UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA

POSLOVNE PRILOŽNOSTI UPORABE PORAZDELJENEGA ZAPISA DIGITALNEGA DOGODKA

Ljubljana, julij 2016

ANŽE PIRC

IZJAVA O AVTORSTVU

Podpisani Anže Pirc, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Poslovne priložnosti uporabe porazdeljenega zapisa digitalnega dogodka, pripravljenega v sodelovanju s svetovalcem prof. dr. Jurij Jaklič

IZJAVLJAM

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 11.7.2016 Podpis študenta:_____

KAZALO

KAZALO SLIK

UVOD

Porazdeljen zapis digitalnega dogodka (angl. *Blockchain*, v nadaljevanju BC) je tehnologija, ki predstavlja ogrodje kriptovalute **Bitni kovanec** (angl. *Bitcoin*, v nadaljevanju BTC). V zaključni nalogi bom predstavil, kako lahko BC pripelje do revolucije v poslovanju in nam pomaga rešiti nekaj temeljnih težav pri izmenjavi blaga, digitalne lastnine in beleženja digitalnih dogodkov. Glavni problemi, ki jih BC skuša rešiti, so zaščita zasebnosti, transparentnost poslovanja in zaupanje v informacije, ki so nam na voljo. Vse to naj bi bilo možno zaradi decentraliziranega sistema porazdeljene BC baze, podprte z močno kriptografsko zaščito. Namen moje naloge je, da preko praktičnih primerov predstavim, kako lahko BC tehnologija reši te probleme in postane temelj razvoja novih poslovnih priložnosti.

V obstoječem finančnem sistemu je pri izmenjavi lastnine nujno potrebno posredovanje neke centralne avtoritete, ki skrbi za validacijo opravljenih transakcij. Kot primer naj navedem banko, brez katere si danes ne moremo zamišljati plačilnega prometa. Vsi pa se verjetno še spomnimo dogodkov v Grčiji med krizo, ko so se banke zaprle in onemogočile dostop ljudem do svojega premoženja. BC tehnologija obljublja, da nas bo rešila takšne odvisnosti od centralne avtoritete.

Izumitelj BTC in BC tehnologije Satoshi Nakamoto je uspel razrešiti uganko dvojne porabe, ki je bila glavna prepreka pri širši uporabi kriptovalut. S tem je dokazal, da je BTC tako valuta kot tudi protokol, in še pomembneje, da se lahko s pomočjo uporabnikov (računalnikov) v porazdeljeni mreži pride do strinjanja glede opravljenih transakcij brez uporabe centralne avtoritete. Pojavljajo se mnogi, ki kritizirajo deflacijski vidik kriptovalute BTC. Kritika izhaja iz dejstva, da je za obtok mišljeno točno določeno število BTC-jev, kar naj bi po mnenju nekaterih pripeljalo do njenega propada. Kljub vsemu se uporaba kriptovalute BTC vztrajno širi.

Možnosti za uporabo BC tehnologije pa so seveda še veliko širše kot le nov način plačevanja v obliki kriptovalute BTC. BC baza namreč ni omejena le na beleženje transakcij v plačilnem prometu, temveč lahko hrani različne informacije. Kot primer naj navedem beleženje informacij o poročni zvezi med dvema osebama, lastniških pravicah in v vedno bolj razširjenem internetu stvari, katera naprava je kupila elektriko od katerega vira. Dejstvo, da podatkov v BC bazi ni možno zlorabiti, odpira veliko možnosti za širšo uporabo. Ne glede na verzijo BC, od katere je BTC najbolj znan, pa je glavna inovacija BC tehnologija sama. Vse temelji na ideji o porazdeljeni bazi, kjer je zaupanje osnovano na sodelovanju vseh udeležencev in na programski kodi, namesto na neki centralni instituciji.

V svoji zaključni nalogi bom v prvem poglavju na primeru kriptovalute BTC prikazal, kako deluje tehnologija BC in kakšni so sestavni deli BC baze. V drugem poglavju bom prikazal nove poslovne priložnosti, ki se ponujajo z uporabo BC tehnologije. To poglavje sem

vsebinsko razdelil na dva dela, in sicer na poslovne rešitve z uporabo BTC verzije BC tehnologije in na poslovne rešitve z uporabo alternativnih verzij BC tehnologije. V tretjem poglavju bom prikazal možnosti uporabe BC tehnologije kot platforme, ki bi lahko v prihodnosti poganjala storitve interneta stvari. V zadnjem poglavju pa bom navedel nekaj nevarnosti in izzivov, s katerimi bi bil BC lahko soočen v prihodnosti.

1 KAJ JE PORAZDELJEN ZAPIS DIGITALNEGA DOGODKA IN KAKO DELUJE

1.1 Inovacije, ki so pripeljale do porazdeljenega zapisa digitalnega dogodka

V decembru 1974 sta Vint Cerf in Robert Kahn predstavila *Transmission Control Protocol/Internet Protocol* (v nadaljevanju TCP/IP). TCP/IP protokol je bil razvit z namenom, da omogoči povezavo in komunikacijo računalnika z omrežjem *Advanced Research Projects Agency Network* (v nadaljevanju ARPANET) (Crocker, 2000). Od takrat je celoten projekt mutiral in postal ogrodje za povezavo med računalniki, kar je pripeljalo do današnjega interneta.

Osnovna tehnologija se do danes ni veliko spremenila. IP številka še vedno pomeni unikatni naslov, s katerim se računalnik identificira na spletu, medtem ko TCP tehnologija omogoča prenos podatkovnih paketov. TCP in IP se uporabljata skupaj in zagotavljata, da podatek pride od izvora do končnega cilja.

Na podlagi te tehnologije je Tim Berners-Lee razvil *Hyper Text Transfer Protocol* (v nadaljevanju HTTP), ki predstavlja način, kako spletni brskalnik komunicira s spletnim strežnikom. HTTP nam skupaj z ostalimi protokoli (DNS, ARP) omogoča današnjo izkušnjo dela na omrežju. E-pošta, spletni brskalniki, spletne strani in ostali modeli računalništva v oblaku (SaaS, Paas, IaaS) so produkti, ki so se razvili na tem ogrodju in nam danes omogočajo tako imenovano digitalno ekonomijo.

E-pošta je z novim načinom komuniciranja s seboj prinesla tudi nove neprijetnosti, kot so nezaželena pošta in *denial of service* (v nadaljevanju DOS) napadi. Ti napadi pomenijo pošiljanje množičnih zahtevkov na spletne strežnike, in ko ti strežniki dosežejo mejo zahtevkov, ki jih še lahko obdelajo, postane izkušnja pri uporabi legitimnih uporabnikov motena. Ker ti napadi običajno potekajo preko posebnih spletnih programov, je odkrivanje njihovega izvora oteženo.

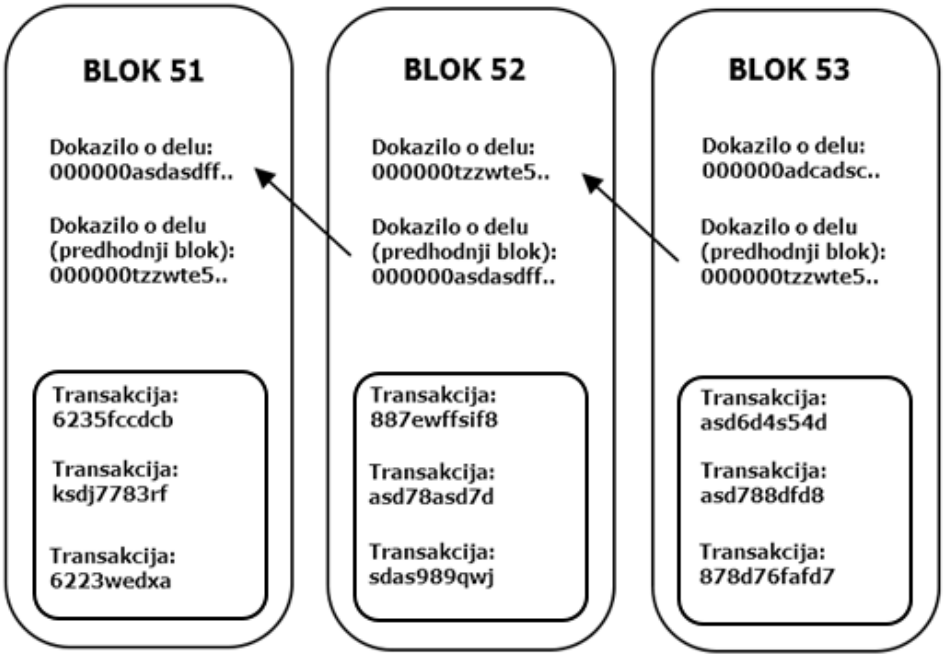
Pošiljanje nezaželene pošte temelji na ekonomiji obsega. V primeru, da pošiljanje nezaželene pošte postane časovno in denarno potratno, tovrstno pošiljanje postane neekonomično. Ravno na tej predpostavki je programer Adam Back razvil koncept **dokazila**

o delu. Njegova ideja je bila, da bi moralo vsako e-poštno sporočilo vsebovati določeno dokazilo, da je bilo pri njegovem nastajanju uporabljeno računsko delo. V ta namen je bil razvit sistem *Hashcash.* Zahteva je bila, da naj ima vsako e-sporočilo v svoji glavi tekstovno potrdilo, da je bila za njegov nastanek potrebna določena računska kalkulacija. Iz tega se je kasneje razvila ideja, da bi poleg dokazila o delu ta računska kalkulacija lahko omogočala tudi način proizvodnje oz. nastajanja vrednosti. Ideja je ostala neizkoriščen potencial vse do prihoda BC tehnologije in BTC kriptovalute (Back, 2003).

