modeli potrjevanja, standardi itd.) in veriga se odcepi v popolnoma nov sistem. Ta deluje po novih pravilih in je nepovraten (Swan, 2015). Uporabniki, ki se odločijo uporabljati nov sistem, ne morejo istočasno delovati tudi v starem sistemu. Na tak način so nastale druge oblike kriptovalut in sistemov, ki so spremenile originalno kodo, pod katero je nastala bitcoin kriptovaluta (Kuo Chuen, 2015).

1.3.4 Modeli potrjevanja transakcij

Modeli potrjevanja transakcij opredeljujejo proces doseganja soglasja, v katerem se večina (ali v nekaterih primerih vsi) potrjevalcev v omrežju strinja glede stanja blockchain sistema. Cilj vseh modelov je zagotavljati varnost omrežja ob odsotnosti centralnih oseb (Swanson, 2015). S tehničnega vidika to dosegajo z različnimi načini reševanja matematičnih ugank za potrjevanje blokov (Tapscott & Tapscott, 2016, str. 262). Ključne diferencialne lastnosti so čas, način in število uporabnikov za potrjevanje in zapis blokov (Financial Industry Regulatory Authority, 2017, str. 3). Predvsem je pomembno, da je protokol soglasja objektiven pri določanju stanja sistema in ga obvladujejo pošteni uporabniki (Milutinovic, He, Wu, & Kanwal, 2017).

»Dokazilo o delu« je med vsemi najbolj razširjen model, predvsem po zaslugi bitcoin verzije tehnologije podatkovnih verig. Kljub temu obstaja vrsta alternativnih modelov doseganja soglasja, ki odpravljajo nekatere slabe lastnosti modela dokazila o delu ali pa so bolj primerne za potrebe posameznih vrst in velikosti blockchain sistemov (Swan, 2015, str. 84).

Koncept dokazila o delu (v nadaljevanju angl. *Proof-of-Work*) je prvi uvedel Back (2002) in temelji na računalniški moči in povezanih stroških energije. Glavna značilnost modela je, da je za pridobitev prave zgoščene vrednosti bloka (rešitev uganke) potrebno vložiti ogromno dela v obliki procesorske moči in energije (elektrike) za poganjanje strojne opreme. Če je za rešitev potrebno ogromno dela, pa je njena preverba hitra in enostavna. Vsakdo lahko objavljeno vrednost lastnoročno preveri, če se ujema z njegovo vrednostjo bloka (Tapscott

& Tapscott, 2016). Najdaljša veriga blokov izraža največ vloženega dela. Če je večina uporabnikov poštenih, potem bo poštena veriga rastla hitreje kot ostale. Napadalec, ki bi želel spremeniti vsebino preteklega bloka, bi moral ponovno izvesti delo tega bloka, vseh nadaljnih blokov in preseči trud obstoječih poštenih uporabnikov na vseh kopijah sistema istočasno. Verjetnost, da bi počasnejši napadalec dohitel trenutni blok, pada eksponentno z vsakim novim dodanim blokom (Nakamoto, 2008, str. 3). Z vidika teorije igre prav potratna narava rudarjenja povečuje varnost tehnologije (Catalini & Gans, 2016, str. 10).

Nasprotniki Proof-of-work modelu očitajo visoko potratnost z vidika energije in odpadnih materialov (strojna oprema). Velik delež nagrade je porabljen za stroške elektrike. Druga negativna stran je časovna neučinkovitost, saj lahko traja tudi eno uro za doseganje razumnega števila potrditev rešitve (Kwon, 2015). Predvsem privatna omrežja raziskujejo uporabo alternativnih modelov potrjevanj, ki omogočajo krajše čase (Financial Industry Regulatory Authority, 2017, str. 3).

Po definiciji je dokazilo o deležu (v nadaljevanju angl. *Proof-of-Stake)* dokaz o lastništvu (Poelstra, 2015, str. 8). Model od udeležencev zahteva, da investirajo in hranijo določeno vrednost žetonov ali sredstev (Tapscott & Tapscott, 2016). S tehničnega vidika je možnost rudarjenja uporabnika sorazmerno odvisna od količine sredstev, ki jih ima v lasti. Če uporabnik drži 5 % vrednosti vseh sredstev omrežja, potem ima 5 % verjetnost, da ustvari in potrdi blok ter prejme nagrado (Kuo Chuen, 2015, str. 47). Uporabniki z največjim deležem v omrežju imajo največ interesa za vzdrževanje varnega omrežja, saj je njihova izguba sicer največja (BitFury Group, 2015c, str. 2). Proof-of-Stake je drugi najbolj razširjen model. Model zmanjšuje čas potrjevanja transakcij, zahteva manj računalniške moči in posledično porablja manj energije in drugih sredstev (npr. opreme) (Swan, 2015, str. 84). Za razliko od modela Proof-of-Work, kjer mora napadalec omrežja upravljati z 51 % procesorske moči, mora v tem modelu imeti v lasti 51 % vrednosti omrežja (Kuo Chuen, 2015, str. 47).

Ena izmed verzij modela je tudi delegirano dokazilo o deležu (angl. *delegated proof-of-stake*), v katerem so bloki soglasno potrjeni s strani vnaprej določenih uporabnikov. Ti so za to nagrajeni ali kaznovani v primeru zlonamernega vedenja. Delegirane uporabnike je mogoče zamenjati po določenem času (mandatu) (BitFury Group, 2015c, str 7).

Model Proof-of-Stake zmanjša stroške vzdrževanja omrežja in vstopne ovire. Na drugi strani prav ti dve lastnosti povečata ranljivost proti vdorom, saj model ne vsebuje iniciative za sledenje le eni verziji verige. Če so sredstva razdeljena enakomerno, obstaja večja možnost za razcepitve in potencialne napade na sistem. V nasprotnem primeru, ko je delež sredstev skoncentriran v manjšem številu uporabnikov, obstaja nevarnost selektivnega in centraliziranega potrjevanja transakcij. Prav tako ta model v svojem konceptu predstavlja skrb, da lastniki večjega deleža sredstev ne bodo imeli iniciative razdeljevati svoja sredstva. Delež sredstev namreč predstavlja njihovo moč v omrežju. V nasprotju so v Proof-of-Work

sistemih rudarji prisiljeni k izboljšanju procesorske moči in optimiziranju, če želijo povečati svojo moč (BitFury Group, 2015c). Bogatejši uporabniki bodo potrjevali nove bloke bolj pogosto in zaradi tega hitreje postajali še bogatejši kot ostali (Patterson, 2015).

Veliko novih blockchain sistemov, predvsem tistih, vezanih na kriptovalute, se poslužuje mešanic obeh sistemov. Proof-of-Work največkrat služi kot način pridobivanja novih sredstev, Proof-of-Stake pa kot način doseganja soglasja. Sistemi v začetku obstoja temeljijo na Proof-of-Work modelu. Proof-of-Stake se nato doda z zamikom, ko sistem postane bolj zrel in so sredstva bolj enakomerno porazdeljena (BitFury Group, 2015c, str. 13).

Modela Proof-of-Work in Proof-of-Stake sta trenutno edina, ki sta uporabljena tudi v praksi. Obstaja tudi vrsta drugih teoretičnih modelov, ki so se razvili iz teh dveh. Primera sta modela dokazilo o aktivnost (angl. *Proof-of-Activity*) in dokazilo o kapaciteti (angl. *Proof-of-Capacity*). Bentov, Gabizon in Mizrahi (2014) so ustvarjalci prvega, ki nadgrajuje Proof-of-Work model na način, da od naključnega števila udeležencev zahteva dodaten podpis bloka s šifriranimi ključi. Ti so izbrani po principu deleža sredstev (Proof-of-Stake model). Drugi model (Proof-of-Capacity) od uporabnikov zahteva dodelitev kapacitete na trdih diskih za izvajanje procesa rudarjenja. Z večjo kapaciteto trdega diska ima rudar večje možnosti, da potrdi naslednji blok in si zagotovi nagrado (Castor, 2017).

1.4 Lastnosti tehnologije podatkovnih verig

Tehnologija uporablja kriptografska orodja in distribuiran proces doseganja soglasja. V naslednjih podpoglavjih so predstavljene ključne lastnosti tehnologije podatkovnih verig.

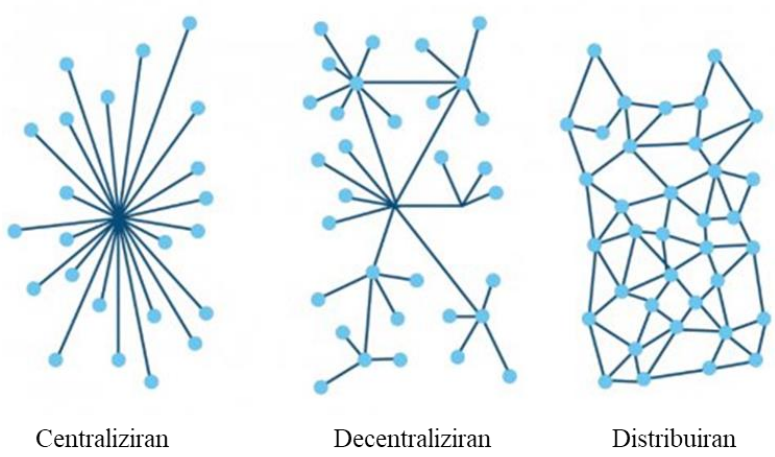
1.4.1 Mrežna integriteta

Integriteta je prisotna v vsakem koraku procesa in je distribuirana med vse uporabnike. Tehnologija vzpostavlja integriteto skozi tri glavne komponente sistema: prva je podatkovna integriteta. Podatki, ki so uporabljeni in hranjeni, so popolni, točni in brez nasprotij. Druga komponenta je vedenjska integriteta, ki narekuje, da sistem deluje na način, kot je bil zasnovan in ne vsebuje logičnih napak. Zadnja, tretja, komponenta je varnost. Sistem je zmožen omejiti dostop do podatkov in funkcionalnosti le za pooblaščene uporabnike (Drescher, 2017, str. 6; Boritz, 2005). Integriteta se izkazuje tudi skozi sposobnost doseganja resničnega stanja lastništva nad sredstvi in zagotavlja, da ima samo zakonit lastnik možnost prenesti lastniške pravice na druge (Drescher, 2017, str. 47). Uporabniki zato izmenjujejo vrednosti in sredstva neposredno s pričakovanjem, da bo proces poskrbel za integriteto nasprotne stranke. Dejanja, ki ne vključujejo principov integritete, so namreč nemogoča ali zahtevajo ogromno časa, denarja, energije in negativnega ugleda (Tapscott & Tapscott, 2016, str. 30–33). Soglasni sistem vzpostavlja integriteto tudi, če določeno število uporabnikov ne ravna skladno s principi integritete (Biella & Zinetti, 2016, str. 7).

1.4.2 Distribuirana moč

Tehnologija veriženja podatkovnih blokov distribuira moč čez celotno P2P omrežje brez enotne točke koordinacije ali kontrole. Potreba po zaupanja vrednem posredniku je odpravljena, ker uporabniki lahko zaupajo sistemu javnih baz podatkov, ki so decentralizirano in distribuirano shranjene in vzdrževane pri mnogih uporabnikih omrežja. Pri tem je potrebno poudariti, da so kopije baz med sabo konsistentne in ažurne (Swan, 2015). Kot grobo pravilo velja, da v trenutku, ko sistem vsebuje enotno komponento, ki lahko ogrozi celoten sistem, tak sistem ne velja kot distribuiran (Drescher, 2017, str. 17). Distribuirano omrežje je popolnoma decentralizirano, medtem ko decentralizirano omrežje še ne pomeni, da je distribuirano. Distribuirano omrežje temelji na sodelovanju številnih uporabnikov, ki si razdelijo upravljanje omrežja in druge funkcije. Decentraliziranost na drugi strani pomeni, da delovanje omrežja ni odvisno le od ene komponente. Bolj kot so funkcije razdeljene enakovredno in med čim večjim številom uporabnikov, tem bolj lahko govorimo o popolni distribuiranosti (Kuo Chuen, 2015, str. 46). Kot prikazuje Slika 11, so v centraliziranem sistemu uporabniki povezani z eno centralno komponento, ki prevladuje nad celotnim sistemom. Tak subjekt upravlja z ogromnimi količinami podatkov, ki jih lahko brez vednosti uporabnikov analizira in uporablja za lastne namene (Tapscott & Tapscott, 2016, str. 119). Točke na Sliki 11 predstavljajo uporabnike, črte pa povezave med njimi.

Slika 11: Slikovni prikaz različnih oblik komuniciranja v sistemih



Vir: P. Baran, On distributed communications: Introduction to distributed communications networks, 1964.

Tanenbaum in Van Steen (2007) opredeljujeta naslednje glavne prednosti distribuiranih sistemov: večja računska moč (z vsakim priključenim računalnikom se ta poveča), delitev stroškov, večja zanesljivost (okvara ali zamenjava posameznega računalnika ne vpliva na delovanje sistema), doseganje naravne rasti (dodajanje novih računalnikov ali povečevanje zmogljivosti obstoječih).

1.4.3 Vrednost kot spodbuda

Tehnologija podatkovnih verig poenoti motiv za vse deležnike preko kompenzacij za nadgrajevanje in vzdrževanje sistemov. Ker vsi sledijo istemu motivu, postane njihovo vedenje sledljivo (Tapscott & Tapscott, 2016, str. 36–37). Instrumenti plačila za kompenziranje uporabnikov morajo čim manj posegati v cilje in vrednote tehnologije. Idealne lastnosti instrumentov so: digitalna oblika, so sprejemljivi za plačilo v realnem svetu in v vseh državah, vrednost je stabilna (tveganje izgube kupne moči), so zaupanja vredni in niso kontrolirani s strani centralne organizacije ali države (Drescher, 2017, str. 186). Na podlagi tega so nastale kriptovalute, neodvisne digitalne valute. Ker si uporabniki lastijo te valute, je v njihovem interesu, da zagotovijo nadaljnji obstoj in dolgoročni uspeh omrežja.

1.4.4 Varnost

Tehnologija podatkovnih verig vključuje varnostne ukrepe, ki omogočajo zaupnost, pristnost, kršitve pa postanejo otežene (Tapscott & Tapscott, 2016, str. 39–40). Najbolj izraziti primeri nepoštenega ravnanja so: predlaganje transakcij v imenu drugega, potrjevanja neveljavnih transakcij, preobremenitev rudarjev z veliko količino mikro transakcij, zavrnitev procesiranja transakcij itd. Kakršne koli spremembe, bodisi v podatkih, sestavi drevesa transakcij ali v glavi bloka, povzročijo nekonsistentnost baze. Infrastruktura deluje popolnoma objektivno, saj je ne zanimajo motivi ali identiteta osebe, ki želi vnesti spremembo. Zanima jo le pravilnost in konsistentnost medsebojno povezanih zgoščenih vrednosti (Drescher, 2017). Nespremenljivost in končnost transakcij sta zagotovljeni z razdelitvijo transakcij v časovno urejene bloke, ki so medsebojno kriptografsko povezani (BitFury Group & Garzik, 2015a, str. 7). Teoretično gledano je sicer spremembe v bazi mogoče doseči, vendar se izkaže, da so s tem povezani ogromni stroški, ki presegajo koristi. Stopnja nespremenljivosti je odvisna od računskih stroškov, povezanih z reševanjem uganke. Nizka težavnost uganke zmanjšuje stroške in posledično povečuje tveganje spreminjanja, ter obratno (Okupski, 2016). Revizijska sled, ki je zgrajena z dodajanjem novih blokov, čez čas hkrati postane bolj odporna proti prirejanju zaradi vse več vloženega računskega dela in energije (Catalini & Gans, str. 9).

1.4.5 Privatnost

Ker uporabnikom ni treba zaupati drugim, ni potrebe po poznavanju identitet drugih. To po eni strani odpravlja moč nadzora centralnih avtoritet, ki podatke o posameznikih izkoriščajo za lastne namene. Transakcije v blockchain sistemu niso vezane na identiteto nasprotne stranke, temveč na njegov naslov (javni ključ) v sistemu, ki deluje kot psevdonim (Athey, Catalini, & Tucker, 2017). Različni sistemi sicer lahko vzpostavijo različne stopnje zasebnosti. Zasebnost je mogoče povečati z različnimi tehnikami (na primer z uporabo novega javnega ključa za vsako transakcijo, zakrivanjem transakcij s pomešanjem različnih transakcij itd.), uporabo popolnoma anonimnih kriptovalut (npr. Zcash), vpeljavo

posrednikov (ponudniki digitalnih denarnic) ali drugih metod (Catalini & Gans, 2016, str. 13–14). Vsak uporabnik prosto določa, katere podatke bo uporabil in kako bo z njimi upravljal. Vzporednice lahko potegnemo s kliničnimi preizkusi. Farmacevti generalno poznajo samo bistvene podatke o uporabnikih, ne pa tudi identitet.

1.4.6 Ohranjanje pravic

Časovno žigosanje transakcij in preprečitev dvojne uporabe digitalnih sredstev pomenita, da si sredstvo lahko v danem trenutku lasti le ena oseba. V blockchain sistemu ne moremo trgovati s stvarmi, ki si jih ne lastimo, pa naj bodo to nepremičnine, intelektualna lastnina ali pravice do osebnosti (Tapscott & Tapscott, 2016, str. 45–49).

1.4.7 Vključenost

Ekonomija deluje najboljše, ko dela za vse. To pomeni zmanjšanje ovir za globalno sodelovanje. Velik del svetovne populacije je še vedno izključen od dostopa do tehnologij, finančnih sistemov in ekonomskih priložnosti. Internet je sicer pripomogel h kreiranju delovnih mest v razvijajočih državah, vendar s strani podjetij v razvitem svetu. Znižal je ovire za podjetnike, vendar hkrati omogočil privilegij dostopa do priložnosti in informacij tistim, ki imajo dostop do tehnologije in interneta. Tehnologija podatkovnih verig občutno zmanjša stroške transakcij, odpravi potrebo po imetju bančnega računa in zmanjša ovire pri investiranju ali pridobitvi kreditov. Podjetništvo podpira na globalni ravni in vsakemu omogoča dostop do priložnosti v svetovni ekonomiji. Temelj blaginje je namreč vključenost vseh in tehnologija podatkovnih verig k temu pomembno prispeva (Tapscott & Tapscott, 2016). Spekter uporabnosti blockchaina je širok in ni vezan le na transakcije. Med drugimi lahko deluje tudi kot register, inventarni sistem, sledilni sistem, nadzorni sistem in sistem za izmenjavo vseh oblik sredstev (digitalnih, neopredmetenih in fizičnih) (Swan, 2015).

1.5 Javni in privatni blockchain sistemi

Glede na dostop do podatkov ločimo (BitFury Group & Garzik, 2015a, str.10):

- javni sistemi: sistemi, v katerih ni omejitev glede dostopa do podatkov in predložitve transakcij za vključitev v sistem.
- privatni sistemi: direkten dostop do podatkov in možnosti objave transakcij je omejen na vnaprej določeno listo uporabnikov.

Sisteme lahko ločimo tudi na podlagi dovoljenja do operiranja sistema oziroma dostopa do procesiranja transakcij (Deloitte, 2016a, str. 8):

- sistemi brez dovoljenj: v teh sistemih ne obstajajo omejitve glede identitet obdelovalcev transakcij. Vsak uporabnik je upravičen in ima dovoljenje do kreiranja blokov.
- sistemi z dovoljenji: procesiranje transakcij je v teh sistemih dovoljeno le vnaprej določenim subjektom s poznanimi identitetami.

V tej nalogi zaradi poenostavitve in podobnosti združujem vse štiri sisteme v dva, in sicer javni sistem, v sklopu katerega je tudi sistem brez dovoljenj, ter privatni sistem, v sklopu katerega je sistem z dovoljenji (Tabela 1).

Tabela 1: Oblike blockchain sistemov glede na dostop do podatkov in procesiranja transakcij

Dostop do procesiranja transakcij	Dostop do podatkov in predložitev transakcij	
	Vsi uporabniki	Omejeno število uporabnikov
Vsi uporabniki	Javni sistem & sistem brez dovoljenj	Privatni sistem & sistem brez dovoljenj
Omejeno število uporabnikov	Javni sistem & sistem z dovoljenji	Privatni sistem & sistem z dovoljenju

Vir: D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

1.5.1 Javni sistemi

Bitcoin je bil oblikovan kot popolnoma javen in distribuiran sistem, kjer ni nikakršnih posrednikov. Ključna lastnost javnih sistemov je, da dostop ni omejen. Vsakdo lahko participira, kot navaden uporabnik, rudar ali potrjevalec transakcij (Tapscott & Tapscott, 2016, str. 66). Masovno sodelovanje ni nekaj novega. Wikipedia in Linux sta dva primera uspešnega javnega in prostega sodelovanja. Odprava centralne avtoritete pomeni, da sta potrjevanje in zapis transakcij odvisna od vseh udeležencev (Financial Industry Regulatory Authority, 2017, str. 3).

Ključne prednosti javnih sistemov brez dovoljenj so:

- javni sistemi nudijo izjemno odpornost proti napadom in cenzuri. Javni sistemi izkoriščajo poln potencial tehnologije podatkovnih verig. Zaradi svoje zasnove so odporni proti zlonamernim dejanjem ter napakam in so primerni za oblikovanje vrstniških omrežij med končnimi uporabniki (npr. plačila). Javni sistemi minimizirajo vpliv človeškega faktorja in poudarjajo algoritemski pristop do varnosti (Buterin, 2015).
- javni sistemi predstavljajo tudi bolj atraktivno okolje za razvijalce in inovacije. S tega vidika so ti sistemi podobni internetnim standardom, kot so IP, TCP in HTTP. Uporabniki imajo direktne ekonomske spodbude za odkrivanje pomanjkljivosti

sistemov. Iz tega vidika je bitcoin sistem doživel največ pozornosti s strani razvijalcev, kriptografov in znanstvenikov (Iansiti & Lakhani, 2017).
- ponujajo priložnosti za večjo transparentnost in konkurenco na trgu. Vsakdo lahko uporabi in nadgradi protokol brez skrbi po razlastitvi ali cenzuri s strani drugih udeležencev (Catalini & Gans, 2016, str. 13).

V naslednjih alinejah predstavljam ključne slabosti in nevarnosti omenjenih sistemov:

- zaradi odvisnosti od večjega števila uporabnikov in potratnih modelov je javen sistem tudi manj učinkovit od centraliziranega plačilnega sistema, kot je na primer VISA (Catalini & Gans, 2016, str. 11).
- javni sistemi predstavljajo velike izzive na področju regulatornih skladnosti (pranje denarja, poznavanje stranke), saj se močno razlikujejo od obstoječih poslovnih modelov in zato predstavljajo grožnjo obstoječim posrednikom (Catalini & Gans, 2016, str. 13).
- pojavlja se dvom, ali sta odprtost in odpornost proti cenzuri primerni lastnosti v lastniških kontekstih. Institucije, ki upravljajo s podatkovnimi registri in finančnimi knjigami, so previdne pri uporabi javnih sistemov. Pomisleki se navezujejo na identitete potrjevalcev transakcij, teoretično pomanjkanje pravnomočnosti transakcij, nezmožnost nadzora procesov in dovzetnost do napadov (BitFury Group & Garzik, 2015b, str. 2).
- pomisleki se pojavljajo tudi glede tajnosti uporabnikov v javnih okoljih (BitFury Group & Garzik, 2015a, str. 4).

1.5.2 Privatni sistemi

Privatni sistemi so sistemi, do katerih imajo dostop le izbrani uporabniki z dovoljenjem. En ali več upravljalcev sistema določa, kdo ima dostop, in s tem ustvarja okolje povezanih, poznanih in zaupanja vrednih uporabnikov. Privatna omrežja dovoljujejo tudi različne stopnje dovoljenj. Uporabniki imajo lahko različne nivoje pooblastil za izmenjavo sredstev in vpogled podatkov (Berke, 2017). Privatna omrežja se lahko torej razlikujejo po stopnji vključenega zaupanja med udeleženci, številu potrjevalcev in drugih lastnostih.

Pozitivne lastnosti privatnih omrežij so:

- uporabniki lahko lažje spremenijo pravila, če se dogovorijo. Omogočajo poznejše urejanje transakcij, kar ni mogoče v javnih sistemih. Zaradi tega so bolj primerni za testiranja, saj so modifikacije lahko sprejete hitro in učinkovito (Buterin, 2015).
- privatna omrežja omogočajo nižje stroške. Transakcije so namreč potrjene samo s strani omejenega števila uporabnikov in ne naključnih rudarjev, ki porabijo ogromno energije v Proof-of-Work sistemih. Po drugi strani ne izkoristijo prednosti zmanjšanja stroškov mreženja, ki jih ponujajo sistemi kriptovalut. Razlog je v tem, da določeni uporabniki še vedno nadzirajo transakcije in sredstva (Catalini & Gans, 2016, str. 12).

- v sistemu sodelujejo predvsem stranke, ki se poznajo in si medsebojno zaupajo že od ustanovitve sistema. Zaradi tega tudi praviloma ni potrebe po zgoraj omenjenih dragih Proof-of-Work sistemih (Parkins, 2015). S tem sicer posegajo v eno izmed ključnih lastnosti tehnologije podatkovnih verig – odsotnost potrebe po zaupanju.
- privatni sistemi so veliko bolj enostavno regulirani in spremljani. S tega vidika so bolj privlačni za implementacijo (BitFury Group & Garzik, 2015b , str. 14).

Ob enem se s privatnimi sistemi povezuje tudi določene slabosti in nevarnosti. Med drugim:

- enostavneje, kot je spremeniti pravila, večja možnost obstaja, da jih kdo izmed sodelujočih ne bo spoštoval ali celo kršil.
- privatni sistemi zavirajo hiter razvoj tehnologije. Precejšnja možnost je, da tehnologija v tem primeru celo stagnira. Človeški faktor ostaja ranljivost in sistemi lahko vključujejo varnostne pomanjkljivosti, ki ostanejo neodkrite dalj časa, kot v primeru javnih sistemov (BitFury Group & Garzik, 2015b, str. 15). Javni sistemi ravno nasprotno, zaradi svoje odprtosti, dosegljivosti in široke uporabe, omogočajo eksponenten razvoj.
- namerno omejevanje določenih pravic lahko zavira nevtralnost sistema in uporabnikov. Privatni sistemi imajo značilno le nekaj zaupanja vrednih upravljalcev, s čimer se izpostavlja tveganje podkupljivosti, prirejanja in sistemskega nadzora (Berke, 2017).
- ko je rudarjenje v celoti odpravljeno iz privatnega sistema, revizorska sled ni več zaščitena s količino vloženega računskega dela. Če so glavni uporabniki ogroženi, potem se pojavi tveganje integritete celotne baze (Catalini & Gans, 2016, str. 12). Končni uporabniki brez posebnih pravic dostopa ne morejo neodvisno preveriti pravilnosti in verodostojnosti podatkov (BitFury Group & Garzik, 2015a, str. 1).

Po politiki delovanja so privatna omrežja precej podobna trenutnim sistemom, ki jih vodijo medsebojno povezane institucije ali podjetja in kjer je pomemben visok centraliziran nadzor nad transakcijami (Financial Industry Regulatory Authority, 2017, str. 3). Institucije, ki operirajo s finančnimi, vladnimi ali drugimi občutljivimi bazami, so zaradi pravnih in tehničnih vidikov bolj nagnjene k uporabi privatnih sistemov na podlagi dovoljenj (BitFury Group & Garzik, 2015a, str. 19). Sistemi namreč nudijo bolj nadzorovano in predvidljivo okolje kot javni sistemi. Spodbuda za vpeljavo tehnologije podatkovnih verig v te sisteme je nadaljnje standardiziranje operacij in povečanje kompatibilnosti med udeleženci trga brez spremembe strukture trga. Verjetnost, da bi zaprti sistemi drastično vplivali na tržno strukturo, je veliko manjša (Catalini & Gans, 2016, str. 12). Zaprta oblika sistemov je z vidika skladnosti verjetnejša oblika na srednji rok.

