UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA POSLOVNIH PRILOŽNOSTI UPORABE VERIG BLOKOV IN PAMETNIH POGODB V ENERGETIKI

Ljubljana, september 2016 GREGOR NOVAK

IZJAVA O AVTORSTVU

Podpisani Gregor Novak, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza poslovnih priložnosti uporabe verig blokov in pametnih pogodb v energetiki, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Boštjanom Antončičem.

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 _____ Podpis študenta:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Današnje poslovno okolje in ostale ravni življenja so izpostavljene nenehnim spremembam. To opažamo tako v zasebnem, poslovnem in naravnem okolju, v katerem živimo. Sposobnost prilagajanja na spremembe je tista lastnost, ki loči uspešne od neuspešnih organizacij. Zaradi vedno večje in globalne konkurence se zahteve na trgu nenehoma in vedno hitreje spreminjajo. Prilagajanje novim možnostim, potrebam in razmeram je še toliko bolj potrebno, saj jim morajo biti sposobni slediti tudi energetski, informacijski in poslovni modeli. Energetika je ena od strateških panog, ki je zaradi globalnih okoljskih sprememb deležna velike preobrazbe. Prav tako se je informatika iz podporne funkcije delovanju organizacij preoblikovala v gonilno silo, ki omogoča učinkovito poslovanje organizacij in odpira popolnoma nove možnosti glede na tehnologijo, obseg, lokacijo in način delovanja organizacij ali povezovanja posameznikov v le-te (Novak, 2007).

S pojavom tehnološke inovacije vzpostavitve odprtokodne javne kriptografske infrastrukture verig blokov (angl. *Blockchain*) se odpira veliko novih možnosti za optimizacijo poslovnih procesov za preglednejše in učinkovitejše delovanje organizacij znotraj energetike. Veriga blokov, ki omogoča izvajanje pametnih pogodb (angl. *Smart Contracts*), deluje globalno, brez centralnega nadzora. Omogoča prenos plačil, lastniških deležev, podatkov o članstvu, glasov pri odločanju, številčnih podatkov, podatkov stanj oz. kakršnih koli drugih podatkov. Omenjena infrastruktura je načrtovana za delovanje v načinu točka točka (angl. *Peer to Peer*), kjer centralni procesor nadomesti veriga blokov, ki deluje kot distribuirani procesor, v katerem se samodejno izvršujejo vnaprej določene pametne pogodbe (Kosba, Miller, Shi, Wen & Papamanthou, 2015).

Na področju energetike se je pojavila velika potreba po uporabi obnovljivih virov predvsem zaradi globalnega segrevanja, ki ga je povzročila prekomerna in neučinkovita uporaba primarnih virov. Obnovljivi viri so decentralizirani, razpršeni in v različnih oblikah dostopni kjerkoli na planetu, so pa nestanovitni, odvisni od lokacije, časa in vremena. Obnovljivi viri so trenutno edina znana uporabna alternativa obstoječim primarnim virom, katerih uporaba lahko omogoči, da se bo naš planet ohranil tudi za bodoče rodove. Obnovljivi viri narekujejo pametno in dinamično upravljanje, na kar je elektroenergetski sektor na splošno slabo pripravljen. Uveljavitev pametnih omrežij (angl. *Smart Grids*) v praksi ni zaživela. Tudi aktivna vloga odjemalcev pri odzivu na povpraševanje elektroenergetskega omrežja (angl. *Demand Response*) se počasi uveljavlja le v nekaterih državah, v večini pa se ravnotežje vzpostavlja zgolj z regulacijo proizvodnje, ne pa tudi porabe.

Investicije v obnovljive vire so v vseh državah regulirane, v različnih državah z različnimi politikami. V preteklosti so bile odvisne od podpornih shem (angl. *Feed-in Tariff*) ali davčnih spodbud. Sedaj se pojavljajo tudi druge oblike ne plačljivih spodbud, predvsem za

samooskrbo (angl. *Net-Metering*). Politikam držav pa ni uspelo narediti platforme oz. zagotoviti možnosti osebnega angažiranja v boju s segrevanjem ozračja, pri katerem sta ključna faktorja učinkovita raba energije in investicije v obnovljive vire energije s ciljem popolnega nadomestila primarnih virov v energetiki.

Cilj magistrskega dela je izdelati analizo poslovnih priložnosti, ki jih prinaša uporaba kriptografske infrastrukture verig blokov in pametnih pogodb v energetiki. Analizirali bomo tudi možnosti izboljšav monitoringa, preglednosti in optimizacije delovanja elektroenergetike pri njenem nujnem prilagajanju na obnovljive vire energije. Tretje področje analiz bo zajemalo možnosti uporabe verige blokov za aktivno vlogo uporabnikov v energetiki in odzivu na povpraševanje v medsebojno povezanih omrežjih z vključitvijo samooskrbe. Analizirali bomo tudi globalne možnosti investiranja ali skupinskega financiranja investicij (angl. *Crowdfunding*) v razpršene vire in učinkovito rabo energije s pomočjo verige blokov in pametnih pogodb. Naše temeljno vprašanje je, ali obstajajo poslovne priložnosti uporabe verig blokov in pametnih pogodb v energetiki?

Magistrsko delo bo vsebovalo poglobljen teoretično-analitičen pregled strokovne literature, znanstvenih razprav in raziskav ter člankov s področja obravnavane tematike. Poleg kritičnega ovrednotenja teoretičnih dognanj bo magistrsko delo vključevalo tudi pregled trenutne prakse ter kritično oceno možnosti implementacije novih znanj s področja kriptografskih infrastrukturnih rešitev na področje energetike.

Prvo poglavje bo namenjeno pregledu tehnoloških platform kriptografske infrastrukture, ki so trenutno na voljo. S pomočjo deskriptivne metode bomo opisali posamezne tehnološke platforme kriptografske infrastrukture, verige blokov prve (Bitcoin) in druge (Ethereum) generacije. Ta analiza bo opravljena s pomočjo strokovne literature, predvsem člankov tujih strokovnjakov s področja kriptografije. V drugem poglavju bomo pregledali obstoječe arhitekturne informacijske rešitve, ki se uporabljajo za monitoring v energetiki, in potencial elektroenergetskega sektorja in področja obnovljivih virov energije. Ta del bo analiziran s pomočjo opisne metode in metode kompilacije, s katero bomo povezovali znanja iz različnih področij (informatike in energetike). Navedeni bodo tudi nekateri praktični primeri trenutnega delovanja monitoringa v energetiki. V tretjem poglavju bomo analizirali prednosti, slabosti, priložnosti in nevarnosti uporabe verig blokov in pametnih pogodb na osnovi kriptografskih infrastrukturnih rešitev za uporabo v energetiki. Uporabljena bo PSPN (angl. *SWOT*) analiza. V četrtem poglavju bomo preučili poslovne priložnosti uporabe verig blokov in pametnih pogodb v energetiki. Nadgradnja arhitekture eksperimentalne verige blokov s pametnimi pogodbami je odprla veliko novih možnosti za uporabo verig blokov, ki jih želimo raziskati in pokazati kot morebitne poslovne priložnosti v energetiki. Osredotočili se bomo na področji monitoringa ter neposredne vključitve uporabnikov pri odzivu na povpraševanje v medsebojno povezanih omrežjih in pri samooskrbi. Prikazali bomo nove možnostim skupinskega financiranja investicij v razpršene vire električne energije s ciljem čim hitrejšega prehoda energetike na obnovljive

vire energije. Teoretična znanja iz prvih treh poglavij bomo aplicirali na morebitne nove storitve v energetiki in nato zaključili s sklepnimi ugotovitvami.

1 PLATFORME KRIPTOGRAFSKE INFRASTRUKTURE

Področje verig blokov je še razmeroma mlado in zato ne v celoti raziskano. Še posebej to lahko trdimo za tehnološko platformo Ethereum, ki je konceptualno stara samo dve leti, deluje pa šele dobro leto. Kot ključni faktor tveganja pri prehodu na tehnologije verig blokov se ocenjuje pomanjkanje znanja tako na poslovnem in informacijskem področju, kot tudi na področju razumevanja delovanja kriptografskih algoritmov, ki so jedro tehnologije. Veriga blokov je s pojavom Bitcoina prinesla nov pogled na delovanje informatike, saj je nakazala možnost prehoda iz klasične arhitekture strežnik – odjemalec na decentralizirano kriptografsko arhitekturo. Veriga blokov, ki se zapisuje v tako imenovano glavno knjigo (angl. *Ledger*), omogoča decentralizirano, pregledno in avtonomno preverjanje dogodkov oz. transakcij znotraj sistema verige brez centralne avtoritete ali nadzora (Roth, 2015). Vse točke povezane v mrežo delujejo tudi kot javni verifikatorji transakcij. Transakcije se z zadovoljivim številom potrditev potrdijo kot nedvoumne, enkratne in neponovljive (Buterin, 2013).

Kot nadgradnja eksperimentalne arhitekture verige blokov, ki se je do sedaj izkazala za delujočo in zaupanja vredno arhiktekturo, se je pojavila nova arhitektura Ethereum z nosilno kripto valuto Ether. Arhitektura Ethereum temelji na verigah blokov, ki poleg verificiranega prenosa informacij omogočajo tudi izvrševanje vnaprej določenih funkcij. Tem funkcijam rečemo pametne pogodbe, ki se v naprej definirajo v obliki računalniškega programa in živijo v verigi blokov. Ta nadgradnja je odprla veliko novih možnosti za uporabo verig blokov, ki jih želimo raziskati in pokazati kot morebitne poslovne priložnosti v energetiki (Buterin, 2013). Potencial verig blokov (angl. *Blockchain*) lahko razberemo iz kratke, a bogate zgodovine verig blokov in izjemnega razcveta digitalnih valut v zadnjih letih (Aron, 2015).

1.1 Začetki razvoja verig blokov

Začetki verig blokov segajo v avgust 2008, ko je bil vložen zahtevek za registracijo kriptografskega patenta. Prijavo so oddali Neal Kin, Vladimir Oksman in Charles Bry. Omenjena trojica je istega meseca tudi registrirala domeno Bitcoin.org. Nato je v mesecu oktobru avtor pod psevdonimom Satoshi Nakamoto v beli knjigi objavil vizijo o popolnoma elektronskem denarju na osnovi P2P tehnologije, čemur je v novembru sledilo odprtje odprtokodnega projekta Bitcoin na uveljavljenem odprto kodnem portalu Sourceforge.