1.2 Definicija porazdeljenega zapisa digitalnega dogodka

Danes BC opravlja podobno pot, kot sta jo pred njim HTTP in TCP/IP protokol, s to razliko da slednja predstavljata komunikacijske protokole, BC pa predstavlja protokol prenosa vrednosti. BC je porazdeljena baza zapisov, katere glavna lastnost je zaščita pred zlonamernim poseganjem v podatke, ki so shranjeni v njej. Baza je sestavljena iz blokov, bloki pa so med seboj povezani z uporabo časovnega žiga in zapisa **razpršene vrednosti** *(*angl. *Hash).* BC je v osnovi glavna inovacija kriptovalute BTC, kjer predstavlja javen zapis vseh transakcij. Deluje po principu *peer-to-peer* (v nadaljevanju P2P) in omogoča vsakemu uporabniku, da postane član omrežja in s tem lahko pošilja in verificira transakcije ter sestavlja nove bloke. Velika prednost tehnologije je tudi njeno decentralizirano omrežje, kar pomeni, da ni nobene centralne avtoritete, ki bi lahko nadzirala celoten sistem. V BC sistemu nadzor nad pravilnostjo podatkov v bazi opravljajo sami uporabniki omrežja v procesu izdelave in validacije blokov, ki tvorijo BC bazo (Crowe, 2016).

Slika 1: Struktura baze porazdeljenega zapisa digitalnega dogodka



Vir: P. Graham, Bitcoin by analogy, 2014

1.3 Registracija uporabnika v sistem

Ko si uporabnik omrežja namesti BTC kriptodenarnico, mu sistem v postopku avtomatsko generira njegov javni in zasebni ključ. Oba ključa sta shranjena v njegovi kriptodenarnici, ki je v tem primeru analogija bančnega računa. Uporabnik ima tudi opcijo, da uporablja spletno denarnico. Spletne denarnice postajajo vse bolj popularne in so v samem bistvu podobne e-poštnim računom, ki jih imamo odprte pri ponudnikih, kot je Google. Nevarnost je seveda, da v primeru napada na ponudnika lahko vsebina naše denarnice postane ogrožena. Navkljub zagotovljeni anonimnosti pa večina ponudnikov denarnic od novih uporabnikov zahteva določena dokazila o identiteti (skenirani osebni dokumenti itd.).

Ne glede na to, kakšen tip denarnice uporabljamo, njena primarna funkcija ni hranjenje BTC kovancev, temveč hramba našega javnega in zasebnega ključa, ki nam ju generira sistem ob izdelavi denarnice. Dejstvo je, da BTC-ji obstajajo izključno na omrežju in ob izvršeni transakciji, uporabniki samo zamenjajo lastništvo nad BTC-ji. Zasebni ključ se uporablja za podpisovanje transakcij, ki jih potem s pomočjo našega javnega ključa lahko preveri katerikoli uporabnik v BC omrežju. Javni ključ torej predstavlja naslov denarnice, kamor prejmemo nakazilo, zasebni ključ pa predstavlja geslo, s katerim uporabnik lahko pošilja oz. dostopa do prejetih BTC-jev.

1.4 Proces opravljanja in validacije transakcij

Ko uporabnik pošlje določeno število BTC-jev neki drugi osebi, uporabi svoj zasebni ključ in z njim podpiše sporočilo, ki vsebuje podatke o prejemniku in količini BTC-jev, ki jih pošilja. Vse opravljene transakcije so objavljene na omrežju in tako predstavljajo javno bazo dogodkov, kjer je vsaka transakcija preverjena, zapisana in nepovratna. Ker so digitalni podpisi vsake transakcije unikatni glede na kombinacijo javnega/zasebnega ključa, lahko tisti uporabnik omrežja, ki preverja transakcijo, iz javnega ključa razbere, ali si uporabnik lasti dovolj BTC-jev za uspešno izvedbo transakcije. Spodaj je opisan natančen postopek nastanka in validacije transakcije (Marshall & Grewal-Carr, 2016):

1. oseba A v svoji digitalni denarnici sproži plačilo 10 BTC-jev v digitalno denarnico osebe B. Oseba A podpiše svojo transakcijo 10 BTC-jev s svojim zasebnim ključem, na drugi strani oseba B lahko potrdi prejem 10 BTC-jev preko javnega ključa osebe A;
2. ko tisti uporabniki v BC omrežju, ki imajo nameščeno celotno BC bazo z zgodovino vseh transakcij, dobijo informacijo o transakciji med osebo A in osebo B, bodo to transakcijo preverili in jo ob uspešni validaciji dodali v blok. Validacija transakcije vsebuje več parametrov, bistveno je seveda, da oseba A dejansko ima na voljo 10 BTC-jev za plačilo osebi B. To je razvidno iz predhodne verige dogodkov v BC. V določenem časovnem okviru je v posameznem bloku več transakcij, velikost bloka pa je omejena na 1 MB;

3. ko je blok sestavljen, se začne dirka med uporabniki glede tega, kdo bo prvi rešil matematično enačbo, potrebno za uspešno sestavo bloka. Pri tem gre za iskanje točno določene oblike **varnostnega algoritma razpršene vrednosti** (angl. *Secure Hash Algorithm 256*, v nadaljevanju SHA 256), ki je sestavljen iz glavnih delov bloka;
4. uporabnik, ki prvi ugane rešitev, bo v omrežju objavil nov blok skupaj z rezultatom potrdila o delu v obliki razpršene vrednosti;
5. v kolikor ostali uporabniki potrdijo pravilnost kriprografskega izračuna, bo nov blok dodan v BC verigo. Prvi uporabnik, ki sestavi nov blok, dobi za plačilo 25 BTC-jev;
6. po 10 minutah, odkar je oseba A sprožila nakazilo, je transakcija potrjena in oseba B dobi nakazilo 10 BTC-jev.

Uporabniki v omrežju potrebujejo vzpodbudo za validacijo oz. sestavo blokov, konec koncev v ta proces vlagajo svoj čas in računske zmogljivosti svojih računalnikov, kar seveda predstavlja določen denarni strošek. Satoshi Nakamoto je to težavo rešil z uporabo teorije igre tako, da je za vsak uspešno potrjen blok potrebno rešiti tudi matematičen problem, ki v tem primeru predstavlja dokazilo o delu. Nagrada za to početje so BTC-ji, ki jih uporabniki dobijo ob uspešni potrditvi transakcij in rešitvi matematičnega problema. Nagrado dobi prvi uporabnik, ki uspešno sestavi blok. Pri vsem tem je pomembno razumeti, da pri procesu sestave bloka ne gre le za slepo dodajanje transakcij v blok, temveč je s tem tudi zajamčeno, da so transakcije pravilne in dovoljene. V primeru, da bi uporabnik v blok dodal nedovoljene transakcije, bi ostali uporabniki omrežja, ki bi na koncu potrjevali nov blok v verigi, le-tega seveda zavrnili in uporabnik, ki bi sestavil nedovoljen blok, bi ostal brez plačila za svoje opravljeno delo. Ta proces ne skrbi le za uvedbo zaupanja v sistem, temveč tudi za kreiranje novih BTC kovancev (Knibbs, 2015).

Proces validacije transakcij in reševanja matematičnega problema je znan kot **rudarjenje**. Maksimalno število kovancev, ki bodo lahko ustvarjeni pri procesu rudarjenja bo 21 milijonov. Trenutno je na trgu približno 15,2 milijona BTC-jev in do leta 2022 jih bo v obtoku 90 % (Southurs, 2016). Ker BTC sledi deflacijski monetarni politiki, ga mnogi ne vidijo le kot alternativno obliko izmenjave vrednosti, ampak tudi kot eksperiment monetarne ekonomije.

1.5 Proces rudarjenja

Matematični problem, katerega rešitev je del procesa sestave novega bloka, opravlja podobno funkcijo kot dokazilo o delu predhodno omenjenega hashcash sistema za e-sporočila. Dokazilo o delu skupaj s transakcijami, ki jih morajo uporabniki potrditi, sestavlja **blok,** ki je glavni sestavni del verige BC. Uporabniki, ki se imenujejo rudarji, opravljajo verifikacijo transakcij in rešujejo matematične težave s pomočjo posebne programske opreme in računske moči svojih računalnikov. S potrjevanjem transakcij in s tem blokov ter s povezovanjem teh blokov med seboj nastaja BC baza.

