UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

REVIDIRANJE KRIPTOVALUT V RAČUNOVODSKIH IZKAZIH

Ljubljana, 23. januar 2019 ŽIGA KRAJNC

IZJAVA O AVTORSTVU

Podpisani Žiga Krajnc, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Revidiranje kriptovalut v računovodskih izkazih, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Markom Hočevarjem

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

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

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

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

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

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

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

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

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

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

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC

ACCA (ang. Association of Charted Certified Accountants) – Zveza pooblaščenih revizorjev

ang. - angleško

ATVP – Agencija za trg vrednostnih papirjev

CPA (ang. Chartered professional accountants of Canada) – pooblaščeni revizorji Kanade

DAO (ang. Decentralized autonomous organization) – Decentralizirana anonimna organizacija

DDV – davek na dodano vrednost

EY – Ernst & Young

EU – Evropska unija

FURS – Finančna uprava Republike Slovenije

ICO (ang. Initial coin offering) – začetna ponudba žetonov

IPO (ang. Initial public offering) – začetna javna ponudba

IT – Informacijska tehnologija

PWC – PricewaterhouseCoopers

SEC (angl. Securities and Exchange Commission) – Komisija za vrednostne papirje

SOX (ang. Sarbanes Oxley Act) – zakon Sarbanes Oxley

SRS – Slovenski računovodski standardi

MSRP – Mednarodni standardi računovodskega poročanja

MRS – Mednarodni računovodski standardi

OZ – Obligacijski zakonik

ZBan – Zakon o bančništvu

ZDDOIFI - Zakon o davku od dobička od odsvojitve izvedenih finančnih instrumentov

ZDDPO - Zakon o davku od dohodkov pravnih oseb

ZDoh – Zakon o dohodnini

ZDP – Zakon o deviznem poslovanju

ZPlaSS - Zakon o plačilnih storitvah in sistemih

ZTFI - Zakon o trgu finančnih instrumentov

ZUE – Zakon o uvedbi eura

UVOD

Kriptovalute so relativno nova tehnološka in ekonomska iznajdba, ki je z izredno hitrostjo pretresla svet v preteklih dveh letih. Danes so najpomembnejše kriptovalute, kot sta bitcoin in ether, del poslovnega vsakdana podjetij, bodisi kot špekulativna naložba bodisi kot valuta, ki jo uporabljajo pri vsakdanjem poslovanju. Ravno uporaba kriptovalut pri vsakdanjem izvajanju transakcij je ideološka ideja snovalcev kriptovalut, ki so si jih zamislili kot svoboden način izvajanja transakcij, brez nadzora in interveniranja bank ter regulatorjev. Tak idealistični pristop snovalcev kriptovalut postavlja tudi večino njihovih lastnosti, ki so se izkazale za tvegane in nepredvidljive. Zaradi njihovega neslutenega razvoja in hitre rasti njihove vrednosti ob koncu leta 2017 so kriptovalute postale tudi zelo priljubljena naložba za najrazličnejše sklade in družbe, ki morajo kriptovalute, tako kot ostala sredstva, zaradi zakonskih zahtev in uporabnosti njihovih računovodskih izkazov tudi pravilno izkazati ter ovrednotiti. Številne unikatne lastnosti kriptovalut predstavljajo za uporabnike izzive, in sicer od novih regulatornih problemov, do številnih izzivov pri revidiranju kriptovalut.

Osnovni problem računovodenja in revidiranja kriptovalut izhaja iz trenutne zakonske praznine, saj ne na nivoju Slovenije ne na nivoju Evropske unije predpis, ki bi celovito urejal področje kriptovalut, trenutno še ne obstaja. V zadnjem času so različne institucije poizkušale to pravno praznino zapolniti z navodili ali pravilniki, ki imajo lahko v najboljšem primeru za uporabnike kriptovalut pogojne posledice. Na računovodskem področju v Sloveniji je celovit pregled računovodske obravnave kriptovalut pripravila mag. Bajuk Mušič (2017, str. 20–32), ki je definirala možne namene uporabe kriptovalut in možnosti njihovega izkazovanja v sklopu bilance stanja, ukvarjala pa se je tudi z vprašanjem primernosti uporabe posameznega izkazovanja glede na namen uporabe kriptovalut. Analiziranja tega problema so se lotile tudi številne mednarodne revizijske hiše (Ernst & Young, 2018; PWC, 2017; Grant Thornton International Ltd, 2018). Ključna ugotovitev vseh je, da je kriptovalute težko enoznačno umestiti v posamezno postavko računovodskih izkazov in da je najprimernejša razvrstitev med zaloge in finančna sredstva.

Osnovni namen revizije računovodskih izkazov je revizorjevo poročanje razumnega zagotovila lastnikom, o pravilnosti računovodskih izkazov organizacije ter njihova skladnost z zakonskimi in usmeritvami aplikativnih standardov. Iz navedenega namena izhaja tudi ključna lastnost revizije, ki je pridobitev razumnega zagotovila oziroma zagotovitev, da so računovodski izkazi brez pomembnih nepravilnosti, ki bi imele vpliv na odločitev uporabnika računovodskih izkazov (BPP Learning Media, 2017; Koletnik, 2009). Pomembne nepravilnosti v izkazih zato označimo s tveganji, iz česar izhaja druga pomembna problematika revidiranja kriptovalut. Tveganja izhajajo bodisi iz pravne in davčne neurejenosti kriptovalut, iz njihovih ekonomsko-tržnih lastnosti, med katerimi je najpogosteje omenjeno izredno visoko nihanje vrednosti (volatilnost) posamezne kriptovalute, bodisi iz tehničnih problemov, ki so posledica uporabe verige blokov (angl. blockchain).

Osnovni namen magistrske naloge je obravnavati problematiko revidiranja kriptovalut v računovodskih izkazih. Namenjena je računovodjem, saj jim predstavlja osnove kriptovalut in jih seznanja s tveganji, s katerimi se soočajo družbe, ki pri svojem poslovanju uporabljajo kriptovalute. Ob posameznih tveganjih so predstavljene tudi notranje kontrole, s katerimi jih lahko podjetja preko internih procesov obvladujejo. Magistrska naloga je namenjena tudi revizorjem, ki se poleg tveganj iz okolja, ukvarjajo tudi s tveganji notranjekontrolnega okolja in tveganji potencialne možnosti za prevare s strani revidirancev ter nepravilnosti, ki jim lahko računovodje nevede podležejo zaradi nepravilnih razlag posameznih pojmov ter podcenjevanja nevarnosti, ki izhajajo iz okolja. Konkretni primeri tveganj in načinov za njihovo obravnavo, ki so v pomoč tako računovodjem kot revizorjem, so prikazani v tretjem poglavju. V tem poglavju so navedeni tudi postopki revidiranja, ki so specifični za revidiranje kriptovalut, saj zaradi njihovih specifičnih lastnosti ne moremo zagotoviti primerne potrditve s standardnimi revizijskimi postopki.

Cilj magistrske naloge je na osnovi literature identificirati in preučiti lastnosti, spremembe in trende s področja revidiranja kriptovalut, ki bodo v prihodnosti omogočali ohranjanje zaupanja v finančni trg. V začetnem delu magistrske naloge imam namen raziskati in predstaviti tehnično in pravno ozadje kriptovalut, iz katerega izhajajo njihove ekonomske lastnosti. Iz posebnosti, ki so eksplicitno značilne samo za kriptovalute, izhajajo tudi dodatna tveganja, ki jih s standardnimi revizijskimi postopki ni mogoče celovito nasloviti in pridobiti zadostnega zagotovila o pravilnosti njihovega izkazovanja. Z magistrsko nalogo želim predstaviti tehnična vprašanja, vezana na pravilno izkazovanje kriptovalut, prednosti in slabosti kriptovalut in tveganja, ki izhajajo iz specifičnih lastnosti kriptovalut, pri čemer se bom osredotočil zlasti na tista tveganja, s katerimi se srečujemo pri njihovi računovodski obravnavi. V vseh predstavljenih tematikah ciljno navajam uporabno vrednost za računovodje, revizorje in uporabnike računovodskih izkazov.

V prvem delu magistrskega dela bo predstavljena in obravnavana problematika kriptovalut, ki ji bo v drugem delu sledila predstavitev revidiranja. Predstavitev bo zasnovana na pregledu domače in tuje literature. Drugi del magistrske naloge bo zasnovan na kritičnem pregledu literature, ki se nanaša neposredno na revidiranje postavk kriptovalut, s poudarkom na tveganjih. Različni avtorji opredeljujejo številna tveganja, povezana s kriptovalutami, in navajajo različne metode njihovega obvladovanja, zato bo drugi del zasnovan kot sinteza različne literature. Z namenom lažjega razumevanja vrednosti dobrega poznavanja kriptovalut in z njimi povezanih tveganj, bom v tem delu kritično predstavil primere dejanskih dogodkov s področja kriptovalut.

1 KRIPTOVALUTE

1.1 Predstavitev kriptovalut

Kriptovaluta je po definiciji Evropske centralne banke »digitalna predstavitev vrednosti, ki ni izdana s strani centralne banke, kreditne institucije ali institucije za izdajo e-denarja in je lahko v nekaterih primerih uporabljena kot alternativa denarju« (European Central Bank, 2015a). Ključno za razumevanja kriptovalut je razumevanje lastnosti in namena denarja. Denar se že več tisočletij uporablja z namenom izmenjave dobrin. Denar se je skozi čas spreminjal predvsem zaradi poenostavitve njegovega prenosa ali transporta in posledičnega razvoja finančnega sistema. Zgodovinsko gledano je bil prva oblika denarja t. i. blagovni denar, ki je bil pravzaprav blago, ki je bilo široko sprejeto in je imelo svojo lastno vrednost. V različnih kulturah so to lahko bili različni »predmeti«, na primer kovanci iz dragih kovin, sol, tobak, kava ali pšenica. Zaradi kompleksnosti transporta in problema z direktno sprejemljivostjo takšnega denarja kot plačilnega sredstva se je v naslednji fazi razvil reprezentančni denar, ki sam po sebi nima vrednosti, vendar za njim stoji blago, za katerega je reprezentančni denar zamenljiv. Zgodovinsko je najpogostejši t. i. zlati standard, pri katerem so centralne banke za denar v obtoku jamčile z zalogo zlata. Danes so vse sodobne valute t. i. fiat denar, katerega vrednost izhaja iz same pravice do uporabe denarja kot uradnega plačilnega sredstva. Ohranjanje vrednosti fiat denarja je naloga centralnih bank, iz česar izhaja zaupanje v vrednost valute. Da lahko neko blago ali sredstvo tretiramo kot denar, mora izpolniti tri kriterije: denar je sredstvo izmenjave, za katerega lahko prejmemo neko drugo sredstvo, je obračunska enota, v kateri izkazujemo ceno drugega blaga, in je hranitelj vrednosti (European Central Bank, 2015b). Na podlagi navedenih funkcij denarja lahko kriptovalute danes v najboljšem primeru pogojno uvrstimo med denar, saj zaradi nereguliranosti s strani institucije, podobne centralni banki, njihova vrednost močno niha, poleg tega se v njih ne izkazuje cene drugega blaga.

Kljub zgoraj opisanemu trenutnemu neizpolnjevanju pogojev za kategorizacijo kriptovalut med denar so kriptovalute postale del našega vsakdana, saj danes, po podatkih strani CoinMarketCap.com, obstaja več kot 1900 različnih kriptovalut, ki imajo v ozadju zelo različne zasnove. Kriptovalute delimo na kripto kovance, alternativne kovance in kriptožetone. Kriptokovanci (ang. cypto coins) izhajajo iz blockchaina in delujejo na podlagi neodvisne platforme. Mednje sodi tudi bitcoin, ki je najpogostejši predstavnik kriptovalut. Za druge kovance se pogosto uporablja izraz aternativni kovanci (ang. Altcoins), saj so alternativa bitcoinu. Druga veja kriptovalut so kriptožetoni (ang. Crypto tokens), ki so kriptovalute, ki za svoje delovanje potrebujejo podlago druge platforme (na primer Bitcoin ali Etherum). Kripto žetoni so izdani preko začetne ponudbe kovancev, ki je bolj poznana pod kratico ICO (ang. Initial Coin Offering), pri kateri izdajatelj izda žetone v zameno za druga sredstva. Zelo pogosto so sredstva menjave druge kriptovalute.

Na osnovi predstavljenega se postavlja vprašanje, kako z ekonomskega vidika pravilno kategorizirati kriptovalute. V strokovni literaturi se kot rešitev omenjene dileme pogosto uporablja termin kriptosredstva, ki zajema vse kriptovalute, kripto kovance in kripto žetone (EY, 2018).

1.2 Idejni koncept kriptovalut

Nastanek kriptovalut je tesno povezan z nezadovoljstvom s trenutnim finančnim sistemom in željo po stvaritvi idealnega sistema, ki bi omogočal hitre, poceni transakcije med osebami po celem svetu, brez nadzora s strani uradnih institucij. Pomemben katalizator za razvoj kriptovalut je bila zadnja finančna kriza leta 2008, ko je med ljudmi narastlo nezaupanje do trenutnega finančnega sistema, s poudarkom na nezaupanju in nezadovoljstvu nad delovanjem centralnih in komercialnih bank, ki omogočajo delovanje celotnega finančnega sistema in ga zaradi tega tudi obvladujejo (Gupta, 2017).

Nakamoto (2018) v dizeraticiji z naslovom *Bitcoin: a Peer-to-Peer Electronic Cash System* obravnava probleme tradicionalnega finančnega sistema. Kot bistven problem tradicionalnega sistema izpostavlja reverzibilnost transakcij, saj lahko znotraj sistema pride do transakcij, pri katerih se (zaradi različnih razlogov) plačnik in prejemnik o višini ali podlagi transakcije ne strinjata. V tem primeru banka ali druga finančna institucija odigra vlogo mediatorja, ki odloča o tem, ali je zahteva po zavrnitvi transakcije upravičena ali ne. Posledica so dodatni stroški, ki nastanejo, ker finančne institucije opravljajo tudi funkcijo mediatorja. Mediatorska funkcija finančnih institucij je nujna za delovanje sistema, saj v digitalnem svetu med kupcem in prodajalcem ni zadostnega zaupanja. Zaradi nezaupanja, ki izhaja iz možnosti, da bi kupec transakcijo preklical, prodajalec kupcu ni pripravljen posredovati blaga, preden prejme plačilo. Zaradi obojestranskega zaupanja v finančne institucije pa to nezaupanje izgine. Kriptovalute predstavljajo sistem, v katerem je transakcijo nemogoče preklicati, zato se lahko prodajalec neovirano zanaša na njeno izvedbo. Uporabniki lahko zaupajo drug drugemu in lahko iz transakcije izločijo mediatorja (finančno institucijo) in tako prihranijo pri stroških (Nakamoto, 2008).Poleg tega, da lahko izločitev posrednika pomembno poceni transakcijske stroške, lahko tudi pomembno zmanjša čas, potreben za izvedbo transakcije v mednarodnem poslovanju, kjer že transakcije znotraj Evropske unije (v nadaljevanju EU) pogosto trajajo več kot en dan, medtem ko lahko transakcije v nekatere dele sveta trajajo tudi teden dni. V trenutnem finančnem sistemu sta čas in cena transakcije močno povezani s pregledi transakcij, ki jih mora finančna institucija izvesti, da zadosti lokalni zakonodaji (na primer pregled transakcij zaradi preprečevanja pranja denarja ali prepovedi poslovanja z določenimi državami zaradi embarga). Sistem kriptovalut takšno regulacijo onemogoča, saj ni centralnega nadzornega organa, ki bi lahko postavljal pogoje in preprečil izvršitev transakcije. S tem zagovorniki kriptovalut izpostavljajo svobodo v danes močno reguliranem svetu. Naslednja, med zagovorniki kriptovalut najpogosteje izpostavljena prednost kriptovalut, je omejenost števila kovancev, ki jih lahko narudarimo in damo v obtok. Fiat denar deluje na podlagi popolnega zaupanja v

finančni sistem in v samo vrednost denarja, ki s časom upada zaradi inflacije. Skeptiki trdijo, da bo vrednost fiat denarja izničena, saj fiat denar nima kritja in ker se število enot denarja neprestano in brez omejitve povečuje. Del zagovornikov kriptovalut trdi, da vrednost vseh predmetov, katerih količina je omejena, raste (na primer zlato in druge plemenite kovine), kar velja tudi za kriptovalute, ki zaradi sistemske omejenosti števila enot nimajo možnosti povečevanja njihovega števila v neskončnost.

Navedene prednosti kriptovalut izhajajo iz stališča prebivalcev razvitega sveta, kjer se lahko zanesemo na državo in finančne institucije, da bodo izvršile svoje funkcije, kot je pričakovano in določeno z zakonodajo. Pozabljamo pa, da se v večjem delu sveta ljudje ne morejo zanesti na delovanje finančnih institucij in države kot zanesljivega in varnega partnerja. Zaradi nezaupanja v finančni sistem v teh državah ljudje ne hranijo denarja na bankah in ga ne morejo prosto nakazati ter s tem pospeševati trgovine in ekonomske aktivnosti. Kriptovalute lahko tem ljudem omogočijo poslovanje, ki je za nas, prebivalce razvitih držav, samoumevno in je pomembno prispevalo k naši blaginji in razvitosti (Gates, 2017).

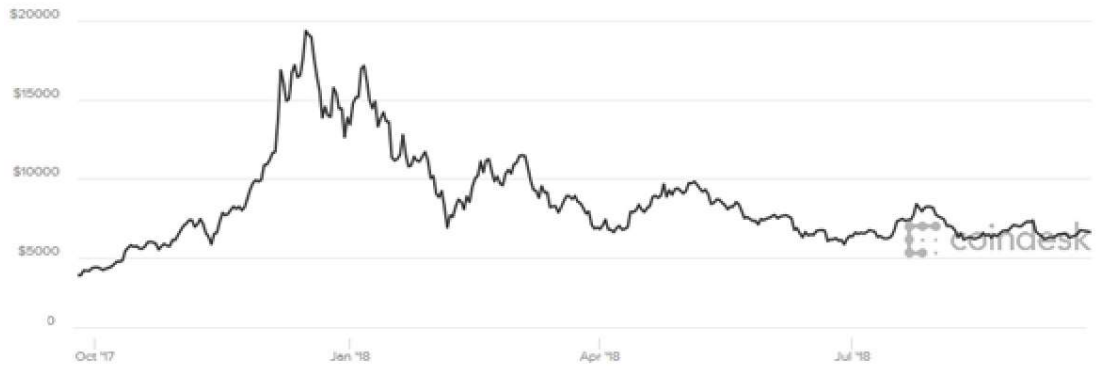
1.3 Predstavitev pomembnih kriptovalut

1.3.1 Bitcoin

Zgodovina kriptovalut je tesno prepletena z najbolj znano, najpomembnejšo in tudi prvo kriptovaluto, imenovano bitcoin. Prvi bitcoin je 3. januarja 2009 narudaril, javnosti neznan, ustanovitelj Bitcoina Satoshi Nakamo in ga nato 12. januarja prenesel s prvo transakcijo kriptovalute, ko je prvih 10 bitcoinov poslal programerju Halu Finneyu. Satoshi Nakamoto je novembra 2008 idejni koncept Bitcoina predstavil v svoji dizertaciji z naslovom Bitcoin: A Peer-to-Peer Electronic Cash System. Z Bitcoinom je svet pridobil prvi odprtokodni sistem, ki je dovolj robusten, da omogoča vzpostavitev soležniške valute (ang. peer to peer currency), ki lahko deluje v popolnoma neodvisnem virtualnem svetu. Ideologija na kateri sloni bitcoin je, da bi omogočal popolnoma nenadzorovan in svoboden plačilni sistem. Bitcoin se je spreminjal in razvijal, saj so bile pri njegovem delovanju ugotovljene nepravilnosti, ki so bile nato s popravki odpravljene, zato danes govorimo o verziji Bitcoina 0.16.3. Najbolj znana nadgradnja Bitcoina je po vsej verjetnosti verzija 0.8, ki je bila implementirana marca 2013. Ob prehodu na to verzijo je prišlo do neželene delitve blockchaina v ozadju, saj računalniki, ki so še vedno delovali na predhodnem sistemu, niso sprejeli novih blokov verzije 0.8. Po šestih urah takšnega delovanja so razvijalci ponovno prešli na prejšnjo verzijo 0.7 in s tem nadaljevali s prvotno serijo blokov. Poleg neželenih delitev verige, imenovanih vilice (ang. fork), je bilo tekom let implementiranih tudi več načrtovanih vilic, s katerimi so nastale variacije Bitcoina, kot sta Bitcoin Cash in Bitcoin Gold.

Bitcoin je daleč najbolj razširjena kriptovaluta, saj s tržno kapitalizacijo v višini 114 milijard ameriških dolarjev (v nadaljevanju USD) (na dan 24. september 2018) predstavlja več kot polovico vrednosti vseh kriptovalut v obtoku. Bitcoin je tudi sinonim za kriptovalute, saj je daleč najpriljubljenejša kriptovaluta, ko govorimo o vsakodnevni rabi za transakcije, saj se število lokacij, ki sprejemajo bitcoin, nenehno povečuje. Med prvimi pomembnimi podjetji, ki so kot plačilno sredstvo začela sprejemati bitcoin, je Microsoft, ki omogoča nakup iger in dodatkov v spletnih trgovinah Xbox in Windows store. Podjetja, ki danes sprejemajo bitcoine, so med drugim tudi Wikipedia, KFC, Bloomberg in T-Mobile. Najbolj zagreti zagovorniki bitcoina trdijo tudi, da že lahko živijo izključno z bitcoin transakcijami.

Slika 1: Gibanje vrednosti bitcoina v obdobju od oktobra 2017 do novembra 2018



Vir: CoinDesk (2018).

1.3.2 Ethereum

Ethereum je druga najbolj razširjena kriptovaluta, s skupno vrednostjo kapitalizacije kriptovalute v višini 23,5 milijarde USD. Ethereum tehnično deluje na enakih principih kot Bitcoin – deluje na osnovi blockchaina, ustvarjanje novih enot poteka z rudarjenjem, z njim se trguje in plačuje na sistemu Ethereum. Na tem mestu se podobnost z Bitcoinom konča, saj Ethereum poleg plačilnega sistema omogoča tudi razvoj novih funkcionalnosti na enotni blockchain platformi. Ethereum omogoča potrjevanje pogodb preko blockchaina in na ta način opravlja overjanje pogodb, kot jih danes opravljajo notarji (Bizant in drugi, 2018). Idejno zasnovo Ethereuma je postavil Vitalik Buterin, čigav namen ni zgolj formiranje plačilne platforme, kar je ustvaril Bitcoin. Vitalik je želel vzpostaviti blockchain platformo, ki omogoča preprosto uporabo za formiranje pametnih pogodb. Pametne pogodbe so virtualne pogodbe, ki ob uporabi blockchaina omogočajo postavljanje dodatnih pogojev v transakcijo. Šele, ko so vsi pogoji izpolnjeni se transakcija avtomatsko izvede. Tak primer je prenos nepremičnine, kjer Ethereum nadomešča notarja, saj bo transakcija izvedena šele, ko bodo izpolnjeni določeni pogoji – zagotovitev denarja in vpis nepremičnine v zemljiško knjigo oziroma drug register. Na ta način lahko nadomestimo marsikaterega posrednika, ki je danes nujen za izvršitev določenega posla. Primer uporabe pametnih pogodb je lahko tudi

ponudnik storitev prevoza, kot sta Uber ali Cameo. S pametno pogodbo se lahko uporabnik in prevoznik zanaseta, da bosta ob koncu opravljene storitve prejela pričakovano.