1.6 Prednosti in koristi ter slabosti in tveganja uporabe tehnologije podatkovnih verig

1.6.1 Prednosti in koristi

Razvoj tehnologije podatkovnih verig prinaša različne prednosti in koristi uporabe, kot tudi slabosti in nevarnosti uporabe. Prednosti in koristi uporabe so (Deloitte, 2016a, str. 10; Consultancy.uk, 2017):

- procesna integriteta: uporabniki lahko zaupajo, da se bodo transakcije izvedle točno po protokolu brez posrednika.
- opolnomočenost uporabnikov: uporabniki imajo nadzor nad svojimi podatki in transakcijami.
- visoka kvaliteta podatkov: podatki so popolni, konsistentni, ažurni, točni in široko dostopni.
- trajnost, zanesljivost in obstojnost: zaradi decentraliziranosti sistemi nimajo osrednje točke odpovedi in so zato odporni proti zlonamernim napadom. V centraliziranih sistemih hitreje pride do namernega popačenja podatkov. Uporabniki zato veliko pozornosti (oblikovanje procesov, podporne službe itd.) namenjajo zaščiti podatkov (Song, Shi, Xu, & Gill, 2016). Tehnologija odpravi nepotrebne stroške in ustvari okolja, v katerih lahko uporabniki pozornost namenjajo pomembnejšim aktivnostim.
- preglednost in nepreklicnost: spremembe na odprtih sistemih so javno vidne in jih ni mogoče spremeniti ali izbrisati.
- poenostavljen ekosistem: vse transakcije se dodajajo v eno javno bazo, kar zmanjšuje neorganiziranost in zapletenost večjega števila baz.
- hitrejše transakcije: medbančne transakcije lahko potrebujejo tudi več dni za obračun in poravnavo transakcije. Še posebej to velja izven delovnih ur. Tehnologija podatkovnih verig je operativna neprestano in ni odvisna od delovnega časa posrednikov.
- nižji stroški transakcij: z odpravo posrednikov se izločijo tudi stroški transakcij teh posrednikov. Tehnologija spodbuja nastanek novih trgov in izziva obstoječe poslovne modele in tržne moči udeležencev. Odpira nove priložnosti za nove regulativne pristope in zagotavljanje javnih dobrin, identitet, sistemov ugleda itd. (Catalini & Gans, 2016).

Splošno mnenje je, da je tehnologija podatkovnih verig obetavno odkritje, saj obstaja veliko problemov, ki jih je z njeno uporabo mogoče rešiti. Z večjim številom uporabnikov postaja tehnologija bolj uporabna. Sčasoma zato lahko pričakujemo eksponentno rast. Eden izmed razlogov, da se tehnologija približuje kritični masi hitreje kot ostale tehnologije, je pravi trenutek odkritja. Pojavila se je namreč sredi digitalne transformacije, ki že močno spreminja globalno ekonomijo (Ernst & Young, 2016, str. 10). Njena uporaba sega od finančnih do nefinančnih aplikacij. Večina aplikacij je radikalnih inovacij, zato so sprejeta tudi precejšnja tveganja (Crosby, Nachiappan, Patanayak, Venna, & Kalynaraman, 2016).

1.6.2 Slabosti in tveganja

Tehnologija podatkovnih verig je še vedno v začetni fazi razvoja, zato obstaja veliko nejasnosti, ovir, omejitev, izzivov in tveganj. Navezujejo se tako na interne omejitve (tehnične), kot tudi na zunanje. Med zunanje vključujemo javno dojemanje tehnologije, skladnost z regulativami in pravnimi okvirji ter masovno sprejetje tehnologije (Swan, 2015, str. 81). Zgodovina kaže, da načina uporabe ne determinirajo nove tehnologije, temveč tisti, ki jih uporabljajo. Tehnologije zato lahko koristijo družbi ali pa jih ogrožajo. Ključna tveganja v naslednjih odstavkih delim na: nezrelost tehnologije, visoki stroški vzdrževanja, kriminalna uporaba tehnologije, skladnost z regulativami, prilastitev tehnologije s strani uveljavljenih igralcev na trgu, nezadostne spodbude, zmanjšanje potrebe po delovni sili.

Nezrelost tehnologije je povezana z dejstvom, da večina ljudi ne razume delovanja tehnologije ali pa zanjo še niso slišali. Problem nezrelosti tehnologije je večplasten:

- uporaba in razvoj tehnologije sta neenakovredno razporejena in skoncentrirana v državah in podjetjih, kjer je miselnost tehnološko bolj napredna. Razumljivost tehnologije je nizka z vidika povprečnega človeka in zato predstavlja pomembno omejitev za masovno sprejetje tehnologije. Ljudje ne bodo zaupali tehnologiji, dokler ne bodo razumeli njenih fundamentalnih funkcionalnosti (Drescher, 2017, str. 210).
- drugič, tehnologija še ne podpira dovolj visokih varnostnih kontrol za masovno uporabo. Privatni ključi imajo bistven pomen pri doseganju varnosti, saj se uporabljajo za digitalni podpis pri prenosu sredstev. To pomeni, da je tveganje varnosti visoko v primeru, da uporabnik svoj ključ posodi, ga izgubi ali pa mu je odtujen. Ni namreč dodatnih varoval, ki bi ščitile premoženje uporabnika. Metoda asimetrične kriptografije sama po sebi zagotavlja visoke varnostne standarde (Drescher, 2017, str. 206). Tehnologija se v tej fazi sooča še z nekaterimi osnovnimi problemi, kot so prenizka kapaciteta, odpovedi sistemov, nepredvideni hrošči in podobno. Ker število transakcij narašča eksponentno z novimi uporabniki, predstavlja pomembno tveganje omejena razširljivost kapacitete. Masovno sprejetje zahteva hitre procese in visoke kapacitetne zmogljivosti. Blockchain sistemi še niso tako zmogljivi kot obstoječi komercialni transakcijski sistemi (Wunsche, 2016). Odpornost proti manipuliranju in zaupanje v verodostojnost podatkov temeljita na predpostavki, da je večina moči kontrolirane s strani poštenih uporabnikov. V manjših ali še nerazvitih sistemih je tveganje večine višje. Poveča se možnost tako imenovanega 51 % napada. Gre za situacijo, v kateri imajo nepošteni uporabniki vsaj 51 % nadzor nad sistemom oziroma njegovimi računskimi zmogljivostmi. V tem primeru lahko poljubno preoblikujejo zgodovino verige in nadzorujejo dodeljevanje novih transakcij po lastni volji (Kuo Chuen, 2015, str. 46). Nadzor jim sicer ne omogoča kraje sredstev drugih uporabnikov, temveč si lahko s spreminjanjem zgodovine povrnejo le lastna, že uporabljena, sredstva (Bentov, Lee, Mizrahi, & Rosenfeld, 2014, str. 3). Razočaranje uporabnikov predstavlja največje tveganje za prihodnost tehnologije, saj bi uporabnike

lahko odvrnilo od ponovne uporabe. Varnost je zato predpogoj, da so stranke pripravljene deliti osebne podatke in sodelovati v sistemih (Financial Industry Regulatory Authority, 2017, str. 10).

- tretjič, visoka latenca se nanaša na čas, ki ga omrežje potrebuje, da se transakcija poravna. Deset minut v primeru bitcoina je sicer manj kot večina trenutnih plačilnih mehanizmov, vendar občutno premalo za delovanje Interneta Stvari. Internet Stvari je omrežje medsebojno povezanih nešteto naprav, ki med seboj v vsakem trenutku brezžično komunicirajo s pomočjo interneta (Li, Xu, & Zhao, 2014).
- vedenjske spremembe so naslednja plast. Ljudje se danes zanašajo na posrednike v primeru, da naredijo kakšno napako, pozabijo geslo ali izgubijo denarnico. Ranljivost sistemov je povezana z odgovornim in skrbnim ravnanjem uporabnikov. Disciplina je izjemnega pomena tudi z vidika zmotnih vnosov (na primer napačno vnesena vrednost transakcije), saj sistem ni odporen proti napakam pri vhodnih podatkih. Rudarji preverijo le, če ima oseba A dovolj sredstev na računu (Barbieri & Gassen, 2017).
- peta plast je pomanjkanje pravne uporabe v svetu nepreklicnih transakcij in pametnih pogodb. Po določitvi pogojev pametne pogodbe ne dovoljujejo odstopanj, ne glede na voljo strank. Vprašanje je, kaj se zgodi, ko stranka ne izpolni pogojev? Kakšni bodo stroški, povezani s pravdanjem? Bo pametna pogodba samodejno vložila tožbo? Bo stranka sploh lahko identificirala nasprotno stranko (Tapscott & Tapscott, 2016)?
- migracija obstoječih baz in sistemov na nove blockchain platforme predstavlja tveganje izgube podatkov in drugih napak. Hkrati bo prenos najverjetneje zahteval ogromno časa in stroškov (Crosby, Nachiappan, Patanayak, Venna, & Kalynaraman, 2016).

Visoki stroški vzdrževanja so povezani predvsem s »Proof-of-Work« modelom. Ta sicer zagotavlja zaupanje med uporabniki in ohranja varnost sistema, vendar je poraba energije izjemno visoka. Bitcoin omrežje po podatkih Digiconomist (2017) trenutno porablja 14,81 TWh energije na letni ravni, kar je primerljivo z državama, kot sta Turkmenistan in Slovenija. Schneider (2015) poroča, da skupna procesorska moč bitcoin omrežja stokrat presega moč 500 največjih svetovnih super računalnikov skupaj. Upravljanje z bitcoin omrežjem na letni ravni stane več kot 100 milijonov $ (elektrika). To ima negativen vpliv tudi na okolje. Ob tem, ko vrednost bitcoina raste, se povpraševanje in število rudarjev povečuje in s tem tudi stroški. Vrednost kriptovalut in nagrad mora na drugi strani pokriti stroške. Prihranke bi lahko dosegli z izdelavo namenskih in energetsko učinkovitih računalnikov za rudarjenje. Navezujoče na visoke stroške in majhne možnosti za nagrade se rudarji povezujejo v oligopolne skupine. Potencialno tveganje se izkazuje v izkoriščanju njihovih moči za selektivno opustitev transakcij ali diskriminiranje uporabnikov. V tem primeru lahko govorimo o skriti centralizaciji, ki ogroža distribuirano naravo tehnologije (Kroll, Davey, & Felten, 2013). Skupine rudarjev bi morale biti locirane v hladnejših klimatskih področjih in tam, kjer je proizvodnja elektrike obnovljiva in poceni. Primeri takih držav so Islandija, Gruzija, Kitajska. Drugi del problema je konstantno posodabljanje

opreme. Povprečna uporabna doba opreme je zaradi intenzivne uporabe le 3–6 mesecev (McCook, 2014).

Tehnologija podatkovnih verig trpi zaradi povezav s kriminalno uporabo bitcoin sistema in drugih kriptovalut. Zaradi svoje psevdonimne narave so kriptovalute popularne tudi pri kriminalcih (Ernst & Young, 2016, str. 13). Bitcoin je bil pogosto označen kot orodje za pranje denarja, trgovanje z ljudmi, nelegalno trgovanje z drogo, posredovanje otroške pornografije, financiranje terorizma, davčne utaje in podobno. Največji udarec za ugled bitcoina in tehnologije je bilo zaprtje spletne tržnice drog Silk Road leta 2013. Preiskava FBI-ja je pokazala, da je v dveh letih tržnica generirala prodajo v višini 9,5 milijona bitcoinov (cena je takrat bila okoli 140 $). Po zaprtju je vrednost bitcoina padla in kriptovalute so postale sinonim za kriminalne aktivnosti (Randewich, 2013). Tehnologija sicer omogoča psevdonimnost, vendar po drugi strani zabeleži vsak prenesen kovanec, tok katerega je viden skozi celotno njegovo zgodovino. Ob enem digitalnih valut ni mogoče ponarediti, kar ne velja za bankovce. Fizični denar zato ostaja dominanten medij za kriminalne aktivnosti. Problem torej ni v sredstvu, temveč v načinu njegove uporabe. S pravo obliko vodenja razvoja, regulativnih ukrepov in izobraževanjem je negativne posledice uporabe tehnologije podatkovnih verig mogoče omejiti (Tapscott & Tapscott, 2016).

Tveganje v povezavi s skladnostjo se sklicuje predvsem na vlogo in vpliv centralnih oblasti in institucij (zakonodajalci, regulatorji, sodišča itd.) pri vpeljavi tehnologije. Način kolektivnega obvladovanja lastništev skozi distribuiran P2P sistem je odprl ogromno vprašanj s pravnega področja. Predpisi so bili oblikovani za popolnoma drugačne infrastrukture in zato ne morejo biti enostavno prilagojeni za operativnost blockchain sistemov. Sistemi delujejo globalno in niso omejeni na državne meje in pristojnosti. To dejstvo dodatno predstavlja izziv z vidika skladnosti s predpisi (Ammous, 2016a). Za sprejetje tehnologije je potrebno zagotoviti skladnost z obstoječimi pravnimi okvirji, jih prilagoditi ali vpeljati nove. Pri tem bo potrebno sodelovanje vlad, regulatornih, zakonodajnih in izvršilnih teles, finančnih institucij, tehnoloških strokovnjakov, podjetij in ostalih na mednarodnem nivoju (Wunsche, 2016). Vodilne institucije se morajo izogibati zatiranju inovacij. Potrebno je izkoristiti priložnost in razviti tehnologijo, ki bo preprečila slabe vrste uporabe bolje, kot to počnejo obstoječi sistemi (Tapscott & Tapscott, 2016).

Močne korporacije so prihod interneta izkoristile za povečanje svoje nadvlade. Dostop do osebnih podatkov in transparentnost potrošnikov izkoriščajo za oglaševanje, promoviranje in druge aktivnosti, s katerimi potrošniki niso seznanjeni. Hranjenje skrivnosti povečuje asimetrijo informacij in prednost korporacij (Tapscott & Tapscott, 2016, str. 265–267). Podobno grožnjo predstavlja tudi vpeljava tehnologije podatkovnih verig. Postavlja se vprašanje, kako preprečiti vodilnim podjetjem in državam, da izkoristijo tehnologijo v svoj prid. To ne pomeni, da te institucije ne bi smele imeti dostopa do tehnologije. Pomislek leži v namenu uporabe tehnologije. Za delovanje tehnologije je potrebna transparentnost

podatkov, ki se nanašajo na sredstva, njihove vrednosti in druge informacije. Dostopnost do teh podatkov zmanjšuje nivo privatnosti, kar v primerih bolj občutljivih podatkov lahko predstavlja tveganje izkoriščanja podatkov za nepoštene namene (Drescher, 2017, str. 206). Dokler jo uporabljajo za ustvarjanje socialne blaginje (ustvarjanje enakovrednih priložnosti za celotno svetovno populacijo itd.), je to sprejemljivo. V nasprotnem primeru, ko omejijo prednosti za družbo, to ni sprejemljivo.

Eden izmed izzivov je tudi vzpostavitev zadostne spodbude in motiviranosti uporabnikov v sistemih, ki ne temeljijo na lastnih kriptovalutah in denarnih nagradah. Gre za vprašanje poslovnih modelov sistemov (Koražija, 2017). Rudarji v bitcoin sistemu so motivirani, da vzdržujejo sistem, ker bi v nasprotnem primeru njihovo premoženje (bitcoini) postalo manj vredno. Iniciativa za rudarjenje se zmanjša, ko vrednost bitcoina pade. Nekateri zaradi prevelikih stroškov v celoti opustijo proces in preusmerijo procesorske moči v rudarjenje drugih kriptovalut. Drugi omejijo delo, vendar nekateri vseeno nadaljujejo, ker se zaradi zmanjšanja števila rudarjev povečajo možnosti za nagrado. Ena izmed rešitev za dodatno spodbudo je zaračunavanje provizij za vsako transakcijo. Po besedah Nakamota (2008) bodo transakcijske provizije povečale motiviranost rudarjev, da procesirajo čim več transakcij. Blok po drugi strani vsebuje omejeno število transakcij. Zato je najverjetneje, da bodo rudarji prioritetno vključevali transakcije z višjimi provizijami. Transakcije z nižjimi provizijami bodo zato potrebovale več časa, da bodo potrjene. Kljub temu je višina provizij (tudi v primeru nadomestitve bitcoina ali druge kriptovalute kot oblike nagrade) zanemarljiva v primerjavi s provizijami v obstoječih plačilnih sistemih. V primeru, da ni sistema nagrajevanja, stopnja ali obseg rudarjenja občutno pade in zmanjša se varnost sistema.

Avtomatizacija je prinesla nadomestitev ljudi. Tehnologija podatkovnih verig prinaša dodatno avtomatizacijo. Tako kot lahko avtonomna vozila nadomestijo delo taksi voznikov, podobno lahko, na primer, platforma za kriptovalute nadomesti delo 500 tisoč podružnic Western Union podjetja (Western Union, 2016). Tehnologija ima potencial odpraviti določena delovna mesta v zalednih, podpornih in birokratskih službah (finančne podporne storitve, računovodstvo, notarstvo, pravništvo ipd.). Tehnološke inovacije praviloma začasno posegajo na trg dela, vendar hkrati generirajo nove službe. Tudi tehnologija podatkovnih verig odpira možnosti za nove službe, nove poslovne modele in priložnosti. Nejasno je, kateri efekt bo prevladal, vendar najverjetneje prvi. V nerazvitem svetu bi ta efekt lahko bil pozitiven, saj bi tehnologija ponudila nove možnosti tudi za revne prebivalce. Ključnega pomena je, da se pozitivne učinke tehnologije izkoristi in spreobrne v višje socialne koristi. Mogoče bo tehnologija povzročila, da se bo pomen dela na novo definiral (na primer krajši delovni časi), medtem ko se bo socialna blaginja povečala (Tapscott & Tapscott, 2016).

1.7 Potencialna uporaba tehnologije podatkovnih verig

Nove tehnologije se danes zaradi močne digitalne transformacije razvijajo hitreje kot kadarkoli v zgodovini. Tehnologija podatkovnih verig spada med glavne transformacijske tehnologije in igra pomembno vlogo, saj lahko pospeši razvoj ostalih (Interneta Stvari, delitvene ekonomije in digitalne transformacije na splošno) in revolucionira globalno ekonomijo (Ernst & Young, 2016, str. 3).

Rogers (2003) definira 5 lastnosti za razširitev inovacij. Višja stopnja teh lastnosti, kot jih ima tehnologija, večja bo stopnja sprejetja. Izjema velja za kompleksnost, pri kateri večja stopnja ovira hitrejše sprejetje inovacije. Lastnosti, njihovi opisi ter primerjava s tehnologijo podatkovnih verig so predstavljene v Tabeli 2. Kot vidimo, tehnologija pooseblja večino lastnosti in zato velja za inovativno tehnologijo.

Tabela 2: Pet lastnosti za razširitev inovacij ter primer tehnologije podatkovnih verig

Lastnosti inovacij	Opis lastnosti	Primer tehnologije podatkovnih verig
Relativna prednost	Do kolikšne mere je inovacija dojeta kot boljša od ideje, ki jo nadomešča.	Tehnologija ponuja produkte in storitve, ki so cenejši, hitrejši in varnejši od ostalih tehnologij.
Kompatibilnost	Do kakšne stopnje se inovacijo dojema kot skladno z obstoječimi vrednotami, preteklimi izkušnjami in potrebami potencialnih uporabnikov.	S pomočjo tehnologije so trenja na obstoječih trgih premagana z vzpostavitvijo P2P omrežij. Mnogo obstoječih poslovnih modelov in industrij je naklonjenih tej inovativnosti.
Kompleksnost	Stopnja dojemanja inovacije kot njene relativne težavnosti razumevanja in uporabe.	Tehnologija sloni na treh stebrih (decentralizacija, soglasje in kriptografija), kombinacija katerih oteži razumevanje koncepta.
Eksperimentalnost	Stopnja, do katere se z inovacijo lahko eksperimentira v omejenem obsegu.	Visoka razširjenost start-upov in investicij med številnimi industrijami in produkti ter storitvami kaže na visoko stopnjo eksperimentiranja.
Zaznavnost	Stopnja, do katere so rezultati inovacije vidni ostalim.	Rezultati inovacije so v tej fazi vidni predvsem strokovnjakom.

Vir: E. M. Rogers, Diffusion of innovations, 2003.

Tehnologija ima potencial spremeniti vse industrije, ki temeljijo na posrednikih in centralnih avtoritetah (Thompson, 2016). Široko sprejetje bi lahko ogrozilo nekatere obstoječe poslovne modele in oblikovalo nove (Wunsche, 2016). Široka uporaba tehnologije je mogoča, ker je blockchain protokol lahko programiran na način, da beleži vse, kar nosi vrednost in je lahko izraženo v kodi. To vključuje denar, razne certifikate (rojstni list, poročni, okoljski, tehnični, izobraževalni certifikat itd.), licence, pravice nad lastništvi digitalnih in fizičnih sredstev, dejanja, finančna poročila, medicinske kartoteke, zavarovalne zahtevke, glasove, porekla izdelkov in tako dalje (Tapscott & Tapscott, 2016).

Stroški uporabe tehnologije bodo na začetku visoki zaradi pomanjkanja človeškega kapitala (znanja), učenja, migracij in prilagoditev. Zato bomo najverjetneje videli visoko vrednostne

aplikacije in privatne aplikacije, namenjene izboljšanju učinkovitosti obstoječih sistemov. Prve aplikacije se bodo najprej razvile na področjih, kjer bodo koristi največje, vendar v začetni fazi najverjetneje ne bodo podpirale množične uporabe. Lažja integracija v obstoječe verige je prav tako pomemben faktor. Prisotnost direktnih in indirektnih tržnih učinkov bi lahko pospešila razpršitev tehnologije na trgih, kjer je prisotnost posrednikov manjša ali pa njihova vloga ni tako pomembna. Oblasti bodo potencialno in primarno najverjetneje izkoristile tehnologijo za odpravo tržnih nepopolnosti in nadzor nad tržnimi udeleženci (Catalini & Gans, 2016, str. 15). Ernst & Young pričakujeta kritično maso sprejetja tehnologije v finančni industriji v naslednjih 3–5 letih. Sledile bodo tudi druge industrije. Tehnologija podatkovnih verig obstaja že 8 let, vendar je še vedno smatrana kot nova, saj je uporabljena le v nekaj nišnih področjih (kriptovalute). Istočasno se drugi načini njene uporabe razvijajo v ozadju in čakajo na primeren trenutek za vpeljavo (Parkins, 2015). V nadaljevanju povzemam spremembe na nekaj ostalih izbranih področjih.

1.7.1 Pametne pogodbe

Pametne pogodbe so bile prvič definirane leta 1994 kot računalniški algoritem, ki samodejno izvaja pogoje pogodbe (Szabo, 1997, str. 23). Pametna pogodba v kodi programske opreme nosi zapis pogojev tradicionalnih pogodb (dobava, plačilo obroka, uveljavljanje garancije, zamudne obresti, prenos lastništva itd.). Skupaj s tehnologijo podatkovnih verig lahko pametne pogodbe ob določenih sprožilnih momentih avtomatsko izvršujejo in uveljavljajo pogoje brez potrebe po posrednikih. Omogoča tudi sklepanje multilateralnih poslov (Šutanovac, 2017). V Prilogi 2 predstavljam podrobnejše opisan primer potencialne uporabe pametnih pogodb. Priloga 3 pa v tabeli prikazuje ključne razlike med tradicionalnimi in pametnimi pogodbami.

1.7.2 Ekonomija delitve

Najbolj znani podjetji v ekonomiji delitve (angl. *sharing economy*) sta Airbnb (agregira ponudbe prostih sob) in Uber (agregira ponudbo prevoznih storitev). Podjetja delujejo kot posredniki med najemniki in najemodajalci storitev. Blockchain neposredno povezuje končne uporabnike brez posrednikov in njihovih provizij (Tapscott & Tapscott, 2016).

1.7.3 Blockchain oskrbovalne verige

Ker tehnologija omogoča nepreklicno beleženje podatkov v časovnem zaporedju, predstavlja popolno orodje za zagotavljanje transparentne sledljivosti blaga skozi celotno oskrbovalno verigo. V blockchain sistemu bi člani v verigi (podjetja) beležili vsak korak in spremembo na izdelku, s čimer bi končni kupci v vsakem trenutku lahko vedeli, od kje izvira izdelek in kje se trenutno nahaja. S takšnim nivojem transparentnosti in odgovornosti bi lahko podjetja povečala zaupanje in lojalnost v blagovno znamko. Pomembno lahko pomaga

v boju proti ponarejevanju blaga. Eden izmed pozitivnih načinov uporabe je tudi bolj učinkovito vodenje zalog na podlagi natančnih podatkov o dobavi in potrošnji v realnem času (Loop, 2016). Wal-Mart, eden največjih trgovcev, tehnologijo že poskusno uporablja za sledenje porekla prehranskih izdelkov. Nadejajo si predvsem časovne in stroškovne prihranke ter boljšo lojanost kupcev. Ugotavljajo namreč, da potrebujejo več dni za identifikacijo proizvajalca vrnjenega pokvarjenega izdelka. Ti podatki bodo dosegljivi v trenutku, kar je lahko ključnega pomena v primeru izbruha bakterij. Podjetje lahko izdelke s polic umika selektivno in poskrbi za pomembne stroškovne prihranke (Koražija, 2017).

1.7.4 Finančna industrija

Finančna industrija je najmočnejša izmed vseh svetovnih industrij in je temelj sodobnega kapitalizma. Predstavlja tudi eno najbolj centraliziranih in tehnološko zaostalih industrij. Počasnost tehnološkega razvoja je posledica narave posla, ki zahteva stabilnost in skladnost z rigidnimi regulatornimi telesi in predpisi (Tapscott & Tapscott, 2016). Finančne institucije kriptovalute in tehnologijo podatkovnih verig smatrajo kot grožnjo, saj izzivajo njihovo vlogo in prinašajo transformacijske spremembe (Biella & Zinetti, 2016). Tehnologija lahko osvobodi mnogo finančnih storitev iz rok obstoječih finančnih institucij, poveča konkurenco in revolucionira delovanje bank, borz, zavarovalnic, računovodskih podjetij, finančnih posrednikov, kartičnih podjetij in tako dalje. Tehnologija vidno posega v naslednje aktivnosti znotraj finančne industrije: mednarodna denarna nakazila, transakcije vrednostih papirjev, sindicirana posojila, repo posli, izdajanje in prenos lastniškega kapitala v javnih in privatnih sistemih, izdaja obveznic, vzpostavljanje zavarovanj in podobno (World Economic Forum, 2016). Sliki v Prilogi 4 prikazujeta obstoječi in nov medbančni plačilni sistem.

Raziskava, ki so jo izvedli Santander InnoVentures, Oliver Wyman in Anthemis Group (2015), ugotavlja, da bi lahko tehnologija do leta 2022 v finančni industriji povzročila do 20 milijard $ letnih prihrankov. Predpostavka pri tem je, da se tehnologija lahko sooča z masovnim prometom transakcij na globalni ravni.

2 KRIPTOVALUTE

Kriptovaluta je opredeljena kot digitalna valuta oziroma denar, ki nima materializirane oblike in ni reguliran s strani finančnih institucij. Obstoječe kriptovalute temeljijo na različnih sistemih kriptografije. Uporaba kriptovalut se dnevno povečuje in ob vse hitrejšem razvoju tehnologije se postavlja vprašanje, ali bodo kriptovalute nadomestile obstoječe valute oziroma denar. Največje vprašanje je, ali lahko podjetje danes posluje izključno samo s kriptovalutami (Rostohar, 2016). V nadaljevanju sledi razlaga razlogov uporabe kriptovalut, njihova opredelitev, lastnosti in funkcije, opis najpogosteje uporabljene kriptovalute bitcoin ter koristi in tveganja uporabe kriptovalut.

2.1 Razlogi uporabe kriptovalut

Razvoj kriptovalut temelji na razreševanju problema dvojne porabe, ki se nanaša na tveganje porabe iste enote digitalne valute na dveh ali več različnih mestih. Digitalna sredstva so namreč ob obstoječi tehnologiji enostavno kopirana, njihove različice pa je nemogoče ločiti. Problem dvojne porabe je še posebej ključen, ko govorimo o denarju na splošno in o digitalnih valutah.