Prvi blok je bil ustvarjen januarja 2009 pod imenom Geneza (angl. *Genesis*). Ta blok je omogočil začetek rudarjenja (angl. *Mining*) Bitcoinov. Prva transakcija je bila narejena med Satoshi Nakamotom in Halom Finneyem istega meseca.

V mesecu oktobru je Bitcoin dobil tudi tržno vrednost v ameriških dolarjih. The New Liberty Standard, je na osnovi porabe električne energije pri rudarjenju ene enote Bitcoina, določil ceno enote Bitcoina (v nadaljevanju BTC) in sicer 1 USD = 1.309 BTC.

Februarja 2010 se je odprlo prvo trgovanje z Bitcoini. Maja 2010 je prostovoljec iz Anglije opravil prvi nakup v BTC. Do maja 2010 se je vrednost BTC spremenila na 1 USD = 400 BTC, tako je za pizzo v vrednosti 25 USDodštel 10.000 Bitcoinov, kar bi trenutno znašalo 6,48 milijona USD (Bitstamp, 26.07.2016 ob 10:40 uri) oz. pomenilo najdražji nakup pizze v zgodovini.

Julija 2010 je zaživela bitcoinska borza Mt. Gox v Tokiju. Borza je delovala do leta 2014, ko je imela 70 % tržni delež trgovanja z Bitcoini. (Decker & Wattenhofer, 2014).

Avgusta 2010 se je zgodil prvi hekerski napad na Bitcoinovo verigo blokov z zlorabo ranljivosti verifikacije vrednosti Bitcoina. Vrednost Bitcoina se je zaradi tega iz 0,8 USD skoraj izničila. Po odpravljeni zlorabljeni ranljivosti in tudi nekaterih drugih ranljivosti je Bitcoin novembra 2010 dosegel prvi milijon USD tržne kapitalizacije pri svoji tržni vrednosti 0,5 USD = 1 BTC.

Februarja 2011 je Bitcoin ponovno dosegel vrednost 1 USD, junija 2011 pa je bil vreden že 31 USD in tako dosegel tržno kapitalizacijo 206 milijonov USD.

Prva alternativa odprtokodni verigi blokov Bitcoin se je pojavila aprila 2011 pod imenom Namecoin. Namecoin je s tem postal prvi tako imenovali altcoin, kar je skrajšava za Bitcoin Alternative (Altcoin, 2016).

Potrebam novih digitalnih valut so sledile tudi nekatere borze, ki so digitalne valute uvrstile na trgovalne sezname in omogočile trgovanje z Bitcoinom in altcoini ter fiat valutami.

Avgusta 2011 je zaživela slovenska borza z Bitcoini (Bitstamp, b.l.), ki sta jo ustanovila mlada slovenska podjetnika z Gorenjske Nejc Kodrič in Damjan Merlak. Podjetje Bitstamp Ltd sta ustanovila v Londonu (Bitstamp, 2016).

Oktobra 2012 je podjetje BitPay, specializirano za nudenje storitev prejemanja plačil v Bitcoinih, objavilo, da je že več kot 1000 trgovcev uporabljalo njegovo storitev (Korošec, 2016).

Marca 2013 je ameriška ustanova FINCEN (angl. *Financial Crimes Enforcement Network*) izdala prva priporočila glede upravljanja, izmenjave in uporabe virtualnih valut. V istem mesecu je tržna kapitalizacija Bitcoina dosegla 1 milijardo USD.

Oktobra 2013 je začel v Vancouveru v Kanadi delovati prvi Bitcoin bankomat (Wagner, 2013).

Novembra 2013 je vrednost Bitcoina narastla že na 700 USD in ameriški senat je opravil prva zaslišanja o digitalnih valutah. Poleg tega je digitalno valuto Bitcoin odobril tudi predsednik Zveznih rezerv (angl. *Federal Reserve System - FED*) Ben Bernanke v pismu Senatnemu odboru za domovinsko varnost in vladne zadeve.

Istega meseca, novembra 2013, je cena Bitcoina zrastla na vrtoglavih 833 EUR.

Decembra 2013 je Kitajska centralna banka prepovedala finančnim ustanovam poslovanje z Bitcoini. Danes pa je Kitajska največji trgovec z Bitcoini s tržnim deležem okoli 80 %.

Februarja 2014 je z izgubo verodostojnosti borze Mt. Gox borza Bitstamp postala največja borza Bitcoinov na svetu (Khaliq, 2016).

Februarja 2014 je britanska HMRC (angl. *Her Majesty's Revenue and Customs*) deklarira Bitcoin kot sredstvo ali privatni denar, kar je pravno povzročilo, da se za rudarjenje (angl. *Mining*) ali izmenjavo Bitcoinov ne zaračunava davka na dodano vrednost.

Junija 2014 je ameriški Zvezni preiskovalni urad (angl. *FBI*) na avkciji ponudil 29.000 BTC, ki jih je zasegel na nelegalnem trgu na ravni temnega spleta - SilkRoad. S tem dejanjem se je tudi pokazalo, da uporaba Bitcoin valute ne omogoča kriminalnim združbam lahkega obvoda pravnih norm. Tako je valuta Bitcoin še pridobila na legitimnosti. Istega meseca je Bitstamp pridobil priznanje za najboljši Currency Startup na Europasu 2014 (Spaven, 2014).

Julija 2014 je *New York State Department of Financial Services* izdal prvi predlog pravil za regulacijo virtualnih valut, tako imenovali Bit Licence. Evropski bančni organ (angl. *European Banking Authority*) je objavil mnenje o virtualnih valutah, v katerem je evropskim zakonodajalcem predlagal, naj naložijo borzam virtualnih valut, da morajo upoštevati pravila o preprečevanju pranja denarja (AML) in financiranja terorizma. Ustanovljen je bil tudi prvi Bitcoinski investicijski sklad GABI (angl. *Global Advisors Bitcoin Investment Fund*), ki je Bitcoinu dodal še več legitimnosti.

V oktobru 2014 je TeraExchange objavi novico o trgovanju z bitcoinskimi izvedenimi instrumenti na regulirani borzi, kar je še utrdilo verodostojnost in zaupanje v virtualno valuto.

V mesecu decembru 2014 je sledila odločitev Microsofta, da je začel sprejemati plačila v Bitcoinih.

Januarja 2015 so napadalci ukradli digitalne denarnice uporabnikov Bitstampa in odtujili 19.000 BTC, kar je takrat znašalo približno 5 milijonov USD. Bitstamp je zato za nekaj časa zamrznil trgovanje, odpravil ranljivosti in kasneje povrnil uporabnikom izgubljena sredstva (Higgins, 2015).

Januarja 2015 je Coinbase postala prva registrirana borza z virtualnimi valutami v polovici zveznih državah ZDA.

April 2016 je Bitstamp pridobil licenco v Luxemburgu za polno regulirano in licencirano bitcoinsko borzo v EU (Bitstamp, b.l.).

Maja 2016 je bil uspešno izveden projekt množičnega zbiranja sredstev za razvojne projekte brez pravne osebe ali centralizirane uprave – DAO (angl. *Decentralized Autonomous Organization*). DAO je izdal žetone, digitalno valuto ali tako imenovane The DAO Tokens, ki so vlagateljem v decenraliziranem skladu nadomestili navidezno digitalno delnico oz. navidezni lastniški delež na osnovi pametne pogodbe.

Julija 2016 je bila aktivirana precej kompleksna pametna pogodba, ki je vsebovala veliko variant, med drugim tudi možnost oddelitve sredstev, če se vlagatelj ne strinja z večinsko odločitvijo za vlaganje v določen projekt. Le to pa je spreten heker izkoristil, da je sebi na svoj podedovani oddelitveni hčerinski račun DAO iz sklada nakazal sredstva v 3,6 milijona ETH v protivrednosti ca. 70 milijonov USD. Pametna pogodba pa je vsebovala tudi časovno omejitev razpolaganja z oddeljenimi sredstvi, kar je hekerja omejilo pri unovčitvi sredstev na trgu. V tem primeru ni šlo za napako v protokolu Ethereum, ampak za napako pri izvedbi pametne pogodbe množičnega zbiranja sredstev za DAO zaradi ranljivosti v programskem jeziku Solidity, ki se uporablja za pisanje pametnih pogodb.

Prav zaradi tega je v skupnosti nastala dilema, zakaj skupnost Ethereum rešuje nepremišljeno napisano pametno pogodbo, ki je zaradi ranljivosti programskega jezika, postala ranljiva in zlorabljena. Skupnost se je s precejšnjo večino na koncu odločila za popravek protokola verige blokov, ki je izničil ranljivost v pametni pogodbi DAO in investitorjem omogočil povrnitev sredstev. Manjši del skupnosti se s tem ni strinjal, saj je menil, da je Ethereum s tem prekršil temeljno načelo o trajnosti in nezmožnosti spreminjanja izvršenih transakcij za nazaj. Posledica tega nesoglasja je bila, da je ta del skupnosti nadalje vztrajal na starem omrežju, in si izbral valuto Ethereum Classic s kratico ETC.

Tako je s koncem julija 2016 nastala nova valuta, ki pa je v tednu dni dosegla tretjo največjo tržno kapitalizacijo, takoj za Bitcoinom in prenovljenim Ethereumom.

Večina rudarjev je sprejela nov prenovljen Ethereum, del rudarjev pa je ostal na starem omrežju Classic. Z selitvijo večine rudarjev na novo omrežje, se je na starem Classic omrežju težavnostna stopnja potrjevanja blokov izjemno zmanjšala, s tem pa se je povečala donosnost in interes rudarjev za ETC omrežje.

1.1.1 Pojav borz kripto valut

Po teoriji Carla Mengerja o nastanku denarja, je le ta naj likvidnejše blago na trgu. Najprej se je uporabljal blagovni denar, večinoma so to bili zlatniki ali srebrniki, ki so tudi sami po sebi imeli vrednost v materialu na enoto mase. Trgovci so vrednostne kovance raje deponirali v bankah in za trgovanje uporabili nadomestke, saj je to bilo bolj varno, izdani bankovci pa so nosili protivrednost deponiranega denarja v žlahtnih kovinah.

Depozitne banke so kmalu začele posojati tudi nekrite bankovce, v kar jih je gotovo peljal pohlep po večjem zaslužku. Tako se je začelo izgubljati pravno načelo popolnih rezerv, saj so prešli na tako imenovano bančništvo z delno rezervo (Birch, 2015).