Poleg potrjevanja transakcij v bloku in zagotavljanja, da ni prišlo do dvojne porabe, morajo uporabniki nad celotnim blokom uporabiti matematično funkcijo v obliki razpršene vrednosti. Funkcija razpršene vrednosti je algoritem, ki za vhod vzame podatke poljubne dolžine, končni produkt pa je podatkovni niz fiksne dolžine. Ko je nad BC blokom uporabljena funkcija razpršene vrednosti, le-ta pretvori celotno vsebino bloka v naključno zaporedje črk in številk. Funkcija razpršene vrednosti, ki jo rudarji uporabljajo kot dokazilo o delu, je tipa SHA 256, ki proizvede niz črk in številk velikosti 256 bitov oz. 32 bajtov. Ne glede na velikost vhodnih podatkov je dolžina razpršene vrednosti vedno enaka. Vhodni podatki so lahko števila, besedilo in celo slike. Vsak edinstven vhodni podatek bo vsakič, ko bo poslan skozi funkcijo, proizvedel enak izhodni rezultat. Na ta način funkcija razpršene vrednosti podatke opremi z edinstvenim digitalnim podpisom in tako omogoča lažjo klasifikacijo in delo s podatki, v našem primeru s transakcijami. Glavna značilnost SHA 256 funkcije je tudi ta, da je iz končnega rezultata nemogoče razbrati, kakšni so vhodni podatki, in vsak bit, ki je spremenjen na vhodnih podatkih, povsem spremeni končno obliko niza SHA 256.

Funkcija SHA 256 je nad blokom izvedena v točno določenem času in je nato pripeta zraven bloka. Poleg tega je potrebno upoštevati tudi, da je v vsakem SHA 256 nizu posameznega bloka vključen tudi SHA 256 niz predhodnega bloka. Z uporabo predhodnih SHA 256 nizov in digitalnega časovnega žiga, ki je del niza, so bloki med seboj povezani v verigo BC. Iz tega sledi, da starejši kot je podatek v BC, težje ga je spremeniti. Dnevno je validiranih približno 150 blokov, in če bi hoteli spremeniti podatke v prvem od teh blokov, bi to pomenilo, da bi morali ponovno izračunati razpršene vrednosti vseh 150 blokov, kar pa je skoraj nemogoče zaradi vgrajene težavnosti pri sestavljanju SHA 256 niza. V večini primerov je oblika SHA 256 niza sledeča:

12fbb162eff6c876385642f0444529cc31ac60c74dfd6cc1af62df05a15a7393

V primeru BTC pa je v programsko kodo vgrajena zahteva, da mora biti niz sestavljen iz določenega števila vodilnih ničel, primer:

00000000000000000000000444529cc31ac60c74dfd6cc1af62df05a15a7393

To seveda močno poveča računsko zahtevnost izvajanja SHA 256 funkcije nad blokom. Da posamezen rudar sploh lahko doseže takšen niz z zapovedanim številom vodilnih ničel, mora zraven bloka transakcij priložiti naključno število. To število se spreminja z vsako ponovitvijo, dokler ni dosežena zahtevana oblika razpršene vrednosti. In prav ta ponavljajoči se proces ugotavljanja pravilnega niza je dejanski matematični problem, ki ga rudarji predložijo kot svoje dokazilo o delu. Trenutno je čas, potreben za validacijo bloka, 10 minut, in rudar, ki prvi predloži dokazilo o delu za posamezen blok, dobi izplačanih 25 BTC-jev. Ko rudar reši problem in verificira blok, ga pošlje v omrežje v dokaz in validacijo ostalim rudarjem, ter doda blok v BC verigo.

V času pisanja je v BC verigi 412.683 blokov in nov blok je dodan približno vsakih 10 minut. Za zagotovitev integritete BC in hitrosti proizvajanja BTC kovancev, omrežje avtomatsko prilagaja težavnost SHA 256 funkcije. Težavnost se preverja vsakih 2016 blokov (približno vsaka dva tedna). S primerjavo časovnih žigov dveh blokov, ki sta 2016 blokov narazen, program lahko ugotovi računsko zmogljivost celotnega omrežja. Z zmanjševanjem nagrade v BTC-jih skozi čas nekateri rudarji lahko zapustijo sistem. To pomeni, da bo v omrežju manj rudarjev in s tem manj računske moči, kar bo pomenilo manjšo težavnost SHA 256 funkcije za preostale rudarje ter obratno.

1.6 Možnosti nedovoljenih operacij v omrežju

Razpršena vrednost, ki je del vsakega bloka, nam ne omogoča le možnosti sledenja od zadnjega bloka pa vse do prvega, preko nje je tudi zelo oteženo kakršno koli spreminjanje podatkov v bloku. Treba se je zavedati, da če bi napadalec želel spremeniti podatke v bloku, se čas v tistem momentu ne bi ustavil, ampak bi ostali rudarji že delali naprej na verifikaciji oz. sestavi novega bloka. To močno oteži delo napadalcu, saj mora spremeniti vsebino bloka in nato ponovno izračunati razpršene vrednosti vseh naknadnih blokov in to v roku 10 minut, ki so potrebne za sestavo novega bloka. To je pomembno zato, ker omrežje kot veljavno vedno sprejme najdaljšo verigo blokov, in če bi napadalec zamudil okno 10 minut, bi ostali rudarji v verigo dodali nov blok, kar bi povzročilo neveljavnost njegove na novo preračunane verige. Edini način, da bi napadalec to lahko izvedel je, če bi imel na voljo računsko moč, ki bi presegla 50 % računske moči celotnega omrežja, zato takšnemu napadu na BC omrežje pravimo napad 51 %. Poleg tehničnega znanja bi bila računska moč potrebna za takšen napad ogromna, če upoštevamo, da je trenutna računska moč BTC BC omrežja kar 256-krat večja od moči 500 najmočnejših svetovnih super računalnikov skupaj (Cohen, 2013).

1.7 Alternativne uporabe rudarjenja

S tem, ko računska moč BC omrežja raste, se postavljajo vprašanja, za kakšne namene, poleg rudarjenja, bi se ta moč še lahko uporabila. Ena od idej je uporaba razpoložljive moči za zlaganje proteinov. S tem konceptom se ukvarja projekt CureCoin. Projekt, ki je bil zagnan leta 2013, želi združiti operacije rudarjenja z medicinskimi raziskavami in pri tem uporablja svojo verzijo BC tehnologije z uporabo lastne kriprovalute. Rudarji poleg že omenjenega reševanja SHA 256 funkcije uporabljajo svojo strojno opremo še za potrebe zlaganja proteinov. Pri tem so za svoje delo plačani glede na ponujeno računsko moč (Khalique, 2014).

2 PORAZDELJEN ZAPIS DIGITALNEGA DOGODKA IN PRILOŽNOSTI UPORABE

V današnjih časih postaja **internet vsega** poslovna realnost in meje med fizičnim ter virtualnim so vedno bolj zabrisane. V tem prehodnem obdobju je izgradnja centraliziranega poslovnega modela prežeta z mnogimi slabostmi predvsem v povezavi s stroški, varnostjo in dolgoročno vzdržljivostjo centralno-upravljalnega sistema.

Sekundarni učinek interneta vsega je tudi nastanek **ekonomije vsega**, saj v tem primeru vsaka naprava, ki je povezana v splet, postane točka transakcije in ustvarjanja vrednosti za uporabnika. V digitalni ekonomiji je decentraliziran model bolj smiseln za implementacijo, saj odstrani možnost **okvare na eni točki**, ki je sestavni del klasičnega klient-strežnik poslovnega modela. V decentralizirani strukturi pomeni dodajanje dodatnih členov v omrežje večjo stabilnost celotnega sistema, saj tudi v primeru izpada posameznega člena delovanje celotnega omrežja ni ogroženo.

Ker vedno več podjetij začenja dojemati prednosti, ki jih prinaša decentraliziran model poslovanja, se tudi možnosti, ki jih ponuja BC tehnologija, zdijo vedno bolj ekonomsko smiselne. Decentralizirana arhitektura za podjetja pomeni manjše stroške, saj prenos informacij med uporabniki decentraliziranega omrežja odstrani odvisnost od centralnega strežnika, s tem pa se optimizira poraba sredstev in zmanjšajo stroški. Z drugimi besedami je celotno omrežje tisto, ki skrbi za varnost in nemoteno delovanje sistema.

S tem, ko porazdeljena omrežja postajajo kanali za transakcije, ki temeljijo na prenosu vrednosti in upoštevajoč predhodno omenjene prednosti, se je začelo pojavljati vedno več podjetij, ki s poslovnim modelom, osnovanim na BC tehnologiji, vstopajo na razne segmente trga. V nadaljnjih poglavjih bom poskušal predstaviti različne možnosti uporabe BC tehnologije, ki so se je začela posluževati podjetja. Glede na to, kako podjetja uporabljajo to tehnologijo, sta se izoblikovali dve skupini:

- podjetja, ki ponujajo svoje storitve in produkte, zgrajene na BTC BC tehnologiji;
- podjetja, ki posnemajo BTC BC, da lahko ponudijo storitve in produkte na decentraliziran način.

2.1 Poslovne rešitve v BTC verziji porazdeljenega zapisa digitalnega dogodka

Podjetja, ki ponujajo BTC storitve, sledijo odprto-kodnemu idealu tehnologije in odpirajo vrata razvijalcem aplikacij. Rezultat tega je, da ta podjetja sedaj ponujajo programske vmesnike za finančne procese, ki so na voljo vsem. Ponudniki BTC programskih vmesnikov so osredotočeni na razvoj programske opreme in ponujajo zastonj orodja zunanjim razvijalcem, ki nato razvijajo produkte, orodja in storitve, ki uporabljajo BC. Rezultat sta

podjetji BitPay in Coinbase, ki ponujata programske vmesnike, ki služijo kot orodja za podporo plačilnega sistema trgovcev. Ta orodja omogočajo trgovcem, da prejmejo BTC-je po fiksnem menjalnem tečaju za valuto in jih tako zaščitijo pred nihanjem vrednosti valute. Podjetji BitPay in Coinbase sta v svoje vrste pridobili že več kot 80.000 trgovcev, med njimi so DELL, Expedia in Microsoft. Stopnja BTC uporabnikov se trenutno podvaja vsakih 8 mesecev, vendar pa zaostaja za številom trgovcev, ki sprejemajo BTC kot plačilno sredstvo (Tepper, 2016).