Kriptovalute na podlagi tehnologije podatkovnih verig odpravljajo težavo obstoječega interneta – digitalno kopiranje in podvajanje podatkov. Tradicionalno problem dvojne porabe pri spletnih plačilih rešujejo posredniki. Transakcije morajo biti potrjene s strani storitev plačilnega prometa (na primer Western Union), komercialnih bank (Citicorp), kartičnega podjetja (Visa International Service Association) ali spletne plačilne platforme, kot je PayPal. Izvedba mednarodnih plačil lahko traja tudi nekaj dni ali v določenih delih sveta celo tedne. Prav tako kriptovalute odpravljajo potrebo po posrednikih pri transakcijah, to so banke. Kljub temu, da banke opravljajo delo verodostojno in kontrolirano, pa imajo vseeno svoje omejitve, ki jih kriptovalute nimajo. Banke namreč uporabljajo centralizirane serverje za shranjevanje podatkov in transakcij, kar povzroča veliko izpostavljenost vdorom. Drugič, za mednarodne transakcije računajo visoke provizije. Svetovna Banka (2017) v junijskem poročilu ugotavlja, da je v drugem kvartalu leta 2017 povprečna provizija nakazila globalno znašala 7,32 %. Včasih so nezanesljive in počasne. Prav tako izključujejo 2 milijardi ljudi, ki nimajo dovolj denarja za odprtje bančnega računa (Smith, 2016). Povprečna provizija za transakcijo z bitcoin valuto je 8. junija 2017 znašala 0,36 % (BitInfoCharts, 2017). Pri izračunu povprečja je zaradi nesimetrične oziroma neenakomerne porazdelitve vrednosti transakcij upoštevana mediana. Znatno nižje provizije pomenijo lažjo vključitev tudi revnejšega dela prebivalstva. Transakcije z nižjimi zneski postanejo smiselne in bolj racionalne na račun nizkih provizij in odprave potrebe po vodenju bančnega računa. Zmožnost dostopati do globalnega plačilnega sistema in ekonomije se poveča, saj ni potrebe po fizičnih bančnih poslovalnicah in odpiranju bančnih računov (Brito & Castillo, 2013). Vse, kar je potrebno, je dostop do interneta in mobilna naprava. Pew Research Center (Poushter, 2016) ugotavlja, da se stopnja uporabe pametnih mobilnih naprav v državah v razvoju hitro povečuje. Leta 2013 je v povprečju 45 % ljudi v državah v razvoju občasno uporabljalo internet ali si lastilo pametni telefon. V letu 2015 je razmerje naraslo na 54 %.

Z uporabo deljenega omrežja in pametne kriptografije je Nakamoto (2008) izdelal mehanizem soglasij, ki rešuje problem dvojne porabe brez vpletenosti tretje osebe. Kriptovalutni sistem na podlagi tehnologije podatkovnih verig časovno zaznamuje vsak porabljen kovanec in zavrne vse preostale transakcije v bloku, ki vsebujejo isti kovanec. Po zgoraj opisanem principu torej odpravlja problem dvojne porabe. Odprava posrednika omogoča tudi občutno skrajšanje časa, potrebnega za prenos sredstev. Slednje sicer velja za

trenutne potrebe kriptovalut, vendar pa sistemi še niso dovolj razviti, da bi lahko podpirali volumen transakcij realnega plačilnega sistema.

Bitcoin, trenutno najbolj razširjena in verodostojna kriptovaluta, temelji na Proof-of-Work mehanizmu, ki omogoča uporabnikom ustvarjanje digitalnih kovancev. Uporabniki izvršujejo svoja plačila z digitalnim podpisom transakcije in s tem preprečijo dvojno porabo svojih kovancev (isti kovanec se podpiše s strani dveh različnih uporabnikov) (Karame, Androulaki, & Čapkun, 2012).

2.2 Opredelitev kriptovalut

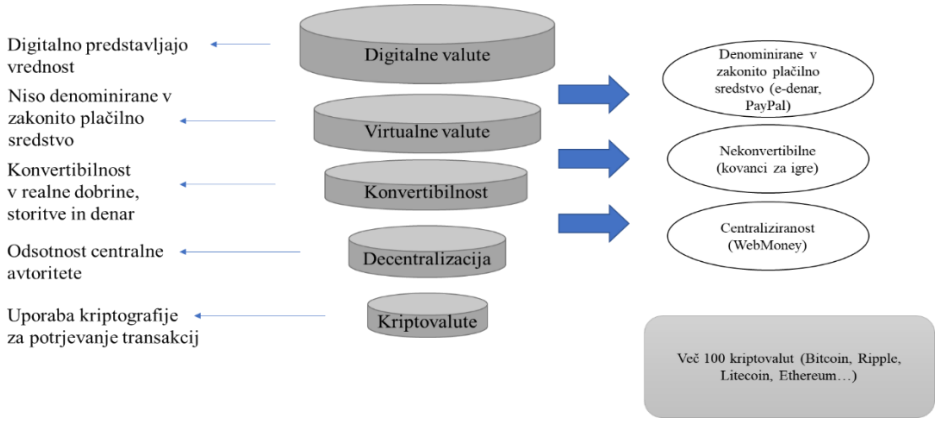
Zamisel o digitalnem denarju je prvič predstavil Chaum (1983 in 1985) v zgodnjih 80. letih. Sledili so poskusi institucij za komercializacijo kriptovalut z uvedbo e-denarja in e-zlata. Vendar pa so vsa ta prizadevanja neuspešna zaradi različnih razlogov, kot je neskladnost z zakonodajo, slabo upravljanje podjetij in mrežna centralizacija (Frisby, 2014). Nove tehnologije, podprte z naprednimi šifriranji in mrežnim računalništvom, prinašajo transformacijske spremembe v globalni ekonomiji. Vključno z novimi načini izmenjave blaga, storitev in sredstev z digitalnimi valutami (He et al., 2016).

Kriptovalute so sredstvo za izmenjavo tako kot običajne valute (evro, dolar …), vendar so zasnovane za izmenjavo digitalnih informacij skozi proces, ki ga omogoča kriptografija. Kriptografija se uporablja za zavarovanje transakcij in nadzor nad ustvarjanjem novih kovancev. Kot že omenjeno, se je prva kriptovaluta bitcoin pojavila na trgu leta 2009, danes pa je na trgu že več sto različnih alternativnih kriptovalut (Graydon. 2014). Razvijalci obstoječega bitcoina blockchain sistema ne morejo spremeniti tako, da bi omogočal izvrševanje transakcij ob določenih pogojih (na primer plačilo ob vnaprej določenem datumu ali času, količina kovancev v obtoku, mehanizem potrjevanja itd.). Spremembe v protokolu bi namreč zahtevale konsenz večine uporabnikov. Zaradi tega so nastale alternativne kriptovalute (angl. *altcoins*), ki se ravnajo po različnih protokolih in omogočajo izvrševanje različnih pogojev. To omogoča odprtokodna narava bitcoin sistema. Pravila so zato lahko enostavno spremenjena, vendar to vzpostavi ločen sistem, ki je neodvisen od prvotnega (bitcoin). Prosto prilagajanje pravil predstavlja vrsto tveganj (pomanjkanje likvidnosti, goljufije, fluktuacije, varnostne pomanjkljivosti itd.) (Back, Corallo, Dashjr, Friedenbach, Maxwell, Miller, Poelstra, Timón, & Wuille, 2014).

Slika 12 prikazuje sistematizacijo digitalnih valut, katere del so virtualne valute in kriptovalute. Digitalne valute določajo štiri ključne značilnosti. Prva značilnost je, da se njihova vrednost lahko hrani in izmenjuje brez uporabe fizičnih bankovcev ali kovancev. Kot drugo, digitalna valuta ni uradna valuta v posamezni državi. Tretjič, namen digitalnih valut je izmenjava za realno ali virtualno blago in storitve. Četrta značilnost je, da se enote lahko prenesejo med posamezniki, med podjetji ali med posamezniki in podjetji (Gerstein &

Hervieux-Payette, 2015). Del digitalnih valut so virtualne valute, ki so digitalna reprezentacija vrednosti, izdane s strani privatnih razvijalcev in denominirane v svoji obračunski enoti. Virtualne valute so lahko pridobljene na številne načine. Konvertibilne so tipično kupljene ali izmenjane iz fiat valut ali drugih virtualnih valut. Druga možnost je prodaja blaga ali storitev v zameno za virtualnih valute. V decentraliziranih sistemih so lahko dodatno pridobljene tudi iz sodelovanja v procesu potrjevanja transakcij (»rudarjenje«). Virtualne valute so praviloma shranjene v e-denarnicah. Pridobljene, shranjene, dostopne in izmenjane so elektronsko in so lahko uporabljene za različne namene, v kolikor se z uporabo strinjata obe nasprotni stranki. Koncept virtualnih valut pokriva široko paleto valut, od neformalnih dokumentov, ki potrjujejo dolg (kuponi, letalske milje itd.), valut, podprtih s sredstvi, kot je zlato, do kriptovalut, kot je bitcoin. Virtualne valute se od drugih digitalnih valut (npr. e-denarja) razlikujejo po tem, da niso denominirane v fiat valutah in imajo lastne obračunske enote (He et al., 2016).

Slika 12: Sistematizacija digitalnih valut



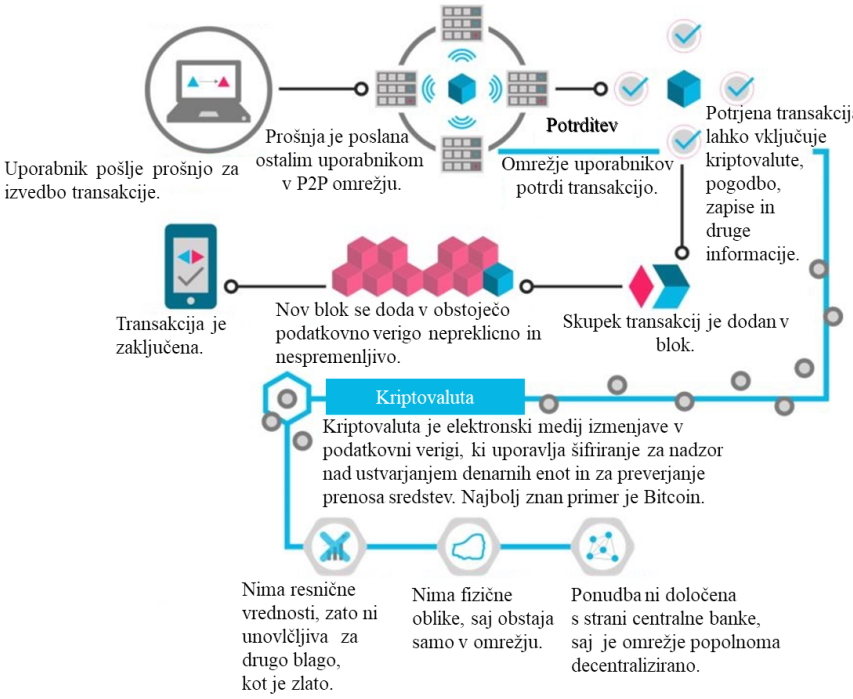
Vir: He et al., Virtual Currencies and Beyond: Initial Considerations, 2016.

Kriptovalute, ki so del digitalnih valut, se od navadnih valut razlikujejo v tem, da niso ustvarjene in kontrolirane s strani držav (Tapscott & Tapscott, 2016). »Kriptovaluta je po sebi peer-to-peer verzija elektronskega denarja, ki spletnim plačilom omogoča, da se izvedejo neposredno med dvema osebama brez potrebe po posredovanju finančne institucije« (Kuo Chuen, 2015, str. 8). Kriptovalute kljubujejo standardnemu konceptu fiat valut (He et al., 2016). V vrstniškem (P2P) omrežju je zelo pomembno večinsko soglasje uporabnikov, kar pomeni, da gre za omejene vnose v bazo podatkov in jih nihče ne more spremeniti. Vsak uporabnik v omrežju ima zapis celotne zgodovine vseh transakcij in s tem ravnotežje svojega računa.

Za razliko od tradicionalnih valut je določitev vrednosti za kriptovalute in elektronska denarna sredstva nekoliko težavna. Vrednost ameriškega dolarja, na primer, je določena s pomočjo tečaja, zakladnih menic in merjenjem deviznih rezerv. Kriptovalute za razliko,

kljub številnim prednostim, nimajo dejanske cene kovancev. Še bolj postane zapleteno pri določitvi, kaj sploh kovanci (na primer bitcoin kovanci) so. Vrednost (bitcoina) se zaznava glede na koristi in uporabnost. Izraz »vrednost« ne smemo zamenjati z izrazom »cena«. Posledica tega je, da je uporaba in vrednost kriptovalut (bitcoina) rezultat številnih inovacij, omrežja in značilnosti (Brown, 2016).

Slika 13: Proces uporabe kriptovalut pri izvedbi posamezne transakcije



Vir: Blockgeeks, What is cryptocurrency, b.l.

Slika 13 prikazuje proces uporabe kriptovalut pri izvedbi posamezne transakcije. Proces se začne s prošnjo izvedbe transakcije v kriptovaluti. Ta prošnja je poslana vsem uporabnikom v vrstniškem omrežju, transakcijo lahko potrdijo samo rudarji z rešitvijo matematične uganke in posredujejo rešitev nazaj v omrežje uporabnikov. Potrjeno transakcijo potem ostali uporabniki preverijo in dodajo v svojo bazo podatkov. Ta proces je opisan že v poglavju o delovanju tehnologije podatkovnih verig. Digitalno menjalno sredstvo v tem primeru je kriptovaluta, ki nima fizične oblike, dejanske vrednosti in ni del posredovanja centralnih bank (Blockgeeks, b.l.).

Poročilo avtorjev Hileman in Rauchs (2017) »The Global Cryptocurrency Benchmarking Study« preučuje trg kriptovalut na podlagi podatkov raziskave, v kateri je sodelovalo skoraj 150 podjetij in posameznikov, aktivnih na tem področju, in pokriva 38 svetovnih držav. Avtorja ugotavljata, da danes uporablja kriptovalute vsaj med 2,9 in 5,8 milijonov ljudi. Študija je industrijo kriptovalut razdelila na štiri ključne sektorje: izmenjava, plačila, denarnice in rudarjenje. Ugotovitve za posamezni sektor so sledeče:

- izmenjava: funkcija izmenjave je nakup, prodaja in trgovanje s kriptovalutami. Ta sektor je bil prvi, ki se je pojavil v industriji kriptovalut in ima najbolj operativne subjekte in zaposluje največ ljudi.
- plačila: funkcija sektorja plačil je omogočanje plačil z uporabo kriptovalut. Podjetja za plačilo s kriptovalutami delujejo kot prehod med uporabniki kriptovalut in širšim gospodarstvom, ki povezuje nacionalne valute in kriptovalute. Ta podjetja se uvrščajo v dve kategoriji. Podjetja, ki uporabljajo kriptovalute za hiter in učinkovit plačilni sistem, sodijo v prvo kategorijo. V drugo kategorijo sodijo podjetja, ki olajšajo uporabo kriptovalut za uporabnike. Študija je pokazala, da velikost povprečnega plačila B2B (angl. *business-to-business*) znaša 1.878 $, medtem ko P2P plačila s povprečno vrednostjo 351 $ presegajo C2B (angl. *customer-to-business*) plačila (210 $).
- denarnice: sektor denarnic ima funkcijo shranjevanja kriptovalut. Denarnice se nanašajo na spletne in mobilne, ki ponujajo različne tehnične funkcije in storitve, pri čemer 52 % denarnic zagotavlja integrirano funkcijo menjave valut. Razlika med denarnicami in izmenjavami je vedno bolj nejasna.
- rudarjenje: sektor ima funkcijo zagotavljanja globalne mreže in reševanja matematičnih ugank. Zaradi odsotnosti centralne avtoritete kriptovalute ustvarjajo proces, imenovan rudarjenje, ki je opredeljen že v prejšnjih poglavjih. Študija je pokazala, kako se je rudarjenje s kriptovalutami razvilo iz stranske aktivnosti v profesionalno kapitalsko industrijo, v kateri so rudarji za bitcoin zaslužili že več kot 2 milijardi $ od leta 2009 do 2017 (ob predpostavki, da so bili vsi kovanci izmenjani v realno valuto na dan prejema).

2.3 Lastnosti in funkcije denarja in kriptovalut

Pri opredeljevanju kriptovalut je zelo pomembno razumevanje lastnosti fiat valut oziroma denarja. Zato v nadaljevanju najprej sledi opredelitev lastnosti fiat denarja in nato opredelitev lastnosti kriptovalut.

Denar je splošno plačilno sredstvo in sredstvo menjave. Za poravnavanje računov posamezniki uporabljajo gotovino in transakcijske račune (plačilne kartice). Njegove funkcije so (Samuelson & Nordhaus, 2010):

- uporabljamo ga kot medij za izmenjavo,
- uporabljamo ga kot obračunsko enoto oziroma mero vrednosti za blaga in storitve,
- uporabljamo ga tudi kot hranilec vrednosti. V primerjavi z delnicami, nepremičninami ali zlatom je denar relativno brez tveganja.

Fiat denar je valuta, ki je razglašena s strani vlade kot zakonito plačilno sredstvo. Vrednost fiat denarja izhaja iz razmerja med ponudbo in povpraševanjem, in ne vrednosti materiala, iz katerega je denar narejen. V preteklosti je večina valut temeljila na fizičnih surovinah, kot

sta zlato ali srebro. Beseda fiat v latinščini pomeni »mora biti« (Smith, 2016, junij). Ponudba fiat denarja in njegova vrednost je zavarovana z regulativo. Je edini standard, ki nosi naslednje lastnosti: pripoznan je kot zakonito plačilno sredstvo, države so dolžne sprejeti bankovce kot način plačila davčnih obveznosti, centralne banke imajo monopolni nadzor nad njegovo izdajo ter lahko je podprt s posrednim zavarovanjem. Te lastnosti zagotavljajo stabilnost cene (Wells, 2004).

Trgi omogočajo prostovoljno izmenjavo blaga in storitev med prodajalci in kupci. Za izvedbo menjave morajo biti potrjeni določeni ključni atributi transakcije s strani vključenih strank, med njimi tudi tretje osebe. Pri fizični izmenjavi je edini posrednik centralna banka, ki izdaja fiat denar za uporabo v menjavi (Catalini & Gans, 2016, str. 2–3). Vrednost fiat valut temelji na kreditni sposobnosti centralne banke in vlade (He et al., 2016). Skoraj vse gospodarske izmenjave potekajo s pomočjo fiat denarja, ki se ne more ločiti od same državne oblasti. Skozi legaliziran monopol, ki ga imajo centralne banke, država v celoti nadzoruje oblike izmenjave in proizvajanje denarja v razvitih kapitalističnih družbah. Po definiciji se fiat denar lahko proizvaja brez omejitev – količinskih, komercialnih in tehnoloških (Hülsman, 2014). Pri virtualnih valutah centralne avtoritete ni in s tem nobene oblasti, ki bi izvrševala nadzor. Zagovorniki digitalnih valut trdijo, da je P2P nadzor enako varen kot sistem centralne banke. Ideja, da vsi uporabniki zaznajo napake v sistemu, omogoča, da ne pride do prevar (Šutanovac, 2017).

Pri digitalni izmenjavi je vpleten vsaj en finančni posrednik, ki v prvi fazi potrdi obstoj in razpoložljivost sredstev ter v naslednji fazi prenese ta sredstva na račun prodajalca. Posrednik za to storitev zaračuna provizijo. Dodatni stroški posredovanja se torej pojavijo, ko nasprotni stranki ne moreta samostojno efektivno preveriti vseh pomembnih lastnosti transakcije (Catalini & Gans, 2016, str. 2–3).

Kriza fiat denarja bo spremenila ne le finance in bančništvo, ampak tudi naravo upravljanja na splošno. Novi hipotetični svetovni denarni sistem, ki bo temeljil na kriptovalutah, je učinkovitejši od vseh trenutnih fiat sistemov. Tak sistem bo temeljil na splošnih nižjih stroških transakcij, v primerjavi z zdajšnjimi stroški transakcij fiat denarja. Uveljavitev novega sistema bi od držav zahtevala legitimiranje kriptovalut kot globalne valute. Trenutna špekulativna narava kriptovalut bi na drugi strani trenutni finančni sistem izpostavila tveganju razvrednotenja fiat valut (Bitcoin Theory, 2016). Obstoječe kriptovalute najverjetneje ne bodo nadomestile fiat valut, vendar lahko povzročijo pomembne premike proti digitalizaciji fiat valut.

Kriptovaluta je denar v obliki številk (ni narejena iz papirja ali kovancev), ki se lahko shrani v datoteki na osebnem računalniku. Te številke so izračun različnih vrst zapletenih formul (Taran, Salmanova, Dokukina, Menshikova, & Skudareva, 2015). Povedano drugače, električna energija kriptovalut se pretvarja v vrstične kode z denarno vrednostjo. Od tu

poimenovanje digitalna valuta. Kriptovaluta je, tako kot običajna valuta, menjalno sredstvo, ki je zasnovano za izmenjavo digitalnih informacij po principu kriptografije. Ta se uporablja za zavarovanje poslov in za nadzor nad ustvarjanjem novih kovancev (Graydon, 2014). Lastnosti kriptovalut so (Blockgeeks, b.l.):

- nepreklicnost: po potrditvi transakcije le-te ni mogoče več razveljaviti. V primeru, da se uporabnik, ki pošlje prošnjo za izvedbo transakcije, zmoti pri znesku in je transakcija potrjena, ni več možno preklicati transakcije.
- psevdonimnost: transakcije in računi uporabnikov ne temeljijo na uporabi realnih identitet. Možno je analizirati potek transakcij, ni pa možno transakcije povezati z identiteto uporabnika v realnem svetu. Čeprav je anonimnost uporabnika ena ključnih lastnosti bitcoina, so analitična podjetja, podprta s strani vladnih sredstev, uspela odkriti identiteto posameznih uporabnikov z uporabo naprednih forenzičnih analitičnih orodij. To je mogoče, ker so vse transakcije permanentno zabeležene v javni bazi in je zato mogoče ugotoviti celotno zgodovino prenosov vsakega bitcoina. Ko enkrat poznaš identiteto uporabnika, lahko ugotoviš, od kje je prišel denar in kako ga je uporabil. Iz tega razloga so nastale nekatere druge kriptovalute, ki želijo uporabnikom zagotoviti še večjo anonimnost (na primer Zcash in Monero) (Ou, 2016).
- hitrost in globalnost: transakcije se hitro množijo znotraj omrežij in so potrjene v nekaj minutah. Ker gre za globalno omrežje uporabnikov, transakcije niso vezane na fizično lokacijo. Hitrost izvedbe transakcije torej ni odvisna od oddaljenosti oseb.
- varnost: kriptovalute so zaklenjena in zaščitena sredstva s pomočjo asimetrične kriptografije. To pomeni, da lahko samo lastnik zasebnega ključa pošlje kriptovaluto. Močna kriptografija in težavnost matematične uganke ščitita pred varnostnimi vdori.
- sistem brez dovoljenj: vsakdo ima pravico do uporabe kriptovalut brez predhodne potrebe po pridobitvi dovoljenja. Gre za preprosto brezplačno programsko opremo, s katero je možno pošiljati in prejemati bitcoine in druge kriptovalute.

Kriptovalute niso izdane ali nadzorovane s strani centralnih bank. Posledično ne obstaja mehanizem postavljanja obrestnih mer in zahtevane stopnje obveznih rezerv za institucije, ki se ukvarjajo z obrestnimi merami. Tradicionalna orodja za analizo denarne politike niso uporabna pri analizi kritovalut. Kriptovalute lahko bolje razumemo s pregledom predvidljive rasti ponudbe valut in stabilnostjo valute. Cilj centralnih bank je oblikovati denarne politike, s katerimi zagotovijo relativno stabilnost cen. Centralne banke upoštevajo pričakovano povpraševanje po denarju in na podlagi tega načrtujejo rast ponudbe denarja, ki ohranja cene nujnih življenjskih potrebščin nizke in stabilne (Ammous, 2016b).

The CoinMarketCap stran je v seznamu vseh obstoječih kriptovalut 9. julija 2017 zabeležila 801 kriptovaluto. Bitcoin ostaja največja svetovna kriptovaluta s tržno vrednostjo nekaj več kot 42 milijard $ ali 44,5 % tržne kapitalizacije vseh kriptovalut. Sledijo mu kriptovalute

ethereum, ripple, litecoin, Ethereum Classic, Dash in druge (CoinMarketCap, 2017). Kriptovaluta bitcoin je zaradi svoje razširjenosti opisana v naslednjem poglavju.

2.4 Bitcoin

Satoshi Nakamoto je z uvedbo bitcoina v letu 2009 poskrbel za velik preskok od obstoječih valut. Pozornost vlagateljev in medijev je bitcoin dosegel v aprilu 2013, ko je dosegel 266 $/bitcoin. Po tem, ko je dosegel tržno vrednost več kot 2 milijardi $, je sprožil veliko razprav o prihodnosti bitcoina in ostalih kriptovalut. Razprave so se nanašale na vprašanja, ali bodo te alternativne valute izpodrinile konvencionalne valute in postale uradna valuta, kot sta evro in dolar. Drugi so s pesimizmom napovedovali neuspeh (Rosic, 2016). Bitcoin je digitalni medij izmenjave, ki je ustvarjen, pridobljen, shranjen in izmenjan elektronsko (Raiborn & Sivitanides, 2015). Medtem ko bitcoin ostaja dominantna kriptovaluta (merjeno v tržni vrednosti ter številu uporabnikov in transakcij), so se na trgu pojavile nove kriptovalute, ki so povzročile padec tržnega deleža bitcoina s 86 % (marec 2015) na 45 % (julij 2017) (Hileman & Rauch, 2017).

Bitcoin je prva izmed kriptovalut, ki temelji na tehnologiji podatkovnih verig. Bitcoin je primer konvertibilne virtualne valute, saj nastopa kot substitut realni valuti. Bitcoin je lahko izmenjan med uporabniki in ga je mogoče kupiti ali zamenjati za druge fiat valute (dolar, evro itd.) (The Financial Crimes Enforcement Network, 2013).

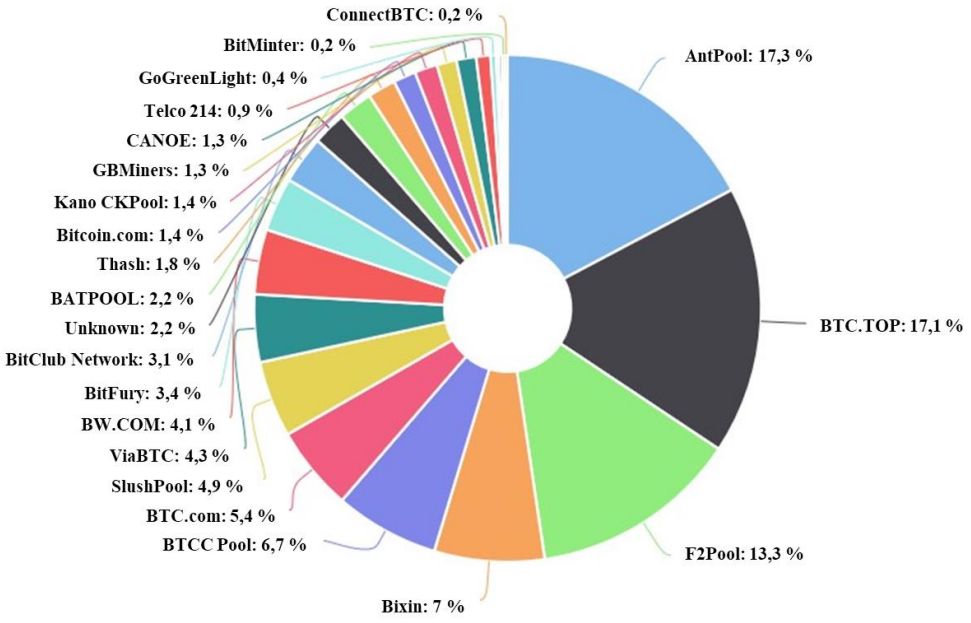
Podobno kot evro ali dolar (cent) tudi bitcoin delimo na manjše enote. Najmanjša se imenuje »satoshi« in predstavlja 0,00000001 bitcoina. 1 bitcoin torej sestavlja 100 milijonov satoshijev, s čimer omogoča plačilo mikro transakcij (Blockchain Luxembourg, 2016). Tako podrobna razčlenitev omogoča mikro plačila, ne glede na vrednost bitcoina. Podjetja lahko s tehnologijo nadzirajo porabo, tako da v vsako enoto denarja programirajo namen porabe, na primer za plače, stroje, material, vzdrževanje ipd. Tako specificiran denar zato ne more biti uporabljen drugje (Niepelt, 2016).

Bitcoini so shranjeni v denarnicah. Obstajata dve vrsti denarnic. Prva je elektronska in je kriptografsko povezana z internetom preko javnega ključa. Druga vrsta denarnice je v fizični obliki in ni neposredno povezana z internetom (USB ključ). Enote valute so izmenjane med denarnicami, oziroma javnimi ključi, brez posrednikov. Transakcije so anonimne vsem, razen strankam v transakciji. Dostop do denarnice je mogoč s privatnim ključem, ki je edinstven za posamezno denarnico in deluje kot geslo (Raiborn & Sivitanides, 2015).