Države so kasneje monopolizirale izdajanje denarja, ki ga kontrolirajo preko centralnih bank, pri čemer sodobne fiat valute, vključno z največjimi, kot so USD, EUR, RMB, in druge, nimajo več kritja v nobeni blagovni depozitni banki ali žlahtnih kovinah, temveč se le izdajo v obtok (Zevnik, 2012).

Kakor obstajajo borze za izmenjavo med fiat valutami, poznane kot FOREX, je bilo potrebno premostiti tudi menjavo med fiat in virtualnimi valutami ali samo med slednjimi. Prva menjava fiat valute za Bitcoine se je zgodila oktobra 2009, ko je New Liberty Standard kupil 5.050 BTC od Siriusa (Bitcoin help, 2014).

Borza virtualnih, kriptografskih ali digitalnih valut (angl. *Digital currency exchanges*) je gospodarska dejavnost, ki omogoča strankam trgovanje oz. zamenjavo digitalnih valut za fiat ali konvencionalne valute izdane s strani centralnih bank ali zamenjavo za druge digitalne valute (Andersen & Bjornskov, 2016).

Dejanski nastanek borze kriptovalut tako pomeni, da organizator trga proti plačilu provizije organizira trg, ponudbo in povpraševanje med fiat in virtualnimi valutami ali med virtualnimi valutami samimi. Takšno borzo je prvi vzpostavil Jeb McCaleb, računalniški programer, ki je pred tem vzpostavil tudi P2P storitev eDonkey. Borza je bila ustanovljena v Tokiju pod imenom Mt. Gox in je bila prva popolna bitcoinska borza. Borza mtgox.com je bila marca 2011 prodana Marku Karpelesu, nato je počasi rastla in bila glavna bitcoinska borza na svetu naslednja tri leta (Bitcoin help, 2014).
Večina digitalnih valut nima vrednostnega pokritja, njihova cena pa se oblikuje na osnovi ponudbe in povpraševanja. Nove digitalne valute nastajajo, za razliko od fiat valut, večinoma z rudarjenjem. Pri izdaji digitalne valute, lahko ustanovitelj valute opravi tako

imenovano predhodno rudarjenje (angl. *Premining*), v nekem deležu ali celo v celoti. Preostali delež valute pa narudarijo rudarji v procesu rudarjenja, ki večinoma služi tudi za decentralizirano potrjevanje transakcij znotraj verige blokov.

Trenutna tržna kapitalizacija digitalnih valut znaša 11,7 milijarde EUR, kar je razvidno iz Slike 1. Med digitalnimi valutami z 80 % dominira Bitcoin, kar je prikazano na Sliki 2. Delež trgovanja z Bitcoinom v skupni kapitalizaciji digitalnih valut se s pojavom novih valut sicer zmanjšuje. Kljub temu Bitcoin še vedno ostaja vodilna digitalna valuta.

Slika 1: Skupna kapitalizacija digitalnih valut

Vir: Coinmarketcap, Total Market Capitalization, b.l.a.

Trenutno je v obtoku 671 digitalnih valut in 61 digitalnih delnic. Prevladujoča valuta je Bitcoin (BTC), sledi pa ji Ether (ETH) in Ether Classic (ETC).

V Tabeli 1 je predstavljenih 100 največjih valut po mesečni povprečni tržni kapitalizaciji. Prve štiri so digitalne valute, naslednja valuta The DAO pa je digitalna delnica.

Slika 2: Odstotek trgovanja z BTC glede na celotno kapitalizacijo digitalnih valut

Vir: Coinmarketcap, Bitcoin Percentage of Total Market Capitalization, b.l.b.

Tabela 1: 100 največjih valut po mesečni tržni kapitalizaciji

Št.	Valuta	Simbol	Dnevna kap. v €	Tedenska kap. v €	Mesečna kap. v €
1	Bitcoin	BTC	155.144.105	817.837.347	3.415.061.448
2	Ethereum	ETH	61.411.735	335.498.519	755.101.678
3	Ethereum Classic	ETC	69.356.636	154.480.867	154.480.867
4	Litecoin	LTC	1.468.022	9.261.108	79.020.188
5	The DAO	DAO	784.188	7.445.997	49.152.842
6	EDRCoin	EDRC	819.460	4.846.359	32.546.102
7	NEM	XEM	288.971	2.019.345	32.017.715
8	Tether	USDT	1.084.825	6.776.656	26.249.579
9	Nxt	NXT	300.052	3.157.492	21.438.666
10	Ripple	XRP	1.206.503	4.589.809	20.767.463
11	Lisk	LSK	1.110.067	4.767.221	19.136.503
12	Steem	STEEM	554.709	3.877.292	16.626.640
13	BitShares	BTS	181.658	969.368	12.506.935
14	Factom	FCT	194.690	1.308.752	12.476.595
15	Siacoin	SC	303.209	1.321.824	10.795.962
16	Dash	DASH	466.673	2.691.744	9.214.509
17	Emercoin	EMC	627.485	4.211.647	7.653.517
18	Dogecoin	DOGE	140.178	1.185.305	7.332.612
19	Monero	XMR	179.534	938.641	7.200.983
20	MaidSafeCoin	MAID	369.203	1.675.871	6.303.353
21	Expanse	EXP	709.213	1.381.567	6.274.280
22	Waves	WAVES	259.287	727.640	4.343.181

se nadaljuje

Tabela 1: 100 največjih valut po mesečni tržni kapitalizaciji (nad.)

Št.	Valuta	Simbol	Dnevna kap. v €	Tedenska kap. v €	Mesečna kap. v €
23	GameCredits	GAME	61.397	479.108	4.200.171
24	NautilusCoin	NAUT	119.803	611.018	3.192.781
25	BlackCoin	BLK	104.433	258.996	3.044.266
26	Stellar	XLM	40.286	746.614	2.883.479
27	Yocoin	YOC	15.634	123.052	2.705.969
28	Einsteinium	EMC2	12.205	48.095	2.719.030
29	YbCoin	YBC	89.961	363.639	2.685.523
30	TRMB	TRMB	318.801	484.297	2.599.049
31	Peercoin	PPC	138.183	519.281	2.584.331
32	EarthCoin	EAC	14.393	170.333	2.281.018
33	Voxels	VOX	101.987	514.455	2.224.486
34	Counterparty	XCP	86.775	314.374	2.102.581
35	LEOcoin	LEO	47.476	376.982	2.018.611
36	Sharkcoin	SAK	12.761	175.634	1.982.755
37	Synereo	AMP	72.749	340.211	1.983.163
38	VeriCoin	VRC	24.194	170.378	1.811.762
39	LBRY Credits	LBC	77.300	385.700	1.717.764
40	VPNCoin	VPN	14.259	132.756	1.600.910
41	Myriadcoin	MYR	2.100	19.578	1.499.797
42	RibbitRewards	RBR	16.697	129.917	1.389.507
43	DigiByte	DGB	65.083	314.487	1.307.329
44	Novacoin	NVC	2.435	122.679	1.248.802
45	SysCoin	SYS	50.179	477.359	1.212.834
46	Steem Dollars	SBD	84.041	564.783	1.126.985
47	Storjcoin X	SJCX	57.944	140.414	1.034.260
48	Decred	DCR	40.733	246.691	919.362
49	Namecoin	NMC	23.317	167.081	830.656
50	ClubCoin	CLUB	11.521	102.309	807.984
51	InvisibleCoin	IVZ	100	65.762	781.715
52	Bitmark	BTM	1.039	39.774	770.437
53	SafeCoin	SFE	32.037	120.953	739.796
54	DigixDAO	DGD	30.862	182.914	735.041
55	HitCoin	HTC	9.366	140.872	627.760
56	Vcash	XVC	20.056	105.246	587.625
57	I/O Coin	IOC	23.148	201.923	502.777
58	WorldCoin	WDC	18.270	50.078	488.428
59	HiCoin	XHI	8.048	80.289	480.994
60	Horizon	HZ	1.171	8.776	485.254
61	Vertcoin	VTC	6.997	57.516	456.498
62	Breakout	BRK	12.438	56.408	453.200
63	Qora	QORA	25.398	81.711	454.761
64	Rise	RISE	21.770	90.330	444.675
65	HyperStake	HYP	685	15.492	425.433

se nadaljuje

Tabela 1: 100 največjih valut po mesečni tržni kapitalizaciji (nad.)

Št.	Valuta	Simbol	Dnevna kap. v €	Tedenska kap. v €	Mesečna kap. v €
66	CrevaCoin	CREVA	12.892	66.214	417.323
67	NuShares	NSR	3.299	39.315	408.032
68	TrumpCoin	TRUMP	5.158	29.734	409.961
69	Primecoin	XPM	6.806	46.953	405.118
70	MMNXT	MMNXT	999	6.432	395.595
71	Bitcrystals	BCY	12.270	60.769	353.536
72	Quark	QRK	3.784	29.772	345.741
73	Radium	RADS	7.997	74.802	344.029
74	Cryptonite	XCN	14.975	104.747	337.712
75	LetItRide	LIR	14.999	73.085	332.739
76	DNotes	NOTE	5.825	72.606	321.185
77	NAV Coin	NAV	4.476	21.588	321.710
78	Cryptojacks	CJ	4.130	73.405	317.540
79	Feathercoin	FTC	8.435	115.002	312.971
80	Burst	BURST	2.550	23.928	315.274
81	Nexus	NIRO	10.637	53.568	302.565
82	FuturePoints	FTP	32.068	224.460	294.711
83	Infinitecoin	IFC	11.160	32.660	297.004
84	Viacoin	VIA	834	33.258	296.814
85	Capricoin	CPC	18.819	112.345	264.990
86	Riecoin	RIC	947	16.409	246.072
87	ZcCoin	ZCC	8.751	32.183	244.852
88	YACCoin	YACC	528	7.261	246.656
89	ShadowCash	SDC	6.658	28.170	240.817
90	bitCNY	BITCNY	6.624	23.032	237.952
91	Clams	CLAM	3.393	28.036	232.325
92	RhinoCoin	RHC	5.869	49.857	226.925
93	FlorinCoin	FLO	1.645	17.698	220.775
94	PinkCoin	PINK	255	6.137	216.828
95	Shift	SHIFT	2.308	14.642	208.995
96	Piggycoin	PIGGY	991	3.582	210.753
97	BilShares	BILS	4.352	29.747	203.436
98	DT Token	DRACO	6.260	114.106	174.862
99	EvergreenCoin	EGC	5.351	111.927	172.638
100	PutinCoin	PUTIN	487	82.284	170.044

Vir: Coinmarketcap, Crypto-Currency Market Capitalizations, b.l.c.