Druga lastnost Ethereuma je, da je na njem mogoče prosto formirati nov kriptožeton. Koda za njegovo formiranje je prosto dostopna na internetu, hkrati pa obstajajo tudi druge internetne aplikacije, ki formiranje kriptožetona skrajšajo na le nekaj klikov. Sistem, ki stoji za valuto, torej predstavlja izredno popularno platformo za formiranje nadaljnjih pametnih pogodb, ki se lahko uporabljajo za najrazličnejše namene, zelo pogosto tudi zgolj za namene zaslužka nekaterih uporabnikov.

1.3.3 Ripple

Tretja kriptovaluta po tržni kapitalizaciji je ripple, ki prav tako kot bitcoin in ether deluje na osnovi blockchaina, vendar pa za razliko od njiju deluje v centraliziranem sistemu, ki ga nadzira istoimenska organizacija. Namen Rippla je ustvariti sistem, ki poudarja nekatere ključne prednosti kriptovalut, ki so komplementarno uporabne za delovanje bank in bančnega sistema in ne suplement za njega. Ripple omogoča izredno hitre in poceni transakcije znotraj sistema, kar omogoča bankam prenose med državami, ki v tradicionalnem bančnem sistemu niso mogoči. Povprečen čas potrditve transakcije z Ripplom znaša samo 3,7 sekunde (pri Bitcoinu je ta čas 168 minut), zaradi česar ga že uporabljajo nekatere banke za testno izvrševanje prenosov med državami. Ker ripple deluje preko centralnega sistema, ga tudi ni mogoče rudariti, vendar ima v obtoku prav tako fiksno število enot. Število enot ne narašča z rudarjenjem, pač pa z aktiviranjem novih enot s strani organizacije Ripple. Zaradi fokusiranja Rippla na bančni sistem, ta sistem ni razširjen med fizičnimi osebami, ki bi ga uporabljale pri vsakdanjih transakcijah. Zaradi centraliziranosti sistema se pojavljajo nekatera tehnična vprašanja, vezana na varnost omrežja, predvsem kako preprečiti delitev kriptovalut na več vej ter morebitnih naknadnih poneverb transakcij, saj celotno delovanje nadzoruje ena sama organizacija, ki ni podvržena regulaciji.

1.4 Blockchain

Blockchain (slov. veriga blokov) je tehnična osnova, na kateri temeljijo vse najbolj poznane kriptovalute. Že samo ime ponazarja dejansko tehnično osnovo delovanja. Osnova blockchaina je tako imenovani blok, ki predstavlja transakcijo. Pod terminom transakcija razumemo posredovanje kriptovalute enega uporabnika drugegemu. Bloki si vedno medsebojno sledijo v vrstnem redu generiranih transakcij in se vedno navezujejo na predhodno transakcijo. Tako se blok št. 15 navezuje na blok št. 14, ta pa na blok št. 13 itd. Ta lastnost omogoča zaporedno potrjevanje transakcij in celotnemu sistemu zagotavlja informacijo, pri kom se nahaja posamezen kovanec. Tak sistem onemogoča, da bi en uporabnik določeno enoto ali kovanec uporabil v dveh ločenih transakcijah in na ta način zlorabil sistem in pridobil korist. Bloki si sledijo v vrsti oziroma se verižijo, iz česar izhaja drugi del imena – »chain« – ki v angleščini pomeni veriga. Ključna novost blockchaina je,

da gre za bazo podatkov, ki se nahajajo v verigi in so znani vsem imetnikom verige, kar je v nasprotju s trenutnim načinom delovanja baz podatkov, kjer se podatki nahajajo na enem mestu, do katerega vsi uporabniki podatkov dostopamo za njihovo uporabo (Gates, 2017).

Takoj ob vzpostavitvi blockchaina se je pojavilo tudi vprašanje glede morebitnih prevar imetnikov enot, ki izhajajo iz poizkušanja izigravanja sistema z namenom pridobitve raznih koristi. Prva lastnost, ki preprečuje manipuliranje s preteklimi bloki, je, da se določene transakcije, ko je enkrat trajno potrjena, ne da nikoli več spremeniti. Sprememba transakcije je nemogoča, saj so vsi bloki med seboj povezani, torej bi bilo potrebno za spremembo posameznega bloka spremeniti vse bloke v verigi. Takšna sprememba je praktično izredno težko izvedljiva, saj bi zanjo potrebovali izjemno velike računalniške zmogljivosti. Iz tega izhaja, da se transakcije praktično ne da preklicati, ko je bila enkrat potrjena. Pri naslednji možnosti izigravanja sistema gre za to, da bi nekdo poizkusil izvesti dveh transakciji ob odpovedi zgolj enemu kovancu. Preprečitev tovrstnega izigravanja sistema je omogočena s tem, da je vsaka transakcija takoj posredovana v potrditev vsem drugim osebam v omrežju. Te osebe ob prejemu informacije o transakciji izvedbo transakcije potrdijo samo, če izpolnjuje določene pogoje. Tipično velja, da mora transakcijo potrditi določen delež vseh oseb v mreži (pri Bitcoinu je to 50 %). S tem se doseže, da potrjevanje transakcij ni preveč enostavno, saj bi se s tem povečala možnost za prevaro, hkrati pa se omogoča razumna hitrost delovanja sistema. Ker je veriga dostopna vsem uporabnikom, tudi vsi vidijo, kakšne so posledice opravljene transakcije. Po potrditvi lahko poljuben posameznik izdela nov blok, ki bo dodan v verigo. Osebe, ki potrjujejo transakcije, za opravljeno delo prejmejo nagrado v obliki novoustvarjenih kovancev. Za postopek potrjevanja transakcij uporabljamo izraz rudarjenje. Pri rudarjenju gre v praksi za izpolnjevanje kompleksnih matematičnih algoritmov, katerih končni produkt je nov blok. Formiranje blokov je zahteven računalniški proces, ki porabi veliko energije in zahteva visoka vlaganja v strojno opremo, zato je nagrada v obliki novih enot kriptovalut plačilo za opravljene stroške. Pomembna tematika formiranja blokov je tudi potrdilo o opravljenem delu (ang. Proof of work), s katerim lahko kdorkoli, ki je vključen v mrežo, preveri, ali je formiranje bloka resnično opravila oseba, ki trdi, da ga je ustvarila. Gre za pravilo kompleksnih algoritmov, ki jih je nato ob razvozlanju enostavno preveriti. Najlažje je to ponazoriti z otroškim šifriranim sporočilom (določene črke so zamenjane z drugimi znaki). Takšna sporočila so ob poznavanju pravilne kombinacije črk enostavno in hitro berljiva, vendar je za ugotovitev pravilnih kombinacij ali dekriptiranje potrebnega veliko truda in časa (Gates, 2017).

Besedo blockchain je prvič uporabil legendarni utemeljitelj Bitcoina Satoshi Nakamoto v opisu izvirne programske kode Bitcoina. Tudi zato je zgodovina blockchaina tesno prepletena z zgodovino Bitcoina. Blockchain je bil v obliki, v kakršni ga poznamo danes, sicer res utemeljen z Bitcoinom, vendar zgodovina osnovnih teorij o ključnih lastnostih blockchaina sega še bolj v preteklost. Prvi zametki segajo že v leto 1982, ko je David Chaum v dizertaciji z naslovom Blind Signatures for Untraceable Payments zasnoval teorijo o digitalnih podpisih, s katerimi lahko potrdimo, da je dokument skladen z originalom, kljub

temu pa ostane njegova vsebina skrita. Gre za utemeljitev kriptografskega podpisa, ki ga danes uporabljajo kriptovalute. Chaumov predlog je vseboval tudi idejo o digitalni valuti, ki bi bila neizsledljiva, imela pa bi tudi varovalo, ki bi onemogočalo, da bi bila večkrat porabljena in na ta način zlorabljena. Chaum je bil tudi eden izmed ustanoviteljev družbe DigiCash, ki je bila vzpostavljena na podlagi te ideje. DigiCash je bila prva sodobna valuta, ki je delovala mimo bank in regulatorjev, vendar je družba neslavno propadla leta 1998. Naslednja pomembna lastnost, uporabljena v blockchainu, je bila utemeljena leta 1997, ko je Adam Back predlagal uporabo t. i. principa »proof of work« na področju e-pošte. Vsiljena pošta je takrat pridobivala na veljavi, predlog o zmanjšanju njenega obsega pa je zajemal, da bi moral biti vsak elektronska pošta pred pošiljanjem enkriptiran na način, na katerega so danes enkriptirani bloki v blockchainu. V opisu e-sporočila bi bil ključ, s katerim bi ga lahko uporabnik enostavno odklenil in odprl, medtem ko bi na drugi strani od pošiljatelja zahteval rešitev zahtevnega algoritma. Pošiljanje vsiljene pošte postane na ta način z vidika procesorske moči bistveno zahtevnejše. Tretjo pomembno teorijo potrebno za vzpostavitev blockchaina je predstavil Nicka Szabo leta 1998, ki je predlagal formiranje platforme za valuto, imenovano bit gold, ki bi slonela na reševanju kriptografskih ugank, ki bi jih potrjevale druge osebe v mreži. Po potrditvi rešitve in strinjanja z opravljeno transakcijo bi se ta zapisala v omrežje in iz nje bi izhajala naslednja uganka, ki bi ob rešitvi dodala naslednji člen verige. Szabo je izpostavil tudi problematiko podvojenega zapravljanja enot. Ideja o bit goldu ni bila nikoli realizirana, ostala je zgolj na ravni teorije.. Prvi, ki je je vse opisane teorije združil v eno, je Wei Dai, ki je že leta 1998 v članku z naslovom B-money, an Anonymous, Distributed Electronic Cash System predlagal vpeljavo kriptovalut, ki delujejo na način, kot ga poznamo danes, in zajema:

- opravljeno računalniško delo in potrdilo o opravljenem delu,
- nagrade za osebo, ki zaključi računalniško delo,
- skupinsko knjigo, ki jo lahko potrjujejo in posodabljajo vsi člani,
- prenos sredstev znotraj skupinske knjige in potrditev transakcij s kriptografsksimi šiframi,
- vse transakcije so podpisane z digitalnimi podpisi, ki uporabljajo javno kriptografsko kodo, in potrjene s strani mreže.

Teoretične osnove Weia Daia je s praktičnimi rešitvami podkrepil Stefan Konst, nato je celotno idejo udejanjil Satoshi Nakamoto, najprej v internetnem članku z naslovom Bitcoin: A Peer-to-Peer Electronic Cash System in nato 3. januarja 2008 tudi s formiranjem prvega bitcoina (Gates, 2017). Zgodovina bitcoina je predstavljena v poglavju Predstavitev pomembnih kriptovalut.

1.5 Pravna podlaga kriptovalut

Eno izmed pomembnejših vprašanj, vezanih na kriptovalute, je njihova pravna ureditev. Kriptovalute so bile večino svoje kratke zgodovine marginalno finančno sredstvo, zaradi

česar organi nadzora niso zaznali potrebe za njihovo regulacijo. Predvsem zaradi hitre rasti vrednosti in razširjenosti kriptovalut, zlasti v času rasti njihove vrednosti leta 2007, so številne odgovorne institucije začele s spremljanjem in reguliranjem kriptovalut. V naslednjih odstavkih bom prikazal možnosti za formalnopravno uvrstitev kriptovalut v zakonodajo Republike Slovenije. Ob tem je potrebno poudariti, da se kriptovalute med seboj razlikujejo, zato lahko nekatere klasificiramo v isto kategorijo, medtem ko drugih ne moremo.

Prva možnost za obravnavo kriptovalut, ki izhaja iz njihovega imena, je, da jih razumemo in klasificiramo kot denar oziroma natančneje kot tujo valuto (devizo). Zakon o deviznem poslovanju (ZDP-2, Ur. l. RS, št. 16/08, 85/09 in 109/12) definira pojem tuja valuta na sledeč način: »Tuja gotovina so bankovci in kovanci v tuji valuti, ki jih je izdala centralna banka ali država.« Ker kriptovalut ne izdajajo centralne banke in za njimi ne stojijo države, ampak jih izdajajo pravne ali fizične osebe, jih ne moremo uvrstiti med denar. Stališče, da kriptovalute niso tuja valuta, je zavzela tudi Banka Slovenije. Iz tega stališča izhaja tudi, da za menjavo kriptovalut ni potrebno pridobiti dovoljenja Banke Slovenija za opravljanje menjalniških poslov po ZDP-2.

Druga možnost za klasifikacijo kriptovalut je, da jih obravnavamo kot elektronski denar, ki je v Zakonu o plačilnih storitvah in sistemih (ZPlaSS, Ur. l. RS, št. 58/09, 34/10, 9/11, 32/12, 81/15, 47/16 in 7/18): »Elektronski denar je shranjena denarna vrednost v obliki terjatve imetnika elektronskega denarja do izdajatelja elektronskega denarja, ki:

- je v elektronski obliki, vključno z magnetno,
- jo izda izdajatelj elektronskega denarja na podlagi prejema denarnih sredstev za namen izvrševanja plačilnih transakcij,
- jo kot plačilno sredstvo sprejme oseba, ki ni izdajatelj elektronskega denarja.«

Kriptovalute imajo lastno obračunsko vrednost, zaradi česar jih ni mogoče šteti med nadomestke fiat valut. Za izpolnjevanja pogoja za fiat valuto bi morale izpolnjevati tri funkcije valut, ki so opisane v prvem poglavju. Stališče, da kriptovalute niso denar, sta zavzela tudi Banka Slovenije in Ministrstvo za Finance RS.

Naslednja možnost pravne klasifikacije kriptovalut je, da jih obravnavamo kot finančne instrumente. Možni finančni instrumenti so navedeni v Zakonu o trgu finančnih instrumentov (ZTFI, Ur. l. RS, št. 108/10 – uradno prečiščeno besedilo, 78/11, 55/12, 105/12 – ZBan-1J, 63/13 – ZS-K, 30/16, 9/17 in 77/18 – ZTFI-1), vendar jih ta opisno ne definira. Njihova definicija je zapisana v Zakonu o bančništvu (ZBan, Ur. l. RS, št. 25/15, 44/16 – ZRPPB, 77/16 – ZCKR, 41/17 in 77/18 – ZTFI-1) in pod finančne instrumente prišteva:

- pogodbe, ki eni stranki prinašajo finančno terjatev, drugi stranki pa finančno obveznost ali lastniški instrument,
- finančni instrument iz drugega odstavka 7. člena ZTFI,

- izvedeni finančni instrument,
- primarni finančni instrument,
- denarni instrument, pri čemer so instrumenti iz prve, druge in tretje alineje finančni instrumenti le, če njihova vrednost izhaja iz cene osnovnega finančnega instrumenta ali druge osnovne postavke, stopnje ali indeksa.

Po združitvi opredelitev obeh zakonov lahko sklenemo, da med finančne instrumente štejemo prenosljive vrednostne papirje, instrumente denarnega trga, investicijske kupone vzajemnih skladov, opcije, terminske pogodbe in podobne produkte. Kriptovalut ne izdajajo vzajemni skladi ali investicijske družbe, zato niso investicijski kuponi vzajemnih skladov. Prav tako tudi niso instrumenti denarnega trga, kamor štejemo komercialne zapise, potrdila o denarnem depozitu in zakladne menice. Na osnovi definicije bi lahko pri nekaterih kriptovalutah zavzeli stališče, da so prenosljivi vrednostni papirji (na primer nekateri kriptožetoni, ki nosijo lastniške ali dolžniške pravice), vendar je Ministrstvo za Finance RS odločilo, da kriptovalute niso finančni instrumenti.

Zaradi zelo popularnih začetnih ponudb kovancev (ICO), ki jih številni strokovnjaki označujejo kot novodobne začetne javne ponudbe (IPO), se pojavi tudi možnost označitve kriptovalut kot vrednostnih papirjev. Vrednostni papir je urejen v Obligacijskem zakoniku (OZ) kot: »Pisna listina, s katero se izdajatelj zavezuje, da bo izpolnil na njej zapisano obveznost njenemu zakonitemu imetniku.« Kriptovaluta bi lahko bila vrednosti papir samo ob predpogoju, da bi že ob sami izdaji bila klasificirana kot vrednostni papir, za kar mora izpolnjevati vse veljavne določbe za prvo javno izdajo vrednostnih papirjev, med katerimi je najbolj očitna priprava prospekta, ki ga mora odobriti Agencija za trg vrednostnih papirjev (v nadaljevanju ATVP). Poleg tega je potrebno poudariti še, da kriptovalute niso izdane kot pravna listina, kar je po Obligacijskem zakoniku pogoj za uvrstitev pod vrednostni papir. V nadaljevanju so predstavljene ključne razlike med postopkoma ICO in IPO. IPO je natančno definiran v Zakonu o trgu finančnih instrumentov. Medtem je iz primerjave v tabeli 1 razvidno, da je ICO popolnoma prepuščen ideji izdajateljev, kar močno poveča tveganje, saj je postopek v celoti odvisen od zaupanja v vlagatelja. Številne naložbe, ki izhajajo iz ICO, so zato zelo špekulativne narave.

V Sloveniji morajo po Zakonu o uvedbi eura (ZUE, Ur. l. RS, št. 114/06) vsa zakonita plačilna sredstva bodisi biti evro bodisi se glasiti na evro. Ker se kriptovalute ne glasijo na evro, niso zakonita plačilna sredstva. Lastnost zakonitega plačilnega sredstva je, da ga morajo sprejeti vsa prodajna mesta. Vendar zakon ne preprečuje in ne prepoveduje uporabe drugih sredstev v postopku izmenjave in njihove uporabe kot plačilnega sredstva. Med ta sredstva lahko zagotovo štejemo tudi kriptovalute, iz česar izhaja, da v Sloveniji sprejemanje kriptovalut za plačilo blaga ali storitve ni nelegalno.

Tabela 1: Primerjava IPO in ICO

Področje razlikovanja	**IPO**	**ICO**
Metoda izdaje	Uveljavljena infrastruktura finančnih trgov	Metoda veriženja blokov
Zaupanje	V izdajatelja vrednostnega papirja	V sam sistem veriženja blokov
Formiranje	Pravni posel, s katerim nastane finančni instrument	Matematični proces veriženja blokov
Pristojnosti in regulacija	Strog regulatoren postopek in kasnejši nadzor z visokimi pristojnostmi regulatorja	Zelo blaga regulacija, ki se je šele začela razvijati in urejati
Narava pravic	Določena bodisi kot lastniška bodisi kot dolžniška pravica	Zelo raznolika, vse je mogoče
Pravice do prihodkov	Obresti ali dividende, postopek za njihovo izplačilo je določen v zakonu	Izplačila, vezana na prihodke ali na sredstva od prodaje
Izdajatelj	Pravne osebe	Pravne in fizične osebe
Privabljanje investitorjev	Preko prospekta in letnih, polletnih, kvartalnih poročil	Oglaševanje preko spleta
Vlagatelji	Večinoma iz ozkega geografskega področja (država, regija)	Iz celega sveta
Investicije institucionalnih vlagateljev	Pomemben in ključen vlagatelj	Jih skoraj ni
Začetna cena	Cena žetonov je zaradi tveganja praviloma nižja kot cena primerljivo vrednotenih vrednostnih papirjev	
Volatilnost	Nižja	Visoka

Vir: lastno delo.

1.6 Davčna problematika kriptovalut

Poleg same formalnopravne uvrstitve kriptovalut v obstoječi pravni red se na vsakdanji ravni srečujemo tudi s problemom davčne obravnave kriptovalut. Osnovna ideja kriptovalut je bila uporaba v plačilnem prometu, vendar za današnjo razširjenostjo in številom transakcij stoji investicijska želja posameznikov. Zaradi različnih namenov uporabe kriptovalut je tudi Finančna uprava Republike Slovenije (v nadaljevanju FURS) izdala pojasnilo, kako obravnavati različne posle s kriptovalutami v trenutni pravni in davčni ureditvi.

Dohodki fizičnih oseb, pridobljeni z rudarjenjem kriptovalut, so zajeti v Zakonu o dohodnini (ZDoh-2, Ur. l. RS, št. 13/11 – uradno prečiščeno besedilo, 9/12 – odl. US, 24/12, 30/12, 40/12 – ZUJF, 75/12, 94/12, 52/13 – odl. US, 96/13, 29/14 – odl. US, 50/14, 23/15, 55/15, 63/16 in 69/17), saj gre po argumentaciji za dohodek iz opravljenega dela. Za rudarjenje se

šteje vso opravljeno delo potrjevanja transakcij kriptovalut. Najprej moramo razlikovati, ali gre za dohodek, prejet znotraj ali zunaj dejavnosti, saj je od tega odvisna nadaljnja obravnava. V kolikor gre za dohodek iz dejavnosti, se plača dohodnina po dohodninski lestvici. Za dohodek se šteje vrednost kriptovalute, ko je dohodek prejet, hkrati pa se od dohodka ne odštevajo stroški, povezani s pridobivanjem (nakup strojne opreme, strošek elektrike, izobraževanj ...). V praksi se pojavlja tudi posojanje procesorskega časa in moči osebam, ki se ukvarjajo z rudarjenjem. Dohodek se v tem primeru šteje med dohodke iz oddajanja premoženja v najem in ne pod dohodke iz rudarjenja. Če pa govorimo o izvajanju rudarjenja kot o dejavnosti organizacije, se mora posameznik temu primerno registrirati za izvajanje dejavnosti. V skladu s tem se tudi dohodnina obračuna kot razlika med prihodki in odhodki in od tega dobička se nato plača dohodnina. Tudi pri rudarjenju kriptovaut se lahko izračun obdavčljivega dohodka naredi na podlagi normiranih odhodkov (FURS, 2018).

Pri transakcijah s kriptovalutami je FURS obral zelo poenostavljeno obravnavo, saj je za vse kriptovalute predpisal davčno obravnavo po Zakonu o davku od dobička od odsvojitve izvedenih finančnih instrumentov (ZDDOIFI, Ur. l. RS, št. 65/08 in 40/12 – ZUJF), po katerem se davek obračuna od razlike med ceno ob odtujitvi in ceno ob pridobitvi. Davčna stopnja tega davka znaša 25 %, ampak se zniža, če imetnik sredstev ne proda v petih letih po pridobitvi (po 5 letih upade na 15 %, nato se vsakih nadaljnjih 5 let zniža za 5 %).