Transakcije v bitcoin sistemu v povprečju potrebujejo 10 minut za potrditev in izvedbo ob obstoječi največji dovoljeni velikosti blokov. Velikost transakcij in blokov se meri v kilobajtih. Zgornja meja enega bloka je 1 megabajt ali 1.000 kilobajtov (Catalini & Gans, 2016, str. 10). Odvisno od velikosti posameznih transakcij, lahko blok vsebuje le določeno

število transakcij. Zaradi limita je bitcoin sistem sposoben izvesti 7 transakcij na sekundo. Za primerjavo, VISA plačilno omrežje je sposobno doseči 56.000 transakcij na sekundo in dnevno procesira več sto milijonov transakcij (Visa International Service Association, 2015). Bitcoin je z vidika kapacitete zato še vedno zelo omejen sistem, kar preprečuje njegovo masovno sprejetje. Obstajata dve rešitvi. Prva je povečanje velikosti posameznega bloka, kar bi povzročilo trdo odcepitev, saj gre za bistveno spremembo v protokolu. Povzročilo bi tudi daljše čase potrjevanja transakcij in posledično še večjo centralizacijo rudarjev. Druga rešitev je tako imenovano »Lightning« omrežje. Gre za vzporedno omrežje, ki bi omogočalo procesiranje mikro in manjših transakcij. Z zmanjšanjem zahtevnosti matematičnih ugank in števila potrebnih potrditev bi rudarji v omrežju lahko občutno hitreje potrjevali transakcije. Tako omrežje bi bilo povezano z glavnim omrežjem. Skupaj bi tvorila večji in razširjen bitcoin sistem. V glavnem sistemu bi se potrjevale le večje transakcije, ki zahtevajo večjo težavnost in varnost (Poon & Dryja, 2016).

Slika 14: Tržni deleži skupin rudarjev v bitcoin omrežju



Vir: Blockchain Luxembourg, Hashrate Distribution, 2017b.

Kot je predstavljeno zgoraj, so za potrjevanje blokov zadolženi rudarji, ki z reševanjem zahtevnih matematičnih ugank dodajajo bloke v verigo in s tem izvršujejo transakcije. Zaradi težavnosti in povečanja možnosti za pridobitev nagradne provizije se le-ti združujejo v skupine. Slika 14 prikazuje ponazarja tržne deleže različnih skupin rudarjev v bitcoin omrežju. Delež je prikazan za obdobje štirih dni (6. 7. 2017–9. 7. 2017), kjer je videti, da imajo največji tržni delež skupine Antpool, BTC.TOP in BTCC Pool in Bixin. Za prevzem omrežja (več kot 51 % procesorske moči omrežja) bi se moralo združiti 5 največjih skupin.

Običajno vlade omejujejo uporabo alternativnih valut zato, da zaščitijo svoj monopol nad izdajanjem denarja. Vlada Združenih Držav Amerike (v nadaljevanju ZDA) je izjavila, da bitcoin ne predstavlja valute, ampak je bolj podoben premoženju oziroma lastnini. Z izjemo nekaj držav (Islandija, Vietnam, Bolivija, Ekvador in ostale) je uporaba bitcoina legalna v večini svetovnih držav (Madeira, 2017).

Dve pomembni lastnosti, ki zagotavljata, da bitcoin nosi vrednost, sta:

- omejena ponudba: bitcoin je zasnovan tako, da omejuje skupno število bitcoinov na 21 milijonov. Bitcoini se v sistem sproščajo preko nagrad, ki jih dobijo rudarji za potrjen blok. Na začetku je bila nagrada v višini 50 bitcoinov, vendar se ta razpolovi vsakih 210.000 blokov ali na približno 4 leta (Grinberg, 2011). Projekcije kažejo, da bo zadnja enota bitcoina generirana leta 2140. Bitcoine bodo nato kot nagrado nadomestile izključno transakcijske provizije, ki bodo ohranjale iniciativo za vzdrževanje omrežja (Brito & Castillo, 2013, str. 7). Trenutno nagrada znaša 12,5 bitcoinov. V obtoku je danes že več kot 16,4 milijonov bitcoinov, kar predstavlja 78 % skupnega števila (Blockchain Luxembourg, 2017d). Omejena količina zagotavlja stabilno rast cene, kar spodbuja kopičenje valute in transakcijsko uporabnost valute (Nugent, 2013). Ko bo ta količina dosežena, bo matematično nemogoče povečati število kovancev v cirkulaciji. Monetarna inflacija bo zato prav tako postala nemogoča (Raiborn & Sivitanides, 2015).
- povpraševanje: povpraševanje je prisotno predvsem zaradi dejstva, da bitcoin ni pod nadzorom vlad, centralnih bank in ga omenjene institucije ne morejo razvrednotiti (Smith, 2016, junij).

Glede na turbulentno stanje virtualnih valut in nepredvidljivo globalno okolje morajo biti kriptovalute oblikovane tako, da minimizirajo tveganje in hkrati zagotavljajo donosnost. Bitcoin je v svoji zgodovini obstoja doživel izjemno volatilnost. Analiza cene, ki so jo izvedli Kemp, Reid in Romero (2016), prikazuje, da je gibanje cene bitcoina močno povezano z naslednjimi vplivi:

- vladne regulacije: novembra 2013 je senat ZDA označil bitcoin kot perspektivno inovacijo, neodvisno od regulatornih in pravnih vplivov. Istočasno je Kitajska prebivalcem dovolila prosto trgovanje z bitcoini. Cena je pozitivno odreagirala na te dogodke, saj je število uporabnikov in transakcij naraslo. To je vodilo do povečanja cene s 685,75 $ na 1.075,16 $. Do podobnega odziva je prišlo, ko je sodišče Evropske unije odločilo, da izmenjava digitalnih valut ni predmet obdavčenja. S tem je bitcoin postal valuta in ne le dobrina. Cena je v naslednjih dneh narasla za 50 $. Po drugi strani je deklaracija Kitajske, da bitcoin ni valuta, povzročila padec vrednosti s 1.022,37 $ na 939,93 $ v samo desetih dneh.
- varnostni vdori: tako bitcoin kot ethereum sta doživela in preživela številne hekerske poskuse. Eden izmed takih je bil vdor v borzo Bitstamp leta 2015, ko je bilo ukradenih

18.866 kovancev in je cena v naslednjih dneh padla za 75 $. Še ena borza oziroma menjalnica, Bitfinex, je bila tarča napada leta 2016, ko je bilo ukradenih skoraj 120.000 kovancev v skupni vrednosti več kot 66 milijonov $. Cena bitcoina je še isti dan padla za 20 %. Ethereum velja za bolj varno valuto izmed obeh, čeprav gre za dva popolnoma različna namena uporabe. Kljub temu je bitcoin bolj likvidna valuta, zaradi bolj množične uporabe. Cenovna analiza je po drugi strani dokazala, da se vpliv varnostnih vdorov s časom zmanjšuje, saj se uporabniki prilagajajo (sprejemajo občasne vdore, s tem ko se istočasno učijo). Ob tem, ko raste število uporabnikov, raste tudi vrednost valut. To omogoča, da trg lažje absorbira šoke.

- notranje upravljanje: medtem, ko je bil bitcoin vpeljan kot popolno decentraliziran sistem, so programerji sčasoma popravljali in izboljševali sistem, kar je bilo sprejeto kot kršenje principa same tehnologije. Ko je Mike Hearn, bivši razvojnik v Googlu in bitcoin sistemu, označil bitcoin kot neuspel poskus, je cena padla za 50 $ v roku enega dne.
- zunanji vplivi: beg kapitala in kontrola nad kapitalom lahko v prihodnosti predstavljata pomembna faktorja vpliva na gibanje vrednosti valut, in sicer predvsem z vidika povečevanja nezaupanja v tradicionalne banke.

Kitajski borzni zlom v letu 2015 je prispeval osnovno razumevanje, kako finančni šoki vplivajo na kriptovalute. Medtem ko je šanghajska borza v enem dnevu izgubila 30 % vrednosti, je vrednost bitcoina na drugi strani zrasla za več kot 20 %. Te spremembe potrjujejo hipotezo, da bitcoin predstavlja pomembno sredstvo vrednosti, ki je lahko uporabljeno kot ščitenje pred negativnimi šoki na kapitalskih trgih. Regresijska analiza je pokazala, da je vrednost šanghajske borze statistično pomembno obratno sorazmerno vplivala na ceno bitcoina (Kemp, Reid, & Romero, 2016).

Brexit referendum je junija 2016 povzročil, da je tržna kapitalizacija bitcoina skočila z 9,6 milijard $ na 12 milijard $ in se je po glasovanju stabilizirala okoli 10 milijard $. Pričakovana ekonomska sprememba bi lahko povzročila beg kapitala v bolj varna in likvidna sredstva, ki so smatrana kot bolj odporna proti drastičnim motnjam na trgu (krize). Poleg tega brexit predstavlja tudi potencial za druge geopolitične spremembe, celo krize (populistična gibanja v Evropi, ZDA in drugje) (Kemp, Reid, & Romero, 2016). Pomemben makro indikator je tudi velika devalvacija valut na trgih, kot sta Indija in Rusija.

Velik preskok v ceni se je zgodil v prvih petih mesecih leta 2017. 1. januarja je vrednost znašala okoli 1.000 $ in je vrh doživela v začetku julija, ko je presegla 3.000 $ (Rizzo, 2017). Rast je mogoče pripisati različnim faktorjem. Prvi faktor je povezan z naraščajočim svetovnim povpraševanjem po kriptovalutah. K temu prispevajo investitorji, ki so v kriptovalutah prepoznali naložbeno priložnost. Večina menjave z bitcoini je špekulativne narave. Nekateri so bitcoin prepoznali kot primeren hranilec vrednosti v politično nestabilnih okoljih. Na povpraševanje bitcoina je pozitivno vplival tudi nastanek in rast drugih kriptovalut, katere je mogoče kupiti tudi z bitcoini. Drugi faktor je povezan z dejanji

Japonske in Kitajske. Prva je aprila predstavila nova pravila, ki bitcoin sprejemajo kot zakonito valuto. Slednje je povzročilo močan narast v menjalnih aktivnostih. Na drugi strani so se razlike v cenah na ameriških in kitajskih borzah zmanjšale, kar pomeni, da je bitcoin postal manj tvegana investicija. Tretji faktor je povezan z valom navdušenja, ki so ga povzročili mediji, konference in priznana svetovna podjetja z visokimi vlaganji na tem področju (IBM, Microsoft itd.) (Roberts, 2017).

Slika 15: Gibanje tržne vrednosti bitcoina, v letih od 2009 do danes

Vir: Blockchain Luxembourg, Market price (USD), 2017c.

Zgoraj opisano ponazarja slika 15, ki podaja grafični prikaz gibanja tržne vrednosti bitcoina skozi celotno obdobje (od 2009 do danes).

Vrednost bitcoinov je mogoče določiti na različne načine. Njihova znanstvena vrednost temelji na rešitvi Byzantinovega generalovega problema, ki ponazarja težavnost komunikacije preko nezanesljivih povezav. Problem je predvsem prisoten v računalniškem svetu. Poleg znanstvene vrednosti imajo kovanci tudi tehnološko vrednost, saj so odporni na cenzuro in jih ni mogoče ukiniti. Imajo tudi socialno vrednost. Uporabljajo namreč javne baze in decentralizirane sisteme, ki odstranjujejo potrebo po tretjih osebah (posrednikih). Obstaja tudi pomembna oblikovna vrednost, saj bitcoin model spodbuja sodelovanje in prispevanje uporabnikov sistema. Druga področja vrednosti kovancev so povezana z njihovo uporabo, za pogodbe, aplikacije, prenos in shranjevanje vrednosti (Brown, 2016).

2.5 Koristi in tveganja uporabe kriptovalut

Koristi in tveganja, ki so našteta v poglavju o tehnologiji podatkovnih verig, lahko apliciramo tudi pri kriptovalutah. Kot pojasnjeno njihovo delovanje temelji na tej tehnologiji. V naslednjih alinejah predstavljam tiste koristi in tveganja, ki so še posebej značilna in pomembna pri kriptovalutah.

Pomembne koristi uporabe kriptovalut so (Rosic, 2016; Investopedia, b.l.):

- preprečevanje goljufij: kriptovalute so digitalne in ne morejo biti ponarejene. Tudi v primeru prevzema omrežja (prevzem 51 % zmogljivosti sistema) napadalci ne morejo ukrasti kovancev drugih. Povrnejo lahko le svoje, že porabljene, kovance in nato izkoristijo prevlado za njihovo večkratno uporabo.
- preprečevanje kraje identitete: plačilne kartice trenutno delujejo po »pull« principu, kjer trgovec sproži transakcijo tako, da iz računa kupca odvzame sredstva. S tem dostopa do celotnega računa. Kriptovalute na drugi strani delujejo po »push« principu, saj kupec trgovcu pošlje le toliko sredstev, kot je potrebno, brez razkritja dodatnih informacij.
- dostopnost: obstaja približno 2,2 milijarde posameznikov, ki imajo dostop do interneta ali mobilnih telefonov, vendar pa trenutno nimajo dostopa do tradicionalnih sistemov za izmenjavo. Ti posamezniki so primerni za trg kriptovalut.
- takojšnje poravnave: časovna izvedba prenosa kriptovalut na globalni ravni je neprimerljivo krajša kot pri obstoječih plačilnih sistemih.
- pripoznanje na globalni ravni: kriptovalute niso vezane na menjalne tečaje, obrestne mere, transakcijske provizije ali druge dajatve s strani države. Zato so lahko uporabljene na globalni ravni brez večjih problemov. Posledično je mogoče pri prenosu denarja med državami doseči velike prihranke pri času in denarju.
- nižje provizije: transakcije s kriptovalutami vključujejo zanemarljive provizije v primerjavi z obstoječimi nakazili. Ponudniki e-denarnic in menjalne borze na drugi strani zaračunavajo provizije.

Ključna prednost kriptovalut je, da omogočajo uporabo pametnih pogodb. Za razliko od dobave standardnega denarja, ki temelji na politiki monetarnih teles, je dobava kriptovalut v teoriji izolirana od človeških dejavnikov ter pogojena glede na želene rezultate (fiksirana rast vrednosti – inflacija). Zaenkrat še obstajajo diskretni posegi v obtok kriptovalut s strani lastnih monetarnih komitejev (spremembe v pravilih protokolov, ki povzročijo nastanek novih kriptovalut). Povpraševanje po kriptovalutah je pogojeno z izgubo zaupanja v politiko centralnih bank in željo po večji zasebnosti pri transakcijah. Sledi torej dejstvo, da več kot je plačil, izvedenih v kriptovalutah, manjša je potreba po tradicionalnem denarju in rezervah. Za centralne banke se v tem primeru zmanjša zmožnost nadzora plačilnega sistema in v skrajnem primeru tudi izgubijo kontrolo nad ponudbo in povpraševanjem. Po drugi strani pa omejena likvidnost kriptovalut povzroča visoko volatilnost v deviznem tečaju. Ko

uporabljivost teh valut doseže kritično maso oziroma jo posvoji dovolj veliko število uporabnikov, se ta omejenost zmanjša in izniči (Orlowski, 2016).

Državni regulatorji so začeli identificirati osnovne probleme in tveganja, povezana s kriptovalutami. Oblikovalci politik in zakonov preučujejo obstoječe okvirje, od bančnih zakonov, blagovnih zakonov do zakonov vrednostnih papirjev in ostalih pravnih okvirjev (Kiviat, 2015). Kriptovalute so ustvarile miselnost, da bi odprt trg valut moral biti popolno dereguliran. Ta pogled je nerealističen in nezaželen, zaradi potrebe po preprečevanju zlorabe in napačne uporabe (Ly, 2014; Swanson, 2014).

Medtem ko je jasno, da ima digitalna valuta svoje koristi, se je potrebno zavedati tudi tveganj, povezanih z vlaganjem in uporabo kriptovalut. Tveganja uporabe kriptovalut so:

- pomanjkanje ozaveščenosti in razumevanja: dejstvo je, da še vedno veliko ljudi ne pozna in razume uporabe kriptovalut. Nekatera podjetja sprejemajo kriptovaluto kot plačilno sredstvo, vendar je zelo pomembno, da imajo ta podjetja usposobljeno osebje, ki razume digitalne valute in lahko pomaga kupcem pri njihovi uporabi. Za usposabljanje ljudi je potrebno nameniti veliko časa in truda.
- volatilnost: kriptovaluta je volatilna predvsem zaradi omejene količine kovancev in naraščajočega povpraševanja. V zgodovini obstoja je menjalna vrednost bitcoina, v primerjavi z ameriškim dolarjem, pogosto skočila ali padla za več kot 20 % znotraj enega dne. Za primerjavo, menjalni tečaj dolar–evro se v istem obdobju ni spremenil za več kot 2,5 % v enem dnevu (Harwick, 2015). Kriptovalute zaradi nestabilnosti zato niso zaželene valute, saj kupna moč lastnikov teh valut lahko drastično naraste ali pade v zelo kratkem času. Visoka volatilnost in negotovost cene zaenkrat preprečuje, da bi bitcoin postal primeren hranilec vrednost. Čeprav so kriptovalute prvotno uporabljene kot hranilec vrednosti (vendar v špekulativne namene), mora njihova vrednost postati stabilna, v kolikor želijo postati fiat valutam enakovreden medij za izmenjavo. Njihova špekulativna narava, ki izhaja iz pričakovanj in pripravljenosti ljudi, da sprejmejo njihovo višjo vrednost, preprečuje njihovo stabilnost. Stabilnost je pomembna za doseganje zaupanja v kriptovaluto in vzpostavitev kriptovalute kot primernega hranilca vrednosti. Slednje igra kritično vlogo pri dolgoročnem uspehu in obstoju kriptovalut. Pri globalni in nenadzorovani valuti, kot je kriptovaluta, je občutno težje zagotoviti njeno vrednost na kratki rok. Kriptovalute lahko pridobijo status hranilca vrednosti na dolgi rok, v kolikor preživijo vsa nihanja in se stabilizirajo. Zadnje je možno zagotoviti s čedalje širšo uporabo kriptovalut na različnih trgih (tržni efekt) (Lo & Wang, 2014; Worstall, 2013; Lingham, 2017). Ob izpolnitvi tega pogoja se bo vzpostavilo tudi zaupanje v kriptovalute in ljudje jih bodo pripravljeni sprejeti kot medij za izmenjavo. Kriptovalute zaradi svoje digitalne oblike predstavljajo odličen potencialni medij za izmenjavo. Trenutno je uporaba kriptovalut kot medija izmenjave omejena, zaradi omejenega števila ponudnikov, ki so pripravljeni blago in storitve izmenjati za

kriptovalute. Kot medij za izmenjavo je najverjetneje uporabljen pri spletnih trgovcih. V povezavi s tretjo lastnostjo denarja so kriptovalute kot obračunske enote popolnoma vezane na njihovo protivrednost v fiat valutah (Lo & Wang, 2014).

- brez nadzora: ne obstaja centralna avtoriteta, ki bi ščitila in nadzorovala vrednost kriptovalut in zaupanje ljudi. Nezmožnost prilagajanja ponudbe valut predstavlja potencialno tveganje pri uravnavanju ekonomij v času ekstremnih pogojev (na primer krize, recesije itd.). Matematična pravila, ki upravljajo delovanje kriptovalut (na primer bitcoina), posnemajo značilnosti zlata. Zakon matematike (v primeru zlata je to zakon narave) upravlja s ponudbo bitcoinov, ki ne more biti prilagojena v časih recesije ali da bi preprečevala destabilizirana obdobje inflacije ali deflacije (Evans, 2014). To tudi pojasnjuje visoko cenovno volatilnost bitcoina in drugih kriptovalut.
- zlorabe in prevare: uporaba kriptovalut je pogosto povezana tudi z negativnimi dejanji. Primeri zlorab so lahko financiranje nelegalnih aktivnosti, pranje denarja, davčne utaje in financiranje terorizma (Brito & Castillo, 2013).
- nerazvitost: kriptovalute so še vedno v začetni fazi z nepopolnimi funkcijami, ki so v razvoju. Da bi bila digitalna valuta bolj varna in dostopna, se trenutno razvijajo nove funkcije, orodja in storitve (CoinReport, 2014).
- nepreklicnost: transakcije so nepreklicne za razliko od obstoječega sistema plačilnih kartic, kjer lahko transakcijo prekličeš, ko je že potrjena. To v primeru napačnih vnosov predstavlja problem, saj je napako mogoče odpraviti le z novo, povratno, transakcijo. To povečuje verjetnost za zlorabe.

V nadaljevanju sledi opredelitev in pojasnjevanje vpliva tehnologije podatkovnih verig in kriptovalut na računovodstvo.

3 VPLIV NA RAČUNOVODSTVO

Medsebojno sodelovanje in investiranje štirih največjih računovodskih in revizijskih hiš (Deloitte, Ernst & Young, KPMG in PriceWaterhouse Coopers) v razvoj aplikacij tehnologije podatkovnih verig pomeni, da so prepoznali resnost njene potencialne uporabe na tem področju. Kot je predstavljeno v nadaljevanju, tehnologija predstavlja grožnjo panogi računovodstva in revizije, vendar hkrati tudi priložnosti. Računovodske in revizijske storitve so prisotne v vsakem podjetju in industriji, kot posledica regulativnih okvirjev, namen katerih je vzpostavljanje zaupanj. To pomeni, da obstaja velika verjetnost, da bo ta panoga med prvimi doživela spremembe, če bo želela podpirati nove poslovne modele in nadaljnji razvoj tehnologije. Kljub revolucionarni tehnologiji bodo spremembe nastajale evolucijsko (Association of Chartered Certified Accountants, 2016, junij). V nadaljevanju opredeljujem razsežnost vpliva tehnologije v panogi računovodstva in revizije skozi različne vidike. Na koncu povzemam njihove aktivnosti pri razvoju aplikacij na tem področju.

Definicija tehnologije podatkovnih verig uporablja mnogo računovodskih izrazov. Izraz »baza podatkov« lahko nadomesti izraz »glavna knjiga«, ki shranjuje zapise o časovno zaznamovanih dogodkih ali transakcijah. Delovanje računovodske glavne knjige, kot produkta tehnologije, temelji na identičnih principih, kot je opisano v prvem poglavju.

3.1 Trenutna oblika in problemi računovodstva

3.1.1 Trenutna oblika računovodstva

Kljub temu da je razvoj splošne tehnologije v zadnjih nekaj desetletjih pomembno optimiziral proces računovodstva, osnovni princip delovanja ostaja nespremenjen. Računovodska praksa še vedno uporablja mehanizem dvostavnega knjigovodstva, ki ga je konec 14. stoletja v delu "Review of Arithmetic, Geometry, Ratio and Proportion" uvedel Luca Pacioli (Lee, 2016). Razlog za uvedbo je bil pojav mednarodne menjave in prvih delniških podjetij. Število in kompleksnost transakcij sta se močno povečali (Tyra, 2014). Glavni namen uvedbe dvostavnega knjigovodstva je bil vzpostavitev zaupanja vodstva v lastne knjige (Deloitte, 2016b).

Medtem ko enostavno knjigovodstvo beleži le dogodek, dvostavno knjigovodstvo pojasnjuje dogodek s protipostavko. Iz te definicije izhajata debet in kredit postavki v računovodstvu, kjer ena beleži stanje in druga spremembo vsake gospodarske kategorije v finančnih izkazih (Spoke, 2015). Dvostavno knjigovodstvo je glavni razlog za nastanek sredstev in obveznosti, ki morata biti vrednostno uravnoteženi ob vsakem zabeleženem dogodku (Grigg, 2005). Zaupanje zunanjih upikov je pridobljeno na podlagi revidiranja izkazov s strani revizorjev.

Dvostavno knjigovodstvo vpeljuje tudi glavno knjigo, ki združuje vse dogodke podjetja v danem obdobju. »Glavna knjiga vsebuje konte postavk sredstev, obveznosti do njihovih virov, prihodkov in odhodkov ter zunajbilančnega razvida. Glavna knjiga omogoča kontroliranje knjiženih postavk po enačbi vsota postavk v breme je enaka vsoti postavk v dobro. S tem prispeva k zanesljivosti glavne knjige kot vira podatkov za pripravljanje bilance stanja in izkaza poslovnega izida pa tudi posameznih knjigovodskih informacij.« (Slovenski inštitut za revizijo, 2016, str. 300–304). Poleg glavne knjige poznamo tudi pomožne knjige, ki skupaj tvorijo poslovne knjige. »Pomožne poslovne knjige so analitične evidence in druge pomožne knjige. Vodenje glavne knjige je obvezno, vodenje pomožnih poslovnih knjig pa samo, če se verodostojni podatki, ki se ponavadi dobivajo na podlagi pomožnih knjig, ne zagotavljajo drugače. Poslovne knjige nastajajo pri knjigovodenju v finančnem računovodstvu in stroškovnem računovodstvu.« (Slovenski inštitut za revizijo, 2016, str. 300–304). Vnosi istih transakcij v glavnih knjigah morajo biti medsebojno usklajeni po postavkah in vrednostih. Terjatev podjetja A velja le, če podjetje B na drugi strani v svojih obveznostih beleži obveznost v enakem znesku. S tem dobijo transakcije direktno povezavo s krajem nastanka, česar prej enostavno računovodstvo ni poznalo.

Za pravilnost in uravnoteženost poslovnih knjig znotraj podjetja skrbijo računovodje. Tradicionalne metode računovodstva in knjigovodenja shranjujejo in poročajo finančne podatke po načelih, določenih v mednarodnih (MSRP, GAAP) ali nacionalnih računovodskih standardih (v Sloveniji SRS). Oblikovanje mednarodnih računovodskih standardov je predvsem v domeni dveh računovodskih teles: Financial Accounting Standards Board (ameriška organizacija; v nadaljevanju FASB) in International Accounting Standards Board (evropska organizacija; v nadaljevanju IASB) (Barker, 2003). Namen standardov je vzpostaviti primerljivost izkazov med podjetji. Za preverjanje uravnoteženosti poslovnih knjig med podjetji in zagotavljanje skladnosti poročanja s standardi skrbijo revizorji (Spoke, 2015). Visoke regulatorne zahteve v računovodstvu in reviziji so potrebne za zagotavljanje enotnega in primerljivega poročanja podjetij. Hkrati skušajo preprečevati ponarejevanje in nepošteno prikazovanje podatkov (Deloitte, 2016b).

Glavne knjige so orodje za pripravo finančnih izkazov (Brown, 2015). Finančni izkazi so reprezentacija delovanja podjetja, kot je predstavljeno s strani vodstva. Pravilnost izkazov je zagotovljena skozi naslednje predpostavke (Tyra, 2014):

- sredstva in obveznosti v bilanci stanja so resnična in točna na datum bilance stanja;
- finančni izkazi prikazujejo vse aktivnosti podjetja v predstavljanem časovnem obdobju;
- vrednosti, na katerih temeljijo finančni izkazi, so pravilne in razumne glede na okoliščine;
- postavke v finančnih izkazih so vrednotene in opisane na pravi način.

Finančni izkazi so sestavljeni iz različnih bilanc. Temeljni izkazi so bilanca stanja, izkaz poslovnega izida, izkaz gibanja kapitala in izkaz denarnih tokov. Finančni izkazi so za organizacije potrebni za privabljanje kapitala, finančnih in človeških virov in za zagotovitev možnosti delitve dobičkov svojim lastnikom. Omogočajo spremljanje gibanja vrednosti, uspešnosti in tveganosti naložb v podjetja. Pomagajo tudi ustvariti stabilnost in dodajo element predvidljivosti delovanja organizacij (Sunder, 2016). Funkcije finančnega računovodstva so evidentiranje poslovnih dogodkov, merjenje vrednosti sredstev in obveznosti po posebnih načelih, izračun poslovnega izida in priprava poročil.

Lastnosti dobrega finančnega poročanja so zaupanje, poštena reprezentacija podatkov, pravočasnost, relevantnost, zanesljivost, preverljivost, enotnost, doslednost, primerljivost, konservativnost in robustnost do manipulacij in goljufij (Sunder, 2016).

Tehnološki trendi v zadnjih letih narekujejo predvsem selitev računovodstva v oblačne storitve, ki računovodjem omogočajo dostop do poenotene programske opreme in podatkov kadarkoli in kjerkoli. Glavne prednosti modela »računovodstvo v oblaku« (angl. *cloud accounting*) so boljša preglednost, fleksibilnost (dostopnost, delovni čas), delna avtomatizacija v smislu posodabljanja finančnih izkazov, bolj tekoči izkazi in stroškovni

prihranki (podatkovna infrastruktura, programska oprema, vzdrževanje, delovna sila). Kljub temu ostajajo določena tveganja. Najbolj pomembna sta odvisnost od dostopnosti do interneta in varnost. Slednje izhaja iz dejstva, da gre še vedno za centralizirano storitev pri ponudniku oblačnih storitev. Model prav tako ne prispeva izboljšav na strani revidiranja. Preverjanje transakcij je še vedno izvedeno po vnosu (Dimitriu & Matei, 2015).