2.1.1 Finančni sektor

Prva podjetja, ki so nastopila na trgu, so bila tista, ki so ponujala storitve kriptodenarnice, saj je bila ravno ta ključni del za razvoj celotnega BTC ekosistema. Mnoga izmed teh podjetij danes ponujajo še dodatne storitve, kot sta izmenjava valut in analiza podatkov. Najpopularnejši ponudniki spletnih kriptodenarnic so XAPO, Blockchain in Circle.

V nasprotju s splošnim prepričanjem tradicionalno bančništvo in bančne storitve niso na voljo celotni svetovni populaciji. Če povzamemo podatke svetovne banke, imata od 7 milijard ljudi na planetu le 2 milijardi dostop do bančnih računov in tako možnost udeležbe v e-trgovini (World Bank, 2013). Ta statistika velja celo v razvitih državah, saj v ZDA skoraj 17 milijonov odraslih oz. 7 % odrasle populacije nima dostopa do bančnih storitev (Klapper, 2012). V Indiji so številke še bolj šokantne, saj je brez bančnega računa skoraj polovica prebivalstva (World Bank, 2013). Če pa upoštevamo, da imajo od 7 milijard ljudi na svetu kar 3,07 milijarde dostop do interneta, postane koncept opravljanja transakcij direktno preko interneta takoj zanimiv za vse trgovce, ki bi lahko z vključitvijo BTC-jev kot plačilnega sredstva povečali svojo bazo kupcev.

V finančnem sektorju je torej možno videti veliko novih inovacij, ki se pojavljajo v luči kriptovalut. BC odstrani potrebo po tretji stranki kot validatorju transakcij in je osnova za zaupanje pri poslovanju med dvema poslovnima subjektoma. To skupaj z nizkimi stroški posamezne transakcije omogoča podjetjem oblikovanje novih poslovnih priložnosti, ki omogočajo udeležencem omrežja izmenjavo vrednosti ne glede na velikost transakcije.

2.1.2 Mikroplačila in nakazila

Večji plačilni posredniki kot sta Mastercard in Visa imajo zaradi narave poslovanja precej visoke pristojbine za vsako opravljeno transakcijo. Zaradi tega je obstoječa centralizirana struktura nepraktična za nakazovanje manjših zneskov oz. ad hoc plačil. Mikroplačila so pomemben korak v načinu plačevanja za digitalno medijsko vsebino, saj uporabnik lahko sedaj s plačilom manjšega zneska dostopa do izbrane vsebine časopisov, revij in blogov, ne da bi moral za to plačevati celotno mesečno naročnino. Plačilo za tovrstno vsebino se torej opravi glede na uporabo, kar poveča branost ter število naročnin in je hkrati vzpodbuda založniku, da ponuja kakovostno vsebino.

Pri denarnih nakazilih po svetu je trenutna pristojbina za transakcijo približno 10 %, v Afriki celo 30 %. V nasprotju znaša pristojbina za pošiljanje nakazil z uporabo BTC-jev med 0,01 % in 0,05 % celotnega nakazila (Tepper, 2016). Uporabniki, ki želijo poslati določeno vsoto denarja v Afriške države, lahko sedaj uporabljajo spletni servis BitPesa, ki omogoča nakazila v obliki BTC-jev. Podjetje, ki zaračunava 3-% pristojbino na transakcijo, pretvori BTC-je v lokalno valuto in izvede nakazilo prejemniku (Boase, 2013). Kot vidimo, lahko z uporabo kriptovalute BTC kot plačilnega sredstva in sredstva za nakazila privarčujemo velike količine denarja pri plačevanju pristojbin.

2.1.3 Pametne pogodbe in pametna lastnina

BTC v svojem jedru vsebuje programsko skripto, ki je del vsake transakcije. Ta skripta v sebi drži pravila, ki morajo biti upoštevana, da lahko BTC valuta zamenja lastnika. Primer takega pravila je recimo, da mora lastnik, ki prejema valuto, potrditi lastništvo svojega zasebnega ključa BTC naslovu, kjer so shranjeni kriptokovanci. Ostali primeri pravil bi lahko bili tudi pogoji večkratnih digitalnih podpisov in zahtev glede časovnega zaklepanja.

Ker je del vsakega BTC-ja programska skripta, je sedaj možno vse takšne storitve programirati kot del valute, kar je pripeljalo do tako imenovanih pametnih pogodb. Pametna pogodba je program, ki na podlagi določenih vhodnih podatkov izvede neke končne operacije. Glede vsebine pametne pogodbe se morajo strinjati vse udeležene stranke, kar pomeni, da morajo biti upoštevani interesi vseh udeležencev. Pametna pogodba je torej zbirka pravil, ki so lahko v obliki poslovne logike, zakonov itd. Ker so ta pravila napisana v programskem jeziku, se lahko pogodba uporablja v vsaki storitvi, ki uporablja kriptografsko podpisane ukaze. Iz tega sledi, da je BTC lahko programiran, da sprejema določene ukaze in na njihovi podlagi opravlja določene operacije (Buterin, 2016).

Za primer vzemimo malo bolj oddaljeno prihodnost, kjer bi lahko kupec avtonomnega avtomobila z opravljeno transakcijo preko pametne pogodbe registriral spremembo lastništva avtomobila. Ko bi bila transakcija potrjena in objavljena v BC, bi bili pogoji pametne pogodbe izpolnjeni. Lastništvo avtomobila sedaj lahko preveri katera koli naprava, ki je povezana v internet in BC, kar je v tem primeru sam avto. V naslednjem koraku bi avto prejel informacijo o novem lastniku in njegovi lokaciji, ki bi jo pridobil preko naslova shranjenega v BC in tako nadaljeval svojo pot do lastnika. Ta primer predstavlja koncept pametne lastnine in podobno idejo prenosa lastnine bi lahko uporabili tudi pri nakupu nepremičnin in ostalih sredstev.

2.1.4 Dvostopenjska potrditev verodostojnosti

V primeru, da je pri transakciji udeleženih več strank oz. če se pojavi potreba po dodatnem zavarovanju transakcij, imajo uporabniki tudi možnost uporabe potrditve verodostojnosti z uporabo večkratnih podpisov. Namesto enega zasebnega ključa je v tem primeru na javni

ključ vezanih več zasebnih ključev. Za dokončanje transakcije je potrebno pridobiti digitalni podpis od vsakega zasebnega ključa.

Z uporabo potrditve verodostojnosti večkratnih podpisov bi lahko podjetja, ki ponujajo storitev založnega računa, strankama ponudila BTC naslov s tem, da bi imela v lasti enega od zasebnih ključev. Za dokončanje transakcije bi bilo v tem primeru potrebno imeti digitalne podpise vsaj dveh udeležencev, eden od njih bi moral biti od podjetja, ki ponuja storitev (Goldfeder, 2014).

CryptoCorp je eno od podjetij, ki uporablja dvostopenjsko potrditev verodostojnosti za zavarovanja (Buterin, 2014). Ko do njih pride zahteva za soudeležbo pri potrjevanju, je transakcija najprej poslana skozi program za strojno učenje, ki preverja možnosti goljufije, in sicer:

- preveri se število transakcij;
- preveri se frekvenca trgovanja z naslovom A;
- preveri se število predhodnih transakcij;
- preveri se naslov B.

Na podlagi teh parametrov se izračuna ocena tveganja za transakcijo. V primeru nizke ocene se transakcija izvede, v primeru srednjega rezultata se za potrditev transakcije pošlje pošta oz. SMS v potrditev uporabniku, v primeru visokega tveganja pa se zahteva natančen pregled. Glede na to, da se v celotnem procesu uporablja strojno učenje, algoritem uporablja vhodne podatke za učenje in s tem prilagaja svoj nivo varnosti glede na vrsto transakcij v omrežju. Z uporabo podobnih tehnologij in BC lahko podjetniki in strokovnjaki sedaj lažje identificirajo goljufije identitete in zlorabe v sektorju zavarovanja.

2.2 Poslovne rešitve z uporabo alternativnih verzij porazdeljenega zapisa digitalnega dogodka

Ena od slabosti BTC transakcij je njihova hitrost, saj je trenutno BTC omrežje sposobno procesirati le 7 transakcij na sekundo. Po drugi strani jih PayPal lahko procesira 150 na sekundo in VISA med 2.000 in 56.000 na sekundo (Gilbert, 2016). Hitrost transakcij je neposredno povezana s številom osirotelih (nevalidiranih) blokov v omrežju. Ko rudarji hitijo z zbiranjem transakcij in vključevanjem le-teh v nov blok, dajejo prednost predvsem manjšim transakcijam. Te transakcije vsebujejo manjše število podatkov o tem, od kje prihajajo in kam gredo, in s tem zasedejo manj prostora v bloku. Posledično je potrebnega manj časa za propagacijo takšnega bloka v omrežje. Iz tega razloga so transakcije z več vhodnimi/izhodnimi podatki povezane z večjimi pristojbinami, kar pomeni spodbudo za rudarje, da v bloke vključujejo tudi večje transakcije.