V kolikor se z rudarjenjem kriptovalut ali z njihovimi transakcijami ukvarja pravna oseba, se davek obračuna v skladu z ZDDPO-2, ki pa hkrati zahteva, da se sredstva, obveznosti in dogodki znotraj leta prikazujejo ali v skladu s Slovenskimi računovodskimi standardi ali v skladu z Mednarodnimi standardi računovodskega poročanja (MSRP). Pravilna obravnava znotraj teh standardov je pojasnjena v nadaljevanju naloge (FURS, 2018).

Pomembna tema je tudi davčna obravnava do davka na dodano vrednost (v nadaljevanju DDV). Samo rudarjenje je izvzeto iz obravnave po DDV, saj je valuta generirana iz sistema samega, zato ne gre za izmenjavo sredstev med dvema strankama. Hkrati te transakcije tudi ne moremo obravnavati kot provizijo, saj s potrditvijo transakcije rudar ne pridobi avtomatske pravice do nove enote kriptovalute, gre namreč za nagrado za opravljeno delo. Samo opravljeno delo rudarjenja je tekmovalna loterija, na katero posameznik nima vpliva, saj bo nov blok, ne glede na njegov vložek, dodan v verigo. Če bi rudar ob vsaki potrditvi transakcije prejel enoto kriptovalute, bi lahko to obravnavali kot plačilo za opravljeno storitev in v tem primeru bi bila transakcija obdavčljiva z DDV. Pri ICO obstajajo nekateri kriptožetoni, ki dajejo imetniku medd drugim tudi pravico do izvedbe storitve ali pravico do blaga. Če je storitev ali blago v znani količini vezano na kriptožeton, je ta obdavčen z DDV že ob izdaji, v primeru, da termin prenosa blaga ali izvedbe storitve ni znan, se z DDV obdavči ob izvedbi (FURS, 2018).

Prav tako so transakcije s kriptovalutami, če gre za storitev, zavezano za DDV, obvezane k obveznemu potrjevanju računov. Iz obveze potrjevanja so izvzeta samo neposredna nakazila z enega na drug transakcijski račun, kamor pa kriptovalute ne spadajo (FURS, 2018).

1.7 Prednosti in slabosti kriptovalut

Kontroverznost kriptovalut je izrazita predvsem zaradi velikega števila zagretih podpornikov na eni strani in nasprotnikov na drugi strani, ki zagovarjajo vsak svoja stališče glede (uporabnosti in potenciala) kriptovalut. Ključne prednosti navajam v spodnjih točkah:

- Transparentnost: transakcije so vidne vsem v mreži in jih ni mogoče (zelo težko) naknadno spreminjati ali brisati, kot je to mogoče v drugih sistemih.
- Delovanje brez posrednikov: izločanje posrednikov, ki niso vredni zaupanja, kot so banke v določenih državah, kjer je zaupanje finančnim institucijam nizko, omogoča izvajanje transakcij, do katerih v nasprotnem primeru sploh ne bi prišlo.
- Decentraliziranost: zmanjšuje verjetnost nedelovanja sistema zaradi tehničnih težav, možnost izgube podatkov ter tveganje vdora v omrežje.
- Varnost: transparentnost med udeleženci v mreži, kjer so vsa dejanja zavedena in prosto dostopna, znižuje verjetnost poizkusov zlorabe sistema.
- Širok uporabni potencial: kriptovalute so lahko široko uporabne za vse transakcije, ki so danes ovirane ali nedovoljene zaradi uvajanja nadzora nad sredstvi.
- Enostavno dostopna tehnologija: blockchain je prosto dostopen na spletu in z njegovo pomočjo ali na njegovi osnovi lahko vsako, ki poseduje potrebno znanje ustvari kriptovaluto. Dokaz za to so številne nove kriptovalute, ki so bile ustvarjene v zadnjih letih.
- Nižji stroški: stroški prenosov sredstev med računi, še posebej v mednarodnih transakcijah, so lahko podvrženi številnim ločenim transakcijam, ki lahko pomenijo zelo velike stroške. Kriptovalute omogočajo pocenitev takšnih transakcij.
- Višja hitrost transakcij: z izločitvijo posrednikov se izvajanje transakcij bistveno pohitri. Kriptovalute omogočajo prenos sredstev z enega na drug konec sveta v nekaj minutah ali urah.

Hkrati imajo kriptovalute tudi sledeče ključne slabosti:

- Pomanjkanje zasebnosti: mnoge kriptovalute ne skrivajo transakcij (med njimi tudi Bitcoin), zato so transakcije vidne vsem v mreži.
- Varnostna vprašanja: tako kot druga finančna sredstva lahko tudi kriptovalute ukradejo. Implementacija dodatnih varnostnih metod je lahko zapletena zaradi nepodpore večine članov mreže.
- So brez centralnega nadzora: spremembe znotraj posameznega blockchaina mora odobriti vsaj 50 %, lahko pa tudi 70 ali 80 % uporabnikov mreže. Nezmožnost nadziranja delovanja mreže je lahko zelo tvegana za določene poslovne uporabnike.
- Nevarnost napada z 51 % procesorske moči: velik del rudarjev valut deluje v državah, v katerih so ljudje nezaupljivi do države zaradi kriminala, neurejenega pravnega sistema ali pomanjkanja regulacije, zaradi nizke cene energije ali nizkih stroškov strojne opreme.

Koncentracija takšnih centrov lahko povzroči njihovo kolaboracijo ali zaseg s strani države in prevzem popolne kontrole nad kriptovaluto.

- Nepreizkušena nova tehnologija: blockchain je tehnologija, ki je bila v praksi uporabljena skoraj izključno za namene kriptovalut, kjer pa se ni izkazala kot vsakdanje uporabna.
- Stroški: blockchain za delovanje uporablja zelo razvejano in obsežno omrežje računalnikov, ki potrebuje za delovanje ogromne količine električne energije. Po določenih ocenah Bitcoin za svoje delovanje porabi toliko elektrike kot celotna država Danska.
- Nerazširjenost: blockhain zaradi zahtevnega formiranja blokov za delovanje potrebuje veliko procesorsko moč. Pri tem naletimo na omejitev možnega procesiranja transakcij. Bitcoin je, na primer, sposoben izvesti zgolj 7 transakcij na sekundo, medtem ko jih operater kreditnih kartic Visa za nemoteno delovanje omrežja na sekundo izvede več kot 20.000.
- Zaupanje, ugled in razumevanje: bitcoin in druge kriptovalute so bile pogosto uporabljene pri raznih ilegalnih transakcijah, povezanih s terorizmom, drogami in preprodajo drugih prepovedanih stvari, predvsem na temnem spletu (ang. dark web), kjer so kriptovalute lahko celo edino sprejeto plačilno sredstvo.
- Regulacija in integracija: proces integracije v obstoječe finančne sisteme bo dolgotrajen zaradi odstopanja delovanja kriptovalut od obstoječih smernic, po katerih deluje finančni sistem. Hkrati kriptovalute še niso regulirane. Prav tako se je regulacija izkazala za zelo zahtevno in na področje kriptovalut vnaša nestanovitnost.
- Navdušenje v letih 2017 in 2018: okoli blockchaina se je letih 2017 in 2018 vrtel val navdušenja, ki je vezan na njegov potencial. Pozablja pa se, da je blockchain zgolj baza podatkov, ki je v veliki meri nedokazana zunaj kriptovalut.

1.8 Izkazovanje kriptovalut v računovodskih izkazih

Finančni izkazi družb v Sloveniji lahko zasledujejo enega izmed dveh standardov, Slovenske računovodske standarde (v nadaljevanju SRS) ali Mednarodne standarde računovodskega poročanja (v nadaljevanju MSRP). V splošnem velja, da SRS uporabljajo manjše družbe, saj so manj kompleksni z vidika zahtevanih razkrivanj, medtem ko MSRP uporabljajo večje organizacije. V to smer se razvija tudi slovenska zakonodaja, ki pri večjih družbah (na primer zavarovalnice, banke, velike skupine) pogosto zahteva uporabo MSRP. Čeprav je razlikovanje v izkazovanju med SRS in MSRP izdatno, sami SRS po Zakonu o gospodarskih družbah (v nadaljevanju ZGD-1) ne smejo biti v nasprotju z MSRP. Ker noben standard še ni podrobneje opredelil problema kriptovalut, se bom v tej magistrski nalogi osredotočil na obravnavo z vidika MSRP.

Z računovodsko-finančnega vidika ključen problem predstavlja vprašanje, kako kriptovalute primerno izkazovati, saj obstaja več možnosti, pod katero postavko ta sredstva lahko izkažemo. V osnovi so kriptovalute sredstva, saj izpolnjujejo definicijo sredstev, organizaciji

bodo namreč prinašale bodoče koristi, in sicer v obliki apreciacije v vrednosti ali uporabe v transakcijah ter s tem zamenjave za denarna sredstva. Hkrati pa kriptovalute tudi obvladuje in jih pridobi s preteklim dogodkom, kot je nakup, rudarjenje ali plačilo izvedene prodaje. Kriptovalute se lahko med seboj razlikujejo v pravicah, ki jih ima njihov imetnik, prav tako jih družbe pridobijo z različnimi nameni. Na teh dveh osnovah se razlikuje tudi primerno izkazovanje kriptovalut v izkazih.

Kot v drugih poglavjih se bomo tudi pri računovodski obravnavi najprej ustavili pri morebitni primerni obravnavi kriptovalut kot denarja ali denarnih ustreznikov. Definicijo denarja ureja MRS 32 – Finančni instrumenti, ki določa, da je denar finančno sredstvo, sredstvo menjave in je podlaga za merjenje in pripoznanje transakcij v računovodskih izkazih. Polog v banki ali drugi finančni instituciji je tako terjatev do te institucije, na podlagi katere obstaja pravica do pridobitve denarja ali drugega podobnega instrumenta, s katerim lahko družba poravna svojo finančno obveznost upniku. Ker kriptovalute za poplačilo svojih terjatev sprejema malo družb, jih ne moremo tretirati kot plačilno sredstvo in jih za računovodske potrebe ne moremo izkazovati med denarnimi sredstvi. Drug razlog, zakaj kriptovalut ne moremo izkazati kot denar je, da bi lahko v primeru kriptovalute kot valute izkaze družbe izkazovali v kateri izmed kriptovalut. Valuto, v kateri vodimo računovodske evidence, imenujemo funkcijska valuta, valuto, v kateri prikazujemo izkaze, pa predstavitvena valuta. V primeru, da bi se družba odločila, da za funkcijsko valuto izbere kriptovaluto, bi vsa ostala sredstva morala izkazovati v kriptovaluti, kar bi zaradi velikega nihanja vrednosti povzročilo enormne prihodke in odhodke iz tečajnih razlik. Prav tako kriptovalute ne ustrezajo niti definiciji denarnega ustreznika, saj so denarni ustrezniki sredstva, ki so hitro in brez pomembnih izgub pretvorjena v denar, kar za kriptovalute zaradi nihanj v vrednosti ne moremo trditi (Bajuk Mušič, 2017; PWC, 2018).

Finančne naložbe ali finančni instrumenti so vse pogodbe, po katerih na eni strani nastane finančno sredstvo ene organizacije in finančna obveznost ali kapital druge organizacije na drugi strani. Pri kriptovalutah ne gre za pogodbeni odnos, saj imetnik kriptovalut ne more od nikogar zahtevati poravnave vrednosti kriptovalute. Kriptovaluta nastane z rudarjenjem in ne s pogodbenim odnosom. Ta situacija je podobna situaciji pri opredelitvi zlata, ki ima neko vrednost, vendar od nikogar ne moremo zahtevati, da nam to vrednost povrne, iz česar sledi, da ne gre za pogodben odnos (Bajuk Mušič, 2017). Vendar obstajajo tudi kriptožetoni, ki lahko izpolnjujejo karakteristike finančnega instrumenta, saj na njihovi podlagi imetnik pridobi pravico do preostalega premoženja po zaključku delovanja in/ali do denarnih prilivov tekom delovanja. Na podlagi teh karakteristik kriptovaluta izpolnjuje pogoje za uvrstitev pod kapitalski finančni instrument (EY, 2018).

Kriptovalute sicer ustrezajo nekaterim pomembnim karakteristikam neopredmetenega sredstva, med katerimi je ključna karakteristika ta, da je kriptovaluta nedenarno sredstvo brez fizičnega obstoja. Hkrati pa se pojavljajo vprašanja glede ustreznosti merjenja neopredmetenih sredstev. Neopredmetena sredstva se po začetnem pripoznanju, večinoma, merijo po nabavni vrednosti, zmanjšani za amortizacijo in morebitne oslabitve. Sicer

poznamo tudi neopredmetena sredstva brez dobe koristnosti, kar pomeni, da jih ne amortiziramo. Z vidika oslabitev pa so kriptovalute samostojna denar ustvarjajoča enota, ki nima bodoče vrednosti pri uporabi, zato je zanje edina merodajna vrednost tržna vrednost, na katero bi nato morali oslabiti vrednost neopredmetenih sredstev. MSRP hkrati omogoča tudi uporabo revalorizacijskega modela za neopredmetena sredstva, vendar izključno ob pogoju, da za takšno vrsto sredstev obstaja aktivni trg, ki ga (vsaj) vse pomembne kriptovalute izpolnjujejo. Zato Zveza računovodji, finančnikov in revizorjev Slovenije predlaga izkazovanje kriptovalut, za katere ima družba dolgoročen naložbeni cilj, med neopredmetenimi sredstvi, predvsem če uporablja MSRP, po katerem lahko uporabi model revalorizacije, s katerim nato prevrednoti kriptovaluto na pošteno vrednost (Bajuk Mušič, 2017; EY, 2017).

Možna je tudi klasifikacija kriptovalut med zaloge. Standardi MRS 2, ki urejajo zaloge, ne zahtevajo, da bi zaloge morale obstajati v fizični obliki, hkrati pa kriptovalute lahko izpolnjujejo tudi pogoj, da se uporabljajo za prodajo tekom rednega poslovanja družbe. Med zalogami ne smemo izkazovati finančnih instrumentov, zato je izkazovanje kriptovalut, ki izpolnjujejo kriterije za finančni instrument, med zalogami neustrezno. Zaloge se vrednotijo po nabavni vrednosti, ki ji pripišemo direktne stroške in jo po potrebi znižamo na iztržljivo vrednost. Prevrednotenje zalog navzgor ni dovoljeno, razen v primeru, če je družba posrednik in drži zaloge z namenom prodaje po višji vrednosti. V tem primeru lahko zaloge vrednoti po pošteni vrednosti, znižani za stroške prodaje. Ker imetniki kriptovalut, kriptovalute pogosto kupujejo z namenom hitre prodaje in realizacije razlike v ceni, je klasifikacija kriptovalut med zaloge ustrezna za številne imetnike. Zaloge so po naravi kratkoročna sredstva, zato je potrebno upoštevati, da družba kriptovalut nima namena obvladovati za obdobje, daljše od enega leta (EY, 2018). Prav tako je izkazovanje kriptovalut med zalogami primerno tudi v primeru, da družba uporablja kriptovalute z namenom plačila svojih obveznosti. Za izkazovanje sredstev med zalogami ni potrebno, da izpolnjujejo pogoje za uradno valuto katere izmed držav.

Poleg že predstavljenih možnosti MSRP predstavljajo tudi možnost, da družba v primeru, ko finančni dogodek ni primeren za klasifikacijo znotraj nobenega standarda, ustvari lastno politiko izkazovanja takšnega dogodka. Namen te politike mora biti, da čim bolj relevantno prikaže nek dogodek uporabniku, da ga lahko ta primerno uporabi za svoje odločanje. Zaradi izredne raznolikosti kriptovalut je ta možnost MSRP lahko primerna za številne družbe, ki s svojimi nameni ne izpolnjujejo kriterijev za uvrstitev v zgornje kategorije izkazov.

2 POSEBNOSTI REVIDIRANJA KRIPTOVALUT

2.1 Osnovni pojmi revidiranja računovodskih izkazov

Revizija je stara panoga, katere prvi zametki segajo že 4.000 let pr. n. š., in sicer v Babilon, na Kitajsko in v stari Egipt. Kasnejše zgodovinske zapise o revizijah najdemo že v srednjem

veku, predvsem v Italiji, zaradi razmaha velikih trgovskih hiš, ki so prve v vsakdanjem delovanju uporabile dvostavno računovodstvo. Hitrejši razvoj zunanje revizije se je začel sočasno s formiranjem velikih gospodarskih družb v času industrijske revolucije in s posledičnim ločevanjem funkcije agenta in principala (Koletnik & Kolar, 2008, str. 12).

Revidiranje računovodskih izkazov je domena zunanje revizije. Razumeti moramo, da odgovornost za sestavo in pravilnost računovodskih izkazov sloni na poslovodstvu družbe. Namen revizije pa je povečati kredibilnost in zaupanje v računovodske izkaze, ki jih izda gospodarska družba, posredno pa tudi v vse nerevizijske informacije. Poleg razumevanja namena revizije je pomembno tudi razumevanje njenega cilja, ki je izdaja mnenja, ali so računovodski izkazi, v vseh pomembnih pogledih, pripravljeni v skladu z izbranim standardom računovodskega poročanja. Iz tega izhaja zahteva Mednarodnih standardov revidiranja (v nadaljevanju MSR), da revizor pridobi sprejemljivo zagotovilo, da v računovodskih izkazih ni pomembno napačne navedbe zaradi prevare ali napake. Takšno zagotovilo revizor pridobi s sistematičnim in objektivnim pridobivanjem revizijskih dokazov, s katerimi lahko potrdi vsako izmed revizijskih trditev. Splošna definicija revizije je podvržena kritiki. In sicer, da zahteva do revizorja ne sme vsebovati zgolj mnenje, da so računovodski izkazi v skladu z zakoni in aplikativnimi standardi poročanja, temveč tudi, da morajo biti izkazi resničen in pošten odraz dejanskega stanja. Pri čemer lahko najboljša predstavitev odstopa od splošnih pravil (Hayes, Dassen, Schilder & Wallage, 2005; Koletnik, 2008; Odar, 2011). Ta kritika je še posebej relevantna v primerih novih praks poslovanja ter tehnoloških iznajdb, saj se zakonodaja in drugi regulatorji ne prilagodijo dovolj hitro spremembam v okolju. Med takšnimi primeri so tudi kriptovalute, katerih računovodska obravnava ni preprosto razumljiva in enoznačna. Ta problematika je obravnavana v poglavju 1.8.

Tabela 2: Merila izpolnjevanja velikosti družb

	Povprečno število zaposlenih v poslovnem letu	**Čisti prihodki od prodaje**	**Vrednost aktive**
Mikro	< 10	< 700.000	< 350.000
Male	< 50	< 8.000.000	< 4.000.000
Srednje	< 250	< 40.000.000	< 20.000.000
Velike	> 250	> 40.000.000	> 20.000.000

Vir: ZGD-1 (2017).

Pravno podlago za izvajanje zunanjega revidiranja družb v Sloveniji predstavljata Zakon o gospodarskih družbah (ZGD-1, Ur. l. RS, št. 42/06, 60/06, 10/08, 68/08, 42/09, 65/09, 33/11, 91/11, 32/12, 57/12, 44/13, 82/13, 55/15, 15/17) in Zakon o revidiranju (ZRev-2a, Ur. l. RS, št. 65/08, 63/13, 84/18). ZGD-1 je temeljni zakon gospodarskega prava v Sloveniji, ki v 57. členu določa tudi zakonsko obvezo za izvedbo revizije letnih poročil. Revizija letnih poročil je določena za vse srednje in velike kapitalske družbe, dvojne družbe in majhne kapitalske

družbe z vrednostnimi papirji, s katerimi se trguje na organiziranem trgu. ZGD-1 deli družbe po velikosti na podlagi zaporednega dvoletnega izpolnjevanja vsaj dveh kazalnikov v tabeli 1. V nadaljnjih odstavkih 57. člen določa tudi obliko revizorjevega poročila in odgovornost ter obveze revizorja.

Pravila za opravljanje dela pooblaščenih revizorjev določa ZRev-2a, v katerem so implementirane tudi direktive in smernice EU. Ključna sfera, ki jo ureja ZRev-2a, je pravna ureditev delovanja Slovenskega inštituta za revizijo ter Agencije za javni nadzor nad revidiranjem.

Po ZRev-2 so najpomembnejše naloge in pristojnosti Slovenskega inštituta za revizijo sledeče:

- sprejemanje in objavljanje strokovnih pravil (računovodski standardi, pravila revidiranja …),
- organiziranje strokovnih izobraževanj, izvajanje preizkusov strokovnih znanj in izdajanje potrdil o strokovnih znanjih,
- določanje strokovnih znanj in izkušenj, potrebnih za pridobitev strokovnega naziva preizkušeni notranji revizor, preizkušeni računovodja, preizkušeni poslovni finančnik, preizkušeni revizor informacijskih sistemov, preizkušeni davčnik.

Agencija za nadzor nad revidiranjem je neodvisna in samostojna agencija, katere organa Strokovni svet in Direktor, sta imenovana s strani Vlade Republike Slovenije. Agencija ima po ZRev-2 pristojnosti in odgovornosti glede:

- sprejemanja pravil revidiranja (standardov revidiranja, etičnih poklicnih standardov, standardov obvladovanja revidiranja) in določanja hierarhije pravil revidiranja, ki niso predpisi,
- izobraževanja za pridobitev naziva pooblaščeni revizor,
- izdaje dovoljenj za opravljanje dejavnosti revidiranja in nalog pooblaščenega revizorja ter registracije zakonitih revizorjev in revizijskih družb tretjih držav,
- stalnega izobraževanja pooblaščenih revizorjev,
- zagotavljanja kakovosti revizijskega dela pooblaščenih revizorjev in revizijskih družb,
- določanje strokovnih znanj in izkušenj, potrebnih za opravljanje nalog pooblaščenega revizorja in pooblaščenega ocenjevalca,
- opravljanje nadzora nad kakovostjo dela revizijskih družb, pooblaščenih revizorjev in pooblaščenih ocenjevalcev,
- vodenje registrov revizijskih družb, pooblaščenih revizorjev, pooblaščenih ocenjevalcev in drugih oseb, ki so pridobile strokovni naziv, ki ga podeljuje Slovenski inštitut za revizijo.

Agencija za nadzor nad revidiranjem in Slovenski inštitut za revizijo sta zato neposredno povezna v svojem delovanju in se dopolnjujeta v izvajanju izvršilne in nadzorne funkcije področja revizije v Sloveniji.