3.1.2 Problemi obstoječega računovodstva

Prvi problem se nanaša na vse bolj prepletene aktivnosti mednarodnih podjetij in ogromno količino podatkov, ki jih generirajo. Trenutni računovodski sistemi težko sledijo vse večjim volumnom globalnega poslovanja in potrebam po pravočasnih in ažurnih informacijah (Association of Chartered Certified Accountants & Grand Thornton, 2016). Problem izhaja iz dejstva, da je vpletenost ljudi še vedno velik del računovodskega procesa (Scott, 2015). Medtem zaupanje in transparentnost postajata ključni lastnosti za obvladovanje prepletenosti globalne ekonomije (Rae, 2017).

Drugi problem obstoječega sistema je medsebojna sinhronizacija številnih poslovnih knjig med podjetji. Tradicionalni sistem dvostavnega računovodstva zagotavlja interno konsistentnost knjig v podjetju. Če se bilanca stanja ujema, potem so bili zapisi pravilno vneseni. Vendar na drugi strani ne rešuje konsistentnosti in usklajenosti med različnimi organizacijami (Vaidyanathan, 2017). Podjetje mora svojo knjigo in vsebujoče postavke sinhronizirati s knjigami vseh subjektov, s katerimi je poslovalo v določenem obdobju (Brown, 2015). Poleg tega usklajevanje dodatno otežujejo različni in izolirani računovodski sistemi med podjetji ter neenotne računovodske prakse med državami.

Pomemben problem je tudi selektivno preverjanje transakcij v postopku revidiranja. Upoštevati je potrebno, da je revidiranje delovno intenziven proces, daleč od avtomatizacije. Zahteva ogromno dokumentacije, visoka prizadevanja in periodične kontrole (Deloitte, 2016b). Trenutni proces izbiranja reprezentativnega vzorca znotraj populacije transakcij je zato posledica človeških omejitev, časovno zamudnih procesov in stroškovnih neučinkovitosti, ki bi se pojavile pri testiranju vsake posamezne transakcije (Vaidyanathan, 2017). Vzorčenje temelji na statističnih metodah, kar omogoča verjetnost odklona (standardno napako) pri zaznavanju vsake goljufije ali prikritja. Zaradi standardizacije metodologije so revizorji postali tudi bolj predvidljivi (Frieswick, 2003).

Kot je omenjeno v začetku magistrskega dela, je problem zaupanja eden temeljih razlogov za nastanek tehnologije podatkovnih verig. Problem se navezuje tudi na področje računovodstva in revizije. Celotna panoga temelji na predpostavki, da gre za zaupanja vredna podjetja, ki svoje naloge opravljajo neodvisno in objektivno (Spoke, 2015). Zgodovina je pokazala, da temu ni vedno tako. Škandali, kot so Enron, WorldCom, Lehman Brothers, so le nekaj primerov, kjer je bilo to zaupanje izrabljeno in so dokazali, da sebična

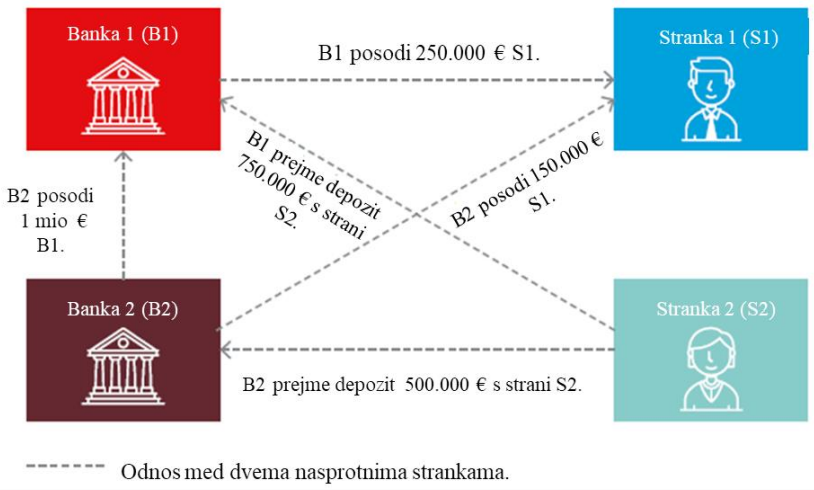
narava ljudi včasih prevlada nad objektivnostjo in etičnostjo. Problem integritete je prišel do izraza v 80. letih prejšnjega stoletja, ko je AICP (angl. *American Institute of Certified Public Accountants*) dovolil oglaševanje računovodskim in revizorskim podjetjem. Generiranje prihodkov je postal temeljni faktor pri nagrajevanju partnerjev v podjetjih (Fireswick, 2003). Nezaupanje povzročajo tudi kreativne in goljufive prakse računovodstva in nepravočasnost poročanja. Večina modelov kreditnega tveganja temelji na računovodskih podatkih, zato je zaupanje v podatke izjemnega pomena (Byström, 2016).

3.2 Definicija tristavnega računovodstva

Naslednji velik preskok v računovodski tehnologiji predstavlja tehnologija podatkovnih verig, ki vpeljuje tako imenovano tristavno računovodstvo. Koncept tristavnega knjigovodstva je prvič vpeljal Yuji Ijiri leta 1986 v delu »A framework for tripple–entry bookkeeping«, ki se sicer razlikuje od koncepta, predstavljenega v nadaljevanju. Tristavno knjigovodstvo, kot produkt tehnologije podatkovnih verig, skupaj poveže standardne tehnike dvostavnega knjigovodstva in inovativnost kriptografije (Grigg, 2005). S pomočjo slednje je isti dogodek hkrati zabeležen v poslovnih knjigah dveh nasprotnih strank in v osrednjem blockchain sistemu (Wunsche, 2016). Kriptografija odpravi problem razlike v podatkih med različnimi strankami in omogoča nespremenljivost podatkov (Grigg, 2005). Tristavno knjigovodstvo torej v terminologiji obstoječega računovodstva vsebuje dogodek, njegovo pojasnilo in potrdilo o veljavnosti dogodka.

Medtem ko je namen dvostavnega knjigovodstva vzpostaviti zaupanje s strani računovodij in revizorjev, je cilj tehnologije podatkovnih verig pridobiti zaupanje tudi zunanjih upnikov. Ti bodo lahko varno preverili kredibilnost finančnih podatkov podjetja (Sharma, 2017).

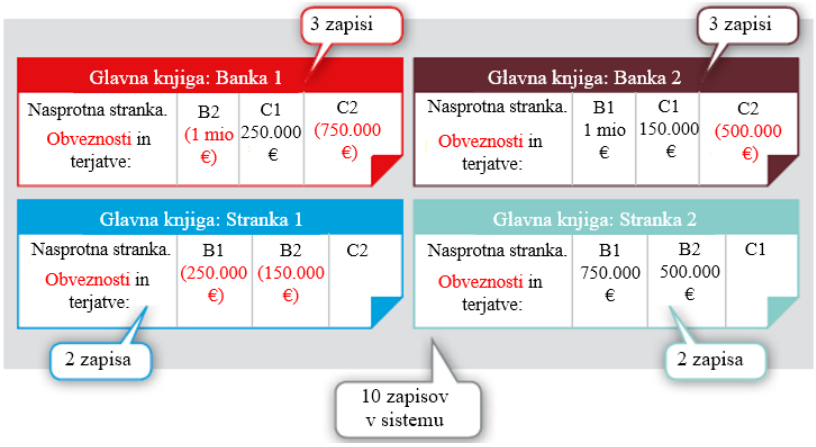
Slika 16: Primer petih različnih transakcij med dvema bankama in dvema strankama



Vir: N. Vaidyanathan, Divided we fall, distributed we stand, 2017.

Slike 16, 17 in 18 predstavljajo praktičen primer razlike med uporabo dvostavnega in tristavnega knjigovodstva. V Sliki 16 je predstavljen primer beleženja transakcij med štirimi subjekti (dve banki in dve stranki). Slika 17 ponazarja zapis, v zgornji sliki prikazanih, transakcij v glavne knjige posameznih podjetij na podlagi dvostavnega knjigovodstva. Vse štiri strani skupno zabeležijo 10 vnosov.

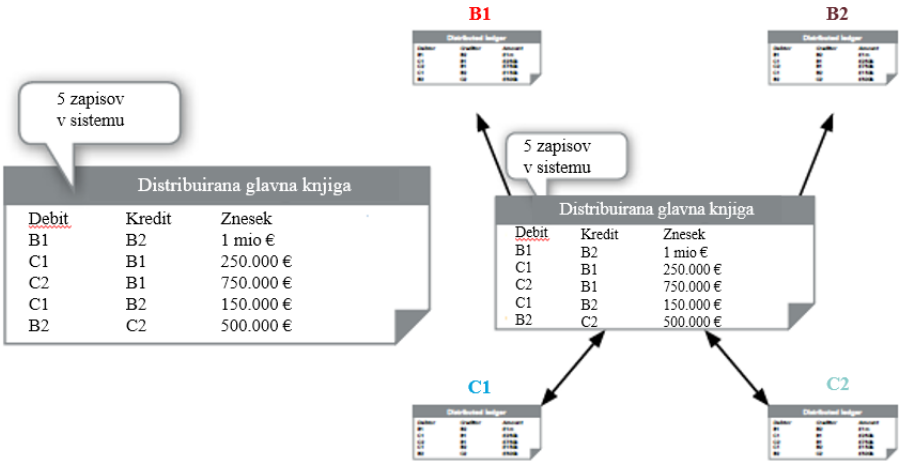
Slika 17: Zapis transakcij zgornjega primera pri vsaki strani na podlagi dvostavnega računovodstva



Vir: N. Vaidyanathan, Divided we fall, distributed we stand, 2017.

Na Sliki 18 je vsaka transakcija zabeležena le enkrat v distribuirano glavno knjigo v blockchain sistemu. Ta knjiga je nato distribuirana pri vsakem uporabniku, ki se ujema z evidenco pri vsakem izmed njih. Tristavno knjigovodstvo v tem primeru razpolovi število potrebnih zapisov z 10 na 5.

Slika 18: Zapis transakcij zgornjega primera pri vsaki strani na podlagi tristavnega računovodstva



Vir: N. Vaidyanathan, Divided we fall, distributed we stand, 2017.

3.3 Računovodstvo, ki temelji na tehnologiji podatkovnih verig

Računovodstvo, ki temelji na tehnologiji podatkovnih verig, lahko razumemo na dva načina, kot tristavno ali enostavno računovodstvo. Kot je opisano zgoraj, dobi vsak dogodek še tretjo protipostavko »potrditev sistema«, kar je bistveno za definicijo tristavnega računovodstva. Ob enem ima glavna knjiga v blockchain sistemu obliko bolj podobno enostavnemu računovodstvu. V principu gre za kronološki seznam celotne zgodovine transakcij (Simon, 2016). Časovna zaznamovanost in nespremenljivost odpravljata ključno pomanjkljivost enostavnega knjigovodstva (manipuliranje podatkov).

Glavna knjiga je univerzalna in je v identični verziji distribuirana pri vseh uporabnikih (pošiljatelj sredstva, prejemnik sredstva in sistem) (Horadan, 2016). V blockchain računovodstvu zato ni potrebe po vodenju ločenih poslovnih knjig (Brown, 2015). Kljub temu bo podjetje najverjetneje vzporedno vodilo lastne poslovne knjige, ki vsebujejo le njihove transakcije. Te knjige bodo sinhronizirane z glavno knjigo, kar ustvari medsebojno povezan sistem računovodskih evidenc. Distribuiranost in sinhronizacija glavne knjige, ki je v isti obliki in verziji shranjena pri vseh uporabnikih, odpravlja problem nekonsistentnosti in neusklajenosti obstoječih poslovnih knjig in sistemov med podjetji (Vaidyanathan, 2017). Poleg medsebojne povezanosti internih računovodskih evidenc pa je za popolno konsistentnost potrebno zagotoviti tudi povezanost z drugimi sistemi (na primer plačilnim). Idealna rešitev bi bila delovanje vseh sistemov na podlagi tehnologije podatkovnih verig, saj je mogoče enostavno zagotoviti njihovo povezanost. Blockchain računovodski sistem je lahko uporabljen kot evidenca za katerokoli sredstvo (opredmeteno, neopredmeteno), zalogo in za izmenjavo teh sredstev (Swan, 2015).

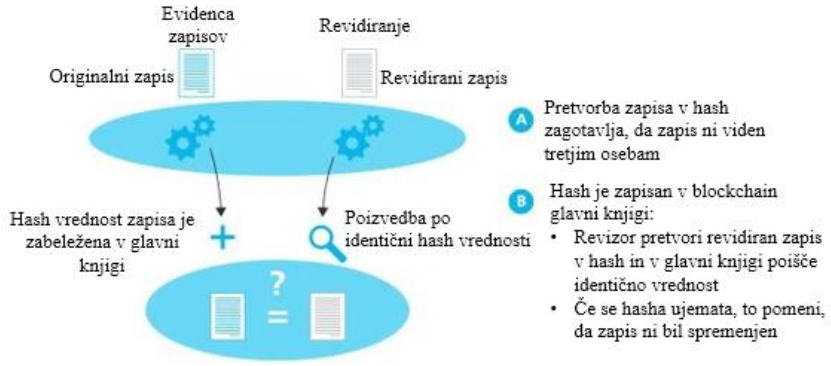
Byström (2016) navaja dva načina, s katerima lahko tehnologija v računovodstvu izboljša kvaliteto informacij. Prvič, računovodske informacije postanejo bolj zaupanja vredne in drugič, informacije postanejo pravočasne in ažurne.

- Nespremenljivost in celovitost bistveno prispevata k ustvarjanju zaupanja vrednih informacij. Transakcije so zaradi časovne zaznamovanosti izsledljive do samega začetka obstoja podjetja, kar ustvarja samodejno popolno revizorsko sled in celovitost podatkov. (Wunsche, 2016). Sled ustvari sistem, ki regulatorjem omogoča celovito spremljanje trgov na različnih lokacijah in v različnih sistemih. Zagotovi tudi večjo preglednost in boljši dostop do kritičnih podatkov (Huber, 2016). S tem se odpravi problem omejenega oziroma strnjenega vpogleda v podatke v obstoječem sistemu. Poleg tega kriptografija omogoča, da so zapisi trajni ter odporni proti retroaktivnim spremembam ali izbrisom. Možnosti manipuliranja računovodskih izkazov se dramatično znižajo (Byström, 2016).
- Izvedba, zapis in potrditev transakcije se zgodijo istočasno in v realnem času (Huber, 2016). Na drugi strani uporabniki dostopajo do glavne knjige v vsakem trenutku. To pomeni možnost generiranja finančnih izkazov v realnem času na podlagi popolnih in

posodobljenih podatkov (Yermack, 2017). Od oblike sistema je odvisno, ali to lahko storijo vsi uporabniki (javni sistem) ali le tisti, ki imajo dostop do vpogleda (privatni sistem). Generiranje izkazov je mogoče za poljubno določeno obdobje, in sicer s seštetjem vseh sprememb v posameznih postavkah (Simon, 2016). Agregiranje posameznih postavk v trenutno obliko izkazov (na primer sredstva in obveznosti v bilanci stanja) lahko predstavlja nepregleden proces, ki pa ga je mogoče poenostaviti z uporabo obarvanih kovancev (vsako sredstvo ima svojo barvo ali simbol) in razvojem programske opreme, ki bi samodejno sestavljalo izkaze. Povezano z enotno glavno knjigo, ki združuje podjetja ali potencialno celotno industrijo, lahko uporabniki generirajo izkaze za celotni sistem (industrijo), del sistema (skupino podjetij, konsolidacijo) ali posamezno podjetje (Horadan, 2016). Deležnikom podjetja se ne bi bilo potrebno zanašati na stare (kvartalne, polletne ali celo letne) izkaze, ki so pogosto na voljo prepozno. S tem je zadovoljena potreba po pravočasnih in ažurnih informacijah. Spremljanje transakcij v realnem času prav tako pomeni dodaten korak naprej na področju skladnosti poslovanja in zmanjšanja prevar in manipulacij (Bradbury, 2015).

Samodejno zapisovanje in istočasna soglasna potrditev posamezne transakcije odpravlja potrebo po vzorčenju v procesu revidiranja. Uporabniki že ob potrditvi preverijo skladnost podatkov na podlagi digitalnih zapisov. Pri tem lahko sodelujejo revizorji, kot je to prikazano na Sliki 19. Revizor s pretvorbo revizorskega zapisa v glavni knjigi išče enako vrednost dobljenega hasha. V kolikor najde identično vrednost, lahko potrdi nespremenjenost zapisa. Seveda je mogoče tudi naknadno preverjanje poljubne transakcije v celotni zgodovini. Ključna prednost za revizorje je popoln dostop do celotne baze podatkov in enostavnejše identificiranje spornih dogodkov. S pregledom nad tokom denarja in sredstev bi označili nenavadne dogodke in jih podrobneje raziskali (Staley, 2016). Podjetja bi z uporabo tehnologije imela možnost opravljati neprekinjeno interno revizijo, ponuditi revizorsko sled in izvesti takojšnje analize računov (Wunsche, 2016). Tak sistem bi podpiral analiziranje podatkov na masovni ravni ter posledično zgodnje negativne signale in preventivno ukrepanje podjetij in ekonomij (Campbell, 2015).

Slika 19: Preverjanje integritete zapisov s pomočjo tehnologije podatkovnih verig

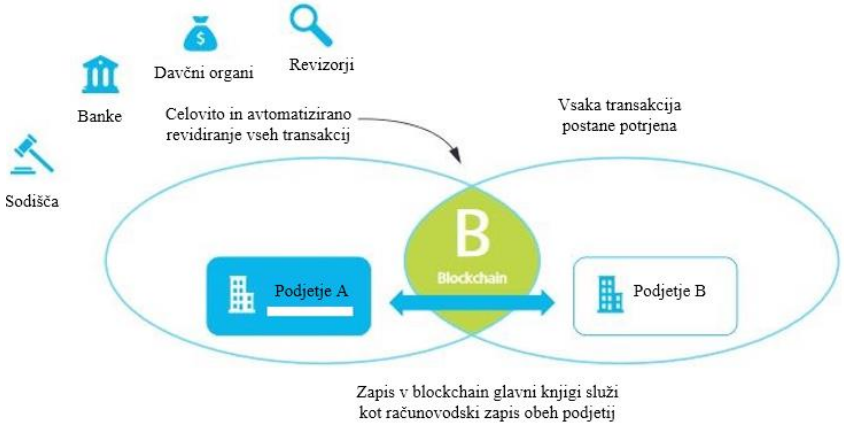


Vir: Deloitte, Blockchain technology. A game changer in accounting?, 2016b.

Ob teh lastnostih računovodskega sistema se vzpostavi integriteta podatkov in reši problem nezaupanja. Za podjetja bi sicer širši dostop do podatkov lahko pomenil tveganja z vidika varovanja poslovnih skrivnosti, vendar hkrati tudi kompromis za zmanjšanje stroškov in privabljanje investitorjev. Slednji bi dajali prednost podjetjem, ki bi delovala in vodila knjige v blockchain sistemu. Za podjetja to predstavlja pomembno iniciativo za spremembo načina poročanja (Yermack, 2017). Ob tem je potrebno poudariti, da bodo podjetja z veliko gotovostjo oblikovala privatne sisteme, kar bi do neke mere ublažilo tveganje razkritja poslovnih skrivnost. Podjetja bi določila, tudi preko pametnih pogodb, kateri uporabniki imajo dostop do katerih podatkov in celo za kakšno časovno obdobje. Revizorji in regulatorji bi, na primer, imeli popoln in trajen dostop, medtem ko bi bankam, investitorjem in drugim upnikom lahko omogočili dostop le v danem trenutku (odvisno od potreb). Tehnologija iz procesov v veliki meri odstranjuje vpliv človeške narave in zaupanje v računovodje ali revizorje nadomešča z zaupanjem v sistem. To velja predvsem takrat, ko gre za odprti sistem. V primeru privatnih sistemov se zaupanje v sistem zmanjšuje z manjšanjem velikosti sistema in omejevanjem dostopov do vpogleda. Tukaj bodo revizorji še vedno igrali pomembno vlogo, vendar bo njihovo delo lažje.

Slika 20 prikazuje računovodski sistem, ki temelji na tehnologiji podatkovnih verig. Podjetji A in B sta povezani v blockchain sistem, ki vodi glavno knjigo za obe podjetji. Zapis v tej knjigi istočasno predstavlja tudi računovodski zapis posameznih podjetij, ki sta udeleženi v transakciji (deljena baza). Dostop do glavne knjige imajo lahko, kot predstavljeno, tudi drugi deležniki podjetij. Predvsem z vidika revizorjev tovrsten sistem omogoča samodejno revidiranje vseh transakcij v realnem času (v trenutku, ko se transakcija ali dogodek zgodi).

Slika 20: Poenostavljen prikaz računovodskega sistema, ki temelji na tehnologiji podatkovnih verig



Vir: Deloitte, Blockchain technology. A game changer in accounting?, 2016b.

Kljub temu, da gre za revolucijske spremembe, bodo te, podobno kot v ostalih industrijah, implementirane evolucijsko pod nadzorom glavnih igralcev na trgu. Transformacije ni

mogoče doseči v kratkem času, saj gre za občutljive in visoko regulirane aktivnosti. Potrebno je zagotoviti celovit prehod, ki bo na koncu omogočil dodatno vrednost in enostavnejšo prilagoditev podjetij in stroke (Rae, 2017). Tehnologija lahko že danes občutno pomaga obstoječim sistemom in je zato lahko postopoma integrirana v standardne računovodske postopke. V prvem koraku lahko pomaga pri zaščiti celovitosti zapisov in avtomatizaciji procesov, ki zahtevajo največ ročnega dela. Z namenom razumeti vplive in posledice bo v prvi vrsti prišlo do implementacije na manj pomembnih procesih. To je najboljši način za vzpostavitve zaupanja znotraj podjetij in pri zunanjih strankah (Rizzo, 2016). Postopoma bodo podjetja ciljala proti zagotavljanju popolne revizijske sledi. V najbolj ekstremni obliki bi tehnologija popolnoma avtomatizirala proces revidiranja (Deloitte, 2016b).

3.4 Spremembe v finančnih izkazih

V nadaljevanju so predstavljene ključne spremembe, ki jih tehnologija z načinom delovanja potencialno povzroča v posameznih postavkah finančnih izkazov. Dileme in vplivi kriptovalut so natančneje predstavljeni ločeno.

Wunsche (2016) v svojem delu navaja naslednje spremembe v postavkah bilance stanja:

- neopredmetena sredstva: pametne pogodbe imajo potencialen vpliv tudi na intelektualno lastnino. Te bi v primeru razvoja lastnega produkta samodejno in natančno prenašale povezane stroške med kapitalizirane stroške. Vrednosti neopredmetenih sredstev se lahko meri tudi glede na pričakovane koristi. V tem primeru obstaja določena subjektivnost pri presoji teh koristi v prihodnosti. Pravice in licence bi bile prav tako vzdrževane s strani samodejnih plačil, določenih v pogodbah. Časovno zaznamovanje zapisa pravic in patentov bi preprečevalo spore glede lastništva nad pravicami. Merjenje intelektualne lastnine podjetja zaradi subjektivnosti in različnih pristopov omogoča določena odstopanja, kar igra pomembno vlogo pri vrednotenju podjetij pri prevzemih in združitvah. Knjigovodska vrednost podjetja se bo še vedno razlikovala od njegove tržne vrednosti. Prikazovanje znanja oziroma intelektualnega premoženja v bilanci stanja podjetja ostaja odprt problem navkljub tehnologiji.
- poslovne terjatve in obveznosti: postavki bi lahko postali predmet pametnih pogodb. Pogodbe s kupci in dobavitelji bi lahko bile programirane na način, da bi se plačila samodejno izvedla, ko bi bili pogoji izpolnjeni. Hkrati bi lahko preverile, ali ima podjetje zadostna sredstva na računu in jih samodejno rezervirala ali prenesla na poseben fiduciarni račun. Uporaba pametnih pogodb bi podjetjem pomagala sodelovati s plačilno sposobnimi podjetji in spodbujala uspešen razvoj zdravih podjetij (zmanjšanje kreditnega tveganja). Vrednost terjatev bi se verjetno znižala, predvsem pa bi se izboljšala struktura terjatev po zapadlosti. Likvidnost podjetij bi se posledično izboljšala, kar bi preko manjših odpisov pozitivno vplivalo tudi na rezultat (dobiček) ter boniteto

podjetja (Deloitte, 2016b). Nedvomnost plačila je zagotovljena in preverljiva zaradi vpogleda v skupno bazo (Carlozo, 2017).

- zaloge: vrednosti zalog bi bile posodobljene na podlagi pametnih pogodb. Primer je samodejna slabitev zalog v realnem času glede na spreminjanje prodajnih cen, stanja zalog (tehnologija v povezavi z Internetom Stvari) in sprememb v stroških proizvodnje. Zaloge bi izkazovale bolj realno vrednost. Prav zaloge so pogosto predmet prilagajanja računovodskih evidenc, saj je njihova vrednost težko določljiva. Tehnologija omogoča spremljanje produkta v dobavni verigi od samega začetka do konca in vzporedno beleži spremembe v vrednosti. Vodenje zalog zato lahko postane bolj učinkovito in s tem tudi upravljanje z obratnim kapitalom. Nespremenljiv in časovno zaznamovan seznam vhodnega materiala in cen omogoča nedvomnost pri uporabi metode FIFO (angl. *first–in–first–out*). Na podlagi točnih podatkov o povpraševanju in dobavi bi podjetja zmanjšala stroške vodenja zalog, izmete in odpise.
- denarna sredstva: v kolikor bi kriptovalute upoštevali kot denar, bi to pri njihovi obstoječi volatilnosti za podjetje predstavljalo visoko tveganje z vidika likvidnosti. Podjetje bi bilo izpostavljeno finančnim izgubam (in dobičkom) iz menjalnih tečajev.
- kapital podjetja: lastništvo in vložki lastnikov bi bili zabeleženi v blockchain sistemu. Prenos pravic bi bil enostaven postopek, ki bi bil viden v realnem času in bi uporabnikom omogočal vpogled v realno kupnino. Število sporov glede lastništev bi se potencialno zmanjšalo. Pogodbe bi lahko eksplicitno določale pravice in dolžnosti lastnikov. Zaradi subjektivnosti pri pripoznanju in uravnavanju določenih sredstev bi tržna vrednost kapitala še vedno odstopala od njegove knjigovodske vrednosti.
- rezervacije: tehnologija omogoča samodejno oblikovanje rezervacij in njihovo sproščanje s pomočjo pametnih pogodb, kar bi zmanjšalo manipuliranje z dobički in posledično povečalo vrednost pobranih davkov za države. Pri rezervacijah je sicer določanje pravil v rokah ljudi, vendar tehnologija omogoča konsistentnost njihovih izvajanj. Slednje onemogoča določanje ekstremnih pravil oziroma pogojev, saj morajo podjetja upoštevati tudi prihodnje poslovanje in potencialno poslabšanje poslovanja. To velja v primeru, ko bi podjetje želelo z višjim oblikovanjem rezervacij uravnavati dobičkonosnost podjetja. Pogoste spremembe pravil bi lahko povzročile signale za notranje in zunanje revizorje, ki bi zahtevali pojasnila.
- dolgovi: finančne in poslovne obveznosti (do dobaviteljev, zaposlenih, države, finančnih institucij in ostalih) so še eno področje, ki bi imelo koristi od pametnih pogodb. Pogodbe posojil in ostalih obveznosti bi se zapisale v sistem in določale pogoje odplačevanja. Poravnavanje glavnic in obresti bi potekalo samodejno.
- amortizacija: kot za ostale podobne razmejevalne postavke tehnologija zagotovi samodejno armotiziranje sredstev ali razmejevanje stroškov in prihodkov ob vnaprej določenih pravilih v pogodbah.
- davki: blockchain računovodstvo bi retroaktivno plačevanje davkov lahko spremenilo v tekoče in transparentno poravnavanje davčnih obveznosti v realnem času. To bi za podjetja pomenilo zmanjšanje stroškov davčne usklajenosti in olajšalo delo računovodij.

Z vidika države bi to lahko bil eden izmed ukrepov za reševanje problemov, povezanih z izogibanjem plačilu davkov, nelegalnim poslovanjem, sivo ekonomijo in podobnimi problemi (Ernst & Young, 2016, str. 9).

- izvenbilančna evidenca: prav tako bi izvebilančna evidenca lahko postala bolj transparentna, saj so te transakcije prav tako vidne v blockchain sistemih (seznamu transakcij in pogojev).