Čas 10 minut za sestavo bloka je bil izbran, da se zagotovi manjše število osirotelih blokov (dnevno število osirotelih blokov je med 0 in 5). Osiroteli bloki so težava, saj lahko vplivajo na čas nastanka bloka in potrditev transakcij bloka. Čas nastanka bloka in potrditev transakcij bloka sta v nekakšnem medsebojnem razmerju, saj hitrejši čas nastanka bloka pomeni zmanjšano integriteto potrditve transakcij. Na trgu se je pojavilo kar nekaj alternativnih kriptovalut, ki poskušajo doseči hitrejše transakcijske čase brez negativnega vpliva na veljavnost potrditve transakcij. Vse kriptovalute, ki so alternativa BTC, imajo skupno ime **alternativni kovanci** (angl. *AltCoins*). Razvoj novih kriptovalut je možen zaradi odprtokodnega značaja BC protokola. Razvijalci lahko enostavno kopirajo izvorno kodo programa in na njej potem razvijejo svoje rešitve in dodelave.

2.2.1 Bitni kovanec 2.0

Ker so vse kriptovalute v osnovi programska koda, je možno kodo preurediti in s tem spremeniti tip transakcij, ki jih je možno izvajati. Ena od možnosti je, da kriptokovance uporabimo kot zastopnike nekega alternativnega premoženja, kot je obveznica, delnica, zlato itd. Na ta način BC ni samo decentraliziran sistem za transakcije s kriptokovanci, temveč postane decentraliziran kanal za trgovanje z dobrinami, ki je zmožen beležiti izmenjavo lastništva nad temi dobrinami.

Eno prvih, ki se je začelo ukvarjati s tem poslom, je podjetje ColouredCoins, ki uporablja označevanje sredstev s kriptokovanci. Proces se imenuje barvanje kovanca. Vsak kriptokovanec tako lahko predstavlja na primer gram zlata, in prenos 10 kriptokovancev je enakovreden prenosu 10 gramov zlata. Vrednost kovancev ostane ista, s tem da novi lastnik kriptokovancev sedaj lahko v zameno zahteva 10 gramov zlata (Bradbury, 2013).

Izraba programljivosti kriptovalut je pripeljala do pojava tako imenovanih **decentraliziranih avtonomnih podjetij** (v nadaljevanju DAP), ki lahko delujejo brez posredovanja ljudi. Tovrstna podjetja so vodena preko programiranega poslanstva v obliki poslovnih pravil (Johnston, 2015). Ta avtonomna podjetja so lahko lastniki kapitala, ki zaposlujejo ljudi, izdajajo delnice in proizvajajo dobiček, ki ga nato izplačujejo delničarjem. Eno od podjetij, ki deluje na tem področju, je Bitshares, ki nudi programsko opremo za zagon DAP.

2.2.2 Porazdeljen zapis digitalnega dogodka 2.0

Ripple je podjetje, ki ponuja opravljanje transakcij z uporabo različnih kriptovalut in ostalih dobrin. Ripple uporablja svojo kriptovaluto, ki se imenuje XRP. Kot pri bitnem kovancu so transakcije porazdeljene in vidne celotnemu omrežju s to razliko, da je v sistemu možno trgovati z XRP, USD, EUR, zlatom itd. Ker se v Ripple omrežju lahko trguje z različnimi sredstvi, omrežje ne uporablja standardnega načina soglasnega potrjevanja transakcij z uporabo dokazila o delu. Namesto tega se uporablja doseganje soglasja na osnovi zaupanja vrednih strežnikov, ki so nosilni členi omrežja (Schwartz, 2014). Tako kot v BTC BC

omrežju imajo tudi v Ripple omrežju uporabniki možnost, da poganjajo strežniško programsko opremo in tako sodelujejo v procesu validacije transakcij, lahko pa uporabljajo samo klient programsko opremo, katere namen je le sodelovanje pri transakcijah. Ena od glavnih prednosti Ripple BC tehnologije je tudi ta, da potrditev transakcije običajno traja nekaj sekund v primerjavi z BTC BC, kjer je potrebnih 10 minut. Zaradi te prednosti in dejstva, da je Ripple zasebno podjetje, ki je podvrženo določenim pravilom in predpisom, se je za tovrstno tehnologijo začel zanimati tudi bančni sektor s ciljem uporabe pri mednarodnih nakazilih sredstev. Kljub temu, da Ripple zaradi strežniško naravnane arhitekture nekoliko odstopa od omrežja BTC BC, gre v osnovi še vedno za isti cilj decentraliziranega soglasja nad izvedenimi transakcijami.

Ethereum je še en projekt, ki ima veliko elementov skupnih z BTC filozofijo. Ethereum ne želi postati le platforma za finančne transakcije, temveč tudi platforma za prej omenjene pametne pogodbe. Ethereum naj bi to dosegel preko razvoja skriptnega jezika za svojo lastno kriptovaluto Ether. BTC skriptni jezik je namenoma preprost, saj to pomeni manjšo možnost napada na sistem. Ethereum pa po drugi strani temelji na bolj robustnem programskem jeziku, ki naj bi razvijalcem omogočal precejšnjo svobodo pri razvoju rešitev. Ethereum ima cilj odpraviti pomanjkljivosti pametnih pogodb v BTC BC z uporabo lastne kriptovalute in svoje verzije BC (Buterin, 2016).

Poleg novih kriptovalut s hitrejšimi transakcijskimi časi se podjetja ukvarjajo tudi z vpeljavo nove metode verifikacije blokov, imenovane **dokazilo o udeležbi** (Back, 2014). Na podlagi te metode rudar za svoje sodelovanje v sistemu zasluži glede na količino kriptovalute v lasti. Torej nekdo, ki ima v lasti 1 % kovancev, lahko verificira 1 % blokov. Zaslužki po tej metodi so torej odvisni od količine valute, ki jo ima v lasti rudar. Prednosti, ki jih navajajo razvijalci, so hitrejši časi transakcij, večja varnost, kompatibilnost z ostalimi BC in predvsem močno zmanjšana poraba električne energije zaradi manjše zahtevnosti verifikacije blokov.

2.2.3 Alternativne možnosti uporabe porazdeljenega zapisa digitalnega dogodka

BC tehnologija zaradi svoje revolucionarne zasnove omogoča nove poslovne priložnosti za podjetja, ki si drznejo biti prva pri sprejemu te tehnološke novosti. Nekatera gradijo svoj posel na idejah, ki sem jih opisal v predhodnih poglavjih, nekatera pa razvijajo povsem nove rešitve, in sicer:

- **Oskrbovalna veriga**: Podjetje SkuChain recimo raziskuje možnosti, kako nadomestiti današnje črtne kode, ki jih uporabljamo za identifikacijo in sledenje produktov z uporabo oznak v obliki razpršenih vrednosti. Podjetje naj bi uporabnikom ponudilo tehnologijo večkratnih podpisov kot sistema za zagotavljanje nesporne verifikacije pri blagovni menjavi. Proizvajalec lahko zaščiti blago, ki ga je prejel od ponudnika, tako da transakcijo podpiše s svojim zasebnim ključem, medtem ko je njegova stranka lastnik drugega zasebnega ključa, oba zasebna ključa pa sta del istega javnega ključa. Poleg

sledenja blagu, dvostopenjska potrditev verodostojnosti preprečuje tudi goljufije in težave s ponaredki. Rešitev bi bila uporabna v farmacevtski industriji, saj imajo farmacevtske družbe velike težave s ponarejenimi zdravili.