Trenutno beležimo na internetu 104 borze z digitalnimi valutami. Borze se razlikujejo po zaračunavanju storitev. Večina jih storitev zamenjave zaračunava, nekatere pa tudi ne. Borze ponujajo različne trgovalne produkte oz. digitalne valute. Nekatere borze omogočajo tudi menjavo digitalnih valut za fiat valute, druge ne. Večina borz prvenstveno menjuje Bitcoine za fiat ali druge digitalne valute.

Če pogledamo seznam največjih 25 borz digitalnih valut ali delnic (Tabela 4) po dnevni kapitalizaciji, vidimo, da na prvih štirih mestih prednjačijo kitajske borze oz. borze, ki trgujejo tudi z CNY.

Tabela 2: Seznam 25 največjih borz digitalnih valut ali delnic

Št.	Borza	Valutni pari	Dnevna kapitalizacija v €
1	OKCoin.cn	BTC/CNY BTC/USD	504.293.155
2	Huobi	BTC/CNY BTC/USD	286.100.126
3	BtcTrade	BTC/CNY YBC/CNY	127.919.831
4	CHBTC	BTC/CNY ETH/CNY LTC/CNY	120.963.010
5	Poloniex	ETC/BTC ETH/BTC ETC/ETH LSK/BTC EXP/BTC ETH/USDT MAID/BTC BTC/USDT STEEM/BTC	102.753.503
6	BTCC	BTC/CNY LTC/CNY LTC/BTC	57.849.336
7	BTC100	BTC/CNY LTC/CNY YBC/CNY DOGE/CNY	22.633.819
8	BitFinex	BTC/USD ETH/USD ETH/BTC USDT/USD LTC/USD LTC/BTC	16.738.814
9	Quoine	BTC/JPY BTC/USD BTC/IDR ETH/BTC ETH/USD BTC/SGD ETH/JPY BTC/EUR ETH/IDR	13.516.123

se nadaljuje

Tabela 2: Seznam 25 največjih borz digitalnih valut ali delnic (nad.)

Št.	Borza	Valutni pari	Dnevna kapitalizacija v €
10	Kraken	ETH/BTC BTC/EUR ETH/EUR ETH/USD BTC/USD DAO/ETH DAO/BTC BTC/CAD DAO/EUR BTC/JPY	12.582.692
11	BTCBOX	BTC/JPY	9.966.578
12	bitFlyer	BTC/JPY	8.892.595
13	itBit	BTC/USD BTC/EUR BTC/SGD	5.851.209
14	GDAX	BTC/USD ETH/USD ETH/BTC	5.830.760
15	BTC-E	BTC/USD ETH/USD ETH/BTC LTC/BTC BTC/RUR LTC/USD ETH/LTC DASH/BTC PPC/BTC NMC/USD PPC/BTC NMC/BTC LTC/EUR PPC/USD NVC/BTC NVC/USD LTC/RUR	4.059.862
16	BitBays	BTC/CNY BTC/USD LSK/BTC LSK/CNY	3.750.618
17	BitMEX	BTC/USD ETH/BTC FCT/BTC LSK/BTC LTC/BTC	3.547.705

se nadaljuje

Tabela 2: Seznam 25 največjih borz digitalnih valut ali delnic (nad.)

Št.	Borza	Valutni pari	Dnevna kapitalizacija v €
18	Yunbi	ETH/CNY BTC/CNY DAO/CNY SC/CNY DGD/CNY BTS/CNY DGD/BTC ETH/BTC BITCNY/CNY DAO/BTC	3.294.965
19	CoinsBank	BTC/USD BTC/EUR BTC/GBP LTC/BTC LTC/GBP LTC/USD LTC/EUR	2.787.787
20	Zaif	BTC/JPY XEM/JPY MONA/JPY MONA/BTC	2.746.045
21	LakeBTC	BTC/USD	2.714.483
22	Bittrex	ETC/BTC ETH/BTC WAVES/BTC STEEM/BTC VOX/BTC BRX/BTC DAO/BTC LSK/BTC SBD/BTC DASH/BTC in še cca. 200 drugih	2.256.008
23	Bitstamp	BTC/USD BTC/EUR	2.038.680
24	OKCoin Intl	BTC/USD LTC/USD	1.662.177
25	CEX.IO	BTC/USD BTC/EUR ETH/BTC LTC/BTC LTC/USD LTC/EUR	1.443.663

Vir: Coinmarketcap, Crypto-Currency Market Capitalizations, b.l.c.

1.2 Verige blokov prve generacije

1.2.1 Bitcoin kot osnovni koncept decentralizirane arhitekture

Bitcoin je prva povsem digitalna valuta, ki je konceptualno potrdila in upravičila svoj obstoj in tako prešla v široko uporabo po celem svetu. Specifika bitcoinske arhitekture je, da ne potrebuje centralnega nadzora ali centralne banke, temveč je njena osnova distribuirana glavna knjiga (angl. *Ledger*) pod imenom knjiga blokov (Beck, Stenum, Czepluch, Lollike & Malone, 2016).

Knjiga vsebuje vse transakcije med uporabniki od samega začetka pa do sedaj. Vse transakcije so tako tudi javne in zapisane na mnogo sistemih in mnogo lokacijah po svetu. Kljub temu, da so transakcije javne, pa se pošiljatelja in naslovnika v bitcoin omrežju ne da avtomatsko povezati z lastništvom sredstev pred ali po transakciji. Arhitektura namreč določa, da le lastnik sredstev v bitcoinski denarnici lahko ta sredstva upravlja ali prenakaže na drug naslov, saj le lastnik lahko dostopa do privatnega kriptografskega ključa, ki podpisuje oz. lahko dovoli transakcijo. Torej gre za podoben koncept kot pri asimetrični kriptografiji, kjer se uporabljata javni in zasebni ključ.

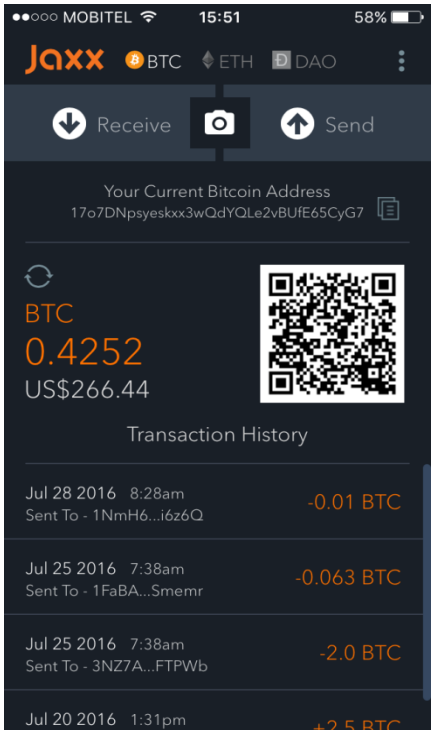
V bitcoinski arhitekturi poznamo bitcoinske naslove, ki so javni in jih ima uporabnik v digitalni denarnici. Število teh naslovov je neomejeno. Celo priporočeno je, da se za vsako transakcijo ustvari nov naslov. Bitcoinski naslov se uporablja za potrebe nakazovanja digitalnih sredstev v denarnico. Maksimalna dolžina javnega bitcoinskega naslova je 35 znakov, po navadi jih pa ima 34, ker se ena ničla na začetku predstavi v začetni enici, ki je karakteristična za bitcoinske naslove. Poleg javnega naslova pa obstaja tudi privatni ključ, ki odpira denarnico in s katerim lahko uporabnik dokaže in tudi upravlja s sredstvi v denarnici.

Sama uporaba denarnice je preprosta. Pogled dveh različnih denarnic, ki sta se v večini prenesli na pametne telefone, lahko vidimo na Sliki 4 in Sliki 5 (Sasson, 2014).

Bitcoin je decentraliziran sistem za plačevanje, ki temelji na konceptu »*Proof of Work*«. Bitcoin se v svojem bistvu zanaša na matematične algoritme in ne na centralne banke. Prav tako njegova vrednost ni vezana na žlahtne kovine kot sta zlato ali srebro, kakor tudi ga ne morejo ustvarjati vlade ali finančne institucije, kot to lahko delajo s fiat valutami (Wright & De Filippi, 2015). Cena je popolnoma odvisna od ponudbe in povpraševanja na borzah digitalnih valut.

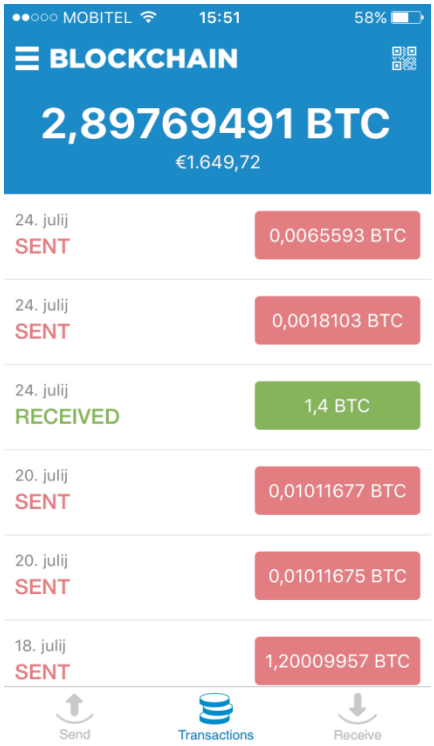
Kripto ali digitalne valute izhajajoč iz bitcoina uporabljajo distribuirano internetno omrežje in omogočajo točka točka povezave, brez potrebe po tretji osebi. Za konsistentnost skrbijo matematični algoritmi in javna knjiga blokov. Vsak blok vsebuje vse transakcije v obdobju od prejšnjega bloka in informacijo od prejšnjega bloka.

Slika 3: Denarnica Jaxx, lahki klient za BTC, ETH in DAO na iPhonu



Vir: Jaxx, Wallet, 2016.