Medtem ko tehnologija lahko občutno spremeni in izboljša spremljanje denarnih postavk, so druge postavke, ki so odvisne od človeških odločitev (vrednotenje, metode spremljanja zalog, upoštevanje ključev za obračunavanje proizvajalnih stroškov, ugotavljanje prihodnih koristi, določanje amortizacijskih stopenj itd.), še vedno v določeni meri odporne proti vplivu tehnologije. Pri nedenarnih postavkah ima tehnologija lahko pomemben vpliv, predvsem v obliki pametnih pogodb, vendar ostaja vpliv človeškega faktorja pri oblikovanju pogojev in pravil pogodb. Najmanj lahko tehnologija prispeva k zanesljivosti izmere poštenih vrednosti sredstev (opredmetena, finančne naložbe, kapital itd.). Tehnologija je odlična za podkrepitev merjenja vrednosti sredstev po izvirnih vrednostih, saj omogoča nedvomno in natančno knjiženje sredstev na podlagi izdanih računov in vrednosti transakcij. Dilema ostaja pri vrednotenju po pošteni vrednosti. Poštena vrednost je znesek, za katerega je mogoče izmenjati sredstvo ali poravnati obveznost med dvema neodvisnima, enakopravnima in dobro obveščenima strankama. Poštena vrednost sredstva predstavlja njegovo tržno vrednost, ki jo ugotavljajo pooblaščeni cenilci na podlagi mednarodnih standardov ocenjevanja vrednosti. Ocenjevanje tržne vrednosti zato tudi v primeru blockchain računovodskega sistema ostaja v človeških rokah. Vsaj dokler se ne oblikujejo blockchain sistemi, ki bodo evidentirali tržne podatke o izmenjavi sredstev (na primer nepremičnin) in, v realnem času, analizirali tržno vrednost. Če bi bili ti sistemi povezani z računovodskim, bi se vrednost sredstev lahko spreminjala vzporedno. Verjetnost takšnega ekosistema je, zaradi kompleksnosti, nizka, vsaj na srednji ali celo dolgi rok. Problem je največji pri modelih vrednotenja z uporabo lastnih ocen (na primer pri upoštevanju diskontnih stopenj). Kljub temu gre razvoj v zadnjih letih v smeri merjenja vrednosti sredstev po tržnih vrednostih, predvsem tam, kjer je to izvedljivo. V sklopu uravnavanja vrednosti sredstev je potrebno poudariti, da slabitev naložb temelji na nastanku škodnega dogodka. Tehnologija v trenutni fazi ne ponuja alternativne možnosti, vendar ima potencial, da oblikuje zanesljivejše in natančnejše napovedovalne modele, kar bi lahko odpravilo retroaktivno slabljenje naložb. Sposobnost in verjetnost nastanka tovrstnih modelov ostaja trenutno velika neznanka in le ideja, uspešnost katere je odvisna od mnogih dejavnikov.

Po drugi strani blockchain sistemi omogočajo boljše pogoje za ustvarjanje delujočih trgov. Njihova globalnost omogoča vključitev večjega števila istovrstnih sredstev in učinkovito povezuje kupce in prodajalce. Prav tako omogoča javno dostopne informacije glede cen, predvsem v javnih sistemih (v privatnih odvisno od nivoja dovoljenj). Vzpostavi pogoj za lažje mednarodno trgovanje, kar poveča število in pogostost transakcij ter razvitost trgov.

Omogoča tudi enostaven pregled nad zgodovinskimi transakcijami za namen primerjave cen. Podjetja lažje dostopajo do svetovnih trgov in bolj neposredno (brez posrednikov in drugih ovir), kar je pomemben pogoj pri ugotavljanju poštenih vrednosti. Glede na to, da tehnologija ponuja popolno revizorsko sled, lahko sicer ublaži prevelika odstopanja ali manipulacije, vendar jih po mojem mnenju ne more v celoti odpraviti. Za to bi bil potreben popoln ekosistem različnih medsebojno povezanih sistemov sredstev in natančno definirani in usklajeni mednarodni računovodski standardi poročanja.

Računovodska poročila niso dovolj za prikaz poštene in resnične vrednosti podjetij. Potrebno je upoštevati dodatne informacije (ocene in analize managerjev, poročila o družbeni odgovornosti, zunanje tržne dejavnike in podobno). Tehnologija ima manjši vpliv na razkrivanje ostalih kvalitativnih, neračunovodskih, informacij.

Pri vrednotenju podjetij tehnologija lahko pripomore k razpolaganju z bolj popolnimi in celovitimi podatki, vendar so modeli vrednotenja podjetij še vedno rezultat predpostavk, ki so določene s strani človeka (predvsem pri donosnostnih načinih). Tržni načini vrednotenja lahko postanejo bolj zanesljivi in primerljivi v primeru, da podjetja uporabljajo in delujejo znotraj enega sistema in pod enakimi standardi. Tehnologija podatkovnih verig zaradi lažje dosegljivosti podatkov izboljša kakovost tega načina.

Kriptovalute izpostavljajo določene težave v povezavi z obstoječimi računovodskimi standardi. Raiborn in Sivitanides (2015) težave ločita na pet ključnih področij:

- klasificiranje sredstva: kriptovaluta ustreza definiciji sredstva, ker potencialno prinaša ekonomsko korist za osebo in izhaja iz pretekle transakcije (Financial Accounting Standards Board, 1985). Problem nastane pri podrobnejši definiciji. Je kriptovaluta denar, denarni ustreznik, neopredmeteno sredstvo ali naložbeno sredstvo? Ker kriptovalute ne zadovoljujejo vseh treh osnovnih lastnosti denarja, jih ni mogoče smatrati kot denar (Kieso, Weygandt, & Warfield, 2013). Prav tako ne veljajo kot denarni ustrezniki, ker niso visoko likvidni. Kljub temu, da so lahko denominirani v fiat valutah, jih ni mogoče deponirati v banki ali drugi varčevalni instituciji. Ena izmed omejitev je tudi visoka volatilnost vrednosti, izražena v realni valuti. Kljub temu, da nimajo fizične oblike, definicija neopredmetenih sredstev izključuje finančne instrumente. Kriptovalute še vedno veljajo za medij finančne izmenjave. Najbolj smiselna klasifikacija je torej finančna naložba. IRS (angl. *Internal Revenue Service*) je leta 2014 izdal prve smernice na temo kriptovalut. Opozarja, da prodaja, izmenjava ali uporaba konvertibilnih kriptovalut kot plačilo za blago ali storitev v ekonomskih transakcijah nosi davčne posledice, ki se izkazujejo v davčnih obveznostih. Ker kriptovalute niso zakonito plačilno sredstvo, jih IRS ne obravnava kot valuta, temveč kot premoženje. Generalni davčni principi premoženja zato veljajo tudi za kriptovalute. Davčni plačnik, ki prejme kriptovalute kot plačilo za blago ali storitve, jih mora pripoznati po pošteni tržni

vrednosti na datum prejema. Ker se uradno ne smatrajo kot valute, ne generirajo dobičkov ali izgub iz menjalnih tečajev (Nevious, 2014).

- knjiženje: nakup kriptovalute bi povečal debet finančne naložbe in zmanjšal kredit sredstva, ki je bil dan za izmenjavo (najverjetneje denar) oziroma bi se pred tem povečal kredit na strani obveznosti. Visoka volatilnost vrednosti izpostavlja tudi vprašanje knjiženja prihodkov, v kolikor je cena produkta ali storitve izražena v kriptovaluti. Je višina prihodkov vezana na ceno, izraženo v realni valuti (število bitcoinov se spreminja) ali na vrednost, ki jo določeno število bitcoinov nosi v trenutku prodaje (število bitcoinov se ne spreminja). Še večji problem se pojavi, če so kriptovalute pridobljene skozi dejavnost rudarjenja (debet oziroma povečanje finančnih naložb). V normalnih okoliščinah podjetja namreč ne ustvarjajo finančnih sredstev skozi interne aktivnosti. Pri fizični osebi bi se lahko investicija v čas in delo smatrala kot vložek lastnika na strani kapitala (protipostavka: kredit kapitala). V primeru podjetja in več kot enega lastnika tovrstna protipostavka ni primerna. Lahko bi sicer podjetje izdalo delnice nekomu, ki je investiral osebni kapital v generiranje enote kriptovalute, v obliki navadne ali prednostne delnice. Druga, enostavnejša, možnost bi bila, da bi tej osebi podjetje plačalo v denarju (protipostavka: kredit denar). Dilema se pojavi, če je ta oseba zaposlena znotraj podjetja. Zaposleni namreč ne morejo generirati prihodkov v lastnem imenu ali ustvariti lastniške investicije znotraj podjetja. Rešitev je, da se kriptovalute obravnava kot produkt, ki je razvit znotraj podjetja in je lahko prodan. Podobno kot zaloga ali programska oprema v primeru storitvenega programskega podjetja. Ker so zaloge praviloma sredstva v opredmeteni obliki, so usredstveni stroški razvijanja primernejša možnost. Stroški generiranja kriptovalut so usredstveni stroški razvijanja, dokler niso enote ustvarjene in pripravljene za prodajo. Vsi stroški, ki so povezani s proizvodnjo enote kriptovalute, bi torej morali biti usredstveni ter enačeni z višino ustvarjenih prihodkov. Če bi bili uporabljeni za plačilo ali nakup drugega blaga, bi morali biti odpisani v višini realiziranega dobička ali izgube pri transakciji. Kriptovalute, ki so namenjene plačilu zaposlenih ali zunanjih partnerjev, so prav tako predmet obdavčenja (Nevious, 2014). Ena izmed rešitev je tudi standardno knjiženje stroškov rudarjenja ob nastanku skozi izkaz poslovnega izida. Ko bi bila enota kriptovalute generirana, bi se prepoznala kot sredstvo in nerealiziran dobiček v izkazu vseobsegajočega donosa. Pridobitev enote bi bila lahko smatrana kot nedokončan proces. Vrednost se bi pripoznala šele ob uporabi kriptovalute za poslovne potrebe. Sredstvo in nerealiziran dobiček bi se zmanjšala oziroma izničila in dejanski realiziran dobiček/izguba bi se pripoznala skozi izkaz poslovnega izida. V končni fazi bi se torej povečala ali zmanjšala vrednost kapitala skozi dobičke ali izgube.
- držanje sredstva: tako kot druge naložbe tudi vrednost kriptovalut narašča in pada medtem, ko jih podjetje drži v knjigah. Zaradi visoke volatilnosti so kriptovalute veliko bolj špekulativne narave. Možnosti za varovanje pred tveganji so redke in nerazvite. Podjetja, ki sprejemajo kriptovalute kot sredstvo plačila, praviloma kriptovalute takoj menjajo za lokalne valute, da se izognejo tveganju izgube vrednosti. Nekatera podjetja v

sredstvih držijo kriptovalute kot naložbeno sredstvo in je zato velika verjetnost, da bodo na datum poročanja prikazana med finančnimi naložbami. Podjetja morajo te naložbe prikazovati po pošteni vrednosti, kar povzroča nerealizirane dobičke ali izgube. Vprašanje se pojavi, ali se te naložbe upoštevajo po enakih pravilih kot naložbe, namenjene za trgovanje (pripoznanje sprememb vrednosti skozi izkaz poslovnega izida), in ali so spremembe prikazane v kapitalu in izkazu vseobsegajočega donosa (naložbe proste za prodajo). Podjetja, ki uporabljajo kriptovalute za poslovne aktivnosti (prodaja, nabava), izkazujejo namero za njihovo uporabo v kratkoročnem obdobju. V tem primeru veljajo enaka pravila kot pri naložbah za trgovanje. Dobiček obdobja bi bil v primeru večje količine posedovanih kriptovalut lahko zelo izkrivljen, zaradi potencialnih fluktuacij na dan poročanja. Kot primer, vrednost bitcoina je bila 4. decembra 2013 1.117 $ in je nato do 7. decembra 2013 padla na 723 $. Če bi podjetje v tem obdobju imelo v lasti 1.000 bitcoinov, bi to pomenilo 394.000 $ izgube v izkazu poslovnega izida.

- menjalni posel: ko je nedenarno sredstvo izmenjano za drugo sredstvo, mora biti novo sredstvo pripoznano po vrednosti danega ali prejeta sredstva. Pri menjavi kriptovalute se pojavi vprašanje, ali vrednost danega sredstva na dan menjave predstavlja najprimernejšo vrednost, po kateri se bo knjižila transakcija. Vprašanje je posledica omenjene visoke fluktuacije valute. Prejemnik bo zato želel dodatne enote, da kompenzira potencialne izgube. V tem primeru bi bilo primerno, da se novo sredstvo pripozna po vrednosti prejetega sredstva in se razliko od danega sredstva pripozna kot dobiček ali izgubo.
- združitve in prevzemi (v nadaljevanju M&A): podobno vprašanja se navezuje tudi na proces združitve in prevzemov podjetij. Pozitivne strani uporabe kriptovlut pri M&A transakcijah so skoraj takojšnja izvedba transakcije, odprava bančnih in ostalih posredniških provizij in odprava stroškov menjave valut pri mednarodnih poslih. Na negativni strani glavno tveganje izhaja iz negotove vrednosti kriptovalut, predvsem pri menjavi v fiat valute. Drugo tveganje se pojavi s pomanjkanjem regulatornega nadzora in pravnih možnosti pri goljufivih transakcijah (Josselyn, 2014). M&A dogovori bi, zaradi zaščite kupcev in prodajalcev, najverjetneje morali določati minimalno in maksimalno nakupno vrednost, izraženo v fiat valuti. Volatilnost bi imela tudi kompleksne posledice na vrednotenje podjetja. Spreminjajoča vrednost sredstev in posledično kapitala bi lahko vplivala na višino cene nakupa in dobrega imena (Yermack, 2017). Analitiki trgov bi sicer imeli večji izziv pri vrednotenju podjetij, vendar bi na drugi strani imeli na voljo veliko več podatkov.

Ugovšek (2017) ob pomoči državnega finančnega urada ugotavlja, da fizična oseba v Sloveniji ne plača dohodnine ali katerega drugega davka iz prodaje kriptovalut. Podlaga je 32. člen ZDoh-2 (Ur.l. RS, št. 13/2011-UPB7, 63/2016, v nadaljevanju ZDoh-2). Nasprotno pa je dohodek, ustvarjen pri rudarjenju, obdavčen po enakih principih kot drugi dohodek po 105. členu ZDoh-2. Vrednost dohodka je enaka vrednosti kriptovalute, izražene v evrih na dan prejema dohodka. Finančni urad Republike Slovenije odmeri 25 % akontacijo davka.

Posameznik ob letnem poračunu zaslužkov doplača ali dobi povrnjene davke. Trgovanje torej ni obdavčeno, medtem ko dohodek iz opravljanja dejavnosti je. Slednje velja, kadar so kriptovalute namenjene nadaljnji prodaji in so hkrati izpolnjeni pogoji trajnosti, neodvisnosti in samostojnosti. Če podjetje prejme kriptovalute kot plačilo za opravljeno storitev ali prodano blago, se obdavči kot dohodek, prejet v naravi ter z upoštevanjem vrednosti na dan, ko je bil dohodek prejet.

3.5 Vpliv na vlogo računovodij in revizorjev

Vloga revizorjev in računovodij bo z vidika stroke v najboljšem primeru spremenjena in v najslabšem, po mnenju nekaterih, popolnoma odstranjena. Kot je predstavljeno v nadaljevanju, je verjetnost, da pride do pesimističnega scenarija, izredno majhna, če ne ničelna. Avstralija je v svojem letnem poročilu Australian Industry Report (Australian Government, 2014) med drugimi označila poklice knjigovodij, računovodij in revizorjev kot poklice, ki bodo z veliko verjetnostjo v prihodnosti avtomatizirani. PriceWaterhouse Coopers (2015) je v svoji študiji leto pozneje prišel do podobnih zaključkov. Splošni razvoj tehnologije je v zadnjih desetletjih prinesel digitalno obliko poslovanja namesto papirnate, samodejno vnašanje podatkov, opravljanje storitev na daljavo in ostale spremembe. To je računovodjem omogočilo, da svoje delo opravljajo hitreje in bolj učinkovito, zmanjšale pa so se tudi možnosti za napake (Ovenden, 2017). Wunsche (2016) je mnenja, da bo tehnologija podatkovnih verig imela pomemben vpliv na vodenje evidenc, poročanja in druge prakse v panogi. Oblika storitev bo doživela velike spremembe.

3.5.1 Računovodje

Po besedah Association of Chartered Certified Accountants (2016) se bo stroka pomembno spremenila do leta 2025. V svoji raziskavi med managerji, finančnimi in računovodskimi strokovnjaki ugotavljajo, da bodo pri tem ključni naslednji faktorji: regulacija in vodenje (večji nadzor), digitalna tehnologija (transformacija dela), pričakovanja (nove kompetence in znanja), globalizacija (nove prakse in poslovni modeli) in zunanji dejavniki. Med zunanjimi dejavniki, ki bodo po njihovih pričakovanjih imeli največji vpliv v naslednjih treh do desetih let, so anketiranci izbrali: razvoj inteligentnih avtomatiziranih računovodskih sistemov (blockchain), stopnja in volatilnost ekonomskih sprememb, harmonizacija računovodskih in poslovnih standardov ter poslovanje v oblaku.

Trenutna vloga računovodij je, da opravljajo naloge, povezane s knjigovodstvom, računovodskim predračunavanjem, računovodskim nadziranjem in analiziranjem. Postati računovodja ni edina možnost, ki jo ima računovodski strokovnjak na voljo. Z računovodskim znanjem lahko opravlja tudi poklic revizorja, poslovnega, računovodskega in davčnega svetovalca in druge strokovne poklice, ki temeljijo na pripravljanju in uporabi

računovodskih informacij (Zaman Groff, Hočevar, & Igličar, 2007). Delo računovodij je torej tesno povezano s procesiranjem in kontrolo transakcij ter usklajevanjem zapisov.

Raziskava, ki jo je izvedla Association of Chartered Certified Accountants (2016), je pokazala, da mnogi računovodje menijo, da jim primanjkuje relevantnih sposobnosti, s katerimi bi se soočili z novimi okvirji, principi, tehnikami, standardi in tehnologijami, ki bodo spremenile njihovo delo. Predvsem izpostavljajo pomanjkanje tehnoloških znanj, kot so apliciranje programske opreme za namene analiz, interpretacijo in prezentacijo finančnih in nefinančnih podatkov. Opozorili so tudi na pomanjkanje znanja finančne matematike, ki je po njihovem mnenju potrebno za apliciranje kompleksnih mednarodnih računovodskih standardov.

Kot omenjeno, tehnologija podatkovnih verig odpravlja pomen posrednikov in podpornih služb, med katere štejemo tudi računovodstvo (Lee, 2016). Računovodska panoga neprestano aktivno deluje v smeri standardizacije, pridobitve zaupanja in zagotovitve skladnosti. To so namreč največje težave, s katerimi se panoga sooča že od samega začetka obstoja. Blockchain ponuja rešitev za vse tri probleme (Westra, 2016).

Nova vloga računovodje se bo oddaljila od knjigovodje in drugih aktivnosti z nizko dodano vrednostjo (funkcije, ki zahtevajo veliko ročnega dela, na primer vnos in preverjanje transakcij) ter se bo najverjetneje približala poslovnemu svetovalcu. Spretnosti pri delu z ljudmi bodo postale prav tako pomembne kot preverjanje številk (Sheedy, 2017). Podjetja bodo od računovodij pričakovala, da jim svetujejo in predlagajo najboljše prakse za zmanjševanje stroškov (Lee, 2016). Prva pomembna funkcija bo vpeljava novega računovodskega sistema v podjetje. To bo od njih zahtevalo razumevanje tehnologije (Westra, 2016). Naslednja funkcija bo pripravljanje izkazov in interpretacija podatkov. Obvladovanje poslovne inteligence in podatkovno-analitskih tehnologij bo bistvena kompetenčna prednost pri interpretaciji in zaznavanju tveganj v podjetjih in dobavnih verigah. V povezavi s tveganjem in njihovo svetovalno vlogo lahko pomembno prispevajo tudi k omejevanju teh tveganj. Tretja pomembna svetovalna funkcija bo davčno svetovanje. Področje davčne zakonodaje bo prav tako doživelo pomembne spremembe (Association of Chartered Certified Accountants, 2016). Priložnosti je torej dovolj. Izkoristili jih bodo tisti, ki bodo razumeli nove tehnologije, poslovne modele in bodo sledili spremembam v regulativah. Na Sliki 21 so predstavljene nekatere funkcije, ki jih računovodja lahko prevzame v novem delovnem okolju.

Slika 21: Primeri novih funkcij računovodij v blockchain okolju

	Področje vloge	Opis funkcije	Potencial za neposredne koristi iz blockchain tehnologije
1	Poslovodno računovodstvo	Priprava in uporaba finančnih in nefinančnih podatkov	√√
2	Finančno-poslovno partnerstvo	Podpora divizijam ali poslovnih enotam za doseganje rezultatov	√
3	Skladnost s predpisi	Implementacija predpisov in spoštovanje predpisov, ki se nanašajo na aktivnosti podjetja	√√√
4	Strategija in uspešnost	Sooblikovanje strategije in vodenje uspešnosti za doseganje strategije	√

Vir: N. Vaidyanathan, Divided we fall, distributed we stand, 2017.

Vpliv na prihodke računovodskih podjetij ne bo viden takoj in v pomembnem skoku. Struktura prihodkov se bo spremenila postopoma. Nekatere storitve ne bodo več potrebne, druge bodo avtomatizirane in bodo prinašale manj prihodkov. Nove storitve bodo postale nov vir prihodkov. Premik od nizko profitabilnih aktivnosti k višje profitabilnim aktivnostim potencialno predstavlja priložnost za višje dobičke. Računovodstva bodo namesto za čas (vhodni model) plačana za strokovno znanje in svetovanje (izhodni model). Sprememba v modelu je odvisna od zmožnosti tehnologije, da doseže masovno sprejetje. Če se to uresniči, bodo računovodska podjetja morala prilagoditi strukturo in organizacijo dela (Vaidyanathan, 2017, str. 6).

V realnosti obstaja torej nizka verjetnost, da bi poklic računovodje bil popolnoma izpodrinjen. Še posebej to velja na srednji ali celo daljši rok (10 let). Potreba po strokovnem znanju računovodij bo ostala na dolgi rok. Tehnične kompetence bodo najverjetneje postale bolj pomembne in cenjene. Od računovodij bo to zahtevalo fleksibilnost in nadgradnjo znanja na novih področjih, ki jih bo prinesla ta tehnologija in tudi druge tehnologije (Association of Chartered Certified Accountants, 2016). Računovodska podjetja, ki bodo sledila razvoju tehnologije, bodo bolje pripravljena na spremembe in bodo uspešneje obdržala stranke in tržne deleže (Vaidyanathan, 2017).

3.5.2 Revizorji

Revizija je dejavnik omogočanja rasti. Podpira tržno zaupanje, zmanjša stroške kapitala in transakcij, povečuje pretakanje kapitala in služi kot temelj za delovanje poslovnega okolja. Visoki standardi revizije pomembno prispevajo k doseganju trajne ekonomske rasti držav. V revizorskem poslu obstaja velika neusklajenost med zahtevami trga in investitorjev, željami podjetij glede razkritij ter zahtevami regulatorjev (Association of Chartered Certified Accountants & Grand Thornton, 2016).

Revidiranje je proces izvajanja neodvisnega pregledovanja računov, knjig in dokumentov organizacije, z namenom ugotoviti, ali finančni izkazi predstavljajo pošten prikaz

poslovanja. Revizorji so neodvisne, zaupanja vredne, tretje osebe, ki izvajajo ta proces na podlagi vnaprej določenih smernic, ki jih postavljajo računovodski standardi (Huber, 2016). Svoje ugotovitve predstavijo v revizorskem poročilu. Njihovo mnenje nosi veliko odgovornost, saj služi za vzpostavljanje zaupanja zunanjih deležnikov v poslovanje podjetja (kupci, dobavitelji, investitorji, banke itd.). Odločitev investitorja temelji na sprejemljivosti rezultatov podjetja in mnenju revizorja, ki investitorju zagotovi, da je bil opravljen skrben pregled in da rezultati predstavljajo resnično sliko podjetja. Moralno delovanje revizorjev je zato bistvenega pomena, saj ščitijo interese zunanjih strank (Lazanis, 2015).

V povezavi z neodvisnostjo se pojavi tveganje pristranskosti ali tako imenovani problem agenta. Podjetje, v katerem revizor opravlja pregled, je namreč hkrati tudi plačnik revizorskih storitev. Denarna povezava med revizorjem in klientom pomeni, da obstaja nevarnost, da revizor izda pristransko mnenje glede točnosti izkazov. Najbolj pogost razlog je zagotavljanje posla za naslednje poslovno obdobje. To velja predvsem za tiste kliente, ki predstavljajo pomemben vir prihodkov za revizorsko podjetje. Tveganje se stopnjuje z velikostjo klientov, katerih uspeh temelji na ugledu (Lazanis, 2015). Velike posledice na koncu lahko nosijo notranji (na primer zaposleni) in zunanji upniki podjetja (na primer banke, dobavitelji itd.). Sarbanes-Oxleyjev zakon, sprejet v letu 2002, je sicer uvedel nekatere ukrepe za zmanjšanje tveganj (pravila glede shranjevanja dokumentov, vzpostavitev internih kontrol, metod poročanja in revizijskih komisij, kazenska odgovornost najvišjih vodij itd.), vendar njihova popolna odprava ni mogoča. Podjetja še vedno plačujejo revizorjem za njihove storitve. Revizorji kljub komitejem še vedno delujejo precej neodvisno na dnevni bazi. Zaradi stroškovnih pritiskov podjetja manj izkušenim revizorjem dodeljujejo naloge, ki bi sicer bile bolj primerne za senior revizorje (Frieswick, 2003).

Trenutni model revizorskega podjetja: Prihodki iz revidiranja so povezani s številom ur, potrebnih za skrben pregled. Urne postavke odražajo kompleksnost revizije, izkušnje ter znanje revizorja. Razlog za tak model je razvidna količina ur dela, ki temelji na dobro definiranem sklopu nalog. Definirane vhodne aktivnosti so oblikovane z namenom vzpostavljanja zaupanja v produkt (mnenje oziroma poročilo). Namen modela je zmanjšati tveganja pred neznankami. Stroga pravila definirajo proces in delujejo kot mehanizem za pregled vseh področjih ter zmanjšanja količine neznank (Vaidyanathan, 2017).

Tehnologija podatkovnih verig v tem smislu lahko nastopi kot ukrep za ublažitev teh tveganj. S svojimi lastnostmi poustvarja vlogo revizorja, torej zagotovi razumnost in točnost finančnih izkazov podjetja in potencialno odpravlja problem agenta (Byström, 2016). Potencialno podjetja ne bi potrebovala revizorjev, saj je integriteta transakcij že zagotovljena s strani samega sistema. S pomočjo pametnih pogodb bi lahko samodejno poskrbeli za skladnost podatkov in izvajanje revizorskih aktivnosti (Karajovic, Narula, Pandya, Patel, & Warring, 2017). Preprečuje tudi manipuliranje vodstva s finančnimi izkazi in zmanjšuje

prostor za napake, predvsem pri bolj kompleksnih transakcijah (Ovenden, 2017). Ob tem se pojavi vprašanje, ali smo sposobni in pripravljeni zaupati tehnologiji namesto ljudem.

Podobne učinke kot v računovodskem poklicu bodo čutili tudi revizorji. Standardizacija procesa pomeni, da bodo porabili manj časa za potrjevanje podatkov in se zaradi tega osredotočili na upravljanje zahtevnejših aktivnosti, kot so ocenjevanje dvomljivih ali neetičnih transakcij (Karajovic, Narula, Pandya, Patel, & Warring, 2017). Deloitte ne verjame, da bodo njihove storitve nadomeščene ali izkoreninjene, temveč bodo postale bolj efektivne. Podobno kot velja za računovodje, veliko priložnost vidijo v svetovalnih storitvah na tem področju (Rizzo, 2015). Revizorji se bodo na podlagi ažurnih podatkov lahko usmerili v uporabo podatkov za prihodnost, namesto da bodo pregledovali historične podatke. S tem bodo ustvarili višjo dodano vrednost (Carlozo, 2017). Med drugim bi lahko skrbeli za pravilno delovanje sistemov, vzpostavljanje internih nadzornih mehanizmov in razumevanje zapletenih poslovnih modelov. Predvsem zadnje postaja pomembna lastnost dobrih revizorjev, zaradi zahtev po razširjenih revizorskih poročilih s poudarkom na nefinančnih informacijah (Vaidyanathan, 2017). Sodelujejo lahko pri pripravi novih mednarodnih računovodskih standardov poročanja in podjetjem pomagajo pri razumevanju in razvoju tehnologije ter postopnem prehodu na nove oblike sistemov. Druge svetovalne funkcije se nanašajo na prepoznavanje in ocenjevanje tveganj ter iskanje rešitev (Baron, 2017). Funkcija revizorja bi se lahko pomaknila navzgor po vrednostni verigi in bi vključevala upravljanje in usklajevanje različnih tipov verig in sistemov (Martindale, 2016).