- **Prevozne storitve**: BC prav tako daje novo perspektivo storitvam tako imenovane ekonomije delitve. Primer je podjetje La'Zooz, ki je nekakšen decentraliziran Uber. Uber je podjetje, ki je močno pretreslo storitveni sektor prevoza in katerega vrednost je ocenjena že na 62 milijard ameriških dolarjev (Shah, 2015). Vendar pa glavna vrednost za Uber niso sredstva, ki si jih lasti, ampak podatki o tem, kako se ljudje gibljejo po mestih. Ti podatki se nato uporabljajo pri planiranju najbolj optimalnih poti za prevoze. Po drugi strani pa je La'Zooz prevozna storitev, ki je v lasti uporabnikov, in katere cilj je združiti koncept deljenih prevozov z BC tehnologijo. Namesto bitnih kovancev uporabniki za plačilo uporabljajo *Zooz* žetone. Tudi sistem nastanka žetonov je drugačen kot tisti, ki ga uporablja bitni kovanec. Namesto dokazila o delu se uporablja dokazilo o premiku, kjer voznik pred začetkom vožnje vklopi La'Zooz aplikacijo in tako služi žetone, medtem ko prevaža potnike. Ta isti voznik lahko sedaj znotraj sistema La'Zooz nastopi tudi kot potnik in plača za prevoz s predhodno zasluženimi žetoni. Uporabnik storitve lahko žetone služi tudi s predlogi o najbolj optimalnih prevoznih poteh (Duivestien, 2014).
- **Odvetniške storitve:** Ena od mnogih funkcij, ki jo opravljajo odvetniki, je tudi zagotavljanje dokazila o obstoju dokumenta npr. oporoke, listine o lastništvu nepremičnine, pooblastil. Ker to običajno pomeni podpis dokumenta ob določenem datumu in času, lahko v tem primeru uporabimo BC za tovrstne operacije, ki potrebujejo časovni žig. Pravne službe lahko pretvorijo vsebino dokumenta v razpršeno vrednost preko SHA 256 funkcije in jo shranijo v BC. Ker vsebine dokumenta ni možno spremeniti, ne da bi spremenili vrednost razpršene vrednosti, je veljavnost tovrstnih dokumentov možno dokazati kadarkoli kasneje.
- **Skupinsko financiranje**: Ena od novih tehnik skupinskega financiranja je, da se preko alternativnih kovancev in BC tehnologije z uporabo dokazila o udeležbi pridobijo sredstva investitorjev. Investitor lahko sedaj prilagodi svojo investicijo glede na mejnike, ki jih doseže projekt. Kot vemo, imajo kriptovalute vgrajen skriptni jezik, ki omogoča izdelavo novih alternativnih valut. Te alternativne valute oz. žetone je sedaj možno programirati, da opravljajo določene finančne operacije. Podjetnik, ki želi pridobiti investicijska sredstva, lahko sedaj uporabi to tehnologijo na porazdeljenem omrežju in v zameno za investicijska sredstva izplačuje žetone. Žetoni v tem primeru pomenijo obliko lastniškega deleža. Sredstva, ki jih prejme podjetnik, so lahko namenjena razvoju, za kritje operativnih stroškov oz. za povečanje obsega poslovanja. Ko projekt doseže določene mejnike, imajo investitorji opcijo, da reprogramirajo svoje žetone in preko njih v projekt vložijo dodatna sredstva. S prepoznavnostjo projekta raste tudi omrežje in z njim vrednost žetonov (Quinn, 2014).

3 INTERNET STVARI IN PORAZDELJEN ZAPIS DIGITALNEGA DOGODKA

Arhitektura sistema BC ponuja tudi nove poslovne priložnosti za razvoj inovativnih storitev v povezavi z internetom stvari. S prehodom na **internetni protokol verzije 6** (v nadaljevanju Ipv6) se odpirajo možnosti, kjer ima lahko vsaka naprava oz. senzor svojo IP številko in s tem povezavo na internet. Naprava oz. senzor se lahko poveže v BC in tako postane točka transakcije in ustvarjanja vrednosti.

Kot primer vzemimo z računalnikom opremljen hladilnik, ki je programiran, da glede na družinski proračun za hrano opravlja določene vnaprej programirane operacije. Hladilnik se lahko glede na prehrambne navade družinskih članov poveže s spletno stranjo lokalnega supermarketa in izvede naročilo. Uporabnik bi po opravljenem naročilu prejel e-poštno sporočilo, kjer bi samo še potrdil transakcijo. Končna potrditev je torej še vedno na strani uporabnika, bi se pa s pomočjo povezave naprav s kriptodenarnico uporabnika lahko močno zmanjšal čas, ki ga porabi uporabnik za opravljanje vsakdanjih opravil. Ta koncept lahko seveda razširimo na ostale naprave, s čimer bi lahko na primer poskrbeli za uravnavanje porabe energije in vode. V osnovi ima uporabnik možnost, da programira svoj denar.

Še en sektor, ki bi lahko ogromno pridobil s to tehnologijo, je proizvodna industrija. Vedno več delavnih mest v proizvodnji se avtomatizira, in procesi, kjer je trenutno potrebno posredovanje delavca, bi lahko bili opravljeni z uporabo stroja. V proizvodno enoto, ki je upravljana s pomočjo umetne inteligence, bi lahko vnesli podatke o željeni proizvedeni količini in časovnih zamikih, ki so povezani s transportom in zalogo. Na podlagi teh parametrov bi proizvodna enota lahko predvidela, koliko materiala potrebuje, da doseže cilj proizvodnje in izračunala, če je trenutna zaloga dovoljšna za dosego cilja. Ker je proizvodna enota povezana v BC, lahko direktno komunicira z dobaviteljem, pošlje naročilo in opravi transakcijo. Z avtomatizacijo določenih proizvodnih procesov in uporabo BC tehnologije za direktno upravljanje z zalogo bi se lahko močno izboljšala učinkovitost proizvodnje.

IBM in Samsung sta začela z idejnimi koncepti, kako uporabiti BC pri upravljanju z internetom stvari. To se zdi smiselno ob predpostavki, da naj bi bilo do leta 2025 po ocenah v splet priključenih že okoli 100 milijard naprav (Saurabh, 2016).

Izhodiščne točke decentraliziranega interneta stvari (IBM, 2015):

- **Porazdeljeno procesiranje transakcij:** Avtonomno delovanje naprav brez centralnega nadzora.
- **Zagotovljena varnost:** Tukaj sta predvsem pomembna enkripcija in preglednost transakcij v sistemu.
- **Zasebnost:** Identiteta vseh naprav je privzeto skrita in se razkrije le po potrebi.

- **Medsebojno trgovanje:** V prihodnjih letih, ko naj bi se število naprav povezanih v omrežje močno povečalo, lahko pričakujemo nastanek tako imenovane ekonomije stvari. To pomeni ustvarjanje tržne vrednosti preko digitalizacije fizičnega sveta.

3.1 Integracija interneta stvari v BC

Življenjska doba vsakega produkta se začne z vnosom v BC bazo, ko produkt zapusti proizvodno linijo. Kasneje, ko je produkt prodan, ga proizvajalec vpiše v svojo regionalno BC bazo, ki je lahko na ravni mesta oz. države. S tem, ko je produkt vpisan v bazo, so skupaj z njim vpisani tudi vsi podatki o samem produktu, njegova zgodovina, podatki o garanciji in konec življenjske dobe. Zaradi varnosti podatkov v BC bazi, le-ta postane zaupanja vreden vir informacij o produktu. Primer bi recimo bila pametna naprava, ki lahko zazna odpoved določenega mehanskega dela. Zaradi povezave v BC omrežje naprava lahko preveri, če je okvarjeni del v garanciji in nato naroči popravilo pri pooblaščenem serviserju. Na koncu serviser preko BC baze preveri še upravičenost do garancijskega zahtevka. Na takšen način bi BC resnično pomenil revolucijo pri demokratizaciji in vse večji avtonomnosti naprav.

3.2 Različni tipi povezanih naprav

Različne naprave, ki so med seboj povezane v omrežje, imajo različne lastnosti. Razlikujejo se glede na procesorsko moč, pomnilnik, diskovni prostor, količino energije, ki jo imajo na voljo, če jih omenimo samo nekaj. Prav zaradi teh razlik ni možno, da bi vsaka naprava imela pri sebi shranjen zapis celotne BC baze oz. zapis dela BC baze.

Zaupanje pri komuniciranju med napravami, ki pri sebi nimajo zapisa BC baze, bi se razvilo skozi čas, s tem ko bi prihajalo do izmenjave informacij med napravami. Določene naprave zaradi kratke življenjske dobe oz. svoje manjše vloge niti ne bi potrebovale potrjevanja transakcij preko BC baze. Zaupanje in obseg verifikacije transakcij bi bila odvisna od tipa naprave, narave interakcije z drugimi napravami in od pravil delovanja, kaj naprava sme in česa ne sme početi, kar bi določili lastniki naprave.

Prav s tem namenom bi bile naprave ločene v tri skupine glede na svoje sposobnosti (IBM, 2015):

- **Lahka naprava:** Sem spadajo vse naprave z majhno računsko močjo in diskovnim prostorom. Raspberry PI in Arduino v obliki manjših senzorjev bi bila primer lahkega uporabnika. Ta pri sebi ne bi imel shranjene BC baze. Da bi pridobil podatke o transakcijah, ki ga zadevajo, bi se lahki uporabnik povezal z nekim drugim zaupanja vrednim uporabnikom v omrežju. Lahki uporabnik ima sposobnost pošiljanja sporočil in lahko uporablja denarnico, na katero je vezan BC naslov naprave.
- **Standardna naprava:** Glede na to, da naj bi se v prihodnjih letih računska sposobnost in diskovni prostor naprav povečala, bi lahko že npr. pralni stroj imel dovolj procesorske

moči in diskovnega prostora, da zadosti potrebam za hrambo dela BC baze. Baza, ki bi jo hranil pralni stroj, bi bila na voljo tudi lahkim uporabnikom v njegovem zaupanja vrednem okolju.

- **Glavni člen omrežja:** Glavni členi bi bili predvsem strežniki, ki bi imeli zaradi svoje procesorske moči in diskovnega prostora pri sebi kopijo celotne BC baze transakcij. Bili bi v lasti organizacij oz. drugih komercialnih subjektov. Ker bi standardni in lahki uporabniki zaradi velike količine informacij lahko hranili le nekaj dni staro bazo dogodkov, bi bili glavni členi vir celotne zgodovine. Vsaka naprava, ki je v uporabi že dalj časa, potrebuje za potrebe servisiranja oz. kakršne koli podpore, dostop do celotne svoje zgodovine obstoja od vpisa v BC naprej. Glavni členi bi lahko tudi uravnavali ponudbo in povpraševanje po raznih dobrinah med napravami. Tu bi kot primer navedel gospodinjstvo A, ki s pomočjo sonca pridobiva električno energijo. Vsak presežek energije, ki ga gospodinjstvo A ne porabi, se lahko ponudi preko glavnih členov na trgu. Na drugi strani pa imamo gospodinjstvo B, ki preko pametnega števca povprašuje po električni energiji. Glavni členi tako postanejo stičišča vseh naprav v omrežju in omogočajo izvajanje raznih ekonomskih aktivnosti.