Slika 4: Denarnica Blockchain, lahki klient za BTC na iPhonu

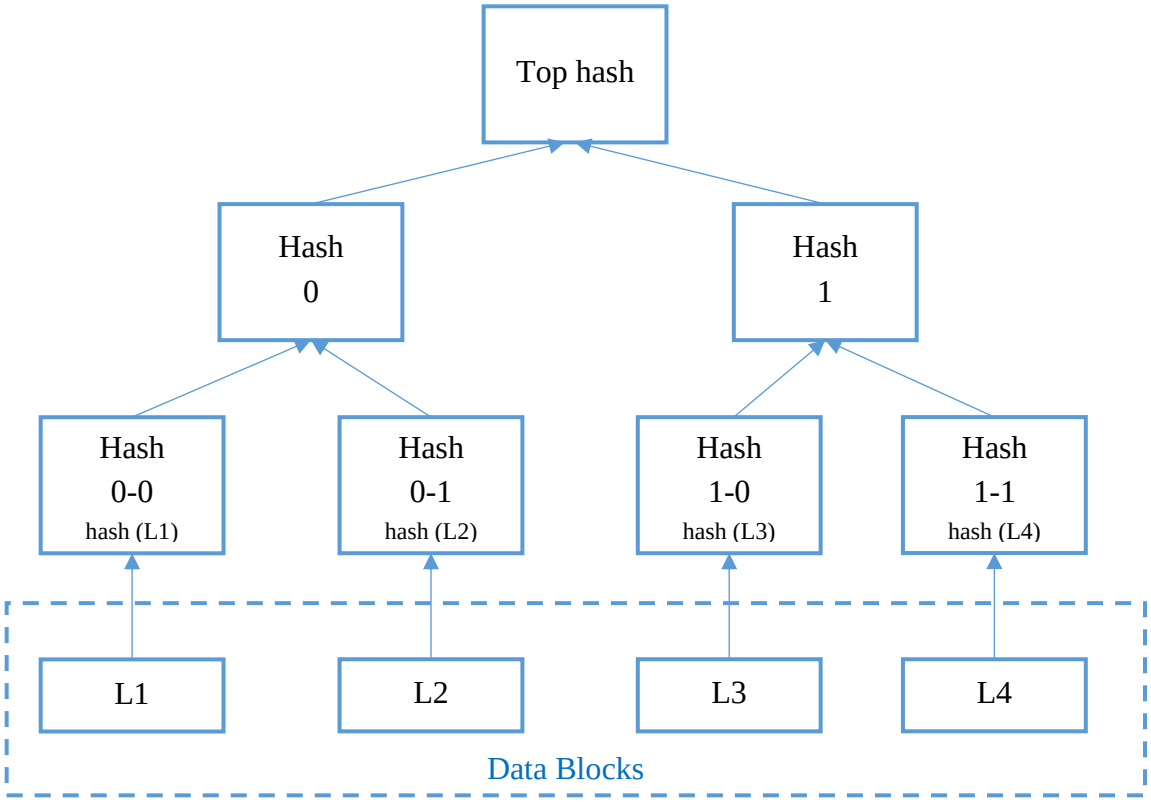


Vir: Blockchain, Wallet, 2016.

V bitcoinski verigi se bloki dodajo v knjigo blokov vsakih 10 minut. Ker gre za decentralizirano arhitekturo, se bloki potrjujejo na vseh računalniških vozliščih, ki so vključeni v omrežje Bitcoin.

Uporabniki računalnikov (rudarji) dajo na razpolago procesorsko moč (centralno procesno enoto ali grafično procesno enoto), ki kreira in preračuna nove bloke. Pogoj, da nastane nov blok in da je le-ta konsistenten, je, da mora vsebovati »Proof of Work«. Za ta namen se podatkom v bloku pripne neka naključna vrednost, časovni žig in zgoščevalni niz iz prejšnjega potrjenega bloka s korenom Merklovega drevesa (Slika 5) vseh transakcij v nizu ali bloku.

Slika 5: Primer Merklovega drevesa



Vir: Becker, Merkle Tree, 2008.

Razlog, da se v blok doda tudi naključna vrednost je, da je nov zgoščevalni niz, ki nastane ob novem posnetku bloka, vedno različen od prejšnjega zgoščevalnega niza in tako konsistenten v knjigi blokov. Ker Bitcoin zahteva posebno obliko zgoščevalnega niza, rudarji (angl. *Miners*) iščejo to obliko s spreminjanjem naključnih vrednosti. Postopek je podoben kot pri iskanju gesla, ki se ujema z zgoščevalnim algoritmom. Težavnost iskanja novega zgoščevalnega niza bloka je odvisna od števila ničel, ki jih zahteva Bitcoin, da nastopijo v nizu. Ko en član omrežja ustvari oz. najde niz, ki ustreza kriterijem, pomeni, da

je našel pravilni niz bloka ali hash, ki ga objavi v verigi blokov. Le-tega mu nato drugi rudarji potrdijo. S tem postopkom se potrdijo tudi vse transakcije, ki so bile vključene v uspešno razrešen blok, kar potrdi celotno omrežje. Z uspešno najdenim hashem bloka, si rudar tudi pridobi pravico do nagrade.

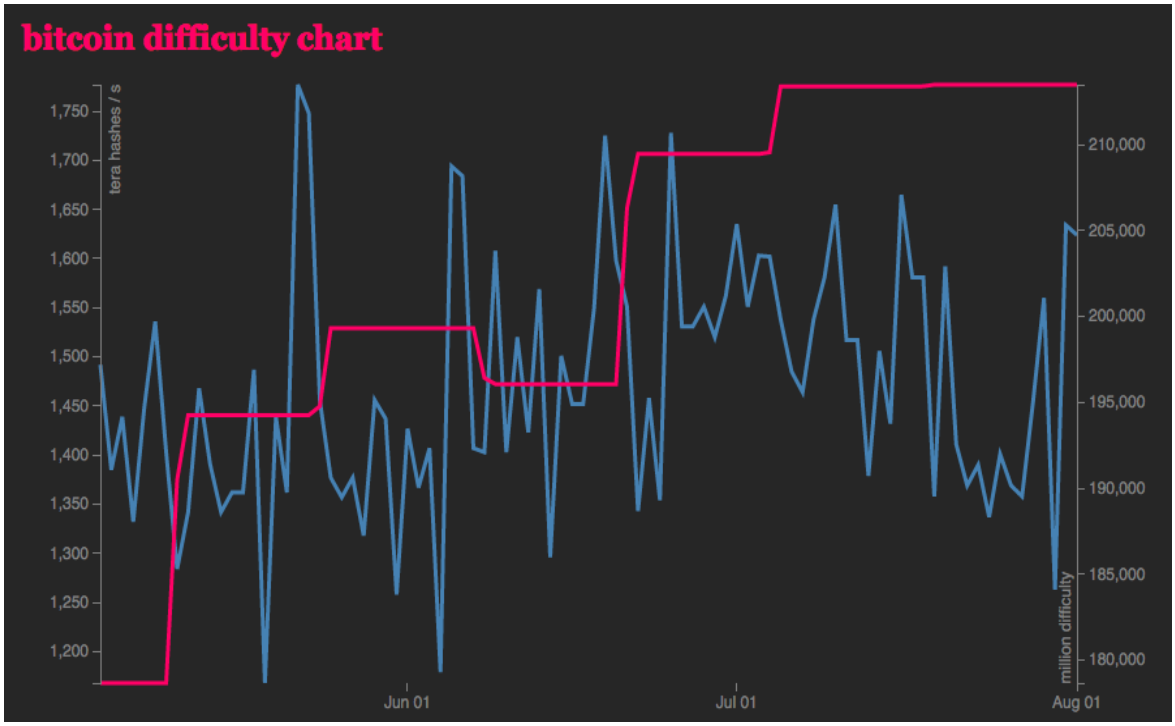
S povečevanjem količine transakciji in procesno močjo rudarjev se prilagaja tudi težavnost rudarjenja. Trenutna težavnost rudarjenja z Bitcoini je razvidna iz Table 3. Gibanje težavnosti rudarjenja z Bitcoini pa prikazuje Slika 6. V nadaljevanju predstavljamo izračun težavnosti rudarjenja na primeru Bitcoina.

Tabela 3: Trenutna težavnost rudarjenja BTC

Ime	**Vrednost**
Težavnostna stopnja [milijon]	213,493
Predvidena nova težavnostna stopnja [milijon]	201,453
Predvideno povečanje težavnostne stopnje [%]	-5,6
Nov cilj [v dneh]	0,3
Mrežni nivo hashiranja [tera hash/s]	1.442.055

Vir: Bitcoin Difficulty, Difficulty of Bitcoin, b.l.

Slika 6: Graf težavnosti od maja do avgusta 2016



Vir: Bitcoin difficult, Bitcoin difficulty chart, b.l.

Povprečna časovna zahtevnost težavnosti iskanja zmagovitega zgoščevalnega niza se izračuna po naslednji enačbi (1) (Bitcoin Difficulty, b.l.):

*povprečni čas v h = težavnost * 2^32 / (3.600 * število zgoščevalnih nizov na s* (1)

Če pri enačbi (1) izpostavimo težavnost dobimo enačbo (2):

*težavnost = povprečni čas v h * (3.600 * število zgoščevalnih nizov na s) / 2^32* (2)

Ker vemo, da se blok kreira povprečno na deset minut, vstavimo v »povprečni čas v urah« 10/60, nato pa še vstavimo trenuten celotni Bitcoinski nivo zgoščevalnih nizov na sekundo, ki trenutno znaša 1.442.055 tera zgoščevalnih nizov na sekundo (angl. *Tera hashes/s*), in dobimo po enačbi (3):

težavnost =1/6(3.600 *1.442.055*10^12)/*
2^32=2,014527563005685806274414062 5e+11
težavnost=201.452 mega hashov (3)

Za izračun prejšnjega bloka je bil potreben tako imenovan »network hash rate«, ki se izračuna po enačbi (4):

network hash
*rate=201.452*10^6*2^32/600=1,442049586189653333333333333333e+18*
network hash rate=1.442.049 tera hash/s (4)

Čas iskanja bloka pa se izračuna po naslednji enačbi (5):

Izračun: *čas iskanja bloka=201.452*10^6 *2^32/1.442.049*10^12=600 sekund* (5)

Iz protokola izhaja, da pri težavnosti 1, algoritem potrebuje približno 7 milijonov hashov na sekundo, da najde blok v 10 minutah. Seveda se z višanjem težavnosti sorazmerno povečuje tudi potreba tako imenovanem »network hash rate«.

Iz izračuna vidimo, da je algoritem potreboval 600 sekund oz. 10 minut in 1.442.049*10^12 hashov na sekundo, da je našel prejšnji blok. Samoregulacija konstantnega časa z regulacijo težavnosti je bila uspešna, saj je bil blok res najden v ca. desetih minutah.