Ugotovimo, da bosta obe vlogi (računovodje in revizorji) doživljali podobne spremembe in se usmerjali k svetovalnim aktivnostim. Obstaja verjetnost, da meje med obema poklicema postanejo manj jasne in pride do združevanja nekaterih aktivnosti.

Revidiranja poštene vrednosti in mednarodnih skupin se smatrata kot največja izziva sodobne revizije. Raziskava ugotavlja, da revizorska podjetja širijo uporabo tehnologije na področju analitike. Konkurenca na tem področju so vsa podjetja, katerih poslovni model temelji na uporabi orodij za analiziranje velike količine podatkov. Do leta 2025 bi Google lahko zaposloval več strokovnjakov s področja revizije kot velika štiri revizroska podjetja (Association of Chartered Certified Accountants, 2016). Nedvomno bodo prednost imela tista podjetja, ki že razvijajo programsko opremo in sisteme za revidiranje na podlagi nove tehnologije (Sheedy, 2017). Po predvidevanjih Association of Chartered Certified Accountants in Ernst & Young (2017) bo revizija leta 2030 povsem drugačna storitev kot danes. Revizorska podjetja bodo zaposlovala več znanstvenikov, informatikov in matematikov, z namenom razvoja tehnologije in izboljšanja kvalitete storitev.

Revizorski model prihodnosti: Če lahko tehnologija ponudi dokončen vpogled v celotno bazo namesto izbranega vzorca, potem obstaja verjetnost zmanjšanja tveganja nepoznavanja in prikrivanja podatkov. Revizorska podjetja se bodo usmerjala na področja, ki zahtevajo

človeško presojo, umestitev številk v poslovni kontekst in razumevanje končnih izvlečkov iz blockchain glavne knjige. Revizorji bi kljub temu še vedno lahko preverjali resničnost in poštenost končnega izdelka (finančni izkazi). Tak model ne bi bil več povezan z vhodnimi aktivnostmi in bi bolj temeljil na rezultatih (produktih tehnologije). Enako velja za model računovodstva. Primeri storitev revizorskega podjetja so: mnenje o računovodskih usmeritvah, revizijski pogled na materialnost težko določljivih sredstev, vplivih na združitve in prevzeme, forenzično revidiranje itd. (Vaidyanathan, 2017).

3.6 Prednosti uporabe tehnologije podatkovnih verig v računovodstvu

Poleg tega, da tehnologija odpravi, v poglavju omenjene, trenutne probleme računovodstva, nudi tudi druge prednosti in priložnosti.

Določeni podatki v poslovnih knjigah lahko postanejo popolnoma ažurni, resnični in celoviti (Bradbury, 2015). Z vidika ključnih deležnikov (na primer investitorjev) to pomeni lažje in učinkovitejše analiziranje, odločanje ter modeliranje kreditnih tveganj (Byström, 2016). Hkrati so zadovoljene arhivske zahteve, saj baza vsebuje celotno zgodovino podatkov, in zmanjšane potrebe po papirnatih oblikah arhiva.

Blockchain računovodstvo vzpostavlja integriteto finančnih izkazov. Manipulacija izkazov je zaradi kriptografije in distribuirane narave poslovnih knjig močno otežena. Ob enem je transparentnost, ena ključnih sestavin integritete podatkov, povečana (Karajovic, Narula, Pandya, Patel, & Warring, 2017). Koristi bi čutila tako velika kot srednja in mala podjetja. Slednja bi lažje dokazovala ekonomske aktivnosti podjetja zunanjim strankam, kot so banke, kupci in dobavitelji (Tyra, 2014). Velika podjetja zaradi svoje prepoznavnosti in velikosti običajno nimajo tovrstnih problemov.

Računovodstvo na podlagi tehnologije lahko pomembno prispeva k zmanjšanju davčnih goljufij. Evropska komisija ocenjuje, da je iz naslova davčnih goljufij in utaj na letni ravni v Evropski uniji izgubljenih do 1 bilijona evrov (Evropska komisija, 2017).

Tehnologija podatkovnih verig z določeno mero avtomatizacije odstrani predvsem aktivnosti in storitve z nizko dodano vrednostjo in namesto tega poveča osredotočenost na storitve z višjo dodano vrednostjo (Rae, 2017). Hkrati obljublja občutno znižanje potrebnega časa in stroškov za opravljanje računovodskih in revizijskih aktivnosti ter zagotavljanje skladnosti. V tem smislu bi prišlo do svojevrstne oblike transformacije računovodske in revizorske panoge, ki bi lahko pomagala pri povečanju ugleda in relevantnosti panoge.

3.7 Izzivi uporabe tehnologije podatkovnih verig v računovodstvu

Digitalizacija računovodskega sistema je še vedno v začetni fazi, v primerjavi z ostalimi industrijami. Eden izmed razlogov je v visokih regulatornih zahtevah glede veljavnosti in celovitosti. Še bolj izrazito pomembno je to za dejavnost računovodstva, ki je sestavni del poslovanja vsakega podjetja iz različnih industrij in predstavlja temelj delovanja finančnih trgov. Stroka in ponudniki računovodskih in revizorskih storitev morajo zato razumeti vpliv in delovanje tehnologije v vseh panogah. To predstavlja velik izziv, razsežnost katerega je nepoznana zaradi zgodnje faze razvoja tehnologije. Dejavnost računovodstva vstopa v novo obdobje negotovosti, ki se navezuje na temelje njenega delovanja. Trgi bodo potrebovali nove standarde, inovativne, tako kot bo inovativna sama tehnologija (Simon, 2016).

Izpostaviti je potrebno tudi izziv, ki se nanaša na kompromis med zaščito privatnosti podatkov in transparentnostjo. Popolna odprtost podatkov je zaradi varovanja poslovnih skrivnosti in kompetenčnih prednosti podjetij nesprejemljiva. Dostop in vpogled v podatke bi zato morala biti primerno prilagojena glede na različne vrste deležnikov (Bradbury, 2015). Logična rešitev so privatni sistemi, ki na drugi strani nosijo druge slabosti. Ne glede na obliko je zaradi visoke občutljivosti podatkov potrebno zagotoviti varnost pred kibernetskimi napadi. Ta nevarnost je sicer manjša kot pri obstoječih centraliziranih sistemih, vendar to ne pomeni, da ne obstaja.

Glede na to, da je eden izmed ključnih problemov ogromna količina podatkov, ki v vedno bolj povezanem svetu narašča, je potrebno razmisliti, kateri sistemi potrjevanja transakcij bi bili sposobni zagotoviti obravnavanje take količine podatkov (Brown, 2015). Računovodski sistemi zahtevajo varen mehanizem (kot je Proof-of-Work), ki pa ima na drugi strani pomembne omejitve (visoki stroški, kapacitete). Potrebno je najti ustrezen kompromis ali počakati na razvoj novih, boljših mehanizmov.

Prehodi iz obstoječih računovodskih sistemov na nove bodo nedvomno povzročili integracijske in migracijske izzive (Wunsche, 2016). Ti morajo biti storjeni postopno in z visoko mero skrbnosti. Izziv ekosistemov medsebojno povezanih posameznih privatnih (računovodskih) sistemov je tudi nadzor in upravljanje teh sistemov na način, da zagotavlja delovanje posameznikov v interesu celotne skupnosti (Vaidyanathan, 2017).

Tveganja izvenbilančnih dogovorov, nepravilnih vrednotenj in prikritih notranjih delovanj bi, navkljub tehnologiji, ostala možna, predvsem v začetni fazi. Nova regulativna pravila bi morala biti sprejeta za upravljanje teh tveganj. V primeru nepravilnih vrednotenj bi sistem lahko povezali z blockchain sistemom, namen katerega bi bil ocenjevati pošteno tržno vrednost sredstev na podlagi znanih podatkov (Tyra, 2014).

Z vidika tveganj bo bistven razvoj smernic in regulative, skladnosti in postopkov (Association of Chartered Certified Accountants, 2016). Obstoječi standardi niso ustvarjeni za spremembe, ki jih obeta tehnologija. FASB in IASB sta se že leta 2002 zavezali k skupnemu razvoju in harmonizaciji računovodskih standardov in pravil (Barker, 2003). Kljub temu danes še vedno vsaj 110 držav uporablja različne standarde (GAAP, IFRS ali nacionalne). Vrednotenje podjetij in njihova medsebojna primerjava je zato še vedno velik izziv za investitorje. Dodatno kompleksnost predstavlja različna vpeljava standardov med državami (Sherman & Young, 2016). Zaradi kompleksnosti kriptovalut in tehnologije podatkovnih verig so pravila po teh razkritjih nedoločena in nejasna. Poleg tega je število uporabnikov, ki imajo zadostno znanje za razumevanje delovanja kriptovalut in tehnologije, nizko. Vodstva podjetij lahko to izkoristijo za dodatno manipuliranje podatkov. Iz te perspektive je potrebno postaviti natančne in jasne smernice poročanja. Ko narašča število kriptovalut in transakcij, narašča tudi potreba po podrobnih računovodskih smernicah in pravilih poročanja in razkrivanja informacij (Raiborn & Sivitanides, 2015). Na začetku bodo najverjetneje oblikovani osnovni principi, kar bo regulatorjem omogočilo večjo svobodo pri obravnavanju posameznih primerov. Sčasoma bodo ti principi na podlagi praktičnih primerov postali bolj specifični in podobni pravilom (Sunder, 2016). Po mnenju Association of Chartered Certified Accountants in Ernst & Young (2017) je zato trenutno čas za testiranja različnih potencialnih aplikacij tehnologije, tako v privatnem kot javnem sektorju.

3.8 Aktivnosti podjetij pri razvoju blockchain računovodstva

V nadaljevanju predstavljam nekaj primerov aktivnosti na področju razvoja aplikacij blockchain računovodstva. Vključenost glavnih igralcev v tej panogi demonstrira njihovo sprejetje tehnologije kot naslednji evolucijski korak v panogi.

Konec leta 2016 so se prvič sestali največji blockchain specialisti znotraj štirih največjih računovodskih in revizijskih podjetij (Deloitte, Ernst & Young, KPMG in PriceWaterhouse Coopers). Namen okrogle mize je bila diskusija o tem, kako bi računovodska industrija lahko sodelovala pri razvoju novih blockchain standardov, ki bi pomagali podjetjem opravljati delo bolj učinkovito. Kot je omenjeno v poglavju, blockchain predstavlja resno grožnjo tem podjetjem, zato je za njih pomembno, da njen potencial spreobrnejo v svojo korist (del Castillo, 2016). Ta računovodska in revizorska podjetja so v zadnjem obdobju investirala veliko sredstev z namenom razvoja lastnih sistemov, ki izkoriščajo lastnosti tehnologije.

Deloitte je januarja 2017 v Dublinu odprl blockchain laboratorij, v katerem bo 50 ljudi razvijalo blockchain aplikacije za namene podjetja (Rae, 2017). Med drugim razvija rešitve, ki bi avtomatizirale določene dele revizorskega procesa. Podjetje bi vsako transakcijo objavilo v blockchain v realnem času in Deloitte bi enostavno preveril bazo podatkov in posamezne transakcije. To bi bil korak v smeri konsolidirane revizijske sledi, ki ga predlaga SEC (angl. *Securities & Exchange Commission*) (Huber, 2016). Ena izmed rešitev je tudi

programska platforma Rubix, ki klientom omogoča lasten razvoj aplikacij na podlagi blockchain infrastrukture. Glavna področja uporabe so predvsem usklajevanje med poslovnimi partnerji, revidiranje v realnem času, nepremičninski registri in sistemi zvestobe. Gre za privatni blockchain sistem, ki bi povezoval Deloitte in njegove stranke (Rizzo, 2015).

Ena izmed organizacij, ki izdeluje blockchain aplikacijo za tristavni računovodski sistem (Balanc3), je Consensys. Gre za odprto platformo, ki upravlja digitalna sredstva, kriptovalute in žetone (Wunsche, 2016).

SKLEP

Skozi magistrsko delo smo poskušali razumeti nastanek tehnologije podatkovnih verig in njeno delovanje. Tehnologija po samem konceptu obljublja revolucionarne spremembe in različni strokovnjaki jo primerjajo s pojavom interneta. Bit tehnologije je odpravljanje potrebe po zaupanju v tretje osebe, ki v sedanjem svetu igrajo pomembno vlogo posrednikov. Ime izhaja iz verige blokov, ki sestavljajo bazo podatkov. V njej se shranjujejo časovno zaznamovane, kronološko urejene in kriptografsko povezane transakcije sredstev. Uporabo tehnologije lahko razdelimo na tri nivoje: shranjevanje digitalnih zapisov, izmenjava digitalnih sredstev in izvajanje pametnih pogodb. Distribuirana narava baze podatkov je bistvena lastnost njene inovativne ideje. Ob različnih oblikah blockchain sistemov in metod potrjevanja transakcij je tehnologija primerna za zaprte skupine uporabnikov ali povezovanje svetovne populacije posameznikov in podjetij.

Ker je tehnologija šele v zametkih razvoja, izpostavljam, da ugotovitve v tem magistrskem delu temeljijo na teoretičnih predpostavkah. Tehnologija se je prvič pojavila kot podporno orodje za nastanek kriptovalute bitcoin, namen katerega je bil predstaviti neodvisno valuto, ki je alternativna obstoječim fiat valutam, in poseči v delovanje finančne industrije. Slednjo je pretresel z uvedbo, časovno in stroškovno, učinkovitega sistema prenosa vrednosti neposredno med uporabniki. Kljub vidnim prednostim na drugi strani obstajajo tudi omejitve, ki kriptovalutam onemogočajo, da postanejo zakonito plačilno sredstvo (volatilnost, omejena količina, nezmožnost reagiranja na šoke v ekonomiji ipd.).

Kriptovalute imajo sicer močan vpliv na finančni sektor, vendar pa ima tehnologija veliko večji potencial. Njene lastnosti omogočajo uporabo tehnologije na globalnem nivoju, tako v poslovnem in finančnem svetu, kot na ravni držav in splošnega prebivalstva. V magistrskem delu sem se osredotočil na njen vpliv v panogi računovodstva in revizije, ki kot temeljna podporna dejavnost globalne ekonomije igra pomembno vlogo pri nadaljnjem razvoju in oblikovanju novih poslovnih modelov. Tehnologijo podatkovnih verig lahko po obliki tesno povežemo tudi z glavno knjigo, ki jo v računovodstvu poznamo kot izhodišče za pripravo finančnih izkazov. Ti služijo kot povezava med podjetjem in njegovimi deležniki, zato je zaupanje v resničnost in poštenost izkazov ključnega pomena. Prvič je to mogoče doseči

brez vpliva človeka. Z istočasno izvedbo, zapisom in preverbo transakcije tehnologija prvič po več kot 500-ih letih prinaša pomemben korak v delovanju obstoječega računovodskega sistema. Dvostavno knjigovodstvo se s tehnologijo lahko razvije v tristavno. Slednje ima potencialne pozitivne učinke v revidiranju in poročanju celovitih in resničnih finančnih izkazov v realnem času ter poenotenju različnih računovodskih sistemov. Ob enem odpravlja potrebo po opravljanju aktivnosti z nizko dodano vrednostjo in računovodjem ter revizorjem ponuja možnost, da transformirajo svoj poklic z opravljanjem aktivnosti z višjo dodano vrednostjo (svetovalne funkcije).

Moje priporočilo stroki je, da se v iskanju odgovora na svojo prihodnost spozna s tehnologijo, njenim delovanjem, načini uporabe in priložnostmi ter tveganji, ki jih le-ta prinaša. V sklopu zaključka svetujem, da spremljajo razvoj tehnologije in razmišljajo o novih poslovnih modelih in potrebnih kompetencah, z namenom, da so pripravljeni na čas, ko bo tehnologija spremenila vsakdanjik njihovega delovnega življenja. Glede na, da so spremembe stalnica v računovodski stroki, menim, da se bodo podjetja in ljudje, tako kot vedno, prilagodili spremembam.

LITERATURA IN VIRI

1. Ammous, S. (2016a). Blockchain Technology: What is it Good for?. *SSRN*. Najdeno 3. junija 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751
2. Ammous, S. (2016b). Can cryptocurrencies fulfil the functions of money?. *SSRN*. Najdeno 3. junija 2017 na spletnem naslovu https://papers.ssrn.com /sol3/papers.cfm?abstract_id=2832769
3. Association of Chartered Certified Accountants, & Ernst & Young. (2017). *Risks and opportunities of Blockchain and Distributed ledgers*. Najdeno 25. junija 2017 na spletnem naslovu http://www.accaglobal.com/lk/en/technical-activities/technical-resources-search/2017/march/risks-and-opportunities-of-blockchain.html pril%202017%20ACCA%20EY%20event%20FINAL%20REPORT.pdf
4. Association of Chartered Certified Accountants, & Grant Thornton. (2016). *The future of audit.* Najdeno 15. junija 2017 na spletnem naslovu http://www.accaglobal.com/content/dam/ACCA_Global/Technical/audit/ea-future-of-audit.pdf
5. Association of Chartered Certified Accountants. (2016). *Professional accountants – the future: Drivers ofchange and future skills*. Najdeno 13. junija 2017 na spletnem naslovu http://www.accaglobal.com/content/dam/members-beta/docs/ea-patf-drivers-of-change-and-future-skills.pdf
6. Athey, S., Catalini, C., & Tucker, C. (2017). The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. *SSRN*. Najdeno 3. junija 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916489
7. Australian Government. (2014). *Australian Industry Report 2014.* Najdeno 29. junija 2017 na spletnem naslovu https://industry.gov.au/Office-of-the-Chief-Economist/Publications/Documents/Australian-Industry-Report.pdf
8. Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *ResearchGate.* Najdeno 12. aprila 2017 na spletnem naslovu https://www.researchgate.net/publication/2482110_Hashcash_A_Denial_of_Service_Counter-Measure
9. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., & Wuille, P. (2014). Enabling blockchain innovations withthrough pegged sidechains. *Blockstream.* Najdeno 16. maja 2017 na spletnem naslovu https://blockstream.com/sidechains.pdf
10. Baran, P. (1964). On distributed communications: Introduction to distributed communications networks. *IEEE Transactions on Communication Systems, 12*(1), 1–9.
11. Barbieri, M., & Gassen, D. (2017). Blockchain – can this new technology really revolutionize the land registry system?. *Notaries of Europe.* Najdeno 2. junija 2017 na spletnem naslovu http://www.notaries-of-europe.eu/index.php?pageID=15101
12. Barker, R. (2003). Global Accounting Is Coming. *Harward Business Review, 81*(4), 24–25.

13. Baron, J. (2017). Blockchain, Accounting and Audit: What Accountants Need to Know. *Thompson Reuters.* Najdeno 30. junija 2017 na spletnem naslovu https://tax.thomsonreuters.com/blog/business/technology/blockchain-accounting-and-audit-what-accountants-need-to-know/
14. Bentov, I., Gabizon, A., & Mizrahi, A. (2014). Cryptocurrencies without Proof of Work. *Smith + Crown.* Najdeno 26. aprila 2017 na spletnem naslovu https://www.smithandcrown.com/open-research/cryptocurrencies-without-proof-of-work-2/
15. Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37.
16. Berke, A. (2017). How Safe Are Blockchains? It Depends. *Harvard Business Review*. Najdeno 25. maja 2017 na spletnem naslovu https://hbr.org/2017/03/how-safe-are-blockchains-it-depends
17. Biella, M., & Zinetti, V. (2016). Blockchain Technology and Applications from a Financial PerspectiveTechnical Report Version 1.0. *UniCredit.* Najdeno 12. februarja 2017 na spletnem naslovu http://www.the-blockchain.com/docs/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf
18. Bitcoin Theory. (2016). *The Economic Efficiency of Digital Currencies.* Najdeno 6. junija 2017 na spletnem naslovu https://btctheory.com/2016/11/17/economic-efficiency-digital-currencies/
19. BitFury Group, & Garzik, J. (2015a). Public versus Private Blockchains Part 1: Permissionless Blockchains. *BitFury Group Limited*. Najdeno 16. februarja 2017 na spletnem naslovu http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf
20. BitFury Group, & Garzik, J. (2015b). Public versus Private Blockchains Part 2: Permissionless Blockchains. *BitFury Group Limited.* Najdeno 13. januarja 2017 na spletnem naslovu http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf
21. BitFury Group. (2015c). Proof of Stake versus Proof of Work. *BitFury Group Limited.* Najdeno 17. januarja 2017 na spletnem naslovu http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf
22. BitInfoCharts. (2017). *Bitcoin Median Transaction Fee vs. Median Transaction Value historical chart.* Najdeno 9. julija 2017 na spletnem naslovu https://bitinfocharts.com/comparison/median_transaction_fee-mediantransactionvalue-btc.html#3m
23. Blockchain Luxembourg. (2016). *Breaking It Down: Bitcoin Units of Measurement*. Najdeno 9. julija 2017 na spletnem naslovu https://blog.blockchain.com/2016/07/01/breaking-it-down-bitcoin-units-of-measurement/
24. Blockchain Luxembourg. (2017d). *Bitcoins in circulation*. Najdeno 8. julija 2017 na spletnem naslovu https://blockchain.info/charts/total-bitcoins
25. Blockchain Luxembourg. (2017a). *Miners Revenue*. Najdeno 16. marca 2017 na spletnem naslovu https://blockchain.info/sl/charts/miners-revenue?timespan=30days
26. Blockchain Luxembourg. (2017b). *Hashrate Distribution.* Najdeno 10. julija 2017 na spletnem naslovu https://blockchain.info/pools

27. Blockchain Luxembourg. (2017c). *Market Price (USD)*. Najdeno 10. julija 2017 na spletnem naslovu https://blockchain.info/charts/market-price
28. Blockgeeks. (b.l.). *What is cryptocurrency.* Najdeno 13. februarja 2017 na spletnem naslovu https://blockgeeks.com/guides/what-is-cryptocurrency/
29. Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260–279.
30. Bradbury, D. (2015). How the Blockchain Could Stop Firms Cooking the Books. *Coindesk.* Najdeno 15. marca 2017 na spletnem naslovu http://www.coindesk.com/how-the-blockchain-could-stop-firms-cooking-the-books/
31. Brito, J., & Castillo, A. (2013). *Bitcoin. A Primer for Policymakers.* Arlington: Mercatus Center.
32. Brown, C. (2016). The Value of Cryptocurrency Today And What The Future Might Hold. *Forbes.* Najdeno 3. junija 2017 na spletnem naslovu https://www.forbes.com/sites/forbestechcouncil/2016/04/13/the-value-of-cryptocurrency-today-and-what-the-future-might-hold/#25c6c4c82e90
33. Brown, R. G. (2015). *Cost? Trust? Something else? What's the killer-app for Block Chain Technology?*. Najdeno 23. junija 2017 na spletnem naslovu https://gendal.me/2015/01/15/cost-trust-something-else-whats-the-killer-app-for-block-chain-technology/
34. Buterin, V. (2015). On Public and Private Blockchains. *Ethereum Blog.* Najdeno 10. maja 2017 na spletnem naslovu https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
35. Byström, H. (2016). *Blockchains, Real-Time Accounting and the Future of Credit Risk Modeling.* Lund University: School of Economics and Management.
36. Campbell, D. (2015). *Bitcoin, Accounting and the Blockchain.* Najdeno 28. junija 2017 na spletnem naslovu http://www.dugcampbell.com/bitcoin-accounting-blockchain/
37. Carlozo, L. (2017). Why CPAs need to get a grip on blockchain?. *Journal of Accontancy.* Najdeno 16. junija 2017 na spletnem naslovu http://www.journalofaccountancy.com/news/2017/jun/blockchain-decentralized-ledger-system-201716738.html
38. Castor, A. (2017). A (Short) Guide to Blockchain Consensus Protocols. *Coindesk.* Najdeno 15. aprila 2017 na spletnem naslovu http://www.coindesk.com/short-guide-blockchain-consensus-protocols/
39. Catalini, C., & Gans, J. (2016). Some Simple Economics of the Blobkchain. *ResearchGate. MIT Sloan School of Management.* Najdeno 16. januarja 2017 na spletnem naslovu https://www.researchgate.net/publication/312486240_Some_Simple_Economics_of_the_Blockchain
40. Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in cryptology-Crypto '82, Springer Verlag*, 199–203.
41. Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28*(10), 1030–1044.