3.3 Primeri uporabe

Na primeru pralnega stroja bom prikazal, kako lahko z uporabo BC tehnologije pralni stroj postane delno avtonomna naprava. Priključen v BC omrežje, lahko upravlja s svojim lastnim potrošnim materialom, naročilom servisa in preko sodelovanja z ostalimi napravami poskrbi za optimizacijo svojega delovanja.

3.3.1 Naročilo potrošnega materiala

Pralni stroj Samsung W9000 ima vgrajeno posodo, kjer lahko hranimo pralni prašek, ki ga stroj potem sam primeša glede na izbran program. V našem primeru bi stroj lahko zaznal, kdaj mu začne primanjkovati pralnega praška in izvedel naslednje korake (IBM, 2015):

1. sprožil poizvedbo, če obstaja pogodba za naročilo pralnega praška pri dobavitelju;
2. preko sporočilnega sistema bi sprožil naročilo pri proizvajalcu;
3. glede na pogodbo bi izvedel plačilo za naročilo pri proizvajalcu;
4. obvestil lastnika o naročilu.

Koraki, ki bi jih izvedel prodajalec (IBM, 2015):

1. najprej bi preveril veljavnost pogodbe s pralnim strojem;
2. prejel bi plačilo;
3. izvedel naročilo pralnega praška;
4. obvestil pralni stroj o podrobnostih dobave.

Ko je naročilo zaključeno, pralni stroj pošlje obvestilo lastniku o zaključenem naročilu, skupaj s podrobnostmi o dostavi.

3.3.2 Naročilo servisa

S tem primerom je prikazano, kako lahko v primeru okvare pralni stroj sam sproži postopek popravila (IBM, 2015):

1. pralni stroj preko senzorjev zazna, da je določen del v okvari oz. njegovo slabše delovanje nakazuje na okvaro, kar sproži servisni zahtevek;
2. pralni stroj preveri, kakšno je stanje garancije;
3. preko BC izbere najbolj primernega serviserja. Serviser je lahko že vnaprej določen s pametno pogodbo;
4. ko je serviser izbran, je sprožen zahtevek za servis. V primeru, da je naprava v garanciji, plačilo storitve ni potrebno, v kolikor pa je stroj izven garancije, se preko lastnika sproži postopek plačila;
5. ko serviser prejme zahtevek, bo v BC bazi preveril, kakšno je stanje garancije pralnega stroja;
6. po opravljeni verifikaciji se zahtevek v serviserjevem sistemu spremeni v naročilo in vse informacije se poslane nazaj do pralnega stroja in njegovega lastnika;
7. lastnik in serviser se nato dogovorita glede točnega časa za prihod serviserja.

4 NEVARNOSTI IN IZIVI ZA PRIHODNOST

Kriptovalute in BC tehnologija odpirajo navadnim uporabnikom in podjetjem vrata do novih poslovnih priložnosti in obljubljajo, da bodo pretresla načine opravljanja storitev na mnogih področjih. Vpeljava teh tehnologij v večjem obsegu pa s seboj prinaša tudi veliko izzivov, nekateri od teh so:

- **Pravne ureditve:** Z vidika računovodstva se kriptovalute danes soočajo s številnimi regulatornimi ovirami. Poleg pomanjkanja smernic glede obdavčitve kriptovalut potrebujejo uporabniki, prodajalci in ponudniki storitev v kriptovalutah tudi določena pravila, ki se nanašajo na pregled nad količino kriptovalut, ki jih imajo uporabniki shranjene v svojih kriptodenarnicah in kolikšna je vrednost teh kriptovalut v nacionalni valuti. Možnost programiranja transakcij in izmenjave sredstev brez posrednika, ki bi nadzoroval prenos lastništva blaga, še bolj oteži celoten postopek regulacije. Največji izziv kriptovalutam pa utegne biti na strani monetarne politike. Centralne banke danes del svojih prihodkov pridobijo iz postopka izdaje denarja, kar bo verjetno negativno vplivalo na njihovo sprejetje kriptovalut. Prav tako, če se valuta, ki jo izdaja centralna banka države, uporablja kot svetovna rezervna valuta, lahko država natisne dodatno količino denarja, ne da bi s tem povzročila inflacijo. Zaradi konkurence, ki jo

kriptovalute predstavljajo nacionalni valuti, obstaja velika verjetnost, da bodo centralne banke nasprotovale širšemu sprejetju (Mougayar, 2016).

- **Nihanje vrednosti:** Kljub temu, da imajo kriptovalute vseh šest lastnosti dobrega denarja (omejena količina, trajnost, deljivost, zamenljivost, prenosnost in prepoznavnost), jih še vedno spremlja visoko nihanje vrednosti. Mnogi ekonomisti opozarjajo na težavo z nihanjem vrednosti, zelo malo pa je pripomb glede same BC tehnologije. Obstaja kar nekaj razlogov za nihanje vrednosti kriptovalut. Ena od njih je, da obstaja končno število bitnih kovancev, ki bodo kadarkoli proizvedeni oz. izdani. Do leta 2140, ko naj bi bil izdan zadnji bitni kovanec, naj bi jih bilo 21 milijonov, in vsak bitni kovanec je možno razdeliti na 100 milijonov *satoshi* enot. Cena bitnega kovanca se izoblikuje glede na povpraševanje po valuti na trgu in je povezana tudi z njeno ponudbo. Ker je stopnja izdaje valute znana, mora povpraševanje slediti tej stopnji ponudbe, da se lahko stabilizira njena cena. Ker je tržna kapitalizacija bitnega kovanca in ostalih kriptovalut precej majhna, že majhne razlike v ponudbi in povpraševanju povzročijo velike spremembe v vrednosti. Na ceno vplivajo tudi razni dogodki, kot je bilo zaprtje borzne hiše MT Gox. Takšni pretresi omajajo zaupanje ljudi v kriptovalute in povzročijo padec vrednosti, podobno kot pri gibanju cen delnic. Na ceno pa vpliva tudi dejstvo, da je danes 50 % vseh bitnih kovancev v lasti nekaj 10 uporabnikov, ki so izkoristili nižje začetne cene. Za rešitev divjega gibanja cen bo v prihodnosti največjega pomena zagotovo širša uporaba, ki bo vplivala na normalizacijo trga (Mougayar, 2016).
- **Težave ponudnikov storitev:** Trenutno večina uporabnikov kriptovalut za povezavo v omrežje uporablja storitve tretjih oseb, kot so borze, spletne denarnice, transakcijske platforme itd. Poleg prednosti za uporabnike predstavljajo tudi nevarnost v primeru napak takšnega ponudnika storitev. Spletne denarnice prav tako niso zaščitene pred napadi, tako kot so komercialni bančni računi v večini držav. Eden od primerov, ko so bili ogroženi strežniki in je prišlo do oškodovanja uporabnikov, je bil propad borze MT Gox leta 2014. Napadi na institucije so v opozorilo vsem uporabnikom, trgovcem in ponudnikom storitev, da je potrebno biti pozoren na varnost sistema (Mougayar, 2016).
- **Grupiranje rudarjev:** Gruče rudarjev so rudarji, ki se združijo z namenom večje skupne računske moči in s tem lažje proizvodnje BTC-jev. Predstavljajo nevarnost za decentralizirano naravo omrežje zaradi prevelikega kopičenja moči. Združevanje rudarjev predstavlja tudi precej večjo nevarnost, da bi prišlo do napada 51 % (Hruska, 2014).
- **Napad 51 %:** Kljub temu, da vedno obstaja nevarnost napada 51 %, ta ne predstavlja večjih nevarnosti za obstoj valute, saj ne more ogroziti zasebnih in javnih ključev uporabnikov. Pošteni člani lahko preprečijo napade tudi s posodobitvijo glavne programske kode. Tudi če bi do napada prišlo, bi napadalec lahko vplival samo na prihodnje transakcije, stari podatki pa bi ostali varni. Bi pa takšen napad sigurno omajal zaupanje v omrežje, povzročil padec vrednosti kriptovalute in celo ogrozil obstoj celotnega omrežja (Hruska, 2014).
- **Zlom kriptografske zaščite:** Ena od večjih groženj v prihodnosti je tudi zlom kriptografske tehnologije, ki skrbi za zaščito vseh kriptovalut. V takšnem scenariju bi

lahko napadalec ogrozil algoritem za kreiranje javnih in zasebnih ključev in bi s tem lahko generiral zasebni ključ s katerega koli javnega naslova. To bi resno ogrozilo omrežje in vrednost vseh kriptovalut v sistemu. Nekatere funkcije razpršene vrednosti so danes že označene kot rizične za uporabo. SHA 256 algoritem je zaenkrat še precej varen, se pa s pojavom vedno zmogljivejše strojne opreme in tudi razvoja na področju kvantnega procesiranja pojavljajo dvomi o robustnosti in varnosti teh algoritmov v prihodnosti. Edini način, da se takšni scenariji preprečijo, so sprotni popravki in posodobitve kriptografske programske opreme (Maden, 2016).