Revizorji morajo poleg upoštevanja zakonskih podlag pri svojem delu upoštevati tudi standarde revidiranja. V Sloveniji se uporabljajo Mednarodni standardi revidiranja, katerih namen je urejanje ključnih tematik s področja revidiranja računovodskih izkazov in posebnih presoj, promovirajo harmonizacijo raznovrstnih lokalnih ureditev standardov ter zagotavljajo konsistentnost in primerljivost revizij med različnimi državami. Med drugim je EU z Direktivo, št. 2006/43/EC v letu 2006 uzakonila, da morajo vsi revizorji v EU pri zakonskih revizijah računovodskih izkazov uporabljati MSR (Hayes, Dassen, Schilder & Wallage, 2005).

2.2 Etični kodeks revizorja

Etika je socialni konstrukt, sestavljen iz moralnih načel, pravil ravnanja in vrednot. Pomen etike pride do izraza, ko se posameznik znajde pred odločitvijo, ki ima lahko različne moralne posledice ali ima lahko pomembne posledice za druge deležnike. Revizorjevo upoštevanje etičnih pravil je za opravljanje revizorjevega dela in izpolnjevanje njegove funkcije v ekonomski sferi družbe ključno. Revizor lahko svojo družbeno funkcijo izpolnjuje zgolj na podlagi zaupanja uporabnikov njegovih storitev v kakovost opravljenih storitev. Etična pravila igrajo ključno vlogo pri vzpostavljanju in ohranjanju tega zaupanja, saj postavljajo omejitve in minimalne standarde, po katerih se morajo udeleženi v procesu revizije ravnati. Pomen etičnih pravil v stroki je tako visok, da so nekatere države pravila implementirala celo v zakonodajo, drugod pa etične standarde urejajo strokovni organi (Hayes, Dassen, Schilder & Wallage, 2005; Gill, 2009; Campbell & Houghton, 2005).

Etični kodeks Mednarodne zveze računovodji navaja temeljna etična načela, ki jim morajo slediti vsi njeni člani, med katerimi so tudi vsi člani s pridobljeno licenco Association of Chartered Certified Accountants (v nadaljevanju ACCA) (BPP Learning Media, 2017). Navedena načela so naslednja:

- Celovitost/integriteta: načelnost in poštenost v vseh strokovnih in poslovnih razmerjih (resnica je temeljna lastnost).
- Objektivnost: pristranskost, konflikt interesov in vpliv drugih ne smejo vplivati na sposobnost strokovne presoje (poštenost je temeljna lastnost).
- Strokovna usposobljenost in skrbnost: ohranjanje strokovnega znanja in sposobnosti na nivoju, ki omogoča kompetentno opravljeno storitev ter zagotavlja sledenje vsem regulativnim spremembam. Hkrati morajo člani ACCA pri opravljanju strokovnih nalog skrbno slediti zakonskim in drugim določilom.

- Zaupnost: informacije, prejete v poslovnem razmerju, ne smejo biti razkrite tretji osebi brez primerne odobritve in pravne ali strokovne zahteve po razkritju. V poslovnem razmerju pridobljenih informacij ni dovoljeno uporabiti za lastno korist.
- Profesionalno obnašanje: člani morajo upoštevati vse relevantne zakone in regulative in se morajo izogibati diskreditaciji poklica.

Etični kodeks zunanjih revizorjev ima pomembno vlogo tudi pri revidiranju kriptovalut, zunanji revizor se bo namreč pri revidiranju kriptovalut poleg vseh obstoječih tveganj soočal tudi z novimi etičnimi tveganji, ki so posledica unikatnih lastnosti kriptovalut. Zunanji revizorji bodo pri revidiranju kriptovalut morali biti strokovno dobro podkovani tudi s področja kriptovalut, ki se tako iz tehničnega, ekonomskega kot tudi s pravnega vidika zelo hitro spreminja, kar od revizorjev zahteva nenehno dodatno izpopolnjevanje in sledenje spremembam. Pomembno vlogo bo imelo tudi izpolnjevanje načela objektivnosti, saj lahko posameznik zaradi lastne koristi ali svojih močnih prepričanj v uspešnost kriptovalut, bodisi posameznih kriptovalut bodisi kriptovalut na splošno, ogrozi nepristransko delovanje zunanjega revizorja.

2.3 Uradne trditve in njihov pomen

Uradne ali revizijske trditve (ang. Assertions) so v prenovljenem MSR 315 definirane kot: »Izrecne ali drugačne trditve poslovodstva, predstavljene v računovodskih izkazih, ki jih revizor uporabi za proučevanje različnih vrst možnih napačnih navedb, ki se lahko pojavijo.« Revizorji zato za vsako trditev ocenijo, kakšne so možne nepravilnosti, in pripravijo revizijske procese, s katerimi lahko pridobijo zadostno zagotovilo za potrditev pravilnega izkazovanja.

Različne postavke računovodskih izkazov so povržene različnim tveganjem, ki se nanašajo na uradne trditve, iz katerih izhaja pošten prikaz računovodskih izkazov. Uradne trditve se razlikujejo predvsem na podlagi tega, ali gre za transakcije in dogodke v revidiranem obdobju (na primer prihodki od prodaje, stroški storitev, finančni odhodki) ali gre za salde ob koncu revidiranega obdobja (na primer terjatve do kupcev, finančne obveznosti do bank, obveznosti za odložene davke). Poleg zgoraj omenjenih kategorij prenovljeni MSR 315 določa tudi uradne trditve za predstavitve in razkritja, katerih namen je, da revizorje dodatno usmerijo k razmisleku glede morebitnih tveganj, vezanih na razkritja. Razkritja so ključen del računovodskih poročil, saj občutno pripomorejo k boljšemu razumevanju izkazov družbe (ACCA, 2015; Arens, Elder & Mark, 2010).

Uradne trditve o transakcijah in dogodkih v revidiranem obdobju po MSR 315 (Mednarodna zveza računovodij, 2009; Turk, 2009) so:

- nastanek: posli in dogodki, ki so bili vpisani, so se zgodili in pripadajo organizaciji,
- popolnost: vsi posli in dogodki, ki jih je treba vpisati, so vpisani,

- točnost: zneski in drugi podatki, ki se nanašajo na vpisane posle in dogodke, so bili ustrezno vpisani,
- časovna uvrstitev: posli in dogodki so bili vpisani v pravilno obračunsko obdobje,
- razvrstitev: posli in dogodki so bili vpisani na pravilne konte.

Uradne trditve o saldih na kontih ob koncu obdobja po MSR 315 so (Mednarodna zveza računovodij, 2009):

- obstoj: sredstva, obveznosti in deleži v lastniškem kapitalu obstajajo,
- pravice in obveze: organizacija poseduje ali obvladuje pravice v zvezi s sredstvi, obveznosti pa so obveza organizacije,
- popolnost: vsa sredstva, obveznosti in deleži v lastniškem kapitalu, ki naj bi bili vpisani, so vpisani,
- vrednotenje in razporeditev: sredstva, obveznosti in deleži v lastniškem kapitalu so vključeni v računovodske izkaze z ustreznimi zneski in vse iz tega izhajajoče prilagoditve vrednotenj in razporeditev so ustrezno vpisane.

Uradne trditve o predstavitvi in razkritju po MSR 315 (Mednarodna zveza računovodij, 2009) so:

- nastanek ter pravice in obveze: razkriti dogodki, posli in druge zahteve so se zgodili in pripadajo organizaciji,
- popolnost: vsa razkritja, ki naj bi bila vključena v računovodske izkaze, so vključena,
- razvrstitev in razumljivost: računovodske informacije so ustrezno predstavljene in opisane, razkritja pa so jasno izražena,
- točnost in vrednotenje: računovodske in druge informacije so razkrite pošteno in z ustreznimi zneski.

V postopku izvedbe revizije je pomembno, da načrtovani in kasneje izvedeni postopki za posamezno postavko zagotovijo ustrezno potrditev vseh relevantnih uradnih trditev in povezanih tveganj. V času predhodne revizije je potrebno identificirati in po potrebi testirati kontrolno okolje posameznih transakcij, v navezavi z njihovo sposobnostjo preprečevanja nepravilnosti za vsako izmed relevantnih uradnih trditev. Revidiranje postavk transakcij in dogodkov je fokus revizije rekom leta. Potrjevanje ustreznosti izpolnjevanja uradnih trditev na sredstvih, obveznostih in kapitalu pa je fokus revizije po koncu leta (ACCA, 2015).

2.4 Opredelitev revizijskih tveganj

Revizijsko tveganje je po definiciji Odbora za mednarodne standarde revidiranja in dajanja zagotovil: »Tveganje, da bo revizor izrazil neprimerno revizijsko mnenje, kadar so računovodski izkazi pomembno napačni. Revizijsko tveganje je odvisno od tveganj pomembno napačne navedbe in od tveganja pri odkrivanju.« Revizijsko tveganje je pri izvedbi revizije ključnega pomena, saj definira področja na katere se bo revizor osredotočil.

Revizorjeva naloga ni, da preveri vse transakcije posamezne družbe. Zaradi izjemnega obsega transakcij v modernih multinacionalkah je vse transakcije tudi nemogoče preveriti, še zlasti ker revizor zasleduje učinkovitost delovanja. Učinkovitost delovanja je pomembna, saj ni nihče pripravljen plačati revizorja za pregled celotnega delovanja družbe. Pri izpolnjevanju svoje naloge, se revizor upre na proces ocenjevanja tveganj, s katerim oceni, katera tveganja bi lahko izkrivila pravilnost izdanega mnenja. Pravilna identifikacija tveganj omogoči revizorjem, da se osredotočijo na področja, kjer lahko pride do nepravilnosti, ter pravilno določijo revizijske postopke, s katerimi bodo preprečili, da bi izdali nepravilno mnenje glede pravilnosti izkazovanja posameznih postavk ali celotnih izkazov (ACCA, brez datuma).

Revizijsko tveganje lahko izhaja iz različnih predpostavk. V osnovi tveganja delimo na: tveganja pri delovanju, tveganja pri kontroliranju in tveganja pri odkrivanju (formula za sestavo revizijskega tveganja je prikazana v tabeli 3). Revizijsko tveganje označimo kot produkt vseh treh tveganj, saj je tovrstno tveganje vedno posledica vseh treh dejavnikov, poleg tega velja tudi, da višje tveganje na posameznem področju hkrati povečuje tudi skupno tveganje. Ključno pri razumevanju je, da je revizijsko tveganje produkt. Vsakega izmed podtveganj je zato pomembno obvladovati do mere, da agregirano tveganje nepravilnosti na posamezno postavko ali izkaze kot celoto ne preseže sprejemljivega tveganja.

Tabela 3: Sestava revizijskega tveganja

Revizijsko tveganje	=	Tveganje pri delovanju	x	Tveganje pri kontroliranju	x	Tveganje pri odkrivanju

Vir: BPP Learning Media (2017).

Tveganje pri delovanju izhaja iz dovzetnosti uradne trditve za nepravilnosti zaradi najrazličnejših zunanjih in zunanjih dejavnikov. Ti dejavniki lahko med drugim izvirajo iz okolja, notranje strukture družbe, panoge, tehnologije ali regulatornih določil. Za revizorja je izredno pomembno, da se revidiranec zaveda tveganj pri delovanju in jih pravilno naslovi in obvladuje v sklopu kontrolnega okolja.

Tveganje pri kontroliranju je potencialna nepravilnost v uradni trditvi zaradi nezadostnega internega kontrolnega sistema družbe, zaradi katere družba ne bi pravočasno preprečila, zaznala in popravila nepravilnosti.

Tveganje pri odkrivanju je tveganje, da revizor v okviru svojih postopkov ne bo odkril nepravilnosti v uradni trditvi, do katere je prišlo v sklopu delovanja in kontroliranja družbe.

2.5 Notranjekontrolno okolje družbe in njegov pomen pri obvladovanju tveganj

Notranje kontrole družbe so bistvena sestavina vsakega podjetja, saj omogočajo tako nadzor nad finančnimi in drugimi evidencami kot tudi upravljanje z družbo. Celoten sistem

notranjih kontrol imenujemo kontrolno okolje družbe. Tako posamezne notranje kontrole kot tudi kontrolno okolje kot celota imajo ključno funkcijo pri upravljanju s tveganji in so v nekaterih primerih celo strogo predpisani (poročanje o notranjekontrolnem okolju po Sarbanes Oxley Act za vse javne družbe v Združenih državah Amerike (v nadaljevanju ZDA)). Na podlagi tega lahko zaključimo, da so notranje kontrole pomembne tako za poslovodstvo kot tudi za regulatorje, zunanje in notranje revizorje ter tudi investitorje in ostale deležnike družb (Hayes, Dassen, Schilder & Wallage, 2005). Notranja kontrola je proces pridobitve razumljivega zagotovila za izpolnjevanje s strani poslovodstva zastavljenih ciljev. Cilji kontrol se lahko razlikujejo, vendar izpolnjujejo vsaj enega izmed spodnjih kriterijev:

- upravljanje rednega delovanja (kontrole nadzora nad transakcijami): učinkovita in kompetentna uporaba sredstev družbe,
- finančno poročanje: zagotavljanje priprave zanesljivih računovodskih izkazov,
- skladnost: zagotavljanje izpolnjevanja zakonodajnih in drugih regulatornih zahtev,
- zaščita sredstev.

Poslovodstvo je odgovorno za implementacijo ustreznega kontrolnega okolja, pri čemer se zanaša na ustrezno izvedbo kontrol s strani ostalih zaposlenih, ter za nadzor nad primernostjo kontrol na notranjo revizijo, v kolikor ta obstaja. Proces implementacije kontrolnega okolja poteka skozi več faz. Prva faza je ocena tveganj, s katerimi se družba srečuje. Tveganja se glede na pomembnost in naravo med družbami razlikujejo saj izhajajo iz potreb družbe, dejavnosti in okolja, prav tako se lahko različne družbe odločijo za različne nivoje sprejemanja tveganj. V praksi je posledica tega različen obseg implementiranega kontrolnega okolja. Podjetja, ki so manj naklonjena tveganju, bodo praviloma dizajnirala zelo stroge in podrobne kontrole, brez pomembnih odstopanj. Pomemben dejavnik pri načrtovanju kontrol je tudi skladnost delovanja, saj so družbe, predvsem tiste v finančnem sektorju, zavezane k strožjim zahtevam glede varovanja interesov zunanjih deležnikov družbe. Dobra praksa je, da so kontrole v fazi načrtovanja tudi pisno dokumentirane, vključno s podatki o postopku izvedbe procesa kontroliranja (postopki kontroliranja so po MSR 315 preiskovanja izvedbe, obdelovanje informacij, fizične kontrole, ločitev nalog in odobritve), o odgovorni osebi za njeno izvedbo, o občutljivosti posamezne kontrole ter o upravljanju z morebitnimi odstopanji od kontrole. V tretji fazi družba implementira kontrole, kar v praksi pomeni, da zaposlene seznani s pravilniki in pravilnimi postopki izvajanja kontrol. Po implementaciji kontrolnega okolja je ključnega pomena, da družba spremlja njegovo delovanje in ga po potrebi modificira, saj brez primernega izvajanja od kontrolnega okolja ne moremo pričakovati pozitivnih rezultatov.

Posebni primeri notranjih kontrol so kontrole, implementirane v proces izvajanja finančnega poročanja, ter kontrole za odkrivanje in preprečevanje prevar. Končni produkt procesa izvajanja finančnega poročanja je priprava računovodskih izkazov za poročevalsko obdobje. Kontrole v procesu finančnega poročanja se v osnovi nanašajo na pravočasno, pravilno in zadostno poročanje osebam, odgovornim za pripravo izkazov. Ključnega pomena je

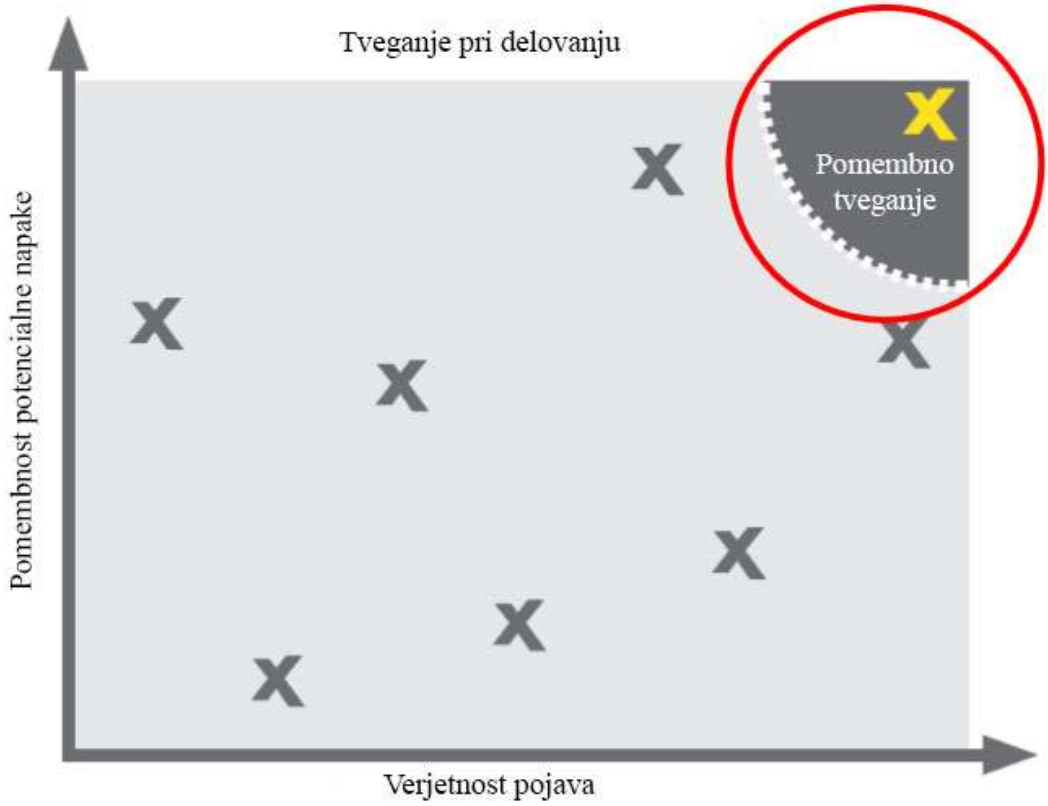
predvsem poročanje o neobičajnih dogodkih ob koncu leta, o ocenah dogodkov, ki bodo nastali po koncu poslovnega leta, ter o drugih računovodskih ocenah. Pri kontrolah za odkrivanje in preprečevanje prevar govorimo o mehkih kontrolah, ki niso strogo definirane, saj bi tak način izvajanja kontrol onemogočal njihovo učinkovitost. Med najučinkovitejše kontrole za odkrivanje in preprečevanje prevar po raziskavi Združenja pooblaščenih preiskovalcev prevar, izvedeni leta 2016, med drugim sodijo medsebojne kontrole zaposlenih, ki nato sum prevare sporočijo odgovornim osebam, pregled s strani managementa in pregled s strani notranje revizije.

Notranje kontrole so za zunanje revizorje pomembne, saj zagotavljajo večjo zanesljivost posredovanih podatkov, implementacija notranjih kontrol namreč, ne glede na njihovo natančnost in doslednost njihovega izvajanja, izboljša kvaliteto podatkov. Hkrati pa implementacija ustreznega kontrolnega okolja zunanjemu revizorju omogoči uporabo t. i. strategije testiranja kontrol, pri kateri preveri zadostnost oblikovanega kontrolnega okolja, da prepreči pomembno napačne navedbe o uradnih trditvah posameznih postavk, in v drugi fazi na vzorcu preveri delovanje notranjekontrolnega okolja družbe pri preprečevanju ali odkrivanju nepravilnosti. Z izpolnitvijo omenjenih pogojev za uporabo strategije testiranja kontrol lahko revizor zmanjša potrebo po naknadnih testiranjih transakcij, s tem pa skrajša čas, potreben za revizijo (Koletnik, 2008).

2.5.1 Določitev pomembnosti tveganja

Določitev pomembnosti tveganja pri delovanju je za izvedbo revizije ključnega pomena. Glede na pomembnost posameznega tveganja nato revizor določi vrsto revizijskih postopkov, predvsem pa obseg testiranj, opravljenih znotraj vsakega postopka. Metodologija revizijske hiše Ernst & Young (v nadaljevanju EY) glede na pomembnost deli tveganja v več razredov in podrazredov. Pomembnost tveganja se oceni na podlagi učinka potencialne napake na eni strani ter na podlagi verjetnosti realizacije dogodka na drugi. Tveganja pri delovanju so nato glede na pomembnost razdeljena na nizka, srednja, visoka in pomembna. Ključna v tej metodologiji so pomembna tveganja. Pomembna tveganja so tveganja, kjer napaka lahko povzroči nepravilno razumevanje računovodskih izkazov družbe, hkrati pa je tudi verjetnost nastanka takšnega dogodka visoka. Pomembna tveganja so pogosto nerutinske transakcije, ki so v veliki meri podvržene ocenam poslovodstva. Pomembna tveganja mora zato revizor obravnavati s pazljivostjo in pri tem ustrezno identificirati potencialne indikatorje, ki bi lahko pomenili, da se bo pomembno tveganje udejanjilo (EY, 2013). Podkategorija pomembnega tveganja je po metodologiji EY tudi tveganje za prevare, ki je obravnavano v naslednjem poglavju.

Slika 2: Matrika tveganja glede na pomembnost in verjetnost



Vir: Prirejeno po EY (2013).

2.5.2 Tveganja prevar

Tveganja so v osnovi posledice udejanjenja nenamerne napake ali posledica drugih dejavnikov iz okolja ali podjetja. Izjema med tveganji so tveganja prevar, ki so že po definiciji namerna dejanja, izvedena z namenom zavesti nekoga v zmoto, da bi s tem pridobili neupravičene ali nezakonite koristi (Slovenski inštitut za revizijo in Odbor za mednarodne standarde revidiranja in dajanja zagotovil, 2018).

Prevare so zelo pereča tema revizijske stroke, saj lahko privedejo do izredno pomembnih nepravilnosti v računovodskih izkazih, ki lahko imajo v skrajnem primeru tudi usodne razsežnosti. Najbolj medijsko odmevne prevare, ki niso bile pravočasno odkrite, so primeri propada družb Enron, Parmalat in Worldcom iz začetka enaindvajsetega stoletja. Vsi ti propadi so pomembno pripomogli k nadaljnjemu razvoju regulacije na področju revizije in revizijskih družb, zlasti na področju neodvisnosti in prevar. Najbolj znan takšen regulatorni ukrep je Sarbanes Oxley Act v ZDA.

Pri ocenjevanju in identificiranju tveganj prevar je ključno razumevanje ozadja nastanka prevar, ki je najbolje predstavljeno s trikotnikom prevar. Teorija trikotnika prevar pravi, da je za izvedbo prevare potreben skupek treh motivov: priložnosti, pritiska in racionalizacije.