Kot enostaven primer lahko vzamemo tekstovni zapis »Hello, world!« za katerega iščemo pravilni rezultat zgoščevalne funkcije SHA-256, ki se mora začeti z 000 v nizu, kar je pravilo. Primer izračuna zgoščevalne funkcije je prikazan v Tabeli 4. V funkcijo dodajamo vrednosti in s tem spreminjamo rezultat zgoščevalne funkcije, ki vsakič znova izračuna

odtis tekstovnega vhoda. V tem primeru je potrebnih 4251 iteracij, da najdemo niz, ki ustreza kriteriju, da se začne z 000.

Tabela 4: Primer izračuna zgoščevalne funkcije

»Hello, World!0«	=>	1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
»Hello, World!1«	=>	e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
»Hello, World!2«	=>	ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
…	=>	…
»Hello, World! 4248«	=>	6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
»Hello, World! 4249«	=>	c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
»Hello, World! 4250«	=>	0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Vir: Povzeto po Bitcoin difficulty, Primer izračuna zgoščevalne funkcije, b.l.

Tak niz se potem zapiše v knjigo blokov skupaj z vsemi transakcijami v bloku, referenco na prejšnji blok in težavnostno stopnjo reševanja uganke reševanja za omenjen blok. Najden niz seveda ne more biti zapisan v knjigo blokov, če ne ustreza zahtevam protokola. Ko je blok najden, ga drugi udeleženci v omrežju zlahka preverijo in potrdijo njegovo veljavnost, kar je tudi potreben pogoj za konsistentnost knjige blokov. Struktura bloka je prikazana v Tabeli 5.

Rudarjenje v tem primeru je tekmovanje, kdo bo prej našel naslednji blok. Ta tekma se dogaja neprestano in omogoča, da se transakcije pravilno zapišejo in potrdijo v knjigi blokov. To tekmovanje pa zmagovalcem prinaša tudi nagrade. V vsakem bloku je izpis, komu pripada nagrada. Ta zapis se imenuje osnovna transakcija (angl. *Generation transaction* ali *Coinbase transaction*) in je prva transakcija v vsakem bloku. Število Bitcoinov, ki se generira na posamezen najden blok je 50 in se razpolovi na vsakih 210.000 blokov, kar se zgodi približno na štiri leta. Naslednja razpolovitev se bo zgodila predvidoma sredi leta 2020, kar se da spremljati tudi na spletnem naslovu (Bitcoinblockhalf, b.l.). Ta proces se bo zaključil, ko bodo rudarji našli vseh 21 milijonov Bitcoinov.

Težavnostna stopnja iskanja rešitve je avtomatsko določena s strani bitcoinskega omrežja samega na način, da omrežje povprečno najde 6 blokov na uro. Vsakih 2016 blokov, ki se kreirajo približno v 2 tednih, se vsa vozlišča primerjajo težavnost glede na prejšnje obdobje in določijo novo ciljno težavnostno stopnjo, da bo povprečen čas kreiranja blokov ostal v predvidenih mejah. Mreža s konsenzom avtomatsko primerno poviša ali zniža težavnostno stopnjo generiranja blokov.

Se pa občasno tudi lahko zgodi, da dva rudarja istočasno najdeta dva različna veljavna zgoščevalna niza za posamezen blok. V tem primeru točka točka omrežje samo poskrbi, da ne bi prišlo do nekonsistence, saj se samo en blok lahko po vrstnem redu zapiše v knjigo blokov. Protokol poskrbi, da se v kot veljavni blok šteje daljši blok, to je blok z večjo težavnostno stopnjo, drugi pa se zavrže.

Bitcoinske transakcije se objavijo v bitcoinski mreži in vsa računalniška vozlišča v omrežju poskušajo najti pravilni niz. Bitcoinski rudarji pa dobijo še dodatno spodbudo, da vključijo transakcije v blok, ki ga rešujejo. Ta spodbuda so plačane pristojbine za transakcije, ki so jih plačali pošiljatelji Bitcoinov oz. kreatorji transakcij.

Tabela 5: Struktura bloka

Polje	Opis	Velikost
srečno število	Vrednost vedno 0xD9B4BEF9	4 bajte
Velikost bloka	Število bajtov do konca bloka	4 bajte
Glava bloka	Sestavljena iz 6 postavk	80 bajtov
Števec transakcij	Pozitivno celo število VI = VarInt	1 – 9 bajtov
Transakcije	Seznam transakcij (ne prazen)	<Števec transakcij> mnogo transakcij

Vir: Povzeto in prirejeno po Block, Structure of Block, b.l.

1.2.2 Druge kriptovalute na osnovi Bitcoin verige blokov

Obstajajo pa tudi alternative bitcoinske arhitekture, ki se s skupnim imenom imenujejo Altcoin. Naj prepoznavnejši altcoini, ki so poskusili v svojo verigo blokov vnesti nekatere izboljšave oz. uporabiti druge kriptografske zgoščevalne alogitme (angl. *Hash Algorithm*) za delovanje protokola verige blokov, so Ripple, Litecoin in Dogecoin.

Vseh altcoinov je trenutno že več kot 600. Med seboj se razlikujejo po več parametrih, vsekakor pa vsi izhajajo iz odprtokodne zasnove Bitcoina (Altcoin, b.l.).

1.3 Verige blokov druge generacije

1.3.1 Ethereum – decentralizirana platforma za pametne pogodbe

Ethereum je odprtokodna, decentralizirana in odprta platforma, ki temelji na verigi blokov in je postavljena na Ethereum navidezni napravi ali računalniku (angl. *Ethereum Virtual Machine,* v nadaljevanju EVM), ki lahko samostojno izvaja programsko kodo različnih zahtevnosti. Širši javnosti omogoča kreiranje in uporabo decentraliziranih aplikacij, ki delujejo na njej. Gre za prvi decentralizirani, objektno orientirani globalni računalnik, ki se ga ne da centralno upravljati, niti ugasniti. Po hitrosti oz. učinkovitosti to ni najbolj hiter računalnik, je pa vsekakor prvi, ki izvaja aplikacije, ki se jih ne da ustaviti. Poleg tega se

ne da ustaviti niti računalnika, niti upravljati načina njegovega delovanja. Ethereum navidezni računalnik (angl. *Turing Complete*) lahko reši katerikoli algoritem, medtem ko obstoječi klasični računalniki ne izpolnjujejo pogoja »Turing Complete«, saj so omejeni s spominom (Kaye, 2000). Uporabniki lahko izdelajo aplikacije, ki se izvršijo na EVM, v programskem jeziku, ki izhaja iz JavaScript and Python.

Za razliko od bitcoinske platforme, je bil Ethereum zasnovan tako, da je bolj fleksibilen in da se lahko bolj prilagodi potrebam uporabnikov. Omogoča na primer enostavno implementacijo novih aplikacij. Ethereum je platforma tako imenovane nove generacije verig blokov, ki ima ambicijo implementacije pametnih pogodb brez potrebe po zaupanju drug drugemu (Odom, 2015). Ethereum omogoča uporabniku, da sam določi pogoje izvrševanja v pametnih pogodbah glede na svoje potrebe in zahtevano kompleksnost (Omohundro, 2014). S to zmožnostjo je Ethereum presegel zmožnost kreiranja digitalne valute in na široko odprl vrata tudi drugim možnostim uporabe platforme verige blokov (Wood, 2014).

Ethereum vključuje tudi točka točka mrežni protokol, pri katerem je podatkovna zbirka verige blokov vzdrževana in posodobljena na vozliščih, ki so povezani v Ethereum mrežo. Vsako vozlišče poganja EVM, ki izvaja enake ukaze, zato EVM lahko opišemo tudi kot svetovni računalnik. Tak način reševanja zahtev ni v prvi vrsti namenjen učinkovitosti reševanja, ampak konsenzu verige blokov. Decentralizirani konsenz daje platformi Ethereum izjemno visok nivo stabilnosti, neobčutljivosti na napake in neprekinjenega delovanja ter omogoča trajno shranjevanje podatkov v verigi blokov kot neke vrste glavni knjigi. Na tak način je tudi onemogočeno cenzuriranje podatkov ali njihovo spreminjanje za nazaj (Riveret & Sartor, 2016).

Ethereum deluje podobno kot bitcoinova veriga blokov, saj uporablja veliko njegovih funkcionalnosti in tehnologij, vendar pa dodaja veliko inovacij in izboljšav. Pri bitcoinu je osnova veriga blokov, ki je lista transakcij, medtem ko pa je pri Ethereumu osnova račun (angl. *Account*). Njegova veriga blokov spremlja status vseh računov in vse spremembe stanj računov so zabeležene kot prenos vrednosti in informacij med računi. Ethereum pozna dva tipa računov in sicer:

- Račun zunanjega lastnika (angl. *Externally Owned Account*, v nadaljevanju EOA), ki se nadzira s privatnim ključem. Zunanji lastnik na svojo napravo prenese elektronsko okolje denarnice (angl. *Wallet*), kjer se ustvari javni in zasebni ključ, in se poveže v Ethereum omrežje;
- Pogodbeni račun (angl. *Contract Account*), ki se nadzira s programsko kodo pogodbe, ki jo lahko izvrši le EOA. Pogodbeni račun se ustvari s pomočjo programske kode ali pametne pogodbe. Upravlja se ga s pomočjo EOA, ki pa je nadziran preko zasebnega ključa in gesla za dostop do tega ključa. Uporabnik s pomočjo EOA lahko generira neomejeno število pogodbenih računov na način, da prenese kodo v verigo blokov, v

kateri se koda tudi izvrši. Pogodbeni račun izvaja transakcije samo v primeru, da dobi za to navodilo s strani EOA. Sam po sebi ne more izvajati naravnih operacij (kot na primer generiranja naključnih števil, klicev zunanjih funkcij preko API itd.). To je zagotovljeno na način, da Ethereum zahteva od vozlišč, da se dogovorijo o enakem izidu izračuna. Na tak način se morebitne napake ali zloraba katerega od vozlišč praktično izniči.