SKLEP

Satoshi Nakamoto je z razvojem BC tehnologije sprožil plaz najrazličnejših inovacij na mnogih tržnih segmentih. Poslovne priložnosti uporabe, ki so bile predstavljene v tej zaključni nalogi, predstavljajo samo vrh ledene gore razvoja in idej na tem področju. Vendar pa kljub velikim obetom, ki jih prinaša tehnologija, še vedno obstaja pomanjkanje raziskav na tem področju. Največja prepreka za širšo uporabo BC in kriptovalut niso nevarnosti, ki so bile opisane v zadnjem poglavju, temveč zakoreninjena miselnost v poslovnih akademskih krogih, ki zaostaja za razvojem. Eden od razlogov je zagotovo ta, da je tema o BC in kriptovalutah precej zapletena, predvsem zaradi uporabe tehnik kot so kriptografija, teorija igre in računalniška infrastruktura, na kateri vse deluje. Za dojemanje vseh možnosti in prednosti tehnologije je potrebno razumevanje vseh naštetih tehnik in kako delujejo skupaj.

Kot je bilo prikazano, ima tehnologija velik potencial, da pretrese mnoge veje industrije v prihodnosti. Za mnoge so te možne spremembe precej neprijetne, saj povsem porušijo njihov trenutni način dela in logiko poslovanja, predvsem bi tukaj omenil bančni sistem. Velik je tudi strah pred izgubo mnogih delovnih mest, kar bi bila posledica avtomatizacije, ki jo omogoča BC tehnologija. V luči tega prehoda na novo tehnologijo postaja vse bolj pomembno, da so iskalci nove zaposlitve in zaposleni jutrišnjega dne vse bolj tehnično podkovani v teh novih tehnologijah, kar jim bo pomagalo pri uspešni vključitvi v digitalno ekonomijo.

Ne smemo tudi pozabiti velikega pomena, ki ga ima BC za zaščito identitete in podatkov na spletu. Ob vsaki transakciji pošljemo v splet le toliko informacij, kot je potrebno za uspešno dokončanje transakcije. Ob uporabi močne kriptografije in decentralizirano zasnovanega sistema, je močno onemogočena kakršna koli poneverba podatkov in zloraba zasebnosti uporabnikov.

BC tehnologija nam ne omogoča le vpogleda v reformacijo ekonomske in monetarne teorije kot celote, temveč je tudi priložnost za akademsko skupnost, da preuči možnosti za spremembo oz. izboljšave trenutnih postopkov delovanja na različnih področjih. Trenutna monetarna teorija temelji na centraliziranem sistemu in je odvisna od porabe in dolga, ki ji

omogočata obstoj. BC nam po drugi strani prinaša nove načine izmenjave in generiranja vrednosti, ki bodo decentralizirani in demokratični.

LITERATURA IN VIRI

1. Buterin, V. (2016, 7. maj). Ethereum. Najdeno 8.maja 2016 na spletni strani: https://github.com/ethereum/wiki/wiki/White-Paper
2. Buterin, V. (2014, 13. marec). Multisig: The Future of Bitcoin. *Bitcoinmagazine.* Najdeno 18. maja 2016 na spletni strani: https://bitcoinmagazine.com/11108/multisig-future-bitcoin
3. Back, A. (2003, 1. september). Hashcash. *Cypherspace.* Najdeno 5. maja 2016 na spletni strani: http://www.cypherspace.org/hashcash
4. Back, A. (2014, 22. oktober). *Enabling Blockchain Innovations with Pegged Sidechains*. Najdeno 17. maja 2016 na spletni strani: http://www.blockstream.com/sidechains.pdf
5. Boase, R. (2013, 28. november). BitPesa Uses Bitcoin to Slash Kenyan Remittance Costs. *Coindesk.* Najdeno 10. maja na spletni strani http://www.coindesk.com/bitpesa-uses-bitcoin-slash-kenyan-remittance-costs
6. Bradbury, D. (2013, 14. junij). Colored coins paint sophisticated future for Bitcoin. *Coindesk.* Najdeno 5. maja 2016 na spletni strani: http://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin
7. Crocker, S. D. (2000, 7. december). ARPANET -- The First Internet. *Livinginternet.* Najdeno 15. maja 2016 na spletni strani: http://www.livinginternet.com/i/ii_arpanet.htm
8. Cohen, R. (2013, 28. november). Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined. *Forbes.* Najdeno 25. maja 2016 na spletni strani: http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#647d493628b7
9. Crowe, P. (2016, 5.marec). There is a 'game changer' technology on Wall Street and people keep confusing it with bitcoin. *Businessinsider.* Najdeno 14.maja na spletni strani: http://www.businessinsider.com/what-is-blockchain-2016-3
10. Duivestien, S. (2014, 11.december). La'zooz, the decentralized version of Uber. Najdeno 25.maja 2016 na spletni strani: http://labs.sogeti.com/lazooz-decentralized-version-uber
11. Goldfeder, S. (2014). *Securing Bitcoin wallets via threshold signatures.* Najdeno 15. maja 2016 na spletni strani: http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf
12. Gilbert, D. (2016, 4. marec). Bitcoin's Big Problem: Transaction Delays Renew Blockchain Debate. *Ibtimes.* Najdeno 12. maja 2016 na spletni strani: http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renew-blockchain-debate-2330143
13. Graham, P. (2014, 24. april). Bitcoin by analogy. *Ybrikman.* Najdeno 16. junija 2016 na spletni strani: http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy
14. Hruska, J. (2014, 16. junij). One Bitcoin group now controls 51% of total mining power, threatening entire currency's safety. *Extremetech.* Najdeno 25. maja 2016 na spletni strani: http://www.extremetech.com/extreme/184427-one-bitcoin-group-now-controls-51-of-total-mining-power-threatening-entire-currencys-safety

15. IBM (2015). *Practical insights on a decentralized Internet of Things*. Najdeno 9. maja 2016 na spletni strani: http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf
16. Johnston, D. (2015, 2. februar). The General Theory of Decentralized Applications, Dapps. Najdeno 16. maja 2016 na spletni strani: https://github.com/DavidJohnstonCEO/DecentralizedApplications
17. Knibbs, K. (2015, 15. april). What's the Blockchain and why does Bitcoin depend on it? *Gizmodo.* Najdeno 23. maja 2016 na spletni strani: http://gizmodo.com/whats-the-blockchain-and-why-does-bitcoin-depend-on-it-1698025216
18. Khalique, F. (2014, 29. avgust). CureCoin: A cryptocurrency aiming to beat cancer. *Euromoney.* Najdeno 10.maja 2016 na spletni strani: http://www.euromoney.com/Article/3375459/CureCoin-A-cryptocurrency-aiming-to-beat-cancer.html
19. Klapper, L. (2012, 13. september). Why are so many Americans unbanked? Najdeno 14.maja 2016 na spletni strani: http://blogs.worldbank.org/allaboutfinance/why-are-so-many-americans-unbanked
20. Marshall, S., & Grewal-Car, V. (2016). *Blockchain Enigma-Paradox-Opportunity.* Najdeno 16. maja 2016 na spletni strani: http://bravenewcoin.com/assets/Industry-Reports-2016/Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf
21. Maden, K. (2016, 29. januar). Quantum Computing & The Future of Bitcoin Cryptography. *Bitcoinnewschannel*. Najdeno 26. maja 2016 na spletni strani: http://bitcoinnewschannel.com/2016/01/29/quantum-computing-the-future-of-bitcoin-cryptography-part-i
22. Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.* New Jersey: John Wiley & Sons.
23. Quinn, G. (2014, 4. junij). AngelList – The Patron Saint of Equity Crowdfunding. *Crowdfundinsider.* Najdeno 13. maja 2016 na spletni strani: http://www.crowdfundinsider.com/2014/06/41007-angellist-patron-saint-equity-crowdfunding
24. Schwartz, D. (2014). *The Ripple Protocol Consensus Algorithm.* Najdeno 13. maja 2016 na spletni strani: https://ripple.com/files/ripple_consensus_whitepaper.pdf
25. Shah, R. (2015, 3. december). New investment round could put Uber valuation at $62.5 billion. *CNBC.* Najdeno 21. maja 2016 na spletni strani: http://www.cnbc.com/2015/12/03/uber-to-be-valued-at-more-than-62-billion.html
26. Saurabh, S. (2016, 25. maj). The IoT Marathon: a Race for 100 billion connected things. Najdeno 19.maja na spletni strani: http://community.comsoc.org/blogs/saurabhsureka/iot-marathon-race-100-billion-connected-things
27. Southurs, J. (2016, 5. februar). How many Bitcoins are currently in circulation? *Quora.* Najdeno 20. maja na spletni strani: https://www.quora.com/How-many-Bitcoins-are-currently-in-circulation
28. Tepper, F. (2016, 28.april). Coinbase is finally letting you instantly buy Bitcoin with a debit card. *Techcrunch.* Najdeno 5. maja 2016 na spletni strani: https://techcrunch.com/2016/04/28/coinbase-is-finally-letting-you-instantly-buy-bitcoin-with-a-debit-card

29. World Bank (2013). *Who are the Unbanked*. Najdeno 20. maja na spletni strani: http://siteresources.worldbank.org/EXTGLOBALFIN/Resources/8519638-1332259343991/world_bank3_Poster.pdf