Pritisk je osnovni dejavnik, ki posameznika motivira, da izvede prevaro. Pritisk je lahko zunanji ali notranji. Zunanji pritisk predstavlja predvsem želja po dvigu vrednosti podjetja, z manipulacijo računovodskih izkazov, da izboljšajo uspešnost podjetja, od katere je pogosto odvisno nagrajevanje poslovodstva in ključnih kadrov ter eventualno tudi zaposlitev teh kadrov. Poznamo pa tudi dejavnike notranjega pritiska, kamor sodita nenasiten pohlep in želja po izboljšanju osebnega, socialnega in ekonomskega položaja (Singleton & Singleton, 2010; Coenen, 2008).

Drugi dejavnik, ki je za izvedbo prevare ključen, je priložnost za udejanjenje motivacije, ki izhaja iz dejavnika pritiska. Družbe imajo že same po sebi vpeljane sisteme, ki nepooblaščenim osebam ne dovoljujejo dostopa do kočljivih informacij in sistemov, s katerimi bi lahko bila prevara izvedena. Iz tega izhaja, da prevare ne more izvesti vsakdo, zato so osebe, povezane s pomembno prevaro, praviloma tudi člani poslovodstva (Singleton & Singleton, 2010).

Zadnja faza pred izvedbo prevare je racionalizacija, ki pomeni, da osebe, vključene v izvedbo prevare, svojega početja ne ocenjujejo kot slabega in mu ne pripisujejo negativnega vpliva na druge osebe. Osebe, ki izvedejo prevaro, pogosto menijo, da si zaslužijo višjo plačo ter boljši status v družbi. Prevaranti so pogosto prepričani tudi, da je izvedba prevare zgolj začasna rešitev, ki jo bodo naknadno popravili, ali da s tem pomagajo drugim (na primer zagotovitev višjega bonusa sodelavcem) (Singleton & Singleton, 2010; Coenen, 2008).

Slika 3: Trikotnik prevar

Vir: Koletnik & Kolar (2008, str. 33).

Zaradi zgoraj omenjenih lastnosti prevar je potrebno razumeti tudi delovanje posamezne družbe in dejavnikov, ki bi motivirali ključne osebe k izvedbi prevare, torej kdo te osebe so in kako bi prevaro lahko izvedli. Pomembno je razumeti, da so nekatere postavke bolj podvržene tveganju prevar. Najbolj tipična postavka, podvržena prevari, so prihodki, saj je cilj vsakega podjetja prav naraščanje prihodkov. Prevare so pogoste tudi pri postavkah, pri katerih je zelo pomembna ocena poslovodstva. Takšen primer so lahko rezervacije,

oblikovanje popravkov vrednosti ali oslabitev sredstev in vrednotenje odvisnih družb in naložb (Koletnik & Kolar, 2008).

Tveganje za napačno navedbo zaradi prevare je višje od tveganja, da do napačne navedbe pride zaradi napake. Prevare so lahko skrbno načrtovane in izvedene s strani ljudi z izredno dobrim poznavanjem delovanja družbe. MSR 240 zato navaja, da mora revizor v sklopu svojih postopkov pridobiti sprejemljivo zagotovilo, da izkazi ne vključujejo pomembne nepravilnosti in v procesu pridobivanja zagotovila ohranjati poklicno nezaupljivost, upoštevati možnost, da kontrolno okolje družbe nepravilnosti zaradi prevare morda ne bo zaznalo zaradi preglasovanja kontrol s strani poslovodstva ter da postopki za odkrivanje napak pri odkrivanju prevar ne bodo učinkoviti (International Auditing and Assurance Standards Board, 2009).

2.5.3 Tveganja, povezana z informacijsko tehnologijo

Informacijska tehnologija je nujen in nepogrešljiv dejavnik vsakega sodobnega podjetja. Vse družbe uporabljajo informacijsko tehnologijo pri evidentiranju in spremljanju vsakodnevnega poslovanja, za nekatere izmed njih pa predstavlja informacijska tehnologija tudi del dejavnosti. Primeri družb, kjer je informacijska tehnologija temelj dejavnosti so spletne trgovine, spletni iskalniki, družabna omrežja ter družbe, ki se ukvarjajo z izdajo kriptovalut. Zaradi velikega obsega, prepletenosti in raznovrstnosti aplicirane informacijske tehnologije se družbe srečujejo s številnimi (edinstvenimi) tveganji, povezanimi s tem področjem, ki pa so jim različne družbe različno resno podvržene ter jih različno uspešno obvladujejo.

Tveganja, povezana z informacijsko tehnologijo, lahko v grobem vsebinsko razdelimo na tri področja: tveganja, povezana z delovanjem informacijsko tehnoloških (v nadaljevanju IT) sistemov, tveganja, povezana z v IT-sistem implementiranim kontrolnim okoljem, ter tveganja povezana s sodobnimi IT-baziranimi dejavnostmi, kamor štejemo tudi kriptovalute in druge poslovne modele, ki slonijo na IT-ju (primeri takšnih dejavnosti so spletne trgovine, socialna omrežja, spletni iskalniki) (Juergensen, 2016).

Tveganja, povezana z delovanjem IT-sistemov, so povezana s pravilnostjo delovanja sistemov samih. Sodobne IT-sisteme izdelujejo večinoma IT-družbe, ki imajo zadostno znanje o potrebah končnih uporabnikov, zato so ti sistemi pravilno zasnovani. Za pravilno zasnovo takšnega sistema je potrebno sodelovanje strokovnjakov iz različnih področji, ki je, zaradi specializiranega znanja vsakega deležnika in njihovega različnega razumevanja posameznih tematik, pogosto težavno in dolgotrajno. Velike IT-družbe lahko zagotovijo zadostna sredstva in nadzor nad tem, da ne pride do pomembnih nepravilnosti pri delovanju IT-sistemov. Do tveganj nepravilnega delovanja IT-aplikacij, pogosteje prihaja pri IT-aplikacijah, ki so bile interno razvite, saj se takšnega razvoja družbe lotijo z namenom finančnega prihranka, kar povečuje tveganje za nepravilnost delovanja. Potrebno pa je poudariti, da se tudi nadaljnjim tveganjem za nepravilno delovanje aplikacije tudi po

končanem razvoju aplikacije ne moremo popolnoma izogniti. Pomembna dejavnika pri pravilnosti delovanja IT-sistemov sta tudi njihova pravilna uporaba in pravilno upravljanje s sistemi po njihovi implementaciji. Pod izrazom uporaba IT-sistemov razumemo nadzor nad primernostjo, zanesljivostjo in zadostnostjo vhodnih podatkov v IT-sistem, saj se brez izpolnitve vseh omenjenih dejavnikov ne moremo zanašati na to, da bo IT-sistem deloval v skladu s pričakovanji. Na pravilnost delovanja IT-sistema imajo velik vpliv tudi ljudje, saj lahko zaradi poenostavitve procesov manipulirajo s podatki do te mere, da sistemu ne zagotovijo pravilnega delovanja (t. i. garbage in, garbage out). Pri tem ni nujno, da gre za prevaro, ki jo izvršijo odgovorne osebe, ampak do nje pride zaradi nepoznavanja delovanja IT-sistemov in podcenjevanja vpliva izvedenih dejanj (Juergensen, 2016; James, Stephanie & Nancy, 2004).

Upravljanje z IT-sistemi predstavlja ključno revizijsko tveganje in vključuje pregled tveganj s področja delovanja IT-sistemov, v katerem so, skladno z metodologijo EY, zajeti naslednji postopki:

- Nadzor nad dostopi: preveritev ustreznosti podeljenih dostopov in določitve uporabniških pravic do IT-sistemov. Ustreznost dostopov je pomembna, da v IT-sistemih ne pride do zlorabe ali manipulacije s podatki, izvedene s strani nepooblaščenih oseb. Nedovoljeni dostopi bi lahko pomembno povečali tveganje prevar v organizaciji. Hkrati z nadzorom pooblaščenih dostopov je del preveritve tudi varnostni vidik dostopov, v katerega so vključene preveritve zadostnosti varnostnih politik, kot je ustrezna zahtevnost gesel za dostop, njihovo dovolj pogosto in pravočasno menjavanje ter nadzor nad zlorabo gesel.
- Pregled spremljave sprememb v IT-sistemih: IT-sistemi so podvrženi pogostim nadgradnjam. s katerimi razvijalci sistemov popravijo (naknadno) ugotovljene pomanjkljivosti sistemov. Ključno je, da so nadgradnje sistemov pravočasno izvedene ter da se pravilnost delovanja sistemov po nadgradnji pred končno implementacijo na operativnem okolju preveri na testnem okolju.
- Druga področja pregleda IT-sistemov: Ta spekter pregleda je fokusiran na dejavnike, ki zagotavljajo fizično varnost (pregled lokacije IT-sistemov s poudarkom na omejitvi dostopa, varnostnem napajanju in dejavnike, ki preprečujejo zlorabo sistema preko nasilnega dostopa) in zanesljivost delovanja (hranjenje varnostne kopije na ločeni lokaciji, ki lahko v primeru katastrofalnega dogodka na primarni lokaciji hrambe podatkov, prevzame samostojno delovanje sistema, ter pregled pravočasnega razreševanja pritožb in ugotovitev uporabnikov).

Sodobni IT-sistemi pomembno pripomorejo k dvigu učinkovitosti delovanja organizacij. Eden izmed pomembnih dejavnikov, ki pripomorejo k dvigu učinkovitosti, je aplikativno izvajanje kontrol, kar pomeni, da so notranje kontrole družbe že vgrajene v IT-sistemu. Splošen opis tveganj, vezanih na notranjekontrolno okolje je opisan v poglavju 2.6.4., v tem poglavju se osredotočam zgolj na notranjekontrolna tveganja, specifična za IT-sisteme. Najpogostejše vgrajene kontrole so logične kontrole, ki javljajo napake pri vnosu podatkov

in preprečujejo nenamerne napake. Primeri takšnih kontrol so: nezmožnost zaključitve postopka, ne da bi izpolnili vse potrebne podatke, usklajevanje medsebojnih dokumentov, opozorila, da materialna stanja v družbi ne zadostujejo za izpolnitev zahtevanih nalog. Drugi sklop kontrol, ki so velikokrat prenesene na IT-sisteme, so kontrole, vezane na primerno hierarhijo odobritev, ki natančno določajo pooblastila vsakega posameznika in avtomatsko preprečujejo delovanje posameznika izven njegovih pooblastil. Kljub vsem kontrolnim možnostim, ki jih omogoča IT-sistem, mora biti revizor pri družbah, ki uporabljajo IT-sisteme, izredno pozoren na človeški faktor, saj lahko ta pomembno vpliva na pravilnost delovanja kontrolnega okolja in na varnost podatkov. Takšen primer je shranjevanje gesel na vidnem mestu, do katerega lahko imajo dostop tudi drugi, kar močno olajša izrabo dostopa do podatkov in njihove zlorabe ali preglasovanje notranjekontrolnega okolja.

Najnovejši sklop tveganj, vezanih na IT-sisteme, so tveganja, ki so povezana s sodobnim in tehnološko podprtim delovanjem družb. To področje se hitro spreminja zaradi naglega razvoja tehnologije in poslovnih modelov in na nekaterih področjih trenutno še nima natančno definiranih revizijskih postopkov. Tveganje za kakovost revidiranja predstavlja tudi omejen obseg izkušenj revizorjev (na primer revidiranje podjetji, ki so izdale kriptovalute). Poleg kompleksnosti in izredne razvejanosti takšnega področja ravno te lastnosti pomembno povečujejo tveganje za morebitne nepravilnosti. Specifična tveganja, ki se navezujejo na kriptovalute, so predstavljena v tretjem poglavju, zato na tem mestu navajam samo tveganja, brez podrobnejših pojasnil (Mar, Johannessenn, Coates, Wegrzynowicz & Andreesen, 2012; Juergensen, 2016):

- Tveganja, vezana na tretjo osebo: v proces je vključenih veliko družb in organizacij iz najrazličnejših delov sveta, kar pomembno otežuje pregled nad celotno sliko IT-okolja ter zagotovilom o popolnosti evidentiranja transakcij.
- Nepravilnost transakcij: potrjevanje transakcij je bistveno kompleksnejše in dolgotrajnejše. Za potrebe revizije so lahko tudi nedvoumne, neodvisne potrditve težje dosegljive.
- Hitre spremembe v tehnološkem okolju: podjetja, ki so vključena v takšne transakcije, so pogosto zalo dovzetna za nove tehnološke iznajdbe, ki niso nujno preizkušene. Takšne spremembe so lahko zelo pogoste in spreminjajo IT-okolje večkrat na leto.
- Kibernetski napadi: nove tehnologije omogočajo večje možnosti za izvedbo kibernetskih napadov, ki povzročijo neposredno in posredno škodo družbi ter potencialno tudi njenim strankam.

2.5.4 Tveganje pri kontroliranju

Namen kontrolnega okolja je preprečevanje neželenih aktivnosti ter ugotavljanje že izvedenih neželenih aktivnosti z namenom primernega naknadnega ukrepanja. Kot je navedeno v poglavju 2.6, je ključna sestavina kontrolnega okolja pravilno načrtovanje posameznih kontrol, da bodo preprečile ali odkrile morebitne nepravilnosti (Hayes, Dassen,

Schilder & Wallage, 2005). Najpogostejši razlogi za povečanje tveganja pri kontroliranju so:

- Nepravilna ocena tveganj: poslovodstvo družbe se ne zaveda obstoja določenega tveganja ali podcenjuje njegov vpliv na delovanje družbe, zato ga pri načrtovanju kontrol niti ne naslovi.
- Nezadostnost kontrol za preprečitev ali odkritje nepravilnosti: kontrole niso primerno načrtovane in zato ne zmanjšujejo verjetnosti identificiranih tveganj. Razlogi za to so lahko na primer nepravilno razumevanje delovanje procesa v fazi načrtovanja, spremembe v orgaznizaciji družbe, ki niso bile primerno implementirane v spremembe kontrolnega okolja ipd.
- Podvajanje kontrol: kontrole se lahko tudi podvajajo. Do podvojitev pride zaradi izvajanja kontrol v različnih oddelkih, zaradi izvajanja kontrol s strani različnih oseb ali zaradi izvajanja več kontrol, ki obvladujejo isto tveganje.
- Pomanjkljivo izvajanje kontrol: kontrole so lahko pomanjkljivo izvedene zaradi nepravilnega razumevanja izvedbe ali namena kontrole s strani odgovorne osebe. Pomanjkljivo izvajanje kontrol je lahko posledica malomarnosti odgovorne osebe pri izvajanju.

2.5.5 Notranja revizija

Poleg zunanjih revizij se nekatere družbe poslužujejo tudi notranjih revizij, ki so vzpostavljene v korist družbe. Dejavnosti notranje revizije v primerjavi z dejavnostmi zunanje revizije niso tako strogo definirane. Notranji revizorji izvajajo naloge, ki jim jih zadata poslovodstvo in nadzorni svet, ob pomoči revizijske komisije. Poleg dejavnosti, vezanih na pregledovanje, preizkušanje in ocenjevanje ureditve notranjega kontrolnega okolja ter preverjanja računovodskih poročil in informacij, kjer se dejavnosti notranjega revizorja prepletajo z dejavnostmi zunanjega, notranji revizor opravlja tudi preverjanja neračunovodskih poročil, se vključuje v pregled učinkovitosti, varčnosti in uspešnosti delovanja podjetja in njegovih organizacijskih enot in preverja spoštovanje zakonov, regulatornih predpisov ter internih poslovodskih usmeritev. Zaradi prepletanja njunih nalog je sodelovanje med notranjim in zunanjim revizorjem lahko zelo koristno. Obe panogi med seboj delita ugotovitve in na ta način prispevata k učinkovitosti delovanja vsake funkcije. Ključna razlika med obema vrstama revizorjev je v zagotavljanju neodvisnosti, saj notranji revizor ne more doseči tako visoke stopnje neodvisnosti kot zunanji, zato je tudi odgovornost za izdajo pravilnega mnenja o računovodskih izkazih popolnoma v domeni slednjega (Koletnik, 2009).

3 REVIDIRANJE KRIPTOVALUT

3.1 Opredelitev tveganj, povezanih s kriptovalutami

Kriptovalute so z vidika imetnika kriptovalut in posledično tudi z vidika revizorja izredno tvegano sredstvo. Osnova za večino revizijskih tveganj je relativna novost kriptovalut, zaradi česar še niso razviti varovalni mehanizmi, ki bi zmanjševali tveganja za imetnike kriptovalut in uporabnike njihovih izkazov. Posebnost kriptovalut, ki revizorjem predstavlja največji izziv, je njihova decentraliziranost ali hramba na različnih lokacijah, ki je osnova blockchaina. Pomen revizorjeve sposobnosti uspešne in zanesljive izvedbe revidiranja blockchaina bo v prihodnosti izrednega pomena zaradi širitve tega koncepta na številna druga področja uporabe.

3.1.1 Pravna tveganja kriptovalut

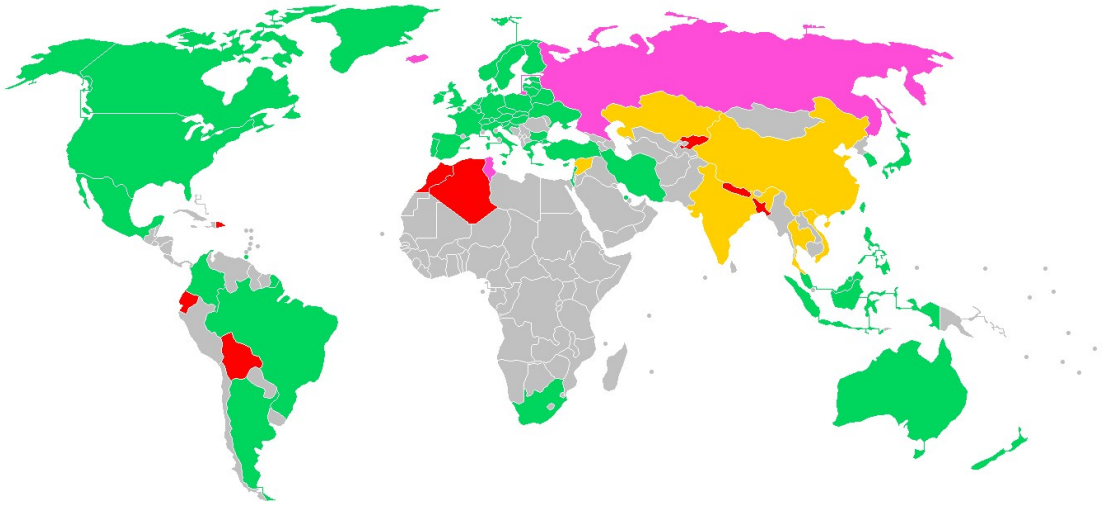
Tveganje, specifično kriptožetonom, je, da jih lahko izdajo organizacije, ki jih ne moremo klasificirati znotraj nobenega pravnega reda. Takšne organizacije se imenujejo digitalne avtonomne organizacije (ang. Digital autonomous organisation). Gre za organizacije, v katerih lahko imetniki žetonov preko glasovanj razpolagajo s premoženjem organizacije. V praksi imetniki kriptožetonov delujejo kot lastniki delnic, ki izvršujejo glasovanje preko skupščine. Takšna oblika organizacije izdajateljice kriptožetonov predstavlja številne revizijske probleme, predvsem v obliki pravne jurisdikcije, v kateri deluje in znotraj katere lahko partnerji organizacije poiščejo pravno varstvo. Vprašanje glede pristojnosti izredno oteži revizijo, saj poveča problem morebitnega nepoznavanja pravilne zakonodaje ter hkrati poveča tudi možnost izrabe lukenj v različnih pravnih okoljih. Prav tako so izdajatelji kriptovalut ali žetonov zaradi že po naravi virtualne vsebine lahko podvrženi tudi dolžnosti izpolnjevanja zakonodaj v različnih državah.

Bodisi zaradi pomanjkanja tehničnega znanja bodisi zaradi drugih praktičnih razlogov so kriptovalute pogosto hranjene pri kriptoborzah, kar pomeni, da imajo ključe za dostop do denarnic tudi borze. Z vidika revizije hranjenje katerih koli sredstev ali posredovanje kontrole nad sredstvi tretji osebi vedno poveča tveganja, povezana z varnostjo hranjenja teh sredstev. Prvi razlog za višje tveganje je posedovanje privatnih dostopnih ključev s strani tretje osebe, kar lahko pomeni onemogočen dostop do kriptovalut v primeru prenehanja delovanja borze. Hkrati je zaradi same narave kripto borz povečano tudi tveganje za morebitno nezmožnost potrditve obstoja kriptovalut družbe zaradi neavtorizirane odtujitve. Takšen primer so lahko transakcije med dvema računoma ene borze, saj transakcije med njimi pogosto niso zapisane v blockchainu, ampak samo v internih bazah kripto borze. V tem primeru je težko ugotoviti dejansko količino enot kriptovalute v denarnici, razen če zahtevamo nakazilo celotne vsebine denarnice drugam, ob pogoju, da bo ob tem formiran tudi zapis v blockchainu (Allen & Overy LLP, 2017).

Eno ključnih tveganj, povezanih s kriptovalutami, je tudi nezmožnost izvedbe izterjave kriptovalute, saj zaradi varnostnega sistema, na katerem delujejo, ne morejo biti nakazane brez odobritve imetnika. To dejstvo predstavlja tveganje za upnike, saj upnik v primeru, da dolžnik ne izkaže volje za poplačilo, po pravni poti ne more izterjati sredstev, kar bistveno poveča tveganje nepoplačljivosti terjatev do imetnikov kriptovalut. Na to tveganje lahko gledamo podobno kot na tveganje poplačljivosti terjatev do podjetij iz držav s slabše delujočim sistemom pravnega varstva upnikov (na primer države na Balkanu, v Afriki). Nezmožnost izterjave kriptovalut povečuje tudi verjetnost, da osebe, ki se želijo izogniti poplačilu, prenesejo svoje premoženje v kriptovalute in se na ta način izognejo izterjavi. Kljub temu je v Sloveniji znan že vsaj en uspešen sodni zaseg kriptovalut, ki ga je izvedlo Okrožno sodišče v Mariboru, v katerem so uspeli od imetnika kriptovalut pridobiti osebni ključ in sredstva tudi izterjati ter nato prodati preko kripto borze (Jadek, 2018).

Kriptovalute so dovoljene in regulirane v Sloveniji in EU, v številnih državah sveta pa so deloma ali popolnoma prepovedane. Prepovedi se med državami razlikujejo in najpogosteje omejujejo ustanavljanje kripto borz in podjetji, ki se lahko ukvarjajo s transakcijami s kriptovalutami, medtem ko je posedovanje kriptovalut za fizične osebe dovoljeno. Nekatere države dodajajo tudi omejitve glede rudarjenja kriptovalut, ponekod pa so kriptovalute popolnoma prepovedane. Poleg omejitev operacij, ki jih lahko izvajamo s kriptovalutami, se med državami razlikujejo tudi omejitve, vezane na posamezne kriptovalute. Na spodnji sliki so prikazane države glede na status prepovedi bitcoina.