Tako kot Bitcoin tudi Ethereum zahteva plačilo za izvedbo transakcije. Temu strošku se reče plin (angl. *Gas*). Plačilo transakcije ščiti verigo blokov pred neresnimi ali škodljivimi računskimi nalogami ali pred mrežnimi napadi kot so DOS (angl. *Denial of Service*), DDOS (angl. *Distributed Denial of Service*) ali neskončne zanke. Izvrševalec transakcije mora plačati manjšo vrednost za vsak korak programa, ki ga aktivira, vključno s stroški računanja in uporabe pomnilnika. To se plača v Etherih, ki so nosilna valuta Ethereuma. Stroške transakcije se razdeli vozliščem, ki potrjujejo Ethereum bloke. Rudarji v Ethereumu so vozlišča, ki sprejemajo, širijo, nadzirajo in potrjujejo transakcije. Rudarji nato zberejo transakcije, ki vključujejo posodobljeno stanje računov v verigi blokov, dodajo le-te v nov blok in le tega dodajo v verigo blokov. Rudarji so za to delo nagrajeni z Etrom za vsak posamezen uspešen blok, ki ga uspejo prvi najti in tako pokrijejo stroške in svoje delo v procesu verifikacije.

Enako kot pri Bitcoinu, morajo rudarji reševati zahtevne matematične kriptografske probleme, da lahko uspešno narudarijo nov blok. Temu procesu se tudi v Ethereumu reče »Proof of Work«. Vsak računalniški problem, ki zahteva bistveno več virov za algoritmično rešitev problema, kakor za njeno preverbo, je dober kandidat za »Proof of Work«. Ethereum je želel odvrniti morebitno prevzemanje večinskega deleža oz. koncentracije procesorske moči rudarjev na enem mestu s pomočjo specifične strojne opreme, kot na primer ASIC (angl. *Application Specific Integrated Circuit*), kakor se je to zgodilo pri omrežju Bitcoin, zato je uporabil spominsko in procesorsko zahtevnejši računalniški algoritem za iskanje blokov. Zaradi tega je Ethereum omrežje neprimerno za ASIC strojno opremo za potrebe potrjevanja oz. rudarjenja, kar pomeni večjo razpršenost rudarjenja oz. potrjevanja blokov (Ethdocs, b.l.).

Ethereum uporablja »Proof of Work« algoritem Ethhash, ki omogoča »Turning complete« poganjanje skript (O'Dwyer, 2015). Za razliko od Bitcoina, ki uporablja SHA-256 dvakratno hash funkcijo, ki omogoča le omejen nabor možnosti za izvedbo, se v omrežju Ethereum lahko izvrši vsaka skripta, za katero je plačana provizija (t.i. plin).

1.3.2 Primerjava Bitcoin in Ethereum omrežja

Logično se poraja vprašanje ali je Ethereum res briljantno, popolnoma posplošeno omrežje, ki bo izpodrinilo in nadomestilo verigo blokov Bitcoin, ali samo briljanten poskus, ki ne bo uspel prevzeti glavne tržne kapitalizacije v digitalnih valutah in ohraniti

vrednosti. Odgovor na to vprašanje bo kmalu pokazal čas, najbrž pa resnica leži nekje vmes med obema skrajnostnima. Res pa je, da Ethereum protokol lahko izvrši programsko kodo v pametnih pogodbah, kar je velika sistemska prednost v primerjavi z Bitcoinom. Bitcoinska veriga blokov kot glavna knjiga hrani samo transakcije, v ethereumsko verigo blokov pa se zapišejo transakcije in programska koda, ki se lahko izvršuje na vozliščih (računalnikih) rudarjev kot distribuirana glavna knjiga ali EVM.

Če primerjamo obe trenutno glavni kripto valutni omrežji, lahko opazimo nekatere bistvene razlike med njima, ki jih podajamo v Tabeli 6.

Tabela 6: Razlike med omrežjema Bitcoin in Ethereum

	Bitcoin	**Ethereum**
Povprečni čas med dvema blokoma	10 minut	12 sekund
Uporaba »Turning Complete« izvrševanja programske kode	Ne	Da
Zgoščevalna funkcija	SHA-256	Ethash
Omejevanje centralizacije rudarjenja s hash algoritmom	Ne	Da
Prepolovitev nagrade blokov rudarjem	vsake 4 leta	nikoli
Plačilo transakcij	provizija	plin
Cena transakcije odvisna od zahtevnosti, omrežja in spomina	Ne	Da
Množično financiran	Ne	Da
Količina kovancev pri zgodnjih rudarjih	večina	50 % v petih letih

Vir: CryptoBond, Why is Ethereum different to Bitcoin, 2016.

1.3.3 Izračun donosnosti rudarjenja

Beseda rudarjenje v digitalnih ali kriptovalutah je izposojenka kot analogija rudarjenja žlahtnih kovin. Žlahtne kovine so v naravi redke in imajo visoko vrednost ter so se v zgodovini uporabljale kot osnova za izdajo denarnih valut ali kot valuta sama v obliki kovancev. Digitalne valute na tem delu vlečejo terminološko vzporednico, saj se v konceptu »Proof of Work« večina digitalnih kovancev pridobi z rudarjenjem. Poleg pridobivanja kovancev pa se z rudarjenjem ureja tudi način zaščite omrežja s potrditvami, preverjanjem in prenosom blokov v verigi blokov.

Ethereum podobno kot Bitcoin uporablja model rudarjenja z nagrajevanjem rudarjev za njihovo delo. Odločitve, potrjevanje blokov in stanje denarnic v omrežju se pri obeh sprejema s konsenzom. Konsenz temelji na bloku z največjo skupno težavnostjo. Rudarji ustvarijo bloke, ki jih potem drugi rudarji preverjajo. V verziji 1.1 Ethereuma je blok veljaven, če med drugim izpolnjuje tudi kriterij »Proof of Work« za posamezno težavnost. V verziji 2.0 Ethereuma pa se pričakuje, da bo koncept potrjevanja »Proof of Work« nadomestil koncept »Proof of Stake«.

Koncept »Proof of Work« uporablja algoritem Ethhash, ki je popravljena verzija algoritma Dagger-Hashimoto, ki išče specifično število (angl. *Nonce* - *»number used once«* ali *»number once«*) za vhod v algoritem, da je rezultat izračuna algoritma pod določenim pragom, ki se nastavi glede na težavnostno stopnjo. Bistvo algoritma »Power of Work« je, da ne obstaja boljša strategija za iskanje takih specifičnih števil, kakor je ugibanje, pri čemer pa je preverjanje pravilnosti le teh trivialno ter časovno in procesorsko nezahtevno. Če lahko potrdimo, da so rezultati funkcije algoritma enakomerno porazdeljeni, potem lahko trdimo, da je povprečen čas potreben za iskanje specifičnega števila odvisen od praga težavnosti. Na tak način lahko protokol s prilagajanjem praga težavnosti nadzira čas, potreben za iskanje novega bloka.

S spreminjanjem težavnosti se algoritem sam vedno znova približa določenemu 12 sekundnem intervalu. To je tudi povprečen sinhronizacijski čas stanja denarnic v omrežju, ki ga rudarji najdejo in zapišejo v nov blok. Na tak način se prepreči tudi, da bi kdo s spremembo protokola uspel spremeniti že obstoječe transakcije ali bloke za nazaj ali omogočil podvojitev transakcij. Algoritem to onemogoča, saj bi tak napad uspel le, če bi napadalec pridobil več kot polovico rudarske moči omrežja v tistem trenutku. Temu se reče tudi napad 51 %.

Vsako vozlišče ali računalnik povezan v omrežje Ethereum je lahko rudar, ki lahko pričakuje plačilo storitev rudarjenja proporcionalno glede na skupno rudarsko moč vseh udeležencev. Ta se izračuna glede na število izračunov specifičnih števil na sekundo in normalizira glede na skupno rudarsko moč celotnega omrežja.

Ethash način izračunavanja je zelo zahteven za spomin računalnika ali grafične kartice, zato ASIC sistemi, ki prevladujejo pri Bitcoin omrežju, za Ethereum niso primerni. Računanje »Power of Work« zahteva izbiro specifičnih števil in glav blokov. Ti viri se imenujejo DAG (angl. *Directed Acyclic Graph*) in so veliki nekaj giga bajtov. DAG se v celoti zamenja vsakih 30.000 blokov ali približno vsakih 100 ur, kar se imenuje doba (angl. *Epoch*). Ker je DAG odvisen samo od velikosti bloka, bi bil sicer lahko pred pripravljen, ampak ni, ker mora uporabnik počakati konec procesa, da se generira blok. Izjema je le, ko vozlišče prvič zažene rudarsko programsko opremo; takrat se rudarjenje šele začne in se ustvari DAG iz trenutne dobe.

Rudar, ki prvi najde zmagoviti blok ali izvede »Proof of Work«, prejme nagrado 5 ETH za zmagovalni rezultat in tudi ves plin, ki je bil plačan za transakcije, ki so znotraj najdenega bloka. Rudar je upravičen do nagrade tudi, če ima v bloku vključene prednike (angl. *Uncles*) in sicer 4,375 ETH na prednika. Predniki so zastareli bloki. Računajo se lahko največ 6 blokov za nazaj od dotičnega bloka. Ti bloki se nagrajujejo zaradi interesa protokola, da se nevtralizira mrežna zakasnitev med rudarjem in verigo blokov, ki je pri vsakem rudarju različna in neenakomerno porazdeljena. Veljaven blok, ki vključuje

prednike, dodatno prispeva 7/8 od statične nagrade, ki v omrežju Ethereum znaša 5 ETH. V najdenem bloku se lahko prizna največ dva prednika.

Nagrada rudarjem se v vsakem omrežju izračunava različno. Trenutno sta glede na investicijo v rudarsko opremo in porabljeno energijo za delovanje najbolj donosni omrežji Ethereum Classic in Ethereum.

Spodaj podajamo pregled donosa rudarjenja pri 150 mega heshih na sekundo procesorske moči. Tako procesorsko moč lahko dosežemo s šestimi grafičnimi karticami AMD Radeon RX480, kakršna je prikazana na Sliki 7, ki so sposobne procesirati bistveno več podatkov, kot to počno klasični več jedrni procesorji na matičnih ploščah.

Vidimo, da je ETC trenutno približno tri krat donosnejši od ETH-ja kljub nekajkrat nižji ceni vrednosti ETC v primerjavi z ETH, kar pa se lahko zelo hitro tudi spremeni, glede na ponudbo in povpraševanje po obeh valutah in glede na selitve rudarjev iz enega v drugo omrežje.

Slika 7: Primer grafične kartice AMD Radeon RX480

Vir: Radeon, Radeon Graphics Cards b.l.