42. CoinMarketCap. (2017). *CryptoCurrency Market Capitalizations*. Najdeno 15. aprila 2017 na spletnem naslovu https://coinmarketcap.com/currencies/volume/monthly/
43. CoinReport. (2014). *What are the Advantages and Disadvantages of Bitcoin?* Najdeno 3. junija 2017 na spletnem naslovu https://coinreport.net/coin-101/advantages-and-disadvantages-of-bitcoin/
44. BLLiZ Consultancy. (2017). *Blockchain Technology: How it works, main advantages and challenges.* Najdeno 25. aprila 2017 na spletnem naslovu http://www.consultancy.uk/news/13484/blockchain-technology-how-it-works-main-advantages-and-challenges
45. Crosby, M., Nachiappan, N., Patanayak, P., Venna, S., & Kalynaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*, *6*(2), 6–19.
46. Del Castillo, M. (2016). 'Big Four' Accounting Firms Meet to Consider Blockchain Consortium. *Coindesk.* Najdeno 25. junija 2017 na spletnem naslovu http://www.coindesk.com/big-four-accounting-firms-meet-to-weigh-benefits-of-blockchain-consortium/
47. Delloite. (2016a). *Israel: A Hotspot for Blockchain Innovation*. Najdeno 15. januarja 2017 na spletnem naslovu https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf
48. Deloitte. (2016b). *Blockchain Technology A game-changer in accounting?* Najdeno 25. aprila 2017 na spletnem naslovu https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf
49. Digiconomist. (2017). *Bitcoin Energy Consumption Index*. Najdeno 7. julija 2017 na spletnem naslovu http://digiconomist.net/bitcoin-energy-consumption
50. Dimitriu, O., & Matei, M. (2015). Cloud accounting: a new business model in a challenging contex. *Procedia Economics and Finance*, *32*, 665–671.
51. Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Germany: Apress.
52. Edelman. (2017). *2017 Edelman TrustRUST BAROMETERarometer Reveals Global Implosion of Trust.* Najdeno 12. februarja 2017 na spletnem naslovu http://www.edelman.com/news/2017-edelman-trust-barometer-reveals-global-implosion/
53. Ernst & Young. (2016). *Blockchain reaction Tech companies plan for critical mass.* Najdeno 25. januarja 2017 na spletnem naslovu http://www.ey.com/Publication/vwLUAssets/ey-blockchain-reaction-tech-companies-plan-for-critical-mass/$FILE/ey-blockchain-reaction.pdf
54. Evans, D. S. (2014). Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. *SSRN.* Najdeno 26. maja 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516
55. Evropska komisija. (2017). *How big is the tax fraud and tax evasion problem ?* Najdeno 25. junija 2017 na spletnem naslovu http://ec.europa.eu/taxation_customs/fight-against-tax-fraud-tax-evasion/a-huge-problem_en

56. Financial Accounting Standards Board. (1985). *Statement of Financial Accounting Concepts No. 6: Elements of Financial Statements.* Najdeno 25. junija 2017 na spletnem naslovu http://www.fasb.org/jsp/FASB/Page/PreCodSectionPage&cid=1176156317989
57. Financial Industry Regulatory Authority. (2017). *Distributed Ledger Technology: Implicationsof Blockchain for the Securities Industry.* Najdeno 6. januarja 2017 na spletnem naslovu http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf
58. Friedlmaier, M., Tumasjan, A., & Welpe, I. (2016). *Disrupting Industries With Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures*. München: TUM School of Management.
59. Frieswick, K. (2003). How Audits Must Change. *CFO Magazine.* Najdeno 25. junija 2017 na spletnem naslovu http://faculty.som.yale.edu/shyamsunder/Financial-Fraud/How%20Audits%20Must%20Change.htm
60. Frisby, D. (2014). *Bitcoin: The Future of Money?* London: Unbound.
61. Gerigg, I. (2005). *Triple Entry Accounting.* Najdeno 16. junija 2017 na spletnem naslovu http://iang.org/papers/triple_entry.html#index
62. Gerstein, I. R., & Hervieux-Payette, C. (2015). *Digital currency: You can't flip this coin! Report of the standing senate committee on banking, trade and commerce*. Canada: State Senat Canada.
63. Graydon, C. (2014). What is Cryptocurrency? *Cryptocoins news*. Najdeno 25. aprila 2017 na spletnem naslovu https://www.cryptocoinsnews.com/cryptocurrency/
64. Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *SSRN*. Najdeno 8. julija 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857
65. Harrington, M. (2017). Survey: People's trust has declined in business, media, government and NGOs. *Harvard Business Review*. Najdeno 16. februarja 2017 na spletnem naslovu https://hbr.org/2017/01/survey-peoples-trust-has-declined-in-business-media-government-and-ngos
66. Harwick, C. (2015). Cryptocurrency and the Problem of Intermediation. *SSRN*. Najdeno 114. junija 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523771
67. He, D., Habermeier, K., Leckow, R., Haksar, V., Almedia, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N., & Verdugo-Yepes, C. (2016). Virtual Currencies and Beyond: Initial Considerations. International monetary fund. *International Monetary Fund.* Najdeno 6. marca 2017 na spletnem naslovu https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
68. Hileman, G., & Rauchs, M. (2017). Global Cryptocurrency Benchmarking Study. *University of Cambridge.* Najdeno 25. junija 2017 na spletnem naslovu https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/#.WVZLg2YUncs

69. Horadan P. (2016). How Blockchain Will Change Business Transactions. *Accounting Today.* Najdeno 26. junija 2017 na spletnem naslovu https://www.accountingtoday.com/news/how-blockchain-will-change-business-transactions
70. Huber, S. (2016). Blockchain and the Auditing Revolution – Real Time Audit within the Capabilities of Blockchain. *Fintech Switzerland.* Najdeno 24. junija 2017 na spletnem naslovu http://fintechnews.ch/blockchain_bitcoin/blockchain-auditing-revolution-real-time-audit-within-the-capabilities-of-blockchain/3864/
71. Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Aplicattions. *Procedia Computer Science, 98,* 461–466.
72. Hülsmann, J. G. (2014). The Cultural and Political Consequences of Fiat Money. *Mises Institute.* Najdeno 1. junija 2017 na spletnem naslovu https://mises.org/library/cultural-and-political-consequences-fiat-money-0
73. Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review.* Najdeno 25. maja 2017 na spletnem naslovu https://hbr.org/2017/01/the-truth-about-blockchain
74. Investopedia. (b.l.). *What are the advantages of paying with Bitcoin?.* Najdeno 23. marca 2017 na spletnem naslovu http://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp
75. Josselyn, S. (2014). Bitcoin: a future currency for M&A transactions?. *Norton Rose Fulbright.* Najdeno 25. junija 2017 na spletnem naslovu http://www.deallawwire.com/2014/02/20/bitcoin-a-future-currency-for-ma-transactions/
76. Karajovic, M., Narula, H., Pandya, K., Patel, J., & Warring, I. (2017). Blockchain: A Manager's Guide. *SSRN.* Najdeno 29. junija 2017 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2897645
77. Karame, G. O., Androulaki, E., & Čapkun, S. (2012). *Double-Spending Fast Payments in Bitcoin.* Raleigh: ACM New York.
78. Kemp, C., Reid, L., & Romero, M. (2016). In blockchain we trust: a comparison of the investment potential of bitcoin and ether over a five-year time horizon. *Middlebury Institute of International Studies at Monterey.* Najdeno 4. junija 2017 na spletnem naslovu http://www.economist.com/sites/default/files/written_submission_middlebury.pdf
79. Kieso , D. , Weygandt , J., & Warfield , T. (2013). *Intermediate accounting* (15th ed.). Hoboken: Wiley.
80. Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal, 65,* 569–608.
81. Koražija, N. (2017). Prihaja tehnologija blockchain. Kaj morate vedeti in kako lahko spremeni vaš posel? *Finance.* Najdeno 15. februarja 2017 na spletnem naslovu https://manager.finance.si/8852997
82. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *Princeton University.* Najdeno 16. aprila 2017

na spletnem naslovu http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf
83. Kuo Chuen, D. L. (2015). *Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Data.* Singapore: Elsevier.
84. Kwon, J. (2015). *Tendermint: Consensus without Mining.* New York: Cornell University.
85. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382–401.
86. Lazanis, R. (2015). How Technology Behind Bitcoin Could Transform Accounting As We Know It. *Techvibes.* Najdeno 29. junija 2017 na spletnem naslovu https://techvibes.com/2015/01/22/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22
87. Lee, D. (2016). Blockchain Technology - What It Is, And How It Can Help Accountants. *Practice Advisor.* Najdeno 20. junija 2017 na spletnem naslovu http://www.cpapracticeadvisor.com/news/12227941/blockchain-technology-what-it-is-and-how-it-can-help-accountants
88. Li, S., Xu, L. D., & Zhao, S. (2014). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259.
89. Lingham, V. (2017). *Bitcoin: Commodity, Store of Value or Digital Currency?* Najdeno 8. julija na spletnem naslovu https://vinnylingham.com/bitcoin-commodity-store-of-value-or-digital-currency-93457cd27c9c
90. Lo, S., & Wang, J. C. (2014). Bitcoin as Money?. *Harvard University.* Najdeno 8. julija 2017 na spletnem naslovu https://scholar.harvard.edu/slo/publications/bitcoin-money
91. Loop, P. (2016). Blockchain: The Next Evolution of Supply Chains. *Material Handling & Logistics.* Najdeno 7. junija 2017 na spletnem naslovu http://mhlnews.com/global-supply-chain/blockchain-next-evolution-supply-chains
92. Ly, M. K.-M. (2014). Coining bitcoin's "legal-bits":examining the regulatory framework for bitcoin and virtual currencies. *Harvard Journal of Law & Technology*, *27*(2), 588–608.
93. Madeira, A. (2017). Bitcoin Still Illegal in Some Countries. *Bitcoinist.com.* Najdeno 8. julija 2017 na spletnem naslovu http://bitcoinist.com/bitcoin-still-illegal-six-countries/
94. Martindale, N. (2016). How blockchain will impact accountants and auditors. *Economia.* Najdeno 23. maja 2017 na spletnem naslovu http://economia.icaew.com/features/july-2016/how-blockchain-will-impact-accountants-and-auditors
95. Mazonka, O. (2016). *Blockcain: Simple Explanation*. Najdeno 12. januarja 2017 na spletnem naslovu http://jrxv.net/x/16/chain.pdf
96. McCook, H. (2014). Under the Microscope: Economic and Environmental Costs of Bitcoin Mining. *Coindesk.* Najdeno 20. aprila 2017 na spletnem naslovu http://www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/

97. Merkle, R. C. (1998). A digital signature based on a conventional encryption function. *Springer-Verlag.* Najdeno 25. februarja 2017 na spletnem naslovu https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf
98. Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2017*). Proof of Luck: an Efficient Blockchain Consensus Protocol.* Najdeno 16 aprila 2017 na spletnem naslovu https://arxiv.org/pdf/1703.05435.pdf
99. Morrison, A. (2016). How smart contracts automate digital business. *PriceWaterhouse Coopers.* Najdeno 17. junija 2017 na spletnem naslovu http://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/
100. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin Project.* Najdeno 15. januarja 2017 na spletnem naslovu https://bitcoin.org/bitcoin.pdf
101. Nevious, A. M. (2014). New guidance clarifies tax treatment of bitcoin and other virtual currencies. *Journal of Accountancy.* Najdeno 15. junija 2017 na spletnem naslovu http://www.journalofaccountancy.com/news/2014/mar/20149850.html
102. Niepelt, D. (2016). Internet-based technology has made it cheap to collect information and to network. *World Economic Forum.* Najdeno 13. marca 2017 na spletnem naslovu https://www.weforum.org/agenda/2016/10/blockchain-cryptocurrencies-and-central-banks-opportunity-or-threat
103. Nugent, J. (2013). The Bitcoin Boom. *Forbes.* Najdeno 26. junija 2017 na spletnem naslovu https://www.forbes.com/sites/riskmap/2013/12/17/the-bitcoin-boom/#2f5f7aaf364e
104. Okupski, K. (2016). *Bitcoin Developer Reference*. The Netherlands: Technische Universiteit Eindhoven.
105. Ou, E. (2016). Bitcoin Isn't Anonymous Enough. *Bloomberg.* Najdeno 16. januarja 2017 na spletnem naslovu https://www.bloomberg.com/view/articles/2016-11-01/bitcoin-isn-t-anonymous-enough
106. Ovenden, J. (2017). Will Blockchain Render Accountants Irrelevant?. *The Innovation Enterprise.* Najdeno 25. junija 2017 na spletnem naslovu https://channels.theinnovationenterprise.com/articles/will-blockchain-render-accountants-irrelevant
107. Parkins, D. (2015). The great chain of being sure about things. *The Economist.* Najdeno 26. aprila 2017 na spletnem naslovu https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable
108. Patterson, R. (2015). Alternatives for Proof of Work, Part 1: Proof Of Stake. *Bytecoin.* Najdeno 15. aprila 2017 na spletnem naslovu https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/
109. Poelstra, A. (2015). *On Stake and Consensus.* Najdeno 25. februarja 2017 na spletnem naslovu https://download.wpsoftware.net/bitcoin/pos.pdf
110. Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Smith + Crown.* Najdeno 13. januarja 2017 na spletnem naslovu

https://www.smithandcrown.com/open-research/the-bitcoin-lightning-network-scalable-off-chain-instant-payments/

111. Poushter, J. (2016). Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. *Pew Research Center*. Najdeno 9. julija 2017 na spletnem naslovu http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/
112. PriceWaterhouse Coopers. (2015). *Future-proofing Australia's workforce by growing skills in science, technology, engineering and maths (STEM*). Najdeno 28. junija 2017 na spletnem naslovu https://www.pwc.com.au/pdf/a-smart-move-pwc-stem-report-april-2015.pdf
113. Rae, D. (2017). Blockchain: accountancy's transformer. *Association of Chartered Certified Accountants.* Najdeno 16. junija 2017 na spletnem naslovu http://www.accaglobal.com/vn/en/member/member/accounting-business/2017/04/insights/blockchain-17.html
114. Raiborn, C., & Sivitanides, M. (2015). Accounting Issues Related to Bitcoins. *Journal of Corporate Accounting & Finance, 26*(2), 25–34.
115. Randewich, N. (2013). Bitcoin sinks in value after FBI busts Silk Road drug market. *Reuters.* Najdeno 28. maja 2017 na spletnem naslovu http://www.reuters.com/article/net-us-crime-silkroad-bitcoin-idUSBRE99113A20131008
116. Rasch, A. (2017). Compatibility, networks effects, and collusion. *Econimics Letters, 151,* 39–43.
117. Rizzo, P. (2015). Risks and opportunities of Blockchain and Distributed. *Coindesk.* Najdeno 25. junija 2017 na spletnem mestu http://www.coindesk.com/deloitte-blockchain-auditing-consulting/
118. Rizzo, P. (2016). KPMG: Blockchain Could Be 'Antidote' to High Cost of Regulation. *Coindesk.* Najdeno 15. junija 2017 na spletnem naslovu http://www.coindesk.com/kpmg-blockchain-antidote-regulatory-costs/
119. Rizzo, P. (2017). Bitcoin Price Crosses $3,000 Milestone to Set New All-Time High. *Coindesk.* Najdeno 7. julija 2017 na spletnem naslovu http://www.coindesk.com/bitcoin-price-crosses-3000-milestone-set-new-time-high/
120. Roberts, J. J. (2017). 3 Reasons Why Bitcoin Broke $2,000. *Fortune.* Najdeno 7. julija 2017 na spletnem naslovu http://fortune.com/2017/05/21/bitcoin-2000/
121. Rogers, E. M. (2003). *Diffusion of innovations*. New York: Free Press.
122. Rosic, A. (2016). 7 Incredible Benefits Of Cryptocurrency. *Huffington Post.* Najdeno 25. aprila 2017 na spletnem naslovu http://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html
123. Rostohar, I. (2016). Kriptovalute v 21., zakonodaja pa v 20. stoletju. *Svet kapitala.* Najdeno 16. aprila 2017 na spletnem naslovu http://svetkapitala.delo.si/finance/kriptovalute-v-21-zakonodaja-pa-v-20-stoletju-493
124. Samuelson, P. A., & Nordhaus, W. D. (2010). *Economics*. New Delhi:Tata McGraw-Hill Education.

125. Santander, InnoVentures, Oliver Wyman, & Anthemis Group. (2015). *The Fintech 2.0 Paper:Rebooting financial services.* Najdeno 25. aprila 2017 na spletnem naslovu http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf
126. Schneider, N. (2015). After the Bitcoin Gold Rush. *New Republic.* Najdeno 16. maja 2017 na spletnem naslovu https://newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle
127. Scott, B. (2015). Open data can unravel the complex dealings of multinationals. *The Guardian.* Najdeno 16. junija 2017 na spletnem naslovu https://www.theguardian.com/sustainable-business/2015/aug/11/open-data-can-unravel-the-complex-dealings-of-multinationals
128. Sharma, V. (2017). How Blockchain Will Change Accounting Business. *Real Time Cloud Services.* Najdeno 26. junija 2017 na spletnem naslovu http://www.myrealdata.com/blog/1979_blockchain-change-accounting-business
129. Sheedy, C. (2017). What CPAs need to do to survive the automation revolution. *Journal of Accountancy.* Najdeno 25. junija 2017 na spletnem naslovu http://www.journalofaccountancy.com/newsletters/2017/jun/survive-automation-revolution.html
130. Sherman, H. D, & Young, S. D. (2016). Where Financial Reporting Still Falls Short. *Harward Business Review, July-August,* 76–84.
131. Sikorski, J. J., Haugton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy, 195,* 234–246.
132. Simon, G. (2016). Blockchain and the Introduction of Single-Entry Bookkeeping. *Medium.* Najdeno 19. junija 2017 na spletnem naslovu https://medium.com/@Loyyal/blockchain-and-the-introduction-of-single-entry-bookkeepingbookkeping-5e5b201db09
133. Slovenski inštitut za revizijo. (2016). *Slovenski računovodski standardi (2016) z dodanimi Pravili srbnega računovodenja.* Ljubljana.: Zveza računovodij, finančnikov in revizorjev Slovenije.
134. Smith, C. H. (2016, junij). Here's why people are flocking to cryptocurrencies. *Business Insider.* Najdeno 25. maja 2017 na spletnem naslovu http://www.businessinsider.com/why-people-buy-cryptocurrencies-2016-6
135. Smith, J. (2016). There is more to blockchain than moving money. It has the potential to transform our lives - here's how. *World Economic Forum.* Najdeno 15. marca 2017 na spletnem naslovu https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money/
136. Song, W., Shi, S., Xu, V., & Gill, G. (2016). Advantages & Disadvantages of Blockchain Technology. *Word Press.* Najdeno 13. aprila 2017 na spletnem naslovu https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

137. Spoke, M. (2015). How Blockchain Tech Will Change Auditing for Good. *Coindesk.* Najdeno 25. maja 2017 na spletnem naslovu http://www.coindesk.com/blockchains-and-the-future-of-audit/
138. Staley, O. (2016). The unsexy future of blockchain is accounting. *Quartz.* Najdeno 27. junija 2017 na spletnem naslovu https://qz.com/629662/the-unsexy-future-of-blockchain-is-accounting/
139. Sunder, S. (2016). Better financial reporting: Meanings and means. *Journal of Accounting Pubic Policy, 35*(3), 211–223.
140. Svetovna Banka. (2017). *An analysis of trends in cost of remittance services. Remittance Prices Worldwide.* Najdeno 9. julija 2017 na spletnem naslovu https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2017.pdf
141. Swan, M. (2015). *Blockchain. Blueprint for a New Economy*. United States of America: O'Reilly.
142. Swanson, T. (2014). Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management. *Amazon Digital Services*. Najdeno 16. maja 2017 na spletnem naslovu https://s3-us-west-2.amazonaws.com/chainbook/Great+Chain+of+Numbers+A+Guide+to+Smart+Contracts,+Smart+Property+and+Trustless+Asset+Management+-+Tim+Swanson.pdf
143. Swanson, T. (2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. *Smith + Crown.* Najdeno 23. januarja 2017 na spletnem naslovu https://www.smithandcrown.com/open-research/consensus-as-a-service/
144. Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*. Najdeno 25. maja 2017 na spletnem naslovu http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First
145. Šutanovac, L. (2017). Pravni fokus: Tehnologija blockchains. *Mladipodjetnik.si.* Najdeno 25. maja 2017 na spletnem naslovu http://mladipodjetnik.si/novice-in-dogodki/novice/pravni-fokus-tehnologija-blockchains
146. Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: principles and paradigms (2nd ed.).* The Netherlands: Pearson Prentice Hall.
147. Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. United States of America: Portfolio Penguin.
148. Tapscott, D., & Ticoll, D. (2003). *The Naked Corporation: How the Age of Transparency Will Revolutionize Business.* New York: Free Press.
149. Taran, E., Salmanova, I., Dokukina, E., Menshikova, M., & Skudareva, N. (2015). Features of Using the Cryptocurrency. *Asian Social Science, 11*(14), 330–336.
150. The Economist. (2015). *How bitcoin minig works.* Najdeno 26. marca 2017 na spletnem naslovu http://www.economist.com/blogs/economist-explains/2015/01/economist-explains-11

151. The Financial Crimes Enforcement Network. (2013). *Application of FinCEN's Regulations to Persons Administering,Exchanging, or Using Virtual Currencies.* Najdeno 25. maja 2017 na spletnem naslovu https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
152. Thompson, C. (2016). How does the Blockchain Work (for Dummies) explained simply. *The Intrepid Review.* Najdeno 16. februarja 2017 na spletnem naslovu https://medium.com/the-intrepid-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093
153. Twenge, J. M., Campbell, W. K., & Carter, N. T. (2014). Declines in trust in others and confidence in institutions among American adults and late adolescents, 1972-2012. *Psychological Science, 25*(10), 1914–1923.
154. Tyra, J. M. (2014). Triple Entry Bookkeeping With Bitcoin. *Bitcoin Magazine.* Najdeno 25. junija 2017 na spletnem naslovu https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656/
155. Ugovšek, J. (2017). Služite s kriptovalutami in se sprašujete, ali bi morali plačevati davke? *Finance.* Najdeno 29. junija 2017 na spletnem naslovu https://www.finance.si/8858267
156. Vaidynathan, N. (2017). Divided we fall, distributed we stand. The professional accountant's guide to distributed ledgers and blockchain. *Association of Chartered Certified Accountants.* Najdeno 21. junija 2017 na spletnem naslovu http://www.accaglobal.com/lk/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html
157. Van Gorp, N., & Batura, O. (2015). Challenges for competition policy in digitalised economy. *European Parliament.* Najdeno 15. januarja 2017 na spletnem naslovu http://www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU%282015%29542235_EN.pdf
158. Van Tilborg, H. C. A., & Jajodia, S. (2014). *Encyclopedia of cryptography and security*. Heidelberg: Springer Science & Business Media.
159. Visa International Service Association (2015). *Visa Inc. at a Glance.* Najdeno 8. julija 2017 na spletnem naslovu https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf
160. Wells, S. R. (2004). *The Federal Reserve System: A History.* United States of America: McFarland.
161. Western Union. (2016). *Our vision.* Najdeno 17. junija 2017 na spletnem naslovu https://corporate.westernunion.com/our-vision.html
162. Westra, S. J. (2016). What opportunities for auditors will arise with blockchain? *Unit4.* Najdeno 23. junija 2017 na spletnem naslovu http://www.unit4.com/blog/2016/01/what-opportunities-for-auditors-will-arise-with-blockchain

163. World Economic Forum. (2015). *How will blockchain technology transform financial services?*. Najdeno 13. marca 2017 na spletnem naslovu https://www.weforum.org/agenda/2015/11/how-will-blockchain-technology-transform-financial-services/
164. World Economic Forum. (2016). *The future of financial infrastructure*. Najdeno 14. aprila 2017 na spletnem naslovu http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
165. Worstall, T. (2013). Paul Krugman on Bitcoin, It's Not A Stable Store Of Value. *Forbes*. Najdeno 7. julija 2017 na spletnem naslovu https://www.forbes.com/sites/timworstall/2013/12/29/paul-krugman-on-bitcoin-its-not-a-stable-store-of-value/#5c456a054967
166. Wunsche, A. (2016). *Technological Disruption of Capital Markets and Reporting? An introduction to blockchain.* Canada: Chartered Proffesional Accountants Canada.
167. Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance*, *21*(1), 7–31.
168. Zakon o dohodnini. *Uradni list RS* št. 13-2011-UPB7, 64/2016.
169. Zaman Groff, M., Hočevar, M., & Igličar, A. (2007). *Temelji računovodstva.* Ljubljana: Ekonomska fakulteta.

PRILOGE

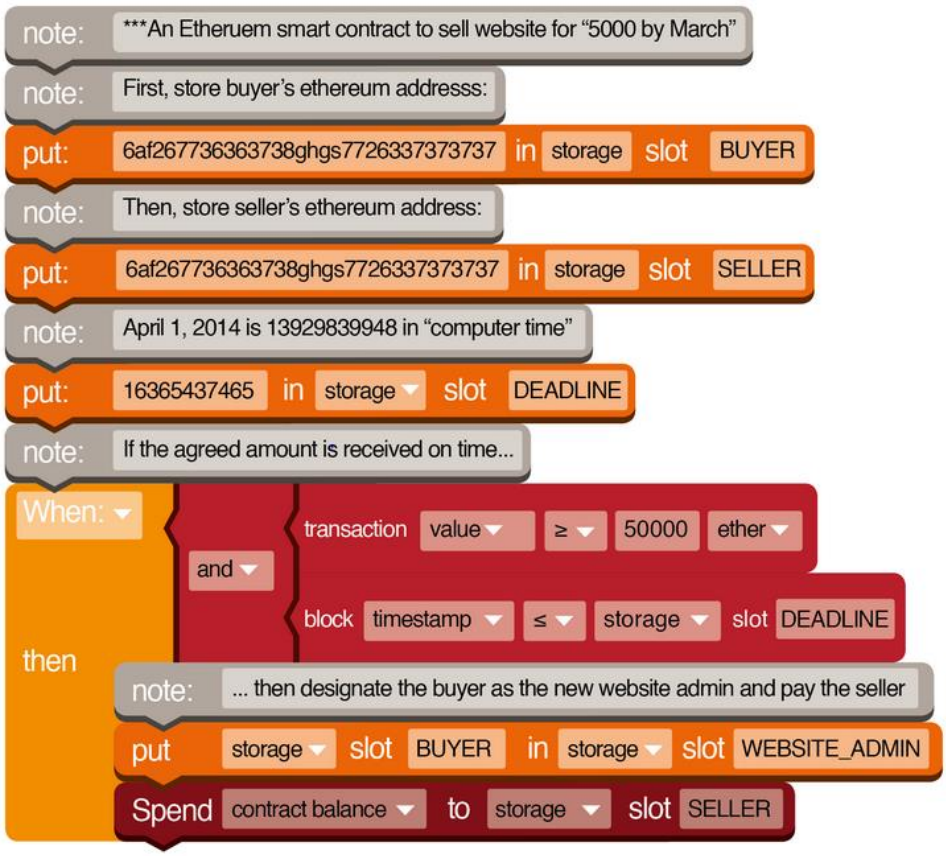
KAZALO PRILOG

PRILOGA 1: Terminološki slovar

Blockchain technology – tehnologija podatkovnih verig
Miners – rudarji
Mining – rudarjenje
Hash – zgoščena vrednost
Hashing – zgoščevalna funkcija
Mergers & acquistions (M&A) – združitve in prevzemi
Nodes – uporabniki
Nonce – naključna vrednost
Public-key cryptography – asimetrična kriptografija
Peer-to-peer (P2P) network – vrstniško omrežje
Token – simbol/žeton
Tokenized assets – simbolična sredstva
Smart contracts – pametne pogodbe
Public ledger – javno omrežje/sistem
Proof-of-Work – dokazilo o delu
Proof-of-Stake – dokazilo o deležu
Delegated proof-of-stake – delegirano dokazilo o deležu
Proof-of-Activity – dokazilo o aktivnosti
Proof-of-Capacity – dokazilo o kapaciteti
Sharing economy – delitvena ekonomija
Altcoins – alternativne kriptovalute
Business-to-business (B2B) – povezava med podjetji
Customer-to-business (C2B) – povezava med kupci in podjetji
Cloud accounting – računovodstvo v oblaku
First-in-first-out (FIFO) – metoda vrednotenja zalog

PRILOGA 2: Oblika pogodbe v sistemu Ethereum

Slika 1: Primer izseka pametne pogodbe, zasnovane v Ethereum sistemu



Vir: A. Morisson, How smart contracts automate digital business, 2016.

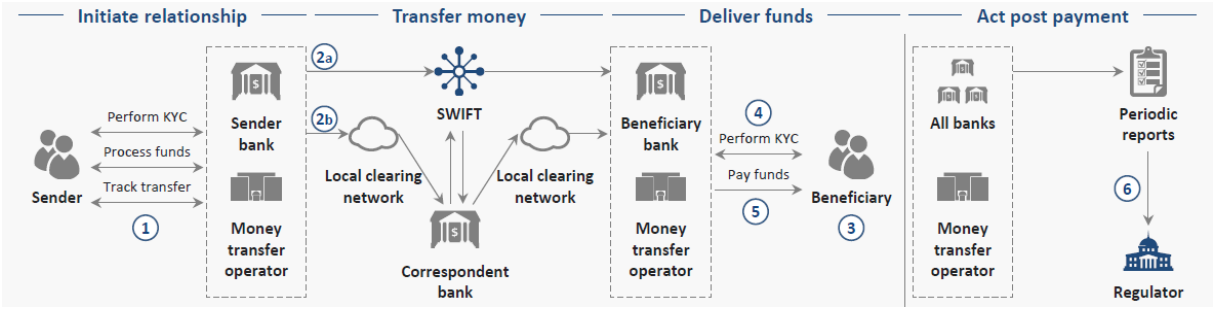
PRILOGA 3: Razlika med tradicionalnimi in pametnimi pogodbami

Slika 2: Primerjava lastnosti tradicionalnih in pametnih pogodb

Vir: A. Morisson, How smart contracts automate digital business, 2016.

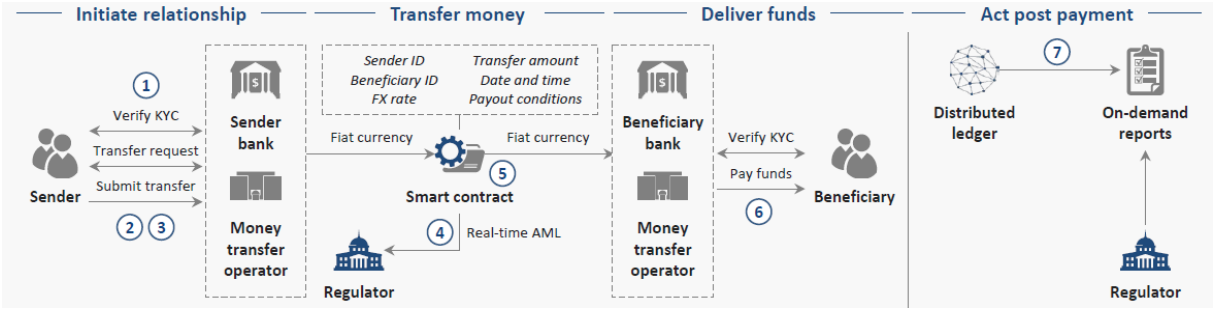
PRILOGA 4: Prikaz obstoječega in novega medbančnega plačilnega sistema, ki temelji na tehnologiji podatkovnih verig

Slika 3: Primer procesa obstoječega medbančnega plačilnega sistema



Vir: World Economic Forum, The future of financial infrastructure, 2016.

Slika 4: Primer procesa medbančnega plačilnega sistema, ki temelji na tehnologiji podatkovnih verig



Vir: World Economic Forum, The future of financial infrastructure, 2016.

PRILOGA 5: Seznam v delu uporabljenih kratic

$ – dolar
AICP – American Institue of Certified Planners
B2B – Business to Business
C2B – Customer to Business
FASB – Financial Accounting Standards Board
FBI - The Federal Bureau of Investigaton
FIFO – first-in-first-out
GAAP – Generally Accepted Accounting Principles
HTTP – HyperText Transfer Protocol
IASB – International Accounting Standards Board
IBM – International Business Machines Corporation
IFRS – International Financial Reporting Standards
IP – Internet Protocol
IRS – Internal Revenue Service
M&A – Mergers and Acquisitions (združitve in prevzemi)
MSRP – Mednarodni standardi računovodskega poročanja
P2P – Peer to Peer
RS – Republika Slovenija
SEC – Securities and Exchange Commission
SHA-256 – Secure Hash Algorithm 256
SRS – Slovenski računovodski standardi
TCP – Transmission Control Protocol
TWh – Terawatt hours (teravatna ura)
USB – Universal Serial Bus
ZDA – Združene Države Amerike
Zdoh-2 – zakon o dohodnini