Slika 4: Legalnost bitcoina po državah



Legenda: zelena – bitcoin je dovoljen; rumena – omejitve pri uporabi bitcoina; roza – bitcoin ni direktno prepovedan, vendar je vprašljiva pravna aplikacija bitcoina v različnih preteklih zakonih; rdeča – bitcoin je prepovedan; siva – ni podatka.

Vir: Wikipedia (brez datuma).

Zakonodaja na področju kriptovalut se spreminja izredno hitro, zato je potrebno redno spremljati spremembe na tem področju in status prepovedi po posameznih državah. Tipičen

primer glede sprememb v zakonodaji je Kitajska. Kitajska je največji trg kriptovalut, ki pogosto spreminja svojo pravno obravnavo. Pomemben mejnik je bila prepoved bitcoina leta 2013, zaradi česar je vrednost bitcoina padla za polovico. Danes je na Kitajskem prepovedano posedovanje kriptovalut s strani finančnih institucij, prav tako se pojavljajo omejitve pri rudarjenju. Nestanoviten pravni status kriptovalut pomembno vpliva na stopnjo tveganja poslovanja s kriptovalutami, zato je potrebno neprestano spremljati spremembe v zakonodaji in hitro urgirati glede nanje ter na ta način obvladovati tveganja. V skrajnem primeru vedno obstaja možnost, da država, v kateri posluje družba, v celoti ali samo za dejavnosti, ki jo izvaja družba, prepove poslovanje s kriptovalutami, kar lahko pomeni, da brez velike spremembe v poslovnem modelu družba ne more več poslovati.

3.1.2 Ekonomsko-finančna tveganja

Kriptovalute niso centraliziran sistem, ki bi bil reguliran, kot to velja za fiat valute. Fiat valute delujejo v rigidnem sistemu, ki je preverljiv in sorazmerno zanesljiv. V ta sistem so vključene centralne in komercialne banke, vanj je tesno vpletena država, vsi omenjeni člani pa delujejo z namenom zagotavljanja zanesljivosti fiat denarja. Vsi ti člani dajejo fiat denarju centraliziran značaj, ki ga pri kriptovalutah ni. Ker so kriptovalute samostojen sistem, razdrobljen na številne lokacije, je revidiranje kriptovalut bolj kot revidiranju organizacije podobno revidiranju celotnega ekosistema. Posledica neobstoja centraliziranega sistema, ki bi deloval z namenom zagotavljanja stabilnosti sistema, je tudi največje tveganje kriptovalut – njihovo veliko volatilnost. Kljub stalni količini enot kriptovalut v obtoku njihova vrednost močno niha. Nihanje je lahko posledica nerazvitosti trga ali drugih manipulacij, ki lahko povzročijo škodo organizaciji. Takšen primer predstavlja naročilo borzi kriptovalut, da v primeru padca vrednosti pod določeno vrednost proda določeno število kriptovalut. V sistemu kriptovalut lahko samo nekaj večjih igralcev povzroči upad vrednosti kriptovalut in pripelje do avtomatske likvidacije pozicije družbe, kar lahko pomeni oškodovanje družbe. Revizor mora zato v sklopu revizije pridobiti zagotovilo, da so mu poznana vsa takšna naročila in njihovi odloženi pogoji za izvedbo v primero volatilnosti na trgu kriptovalut (Broby & Paul, 2017).

3.1.3 Računovodska tveganja

Izkaz poslovnega izida obsega vse transakcije, ki so bile opravljene v nekem obdobju. Pomembna naloga revizije je identifikacija pravilnosti časovne umestitve posameznih transakcij (kar v angleščini imenujemo cutoff). Identifikacija pravilnosti časovne umestitve je zato ključnega pomena, da lahko revizor preveri čas vsake opravljene transakcije, ki se nanaša na predstavitveno obdobje. Transakcije kriptovalut so v osnovi enostavno potrdljive, saj so umeščene v blockchain, v katerem si sledijo v časovnem zaporedju, ki ga lahko tudi identificiramo. Pri tem je potrebno poudariti, da vsaka transakcija ni označena s svojo časovno komponento, ampak so transakcije združene v bloke. Vključenost neke transakcije v blok nam torej ne zagotavlja informacije o tem, kdaj je bila transakcija izvedena, pač pa

samo informacijo o tem, kdaj je bila transakcija v blockchainu potrjena. Čas potrditve transakcije torej ni nujno enak času poročanja o transakciji. Tako imamo dve situaciji**:** na eni strani transakcije izpadejo iz potrjevanja in so potrjene kasneje, na drugi strani pa so transakcije avtorizirane in generirane, vendar v trenutku izvedbe niso poročane v blockchain. Omenjeni problem lahko povzroči, da revizor ni seznanjen z vsemi transakcijami, bodisi zaradi malomarnosti bodisi zaradi prevare. Kot primere takšnih transakcij lahko navedemo prenose sredstev med različnimi kripto denarnicami revidinaranca, ki niso bili poročani v blockchain, ali pa primere transakcij, ki so bile izvedene s pomočjo kraje gesla za dostop do denarnice in so bile naknadno poročane v blockchain. Pri obvladovanju tveganja skritih transakcij je ključnega pomena učinkovito notranjekontrolno okolje, ki omogoča pravilno identifikacijo avtoriziranih transakcij in s tem pravilno umestitev v obdobje dejanske izvedbe. Čeprav notranjekontrolno okolje zmanjšuje tveganje za nepravilno prezentacijo transakcije, ne naslavlja drugih dejavnikov neobvladovanja transakcij. V primeru neobvladovanja transakcij je predlagan revizijski postopek, da prenesemo vsa sredstva iz trenutne denarnice v drugo in na ta način potrdimo, da nobena enota kriptovalute ni bila vključena v drugo preteklo transakcijo, ki bi jo revidiranec želel prikriti (Broby & Paul, 2017). Poleg tega ta revizijski postopek omogoča tudi potrditev začetnega stanja kriptovalut za prihajajoče obdobje.

V kriptosvetu so del vsakdana tudi reverzibilne in odložene transakcije. Primeri takšnih transakcij so:

- Mikroplačila: so transakcije nizke vrednosti, ki jih tretja oseba združi v eno transakcijo, ta transakcija je nato poročana v blockchain. Namen takšnih transakcij je izogibanje potencialno visokim transakcijskim stroškom.
- Pametne pogodbe in odložene transakcije: imajo vgrajeno klavzulo, po kateri bo transakcija izvedena ob izpolnitvi določenih pogojev v prihodnosti.
- Pogodbe s preddeterminiranim pogojem (ang. Hashlock contracts): so kriptografsko zaklenjena sredstva, ki jih lahko odkleni samo imetnik preddeterminiranega ključa. Ob vnosu pravilnega ključa se sredstva porabijo na predhodno določen način. Te pogodbe so v praksi izredno podobne notarski hrambi denarja, ki ob vnaprej določenih pogojih sprosti sredstva upravičenca.

Vsem omenjenim transakcijam je skupno, da upravičenec s sredstvi še ne razpolaga. Ker je upravičenost do sredstev, ki so vezane na takšne transakcije, pravno zelo težko ali nemogoče izterjati, mora revizor potrditi obstoj in dejansko zmožnost izterjave sredstev za upravičenca. Najlažji rešitvi sta, da revizor počaka, da bo vprašljiva transakcija izvedena, ter da revidiranec izvrši nakazilo sredstev v drugo denarnico, s čimer dokaže, da sredstva dejansko obvladuje. Vendar je lahko zaradi same narave primerov to nemogoče. Rezervni načrt za potrditev pametnih pogodb in odloženih transakcij je preveritev kode pametne pogodbe, pri čemer so vidni tudi pogoji za izvedbo transakcije.

3.1.4 Tveganja notranjekontrolnega okolja

Poslovanje s kriptovalutami vpelje popolnoma novo okolje delovanja, z novimi notranjimi kontrolami, ki jih družbe uporabljajo za obvladovanje tveganj. Zlasti pomembno je delovanje kontrol pri avtorizaciji transakcij. Kontrole avtorizacije so izredno pomembne tudi pri transakcijah s konvencionalnimi valutami. Pomen delovanja teh kontrol je v kriptosvetu še večji kot v tradicionalni družbi, saj je izterjava morebitnih neželenih in nepravilnih transakcij kriptovalut bistveno težja.

Pomembna naloga notranjekontrolnega okolja je tudi planiranje denarnih tokov družb. Namen planiranja denarnih tokov je sposobnost družbe, da izpolni bodoče finančne obveznosti, v skladu s politiko družbe ter pravnimi in zakonskimi predpisi in s tem omogočanje sprotnega poslovanje družbe. Poslovanje s kriptovalutami pomembno poveča obseg in zahtevnost planiranja, saj se lahko bistveno poveča obseg števila plačilnih sredstev, s katerimi operiramo (večina družb v Sloveniji posluje samo z eno valuto (z EUR), vpeljava kriptovalut kot plačilnega sredstva lahko poveča število plačilnih sredstev tudi na 3,4 ali več). Poleg večjega števila valut je potrebno pri planiranju upoštevati tudi volatilnost kriptovalut, saj lahko ta nihanja pomembno vplivajo na likvidnost družbe. Obvladovanje volatilnosti se najpogosteje dosega s postopkom zasledovanja čim večje usklajenosti med terjatvami in obveznostmi ali z vpeljavo časovne komponente med prilivi in odlivi v posamezni valuti. Planiranja denarnega toka se običajno izvajajo enkrat dnevno, bi jih pa bilo zaradi volatilnosti kriptovalut najverjetneje potrebno izvajati pogosteje.

V zgodnejši fazi njihovega razvoja so bile kriptovalute zelo pogosto uporabljene v prepovedanih transakcijah, na primer za potrebe pranja denarja, izogibanje gospodarskim sankcijam, nakupe prepovedanih substanc ali orožja. Takšne transakcije so bile večinoma izvedene preko t. i. temnega spleta (angl. dark web), ki je obvod vsakdanjega interneta in je deležen številnih kritik zaradi izvajanja nedovoljenih dejanj. Zaradi takšnih situacij so finančni regulatorji v številnih državah začeli sprejemati pravila, ki poostrujejo nadzor nad številnimi deli kriptotrga. Največji del v Sloveniji aplikativnih pravil je zajet v zakonodaji o preprečevanju pranja denarja in financiranja terorizma in v Peti direktivi EU o preprečevanju pranja denarja. Ta v regulirano okolje vključuje kriptoborze in podjetja za hranjenje kriptovalut za tretje osebe in od njih zahteva enako poročanje in preprečevanje transakcij, kot sicer velja za konvencionalne finančne institucije. Obstajajo pa tudi področja poslovanja s kriptovalutami, ki po trenutni zakonodaji EU niso zavezana k poročanju in preprečevanju po zakonodaji o preprečevanju pranja denarja. Ob nadaljnjem razvoju kriptovalut lahko upravičeno pričakujemo, da se bo regulativa o preprečevanju pranja denarja in financiranju terorizma razširila na kriptovalute. Neprestano spreminjanje zakonodaje povečuje zahtevnost izpolnjevanja novih zakonskih zahtev, s čimer se poveča tveganje njihovega neizpolnjevanja (Houben & Snyers, 2018). Za pravilno izvajanje zakonodaje o preprečevanju pranja denarja in financiranju terorizma sta ključnega pomena delovanje avtomatiziranega notranjekontrolnega okolja, ki omogoča identifikacijo vseh transakcij, ki izpolnjujejo zahtevane parametre, in primerno ukrepanje. V primeru neizpolnjevanja

zakonskih zahtev podjetjem pretijo izredno visoke denarne kazni in morebitna omejitev ali prepoved poslovanja, : kar ima lahko za družbo zelo negativne posledice.

Svet kriptovalut so v preteklosti večkrat pretresli škandali zaradi vdorov v sisteme kriptoborz ali drugih hraniteljev kriptovalut, v katerih je prišlo do sistematičnih kraj kriptovalut z računov imetnikov. Obseg največjih tovrstnih kraj je bil z vidika finančnega sistema nepredstavljiv, saj je največja kraja Bitcoinov z borze Mt. Gox leta 2014 privedla to borzo celo do stečaja. Mt. Gox je bila takrat največja kriptoborza na svetu, odgovorna za skoraj dve tretjini vseh transakcij s kriptovalutami. Kraja pa je zajela kar 7 % Bitcoinov, ki so bili takrat v obtoku. Največje presenečenje po odkritju kraje je bilo, da je potekala kar 2 leti. Kraja Mt. Goxa ni bil edini tak primer v zgodovini kriptovalut. Glede na obseg števila transakcij s kriptovalutami, sta pogostost in obseg tovrstnih kraj izjemno visoka. Poudariti je potrebno še pomembno dejstvo, da za primer kraje kriptovalut ne obstaja noben varnostni mehanizem, ki bi kompenziral izgubo tistih, ki so jim bile kriptovalute ukradene. Zaradi napisanega obstaja tveganje, da bi bile kriptovalute ukradene, brez vednosti organizacije, ki jih hrani. Neopažena kraja povečuje tveganje neobstoja kriptovalut, saj bi bil imetnik prepričan v obstoj enot kriptovalut, kar bi mu potrjeval tudi hranitelj kriptovalut.

3.1.5 Davčna tveganja

Obdavčitev transakcij s kriptovalutami zaenkrat ni urejena niti na ravni Slovenije niti na ravni EU ali druge širše skupnosti držav. Nedorečeno stanje odpira številne možnosti za interpretacijo pravilne obravnave kriptovalut. Najkompleksnejši del regulacije je odgovornost finančnih organov, ki z različno uspešnostjo naslavljajo pravne praznine vezane na davčno obravnavo. Pravna praznina, ki je posledica nedorečenosti glede davčnih vprašanj, povzroča tveganje za nepravilno obdavčitev ali nepravilno poročanje finančnim organom, posledično pa tudi kazni, ki jih lahko prejmejo imetniki kriptovalut. Dejanski primer sprememb davčnega okolja je primer iz Slovenije, saj je FURS spreminjal svoja pojasnila o obdavčevanju ter jih implementiral z retroaktivno uporabo, kar lahko pomembno spremeni način poslovnega odločanja in sposobnosti po implementiranju sprememb v zahtevah na tem področju.

3.1.6 Druga specifična tveganja kriptovalut

Najpogostejše tveganje, povezano s kriptovalutami, je tveganje podvojenega zapravljanja. Pomen tega tveganja je tako velik, da je Satoshi Nakamoto o njem ob formiranju Bitcoina napisal dizertacijo. Transakcije v blockchainu so skoraj popolnoma ireverzibilne, vendar pa je stanje ireverzibilnosti doseženo šele, ko določeno transakcijo potrdi zadostno število uporabnikov. V vmesnem času lahko pošiljatelj enot transakcijo prekliče, lahko pa do neizvedbe transakcije pride tudi zaradi nezadostnega števila enot na računu plačnika ali zaradi tehnične težave pri prenosu enot kriptovalute (Broby & Paul, 2017). Potrjevanje transakcij pri nekaterih kriptovalutah poteka dalj časa, kot je to običajno, kar bi lahko

izkoristili prevaranti, ki bi iste enote kriptovalut skušali večkrat zamenjati za blago ali storitev. Govorimo o obstoju nevarnosti za izvedbo prevare v obliki dvojnega ali večkratnega zapravljanja. V praksi se prejemniki plačila pred tem tveganjem najpogosteje zavarujejo z odloženo predajo blaga uporabniku, in sicer do trenutka, ko je transakcija zapisana v blockchainu posamezne valute oziroma potrjena.

Transakcije kriptovalut se lahko sprožijo zelo enostavno in skoraj popolnoma neodvisno od geografskih pogojev, saj je za izvedbo takšne transakcije potreben samo ključ, s katerim pobudnik dostopa do denarnice s kriptovalutami, kakršnakoli druga preveritev istovetnosti ni potrebna. V klasičnem finančnem sistemu se pogosto zahtevajo dodatne preveritve, kot sta zahtevana osebna zglasitev v poslovalnici banke pri večjih transakcijah ali vpis enkratno generiranega gesla pred potrditvijo elektronske transakcije, da bi se s tem preprečile možnosti prevar. Transakcije, ki so posledica prevar, pomenijo za revizorje izvedbo dodatnih postopkov, s katerimi preverjajo, ali je bila transakcija izvedena s prevaro ali ne. Kritične transakcije na področju prevar so transakcije s povezanimi osebami družbe oziroma navidezno nepovezanimi osebami, saj lahko družbe preko takšnih transakcij prirejajo podatke v računovodskih izkazih.

3.2 Postopki revidiranja kriptovalut

V poglavju 1.8 Izkazovanje kriptovalut v računovodskih izkazih sem navedel, v katerih postavkah računovodskih izkazov je primerno izkazovati kriptovalute. Kljub temu, da prikazovanje sredstev v različnih postavkah sledi različnim računovodskim pravilom, bo izvajanje revizijskih postopkov kriptovalut v vseh primerih podobno. V nadaljevanju navajam postopke, s katerimi je najprimerneje potrditi posamezne revizijske trditve. En postopek je lahko uporabljen za potrditev več revizijskih trditev, vendar je naveden zgolj pri postopkih za najbolj relevantno trditev.

3.2.1 Postopki revidiranja obstoja

Kriptovalute lahko podjetja hranijo pri za hrambo specializiranih družbah (takšni primeri so kriptoborze in skrbniki kripto denarnic). V takšnem primeru je najenostavneje pridobiti potrditev enot na računu v obliki neodvisne potrditve količine s strani hranitelja enot. Takšno prakso potrjevanja enot revizorji redno uporabljajo pri potrjevanju finančnih naložb ali denarnih sredstev. Neodvisna potrditev je tudi pravno zavezujoča za potrjevalca, zato je verjetnost za prevaro s strani družbe nižja. Vendar se moramo zavedati, da lahko pri potrjevanju kriptovalut hitro naletimo na ovire, med katerimi je smiselno izpostaviti zlasti dve. Prva je, da hranitelj enot kriptovalut morda ne deluje v pravnem sistemu, kjer bi morebitne potrditve nepravilnih vrednosti lahko bile sankcionirane. Poleg tega takšne družbe pogosto niso nadzorovane s strani nadzornih organov (v Sloveniji sta to Banka Slovenije za nadzor bank in ATVP za nadzor borznoposredniških hiš), kar privede do vprašanja o zanesljivosti delovanja teh družb in o zanesljivosti njihovih evidenc. Drugo oviro pri

potrditvi pa predstavlja velika verjetnost, da te potrditve s strani hranitelja kriptovalut sploh ne bi prejeli. Praksa vračanja potrditev stanj se v svetu razlikuje, zato lahko hitro naletimo na hranitelja, ki števila enot zaradi različnih razlogov ne bi želel potrditi. Razlogi za to so lahko nerazumevanju pomena potrditve, potencialnem tveganju za družbo, da potrdi stanje, ki ni resnično, ali nezaupanje v svoje interne procese, da lahko dejansko zagotovijo relevanten podatek. Pomemben dejavnik za potrditev je tudi število kraj z računov hraniteljev, do katerih je prišlo tudi brez vednosti hranitelja. Iz zapisanega izhaja, da je potrditev, podana s strani hranitelja sredstev, manj zanesljiva in ne zadošča za potrditev stanja števila enot kriptovalut. Vendar pa nekatere družbe, ki hranijo sredstva, opravljajo dodatne postopke, s katerimi želijo zagotoviti večjo zanesljivost svojega delovanja in na ta način doseči zanesljivejše delovanje za imetnike računov. Gre za primere izvajanja obsežnih revizijskih pregledov internih postopkov in stanj v denarnicah s strani neodvisnih revizorjev ali pridobivanja mednarodnih certifikatov zanesljivosti delovanja. Drugi pomemben dejavnik zaupanja v hranitelje kriptovalut je tudi regulatorno okolje, v katerem deluje hranitelj kriptovalut, saj so nekatera okolja z vidika nadzora in pravnega varstva imetnikov kriptodenarnic bolj rigorozna. Revizor mora na podlagi zgoraj opisanih dejavnikov presoditi, ali bo hranitelj zanesljivo zagotovil potrditev obstoja v obliki neodvisne potrditve.

V poglavju, ki govori o tveganjih, povezanih s kriptovalutami, sem opisal tudi tveganja morebitnih naknadno nepotrjenih in preklicanih transakcij ter transakcij, ki še čakajo na izpolnitev vseh pogojev za izvedbo. Za kriptovalute v teh transakcijah veljajo določene omejitve ali pa so lahko prikazane na nepravilnem računu, vendar bodo vrnjene na račun pobudnika transakcije. Ker so lahko te transakcije skrite upravljalcu kriptodenarnice, jih ta tudi ne more pravilno potrditi znotraj neodvisne potrditve. Alternativni postopek je v tem primeru postopek potrditve z nakazilom sredstev na drugo denarnico. V tem primeru bo izveden prenos vseh sredstev, za katera ne veljajo nobene omejitve. S tem bi tudi potrdili obstoj in obvladovanje vseh enot kriptovalut s strani lastnika denarnice. Ta način potrditve obstoja je pri kriptovalutah enostaven, saj je nakazilo mogoče v vsakem trenutku, prav tako je tudi strošek nakazila v primeru, da ne operiramo z velikim številom valut, nizek. Težava lahko nastane zaradi dejstva, da je potrebno nakazilo izvesti v trenutku preseka poslovnega leta. Družbe, ki bi neprestano poslovale s kriptovalutami, bi lahko prejele v nekaj urah, ki bi bile potrebne za potrditev transakcije, znaten obseg kriptovalut, ki tako ne bi bile potrjene in bi jih bilo potrebno obravnavati v sklopu pravilne časovne umestitve transakcij. Poleg tega se pojavlja vprašanje, kakšen bi bil odziv omrežja in njegova zanesljivost, če bi ob datumih, ko se končuje največ poslovnih let (na primer 31. 12.). Takrat bi bilo namreč prenakazanih veliko enot kriptovalut v zelo kratkem času.

3.2.2 Postopki revidiranja popolnosti

Družba lahko poseduje več kriptodenarnic, zato je pomembno, da revizor identificira vse izmed njih, saj lahko samo na ta način zagotovi popolnost vseh sredstev in morebitnih obveznosti, ki bi izhajale iz sredstev v posamezni kriptodenarnici. Nerazkritje vseh

kriptodenarnic s strani revidiranca je lahko indikator za prevaro, izvedeno s strani revidiranca, vključno z možnostjo preglasovanja internih kontrol s strani managementa. Ugotovljeno nerazkritje kriptodenarnic je potrebno nasloviti in od družbe pridobiti zadostno zagotovilo, da nima drugih zamolčanih denarnic. Ta proces je lahko zelo zahteven, saj obstaja verjetnost, da določene denarnice obstajajo kratek čas, zato transakcij z njimi ni enostavno identificirati, poleg tega pa tudi ne obstaja register kriptodenarnic, podoben registru, ki obstaja za transakcijske račune družb, v katerem bi lahko preverili, katere kriptodenarnice pripadajo posamezni družbi. Način za zmanjšanje tveganj prikritja denarnic je delujoč sistem linij odgovornosti in notranjih kontrol, vezanih na odprtje nove kriptodenarnice (Chartered Professional Accountants Canada, 2018a). Poleg tega mora revizor opraviti izdatne procese identificiranja sumljivih transakcij, tako v glavni knjigi kot tudi na drugih kriptodenarnicah in transakcijskih računih, kjer bi lahko odkril transakcije z do tedaj neznano denarnico.

Z vidika popolnosti transakcij mora revizor poskrbeti tudi, da zajame vse transakcije, ki se nanašajo na posamezno obdobje, kar v revizijski terminologiji imenujemo cutoff. Pri transakcijah s kriptovalutami obstaja povečano tveganje za nepravilnosti, saj lahko potrditev transakcije traja sorazmerno dolgo, v nekaterih primerih tudi po več dni. Priporočljiv revizijski postopek je zato pregled transakcij, ki so se zgodile pred in po koncu revidiranega obdobja, ter preveritev, ali se transakcija nanaša na pravilno obdobje. Še posebej morajo revizorji biti pozorni na razloge, ki lahko privedejo do zakasnitve izvedbe transakcije, kot so zamude pri posameznem upravljalcu kriptodenarnice ali v primeru nekaterih kriptovalut kompenziranje rudarjev (nižja kompenzacija pripelje do kasnejše potrditve) (CPA, 2018a).

3.2.3 Postopki revidiranja vrednotenja

Družba se lahko odloči za različne načine izkazovanja kriptovalut v svojih računovodskih izkazih. Glede na izbiro naj bi sledilo tudi vrednotenje teh postavk, vendar je v primeru kriptovalut, ne glede na izbor načina izkazovanja, najprimernejše izkazovanje po pošteni vrednosti. Pri izkazovanju po pošteni vrednosti je pomembno izpolnjevanje izkazovanja v skladu s standardi (med zalogami jih vrednotimo po pošteni vrednosti, zmanjšani za stroške prodaje, med finančnimi instrumenti jih upoštevamo samo po pošteni vrednosti) in računovodsko politiko podjetja. Dodatne specifične lastnosti, ki vplivajo na vrednotenje kriptovalut so tudi (CPA, 2018b):

- Kriptoborze delujejo 24 ur na dan, 7 dni v tednu in zaradi velike volatilnosti kriptovalut lahko ima ura vrednotenja pomemben vpliv na ceno kriptovalute. Iz tega izhaja, da mora biti način vrednotenja kriptovalut natančno definiran (na primer ob 23.59 na dan izkaza finančnega položaja) in konsistentno uporabljan za različne kriptovalute in različne dneve vrednotenja.
- Tako kot pri trgovanju z delnicami in blagom, obstaja tudi pri kriptovalutah na vsak dan odprtih več nakupnih in prodajnih naročil, katerih cena lahko pomembno odstopa od

uradnega tečaja na borzi. Ob dejstvu, da je lahko obseg transakcij na posamezni kriptoborzi, kjer želimo izvesti transakcijo, nizek, lahko to privede do pomembnega likvidnostnega tveganja pri vrednotenju kriptovalut.

- S vsako kriptovaluto lahko praviloma trgujemo na več kriptoborzah, na katerih se lahko tečaji za posamezne kriptovalute pomembno razlikujejo med seboj.
- Različna regulacija trgov kriptovalut in kriptoborz, lahko med drugim pripelje do pomanjkanja jasnosti glede tega, kako je cena določene kriptovalute poročana, kar lahko posledično privede do razlikovanja v vrednostih.
- Številne transakcije so lahko izvedene izven blockchaina in bodo vanj vpisane šele po nekaj dneh ali celo tednih.

Zaradi zgoraj navedenih karakteristik vrednotenja kriptovalut obstaja dvom glede primernosti vrednotenja kriptovalut izključno z uporabo tečaja določene kriptoborze, saj s tem ne pridobimo nujno informacije o najprimernejši ceni. Smiselno je zahtevati izvedbo modelskega vrednotenja, kjer so upoštevane vrednosti kriptovalute na več borzah, saj s tem izločimo morebitna večja odstopanja v ceni. Drugi pomemben faktor v modelu je ocena likvidnosti trga. Ta ocena je še toliko bolj pomembna, če uporabljamo kriptovaluto pri vsakdanjem poslovanju in ne kot naložbo, saj lahko povzroči nezmožnost zamenjave kriptovalut v želeno valuto velike neposredne in posredne izgube. Revizor mora pri pregledu vrednotenja oceniti primernost uporabljenih predpostavk in argumentacijo primernosti njihove uporabe, s strani revidiranca. Revidiranje vrednotenja kriptovalut je za revizorja izredno zahtevno, saj mora poznati številne specifike kriptotrga, da lahko oceni primernost posredovanega modela in trditve revidiranca.

Transakcije kriptovalut niso popolnoma anonimne, saj sta znana tako prejemnik kot pošiljatelj sredstev, vendar sta znana zgolj pod psevdonimom, ki ga je uporabnik izbral za poimenovanje svoje kriptodenarnice. Ker so psevdonimi popolnoma nepovezani z dejanskim imenom fizične osebe ali družbe, jih ne moremo preveriti. Iz tega izhaja, da je izredno enostavno skriti transakcije med povezanimi osebami. Takšne transakcije so lahko zelo tvegane, saj lahko privedejo do nepravilnih vrednotenj ali celo do prevar na področju vrednotenja in popolnosti razkrivanja transakcij s povezanimi osebami (CPA, 2018b). Na zanesljivost zanašanja na popolno razkritje vseh transakcij s povezanimi osebami lahko vpliva učinkovito kontrolno okolje, v katerem revidiranec pripravi za vse osebe, s katerimi posluje, skrben pregled imetnika kriptodenarnice in ne posluje z neznanimi imetniki denarnic. Revizijski postopki, s katerimi lahko revizor preveri popolnost identifikacije povezanih oseb, tako poleg preveritve delovanja notranjekontrolnega okolja zajemajo tudi preveritev sumljivih transakcij z računi, ki pomembno odstopajo od vsakdanjega posla (višina transakcij, odstopajoča cena na enoto, nenavadni dnevi transakcij, transakcije v podobnih zneskih ipd.).

Pri razkrivanju vrednosti kot primer dobre prakse nekatera strokovna združenja (na primer Chartered Professional Accountants Canada) priporočajo razkrivanje uporabljenih vrednosti kriptovalut. Argumentacija za dodatno razkrivanje izhaja iz razlik v vrednosti med

različnimi kriptoborzami in iz visoke volatilnosti. Razkritja lahko zajemajo samo vrednost ali so podobna razkrivanju uporabljenih predpostavk za vrednotenje finančnih naložb, ki so po MSRP 13 razvrščena v raven 3. Dodatno mora biti revizor pozoren tudi na to, da družba razkrije morebitna materialna odstopanja od vrednotenja na datum izkaza finančnega položaja v dogodkih po datumu bilance (EY, 2012).

3.2.4 Postopki revidiranja pravic in obvez

Zelo specifična težava revidiranja kriptovalut je primerna obravnava dostopa do njih. V delujočem pravnem sistemu lahko uporabnik po pravni poti pridobi nadzor nad sredstvi tudi ob izgubi elektronskih podatkov za dostop do njih. Ob izgubi ali kraji osebnega ključa za dostop do kriptodenarnice pa revidirancu ni omogočen podoben dostop do kriptovalut v denarnici. Dostopa do sredstev uporabnik ne more pridobiti po pravni poti, saj tehnično ni mogoče dostopati do teh sredstev, ker so tajno shranjena v blockchainu, do katerega nima dostopa nihče oziroma ima dostop do njega neznani imetnik. Revizor lahko obravnavati dostop do kriptodenarnice, kjer mora revidiranec dokazati sposobnost dostopanja do sredstev s strani ali dokazati, da ima primeren ključ. Hkrati sta za revidiranca zelo pomembna primerna hramba osebnega ključa na varnem mestu ter hramba in nadzor nad postopkom hrambe duplikata v primeru izgube primarnega ključa. Namen tega postopka je zagotovitev, da ključ ne bo izgubljen v času po izvedbi samih revizijskih postopkov. Primerna hramba sekundarnega ključa je hranjenje kopije digitalnega ključa na drugi elektronski napravi ali hramba ključa v papirni obliki. Poleg tega postopki za nadzor nad osebnimi ključi omogočajo pravočasno evidentiranje morebitne izgube ključa in primerno posredovanje teh informacij poslovodstvu ter revizorjem.

Evidenca dejanskih lastnikov kriptodenarnic ne obstaja, niti je ni mogoče sestaviti brez prostovoljnega poročanja vseh imetnikov kriptodenarnic. Zaradi neobstoja takšne evidence je postopek pridobitve zagotovila o dejanski lasti kriptovalut v denarnici zahtevnejši od postopka standardne potrditve lastništva. Lastništvo sredstev ni nujno enako obvladovanju osebnega ključa za dostop do kriptodenarnice. V praksi se lahko pojavijo situacije, ko je lastnik kriptovalut v denarnici fizična oseba in ne družba, prav tako lahko sredstva v eni kriptodenarnici pripadajo večjemu številu lastnikov. V primeru, da družba revizorju ne razkrije vseh dejanskih lastnikov sredstev, gre za prevaro, ki pa jo revizor težko identificira samo z uporabo standardnih revizijskih postopkov. Prevaro lahko revizor identificira zgolj s profesionalnim skepticizmom skozi celoten proces revizije družbe in s specializiranimi postopki, ki morajo biti prilagojeni poslovnemu okolju in modelu revidiranca. Zmanjšanje možnosti za prevaro pri potrditvi obstoja je mogoče doseči z delujočim sistemom notranjih kontrol, v katerem se hranijo vsi dokumenti, s katerimi lahko vplivamo na lastništvo vsebine kriptodenarnice. Predložitev te primerno nadzorovane in arhivirane dokumentacije lahko revizorju da delno zagotovilo o pravilnosti izkazovanja lastništva, vendar ne more biti edini postopek potrjevanja (CPA, 2018b).

Lastnost transakcij v blockchainu je, da so ireverzibilne, kar ima poleg številnih pozitivnih lastnosti tudi negativno plat. V primeru, da je nakazilo preneseno na napačen račun, ni mogoče zahtevati vračila sredstev, če transakcija ni bila izvedena s partnerjem, ki bo sredstva prostovoljno vrnil. Ključnega pomena za preprečitev nakazila sredstev na napačno kriptodenarnico je, da ima družba vpeljane notranje kontrole, ki onemogočajo nakazilo na račun, ki ni vnesen v sistem, ter da so bili vsi računi, vneseni v sistem, primerno pregledani in potrjeni pred vnosom. Priporočljivo je, da revidiranec od dobavitelja pridobi potrjen dokument, ki dokazuje pravilnost podatkov o kriptodenarnici, s katerim lahko revidiranec in revizor kadarkoli preverita pravilnost vnosa podatkov v sistem. Poleg zagotovila, da sistem notranjih kontrol deluje, mora revizor pridobiti tudi zagotovilo, da tekom leta ni prišlo do napačnih transakcij. Postopki za odkritje nakazil napačnemu prejemniku zajemajo preverjanje morebitnih izvršb, izvedenih s strani dobaviteljev, ter pridobitev dodatnih zagotovil oseb, odgovornih za delo z dobavitelji, da niso seznanjeni s takšnimi primeri.

3.3 Dodatna razkritja kriptovalut

Kriptovalute so specifične zaradi dveh razlogov, in sicer zaradi neoptimalnega izkazovanja v računovodskih izkazih, ki ne omogočajo prikaza, po katerem bi lahko bile kriptovalute umeščene v trenutno shemo izkaza finančnega položaja, ki bi omogočila nedvoumno razumevanje za uporabnika, ter zaradi velikih nihanj vrednosti, ki so značilne za njih. Zaradi omenjenih lastnosti kriptovalut je smiselno poleg splošnih razkritij tveganj, ki so predstavljena v naslednjem poglavju, izkazati tudi dodatna razkritja, da izkazi zadostijo MRS 19, ki navaja, da morajo biti računovodski izkazi razumljivi širokemu krogu uporabnikov, ki izkaze uporabljajo pri ekonomskih odločitvah, ter da izkazovanje informacij, ki pomembno vplivajo na razumevanje izkazov, ni omejeno na same zahteve, ki izhajajo iz drugih MSRP. Takšna razkritja, ki lahko bistveno izboljšajo razumevanje izkazov, ki vsebujejo kriptovalute, so tudi (CPA, 2018b):

- opis kriptovalut, ki jih družba poseduje, njihovih pomembnih lastnosti in razlogov zakaj jih družba poseduje,
- število enot posameznih kriptovalut, ki jih ima družba v lasti ob koncu poslovnega leta,
- opis računovodske politike obravnave kriptovalut,
- če je uporabljen model vrednotenja po izvirni vrednosti, tudi razkritje poštene vrednosti z dodatnimi zahtevanimi razkritji po MSRP 13,
- informacije o tržnih tveganjih, povezanih s posamezno kriptovaluto (na primer volatilnost v preteklosti).

MSRP 13 zahteva dodatna razkritja, vezana na pošteno vrednost, ter definira ogrodje za formiranje poštene vrednosti. Skladno s tem standardom je poštena vrednost tista vrednost, ki jo je za neko sredstvo pripravljena plačati neodvisna stranka, ki poseduje zadostno ekonomsko znanje, pozna karakteristike tega sredstva in je prostovoljno vstopila v transakcijo. Poštena vrednost je po MSRP 13 razdeljena na tri ravni na podlagi predpostavk,

ki so uporabljene pri vrednotenju. Prva raven vključuje kotirajočo ceno na aktivnem trgu za identično sredstvo ali obveznost, ki je lahko dostopna na datum merjenja. Pod drugo ravnjo so izkazani instrumenti po pošteni vrednosti, ki v vrednotenje vključujejo predpostavke, ki so prosto dostopne, opazovane na trgu in niso zajete v prvi ravni. Tretja raven vključuje predpostavke, ki jih ne moremo prosto opazovati na trgu. Pri merjenju kriptovalut se moramo zato najprej vprašati, ali obstaja aktiven trg za posamezno kriptovaluto in ali je na njem izvedenih dovolj transakcij, da ga lahko tretiramo kot likvidnega, saj lahko samo tako predpostavimo, da je cena na borzi primerna za definiranje poštene vrednosti. V primeru, da neko sredstvo kotira na več trgih, je potrebno identificirati primarni trg. V primeru, da je primarnih trgov več (v primeru, da je obseg transakcij na več trgih primerljiv), lahko finančna sredstva izkazujemo po vrednosti, ki je za družbo najugodnejša, vendar ob predpogoju, da finančne naložbe na tem trgu lahko dejansko prodamo. Pri kriptovalutah je trgov praviloma več, vendar mora revidiranec pri vrednotenju upoštevati likvidnost teh trgov in morebitne druge omejitve, ki jih predstavljajo posamezni trgi. Različni trgi lahko omogočajo trgovanje v različnih velikostih enot (na primer ena enota ali del enote), kar lahko še dodatno oteži oceno primarnega trga posamezne kriptovalute. Družba mora pri vrednotenju po potrebi aplicirati tudi likvidnostni faktor. Posamezne kriptovalute pogosto tudi ne bodo izpolnjevale vrednotenja znotraj ravni 1. Zaradi številnih faktorjev, ki vplivajo na vrednotenje, lahko za večjo konsistentnost družba uporabi vrednotenje na ravni 3, če meni, da je to primernejše in bolje odraža pošteno vrednost neke kriptovalute. Revizor mora kritično oceniti argumentacijo za takšen pristop, ki je lahko resnično bolj smiseln, in ne sme avtomatsko zahtevati vrednotenja po ravni 1. Pri vrednotenju po ravni 3 obstaja tveganje, da niso razkrite vse pomembne predpostavke, ki so uporabljene pri vrednotenju, zato mora revizor kritično preveriti takšna razkritja (CPA, 2018b).

Poleg razkritij, zahtevanih po MSRP, lahko regulatorni organi zahtevajo, da se morajo v letna poročila vključiti tudi dodatna razkritja. Prav tako je lahko smiselno v izkaze vključiti razkritja, ki jih družba poroča poslovodstvu.

Poleg izkazovanja vrednosti v izidu finančnega položaja mora družba spremembe v vrednosti kriptovalut vključiti tudi v izkaz poslovnega izida. Ne glede na to, na kak način so kriptovalute izkazane v izkazu finančnega položaja, obstaja velika verjetnost, da družba v posamezni postavki ne bo izkazovala samo kriptovalut. Ker lahko kriptovalute privedejo do velikih nihanj v vrednosti posameznih postavk in posledično tudi do visokih prihodkov ali odhodkov iz njihovega naslova, je priporočljivo celoten učinek vrednotenja kriptovalut skozi leto izkazati ločeno, saj tako družba ne zamegli in ne razvrednoti razkritij ostalih sredstev znotraj postavke.

Družba mora kot obvezni sestavni del letnega poročila razkriti dogodke po datumu bilance, pri čemer mora navesti vse pomembne dogodke, ki bi za uporabnika izkazov lahko predstavljali pomembna dejstva za razumevanje izkazov kot celote. Kot vsa ostala sredstva in obveznosti so tudi kriptovalute podvržene morebitnim neljubim dogodkom, kot sta kraja sredstev ali izguba dostopa do ključa, o čemer mora revidiranec prilagoditi izkaze ali pa

mora te dogodke razkriti med dogodki po datumu bilance. Poleg tega je pri kriptovalutah priporočljivo razkriti tudi vrednost premoženja ali enot kriptovalut na datum izdaje bilance, saj lahko ta vrednost bistveno odstopa od vrednosti ob koncu leta. V primeru, da so bila vsa sredstva ali obveznosti v kriptovalutah že udenarjena, pa je priporočljivo razkriti tudi efekt, ki ga ima transakcija na bodoče izkaze. Tudi če revidiranec ne razkrije teh dodatnih podatkov, lahko revizor presodi, da je potrebno nek dogodek vendarle razkriti, saj brez njega uporabniki ne bodo prejeli zadostnih informacij, potrebnih za pošteno razumevanje izkazov.

3.4 Izkazovanje finančnih tveganj, povezanih s kriptovalutami

MSRP zahtevajo izkazovanje finančnih tveganj, ki izhajajo iz bodočih sprememb v okolju. Namen teh razkrivanj je pojasniti tveganja, ki jih predstavlja poslovni model podjetja in niso vidne v izkazih. Med finančna tveganja med drugim štejemo tveganja sprememb obrestne mere, deviznih tečajev, tveganosti finančnih naložb in tveganja sprememb v predpostavkah merjenja. Različne postavke so podvržene različnim tveganjem. Prvo tveganje, ki je relavantno pri kriptovalutah, je nihanje vrednosti kriptovalut, ki jih družba poseduje. Zaradi nihanja v tržni vrednosti, ki ga je smiselno prikazati med tržnimi tveganji postavke, v kateri izkazujemo kriptovalute. Izkazovanje tveganj lahko zaradi posedovanja kriptovalut privede do redko videnih kombinacij tveganj in postavk. Takšen primer so lahko izkazovanja tržnega tveganja v postavkah neopredmetenih osnovnih sredstev. Drugo nenavadno izkazovanje tržnega tveganja je njegovo izkazovanje pri obveznostih in terjatvah, ki so posledica sprejemanja in poravnavanja kriptovalut v sklopu splošnega poslovnega modela. Po naravi so ta tveganja enaka valutnemu tveganju, saj družba izkazuje terjatve ali obveznosti v neki kriptovaluti, ki jo mora prevesti na funkcijsko valuto, v kateri so pripravljeni izkazi. Ker kriptovalute po definiciji ne spadajo med valute, izkazovanje valutnega tveganja ni pravilno. Bralec izkazov mora zato razumeti, da so zaradi nihanja v vrednosti tveganja kriptovalut pri terjatvah in obveznostih izkazana kot tveganja pri spremembi poštene vrednosti. Primerno je, da revidiranec med valutnimi tveganji predstavi tudi usklajenost med terjatvami in obveznostmi iz posameznih kriptovalut, saj lahko to pomembno pripomorejo k zagotavljanju bodoče likvidnosti v nekem časovnem intervalu. Pomembno tveganje, ki lahko izhaja iz poslovanja s kriptovalutami, je tudi likvidnostno tveganje, ki je posledica nedelujočega trga večine kriptovalut. Likvidnostno tveganje pri poslovanju s kriptovalutami v praksi pomeni nezmožnost udenarljivosti določenih kriptovalut, ker obseg transakcij ni dovolj velik, da bi lahko kriptovalute pretvorili v denar v doglednem roku. Likvidnostno tveganje lahko obvladujemo z »valutnim tveganjem«, ki je omenjeno v začetku odstavka.

3.5 Primeri prevar na področju kriptovalut in z njimi povezana tveganja za revizorje

V magistrski nalogi sem večkrat omenil prevare na področju kriptovalut in nevarnosti, ki pretijo imetnikom kriptovalut. V tem poglavju bom predstavil nekaj primerov prevar, ki smo jim bili priča v desetletju obstoja kriptovalut. Pri najbolj odmevnih krajah kriptovalut gre za

kraje kriptovalut s kriptoborz ali iz računov pri drugih podjetjih, ki omogočajo njihovo hrambo. Najodmevnejša je kraja kriptovalut v protivrednosti 350 milijonov USD iz takrat največje kriptoborze Mt. Gox. Ta kraja je trajala od leta 2011 do 2014 in je posledično privedla do propada omenjene borze (podrobnejši opis je zapisan v poglavju o notranjekontrolnih tveganjih). V Sloveniji sta bili odmevni tudi kraji ekvivalenta 5 milijonov USD z računov, odprtih pri Bitstampu, ter 56 milijonov USD z računov, odprtih pri družbi NiceHash. V vseh primerih je bila kraja izvedena zaradi varnostne pomanjkljivosti blockchaina, s pomočjo katere je neznanec pridobil dostop do denarnic oškodovancev. Družbe bi lahko, če že ne preprečile, pa zagotovo močno omejile obseg tovrstnih kraj z uvedbo učinkovitih notranjih kontrol, ki bi zaznale vdor. Kljub konstantnemu napredku pri razvoju varnostnih mehanizmov se pogostost kraj kriptovalut ne niža. Največja kraja v zgodovini kriptovalut se je zgodila leta 2018, ko je bilo ukradenih za 400 milijonov USD kriptovalut z Japonske borze Coincheck.

Poleg kraj s kriptoborz je bilo v preteklosti izvedenih tudi nekaj večjih kraj, pri katerih so posamezniki ali skupine izrabili varnostne pomanjkljivosti blockchaina posamezne kriptovalute in na ta način pridobili večje količine kriptovalut. Pogosto po takšnem dogodku uporabniki kriptovalut naredijo delitev (ang. hard fork), pri čemer se naredi kopija sistema pred takšno transakcijo, od tam naprej pa obstajata dve kriptovaluti. Najbolj znana delitev je nastal pri Ethereumu, ko je skupina, imenovana The DAO (kratica za decentralized authonomus organization), ukradla velik del ethrov v obtoku. Zaradi te kraje so se člani ožje skupnosti Ethereuma odločili za izvedbo delitve Ethereuma na Ethereum in Ethereum classic. Ethereum classic je platforma, kjer ostaja vidna kraja, in še danes obstaja med aktivnimi kriptovalutami. Omrežje vzdržuje ravno The DAO, ki je ukradel ethre. Kljub nadaljevanju delovanja ether classic, je ta valuta danes bistveno manj popularna kot ether. Od nastanka kriptovalut je bilo zaradi kraje kriptovalut na podlagi »luknje« v blockchainu izvedenih več takšnih delitev verig kriptovalut (ang. fork) ali razveljavitev transakcij v nekem obdobju (Wikipedia, 2018).

Poleg omenjenih kraj, vezanih na izrabo tehnologije, je bilo, predvsem v času nagle rasti vrednosti kriptovalut, izvedenih veliko konvencionalnih prevar, ki so bile aplicirane na kriptosvet. Ob visokih donosih so številni uporabniki podcenili tveganja, ki spremljajo poslovanje z novimi vrstami sredstev, kamor spadajo tudi kriptovalute. Prevare so lahko izvedene v naslednjih oblikah:

- Prevarantski ICO: V času največjega razcveta kriptovalut je bilo ustanovljenih veliko družb, ki so izdale kriptovalute z namenom izkoristiti investitorje v kriptovalute, ki so zaradi želje po bajnih donosih pogosto brezglavo vlagali denar v nove projekte. Največja prevara z ICO je bila izvršena na Kitajskem, kjer je skupina Shenzhen Puyin Blockchain izvedla tri ICO-je (ACChain, Puyin in BioLifeChain), s katerimi je 3.000 investirorjem ukradla 60 milijonov USD.
- Neresnične kriptoborze: Podobno kot druga prevarantska podjetja tudi neresnične kriptoborze zahtevajo nakazilo denarja na lažne denarnice, ki niso v lasti oškodovanca.

Samo v enem primeru v Ukrajini je tamkajšnja policija zaprla šest kriptoborz, ki so jih vodili trije posamezniki. Kljub vedenju o njihovem obstoju številne lažne kriptoborze še vedno nemoteno poslujejo, zato mora vsak uporabnik biti še posebej pozoren pri izbiri borze, s katero bo sodeloval.

- Piramidne sheme: Poleg formiranja dejanskih skladov, ki so investirala v kriptovalute, je nastalo tudi nekaj družb, ki so delovale po principu piramidne sheme. Najbolj poznano takšno prevaro je izvedel Homer Josh Garza, ki je ustanovil družbi GAW Miners in ZenMiners, ki sta obe namesto, da bi vlagali v rudarjenje kriptovalut, postali piramidni shemi. Skupna vrednost ukradenih sredstev je znašala 9 milijonov USD, za izvedbo kraje je regulator Securities and Exchange Commission (v nadaljevanju SEC), ki je v ZDA zadolžen za nadzor nad trgom vrednostnih papirjev, ustanovitelja strani, tudi uspešno sodno preganjal. Garza je bil obsojen na 21 mesecev zaporne kazni ter na vračilo vseh sredstev vlagateljem.

3.6 Potencial kriptovalut za računovodje in revizorje

Poleg številnih omejitev in izzivov na področju računovodenja in revizije kriptovalut, s katerimi se srečujejo gospodarske družbe, imajo kriptovalute tudi nekatere prednosti, katerih implementacija na druga področja lahko pomembno pripomore k razvoju revidiranja izkazov v prihodnje. Med najpomembnejše prednosti spadajo lastnosti kriptovalut, ki onemogočajo nekatere prevare ali manipulacije z izkazi. Med te spada nezmožnost podvajanja transakcij z istimi enotami kriptovalut, kar preprečuje tako prevare s strani kupcev, ki bi želeli protipravno pridobiti dvojno storitev ali blago ali drugače dvojno izkazovati prihodke, ki bi bili nato razveljavljeni. Pomembna pozitivna lastnost kriptovalut je tudi njihova transparentnost, saj so transakcije, če je imetnik računa znan, vidne vsem v blockchainu, kar otežuje prikrivanje transakcij z rizičnimi osebami. Naslednja pomembna prednost kriptovalut je, da nobene izvedene transakcije ni mogoče izbrisati iz registra, kar skoraj onemogoča : prevar s področja ilegalnih transakcij. Prav tako lahko revizor do teh preteklih transakcij kadarkoli dostopa in jih preveri, kar mu poenostavi izvajanje revizijskih postopkov na preteklih transakcijah. Nedvomno pa je ena izmed ključnih prednosti kriptovalut in blockchina njihova varnost. Blockchain shranjuje podatke na številnih mestih, zaradi česar je skoraj nemogoče izvesti vdor in uničenje podatkov, ki so hranjeni v njem.

Vse navedene prednosti izhajajo iz blockchaina in bodo v prihodnosti lahko implementirane na številna druga področja finančnega poročanja in revidiranja, kjer bodo pomembno izboljšale notranjekontrolno okolje družb, saj jih je skoraj nemogoče obiti ali pretentati. Hkrati blockchain omogoča tudi varno hrambo podatkov, kar je v današnjem času izredno pomembna lastnost vseh sodobnih IT-sistemov in omrežij. V bolj oddaljeni prihodnosti bomo morda priča tudi omrežjem, ki bodo temeljila na blockchainu in bodo vključevala številne lastnosti revidiranja samih sebe, v blochchain lahko namreč uvedemo številne kontrole in prepreke, ki onemogočajo izvedbo neželenih procesov. Takšne kontrole je tudi skoraj nemogoče obiti, zaradi česar je zanesljivost kontrolnega okolja zelo visoka.

3.7 Priporočila in ugotovitve

Pri raziskovalnem delu, izvedenem v sklopu pisanja magistrske naloge, sem ugotovil, da je področje kriptovalut zelo raznoliko in se v marsičem razlikuje od lastnosti konvencionalnih sredstev, s katerimi računovodje in revizorji operirajo na vsakodnevni bazi. Velik del lastnosti, iz katerih izhajajo omenjene razlike, je posledica njihovih tehničnih posebnosti, še zlasti tistih, ki izhajajo iz blockchaina. Vse te lastnosti pripeljejo do pogosto unikatnega položaja kriptovalut v ekonomskem, pravnem ter tehničnem okolju, kar v osnovi onemogoča njihovo enoznačno obravnavo v računovodskih izkazih in predstavlja tudi številna dodatna tveganja, za katera še ni vzpostavljenih učinkovitih odzivov. Kljub vsemu so se številne mednarodne revizijske hiše in posamični regulatorji lotili obravnave kriptovalut za potrebe računovodenja in revizije, obravnavali so izzive in izdali priporočila za primerno obravnavo kriptovalut.

Računovodjem pred začetkom uporabe kriptovalut priporočam, da se temeljito pripravijo na njihovo implementacijo. Priprava mora vključevati spoznavanje kriptovalut, s katerimi bo družba poslovala, njihovo aktualno pravno in davčno obravnavo in načrtovanje notranjega kontrolnega okolja, da lahko družba zajame vse potrebne podatke, ki jih potrebuje za primerno obvladovanje tveganj in poročanje državnim organom, poslovodstvu ter preko računovodskih izkazov tudi drugim deležnikom. Pri odgovarjanju na v prejšnji povedi navedena vprašanja in pri implementiranju odločitev ni enoznačnega pravila, saj je pri kompleksnosti obravnave kriptovalut, potrebno upoštevati obseg, namen in druge podrobnosti poslovanja družbe, kot so poslovni model in vrste kriptovalut v uporabi. Računovodjem pri družbah, ki kriptovalute uporabljajo kot plačilno sredstvo, predlagam, da obseg kriptovalut, ki jih družba ohranja v izkazih, redno znižujejo na obseg, potreben za pokritje obveznosti v kriptovalutah, saj se na ta način močno zmanjša izpostavljenost tveganjem, ki so za kriptovalute specifična. V primeru tega poslovnega modela so poudarjena tveganja vezana na likvidnost in davčno področje. Na drugi strani pa računovodjem družb, ki posedujejo kriptovalute z namenom investiranja, priporočam, da v prvi vrsti poskrbijo, da osebe, odgovorne za trgovanje, upoštevajo vsa tržna tveganja, katerim so dodatno ali izdatneje podvržene kriptovalute. Ta tveganja so predvsem volatilnost in tveganja vezana na izgubo dostopa do kriptodenarnic, kjer družbe hranijo kriptovalute. Prilagajanje notranjih kontrol in vprašanj, vezanih na preostalo obravnavo, je v računovodstvu vedno odvisno od ocene dejanske izpostavljenosti določenemu tveganju, saj je ekonomsko nesmiselno naslavljati tveganja, katerih potencialni efekt je nižji od stroškov učinkovitega nadziranja teh izgub. Revizorjem na drugi strani priporočam, da kritično preverijo notranjekontrolno okolje in preverijo, ali so s kontrolami naslovljena vsa za družbo pomembna tveganja ter ali kontrole tudi primerno zmanjšujejo tveganje, obvladovanju katerega so namenjene. Pri načrtovanju revizijskih procesov revidiranja podrobnosti je potrebno dobro razumeti delovanje kriptovalut in ponudnikov storitev, ki so nanje vezani, saj lahko samo na ta način pridobimo zadostno zagotovilo, da bo izkazovanje v revidiranih izkazih brez pomembnih nepravilnosti. Revizor se mora pred sprejemom posla, pri katerem

se bo soočil s kriptovalutami, zavedati, da so situacije, vezane na kriptovalute, pogosto unikatne in da s konvencionalnimi revizijskimi postopki bodisi ne bo mogoče pridobiti potrditve bodisi ta ne bo naslavljala vseh tveganj, ki se pojavljajo pri kriptovalutah. Vse omenjene razsežnosti, ki so vezane na poslovanje s kriptovalutami, bistveno povečujejo tveganje same revizije s stališča revizorja, zato tega tveganja revizor ne sme zanemariti.

SKLEP

Kriptovalute so bile zamišljene kot pregleden, moralno nesporen in cenovno ugoden plačilni sistem, ki bi ga lahko uporabljali kadarkoli in kjerkoli na svetu. Te lastnosti kriptovalut so še vedno globoko zakoreninjene v argumentih njihovih zagovornikov, vendar je praksa pokazala, da je poleg prednosti, ki jih kriptovalute prinašajo na eni strani, na drugi strani vsaj toliko ovir in vprašanj, ki še niso bila primerno naslovljena, da bi kriptovalute lahko ogrozile primat fiat denarja, kar je bila tudi osnovna ideja utemeljiteljev kriptovalut. Kljub vsemu so dogodki v zadnjem letu zagotovili, da bodo kriptovalute in blockchain tehnologija ostali za vedno v uporabi. Ravno nesluten razvoj kriptovalut je pripeljal do prvih praktičnih uporab kriptovalut v svetu in posledično do računovodskih vprašanj glede njihove primerne obravnave in izzivov njihovega revidiranja.

Kriptovalute so sorazmerno nova kategorija sredstev, ki še nima enoznačne obravnave v računovodskih standardih, kar lahko že v samem začetku privede do namernega zavajanja družb pri njihovem izkazovanju. Poleg tega so bile kriptovalute večkrat že uporabljene kot sredstvo prevare in zavajanja investitorjev z namenom pridobitve koristi za družbo oziroma povedano konkretneje za njene lastnike. V takšnih situacijah je zato prisotnost revizorja ključnega pomena za to, da zmanjša tveganja v delovanju finančnega sistema kot celote, kamor posredno spadajo tudi kriptovalute. Tveganja za družbe uporabnike kriptovalut so bistveno širša kot za druge družbe, saj so številna vprašanja glede njihovih lastnosti in obravnave še nedorečena in se zato hitro spreminjajo. Za kvalitetno opravljanje naloge revizorja je zato poznavanje ozadja kriptovalut in vseh tveganj, povezanih z njimi, izjemno pomembno.

Naj zaključim z mislijo, da so kriptovalute povzročile pravi pretres, tako na finančnih trgih kot tudi na področju računovodstva in revizije. Ta pretres je pokazal, da tudi posel z več kot stoletno zgodovino ni imun na spremembe iz okolice in da je potrebno na takšne situacije hitro odreagirati, saj je samo vprašanje časa, kdaj se bo odprlo novo tehnološko področje, ki po lastnostih ne bo ustrezalo ničemur, do tedaj znanem. Kljub začetni evforiji okoli kriptovalut se je prah okoli njih polegel, kot je padala njihova vrednost, kljub temu pa ostajajo ena izmed kategorij sredstev, ki nas bo spremljala še vrsto let, tako v ekonomskem kot v tehničnem smislu. Z vidika revizorjev je ključno razumevanje tveganj, ki spremljajo poslovanje s kriptovalutami, in postopkov, s katerimi jih lahko obvladujemo, saj številne institucije načrtujejo uporabo blockchaina na številnih novih področjih, ki jih bo prav tako potrebno revidirati v izkazih družb.

LITERATURA IN VIRI

1. Allen & Overy LLP. (2017). *Legal & Regulatory Risk Note Cryptocurrency AML risk considerations.* Pridobljeno 18. avgusta 2018 iz http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Cryptocurrency-AML-risk-considerations.aspx
2. Arens, A. A., Elder, R. J. & Mark, B. (2010). *Auditing and assurance services: an integrated approach*. Boston: Prentice Hall.
3. Association of Chartered Certified Accountants - ACCA (brez datuma). *What is audit risk?* Pridobljeno 18. avgusta 2018 iz https://www.accaglobal.com/caribbean/en/student/exam-support-resources/professional-exams-study-resources/p7/technical-articles/audit-risk.html
4. Association of Chartered Certified Accountants – ACCA. (2015). *Addressing Disclosures in the Audit of Financial Statements – Revised ISA's and Related Conforming Amendments*. Pridobljeno 5. junija 2018 iz https://www.accaglobal.com/caribbean/en/student/exam-support-resources/fundamentals-exams-study-resources/f8/technical-articles/assertions.html
5. Bajuk Mušič, A. (2017, oktober). Računovodenje poslov s kriptovalutami. *IKS, 10*, 20–32.
6. Bizant, E., Černe, I., Dukič, U., Hrovat, J., Jan, K., Reya, V., Simčič, M. & Vrhovec, J. (2018). *Problematika pomanjkanja pravne regulacije pri poslovanju in izdaji kriptovalut*. Pridobljeno 24. avgusta 2018 iz http://www.pf.uni-lj.si/media/kriptovalute.-.koncni.elaborat.pdf
7. BPP Learning Media. (2017). *P7 Advanced Audit and Assurance.* London: BPP Learning Media.
8. Broby D. & Paul, G. (2017). *The Financial Auditing od Distibuted Ledgers, Blockchain and Cryptocurrencies*. Pridobljeno 18. avgusta 2018 iz https://www.capco.com/Intelligence/Capco-Institute/Journal-46-Automation/The-financial-auditing-of-distributed-ledgers-blockchain-and-cryptocurrencies
9. Campbell, T. & Houghton, K. (2005). *Ethics and Auditing*. Canberra: ANU E Press.
10. Chartered Professional Accountants Canada – CPA. (2018a). *Audit Considerations Related to Cryptocurrency Assets and Transactions.* Pridobljeno 18. avgusta 2018 iz https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations
11. Chartered Professional Accountants Canada – CPA. (2018b). *Introduction to Accounting for Cryptocurrencies*. Pridobljeno 4. junija 2018 iz https://www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/international-financial-reporting-standards-ifrs/publications/accounting-for-cryptocurrencies-under-ifrs
12. Coenen, T. (2008). *Essentials of corporate fraud*. Hoboken: John Wiley.

13. CoinDesk. (2018). *Bitcoin Price (BTC).* Pridobljeno 2. decembra 2018 iz https://www.coindesk.com/price/bitcoin
14. Ernst & Young. (2012). *Applying IFRS 13 Fair Value Measurment*. Pridobljeno 20. junija 2018 iz http://www.ey.com/Publication/vwLUAssets/ey-applying-ifrs-fair-value-measurement/$FILE/ey-applying-ifrs-fair-value-measurement.pdf
15. Ernst & Young. (2013). *Audit performance handbook 2013*. London: EYGM Limited.
16. Ernst & Young. (2017). *International GAAP 2017*. London: EYGM Limited.
17. Ernst & Young. (2018). *IFRS Accounting for crypto-assets*. Pridobljeno 5. junija 2018 iz http://www.ey.com/Publication/vwLUAssets/EY-IFRS-Accounting-for-crypto-assets/$File/EY-IFRS-Accounting-for-crypto-assets.pdf
18. European Central Bank. (2015a). *Virtual Currency Schemes – a further analysis.* Pridobljeno 18. avgusta 2018 iz http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
19. European Central Bank. (2015b). *What is Money?* Pridobljeno 18. avgusta 2018 iz http://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html
20. Finančna uprava Republike Slovenije – FURS. (2018). *Davčna obravnava poslovanja z virtualnimi valutami po ZDoh-2, ZDDPO-2 in ZDDV-1.* Pridobljeno 12. junija 2018 iz http://www.fu.gov.si/fileadmin/Internet/Davki_in_druge_dajatve/Podrocja/Dohodnina/Drugi_dohodki/Opis/Podrobnejsi_opis_2_izdaja_Davcna_obravnava_poslovanja_z_virtualno_valuto_po_ZDoh-2_ZDDPO-2_in_ZDDV-1.pdf
21. Gates, M. (2017). *Blockchain: ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*. Scotts Valley: CreateSpace Independent Publishing Platform.
22. Gill, M. (2009). *Accountants' truth: knowledge and ethics in the financial world*. Oxford: Oxford University Press.
23. Grant Thornton International Ltd. (2018). *IFRS Viewpoint: Accounting for Cryptocurrencies – the Basics*. Pridobljeno 20. avgusta 2018 iz https://www.grantthornton.global/globalassets/1.-member-firms/global/insights/article-pdfs/ifrs/ifrs-viewpoint-9---accounting-for-cryptocurrencies--the-basics.pdf
24. Gupta, V. (2017, 28. februar). A Brief History of Blockchain. *Harvard Business Review.* Pridobljeno 12. junija 2018 iz https://hbr.org/2017/02/a-brief-history-of-blockchain
25. Hayes, R., Dassen, R., Schilder, A. & Wallage, (2005). *Principles of Auditing: An Introduction to International Standards on Auditing.* Harlow: Prentice Hall/Financial Times.
26. Houben, R. & Snyers, A. (2018). *Cryptocurrencies and blockchain*. Pridobljeno 18. avgusta 2018 iz http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
27. James, E. H., Stephanie, M. B. & Nancy, A. B. (2004). *Core concepts of information technology auditing.* Hoboken: John Wiley.
28. International Auditing and Assurance Standards Board. (2009). *International Accounting Standard 2 Inventories*. Pridobljeno 20. junija 2018 iz http://ec.europa.eu/internal_market/accounting/docs/consolidated/ias2_en.pdf

29. Jadek, A. (2018). *Pravo in blockchain*. Kranjska Gora: Odvetniška pisarna Jadek & Pensa d. o. o.
30. Juergensen, M. (2016). *Top Ten Information Technology (IT) Internal Audit Issues*. Pridobljeno 19. avgusta 2018 iz https://chapters.theiia.org/san-francisco/ChapterDocuments/2820751%20Top%2010%20Information%20%20Technology%20(IT)%20Audit%20Issues%202016%20(1).pdf
31. Koletnik, F. & Kolar, I. (2008). *Forenzično računovodstvo.* Ljubljana: Zveza računovodij, finančnikov in revizorjev Slovenije.
32. Koletnik, F. (2009). *Zunanje revidiranje*. Maribor: Ekonomsko-poslovna fakulteta.
33. Mar, S., Johannessen, R., Coates, S., Wegrzynowicz, K. & Andreesen, T. (2012). *Information Technology Risk and Controls*. Pridobljeno 19. avgusta 2018 iz https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf
34. Mednarodna zveza računovodij. (2009). *Preoblikovani MSR 315*. Pridobljeno 5. junija 2018 iz http://www.si-revizija.si/sites/default/files/standardi/msr_315.pdf
35. Nakamoto, S. (2008). Bitcoin: *A Peer-to-Peer Electronic Cash System*. Pridobljeno 18. avgusta 2018 iz https://bitcoin.org/bitcoin.pdf
36. Odar, M. (2011). Pregled standarda MRS 36 – Vloga poslovodstva, pooblaščenega revizorja, v tej zvezi. *Zbornik referatov 14. letne konference ocenjevalcev vrednosti Slovenskega inštituta za revizijo* (str. 51–72). Rogaška Slatina: Slovenski inštitut za revizijo.
37. PWC. (2017). *IFRS 9, Financial Instruments Understanding the Basics*. Pridobljeno 5. junija 2018 iz https://www.pwc.com/gx/en/audit-services/ifrs/publications/ifrs-9/ifrs-9-understanding-the-basics.pdf
38. PWC. (2018). *Cryptocurrencies Time to consider plan B*. Pridobljeno 5. junija 2018 iz https://www.pwc.com/us/en/cfodirect/assets/pdf/point-of-view/cryptocurrency-bitcoin-accounting.pdf
39. Singleton, T. W. & Singleton, A. J. (2010). *Fraud auditing and forensic accounting* (4. izd.). New Jersey: John Wiley & Sons.
40. Slovenski inštitut za revizijo in Odbor za mednarodne standarde revidiranja in dajanja zagotovil. (2018). *Razlagalni slovar*. Pridobljeno 18. avgusta 2018 iz http://www.si-revizija.si/sites/default/files/standardi/razlagalni-slovar-2018.pdf
41. Turk, I. (2009). *Temeljni ekonomski pojmovnik s slovensko-angleškim in angleško-slovenskim strokovnim slovarjem*. Ljubljana: Zveza računovodji, finančnikov in revizorjev Slovenije.
42. Wikipedia. (brez datuma). *Financial audit*. Pridobljeno 5. junija 2018 iz https://en.wikipedia.org/wiki/Financial_audit
43. Wikipedia. (2018). *Ethereum.* Pridobljeno 18. avgusta 2018 iz https://en.wikipedia.org/wiki/Ethereum#The_DAO_event