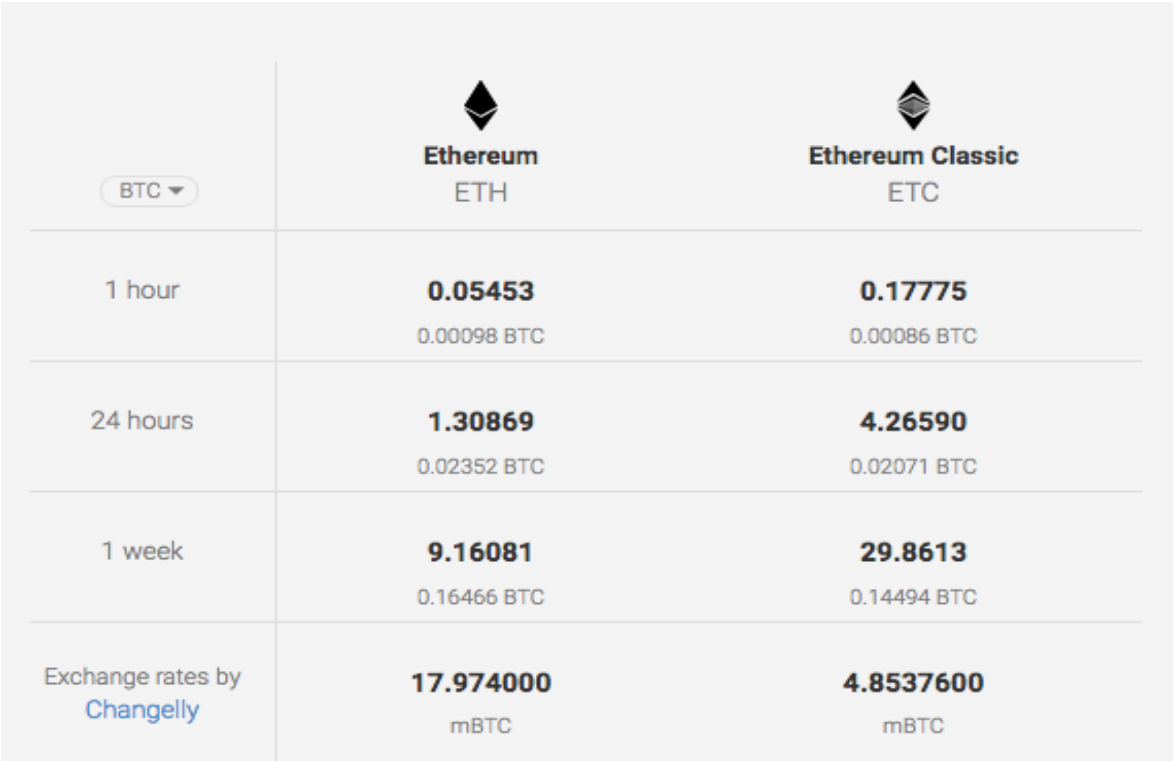
Težavnost in višina nagrade se v omrežju Ethereum ali Ethereum Classic izračunata drugače, kot v omrežju Bitcoin. Nagrada v omrežju Ethereum Classic izražena v ETH se izračuna po enačbi (6):

$$Nagrada\ ETH=((hitrost\ obdelave\ hashov*nagrada\ za\ najden\ blok)/težavnost)*3600 \quad (6)$$

Kalkulatorji rudarjenja v omrežjih Ethereum in Ethereum Classic so dostopni tudi na več spletnih naslovih:

- Karldiab (b.l.);
- Minergate (b.l.) (Slika 8);
- Etherscan (b.l.) (Slika 9);
- Nanopool (b.l.) (Slika 10).

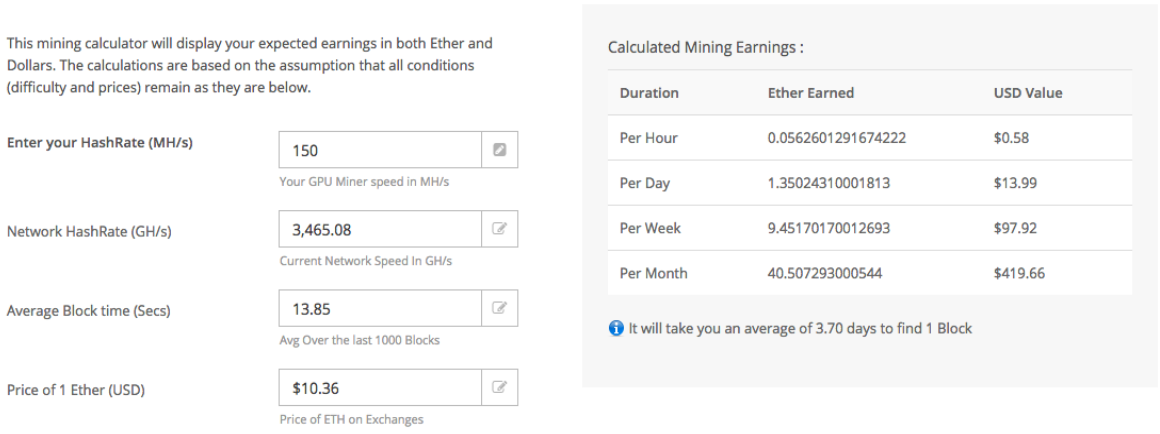
Slika 8: Kalkulator rudarjenja Minergate



BTC	Ethereum ETH	Ethereum Classic ETC
1 hour	**0.05453** 0.00098 BTC	**0.17775** 0.00086 BTC
24 hours	**1.30869** 0.02352 BTC	**4.26590** 0.02071 BTC
1 week	**9.16081** 0.16466 BTC	**29.8613** 0.14494 BTC
Exchange rates by Changelly	**17.974000** mBTC	**4.8537600** mBTC

Vir: Minergate, Mining profitability calculator, b.l.

Slika 9: Kalkulator rudarjenja Etherscan



This mining calculator will display your expected earnings in both Ether and Dollars. The calculations are based on the assumption that all conditions (difficulty and prices) remain as they are below.

Enter your HashRate (MH/s)	150	Your GPU Miner speed in MH/s
Network HashRate (GH/s)	3,465.08	Current Network Speed In GH/s
Average Block time (Secs)	13.85	Avg Over the last 1000 Blocks
Price of 1 Ether (USD)	$10.36	Price of ETH on Exchanges

Calculated Mining Earnings :

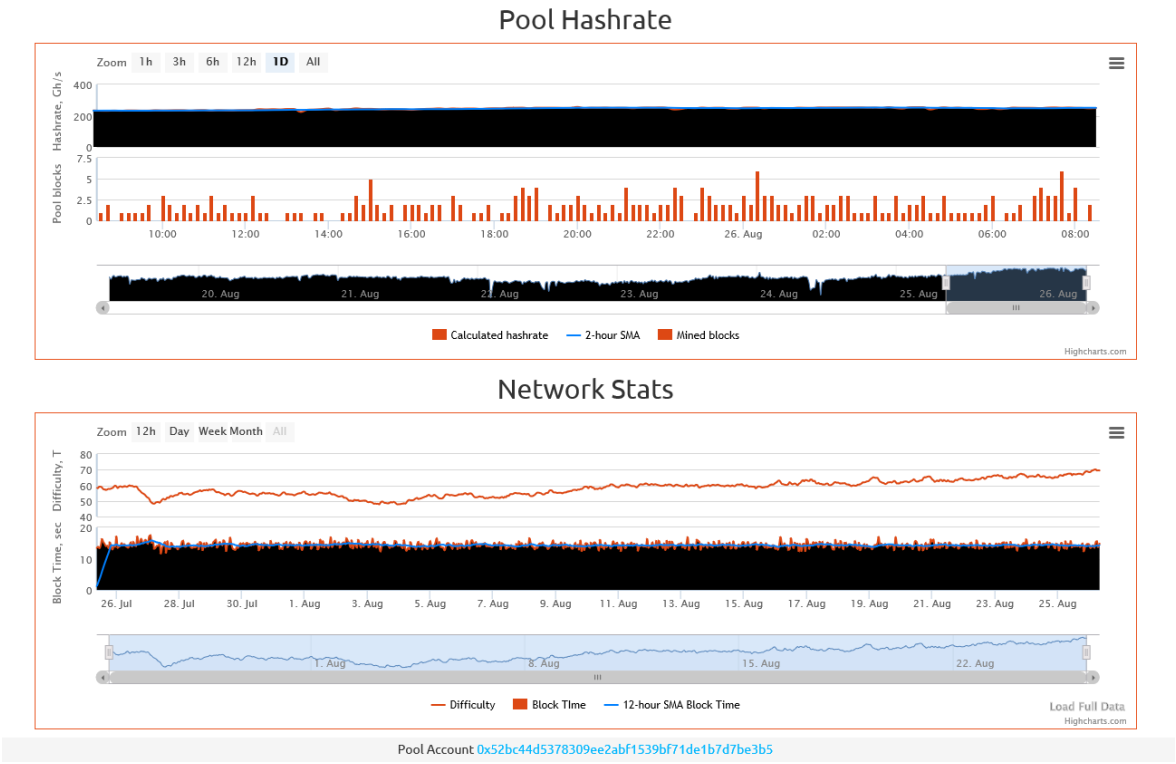
Duration	Ether Earned	USD Value
Per Hour	0.0562601291674222	$0.58
Per Day	1.35024310001813	$13.99
Per Week	9.45170170012693	$97.92
Per Month	40.507293000544	$419.66

It will take you an average of 3.70 days to find 1 Block

Vir: Etherscan, Ethereum Mining Calculator, b.l.

Za investicijo cca 1.600 EUR v rudarsko opremo za ETH rudarjenje s hitrostjo 150 mega hashov na sekundo, bi se po trenutnih trendih in predvidevanjih, le ta povrnila v cca 5 mesecih, seveda, če ne bo preveč presenečenj na trgu.

Slika 10: Grafični prikaz rezultatov rudarjenja



Vir: Nanopool, Pool Hashrate and Network Stats, 2016.

1.3.3 Druge platforme - Bitshares 2.0 – decentralizirana finančna platforma

Bitshares je finančna platforma, ki podpira tehnologije nove generacije za podjetnike, investitorje in razvojnike. Skupni imenovalec je skupni interes globalni prosti trg, ki ga platforma podpira z decentraliziranim konsenzom in decentraliziranim načinom sprejemanja odločitev.

Tehnološko platforma Bitshares, ki jo vodi in upravlja skupnost, ki deluje kot odprti konzorcij posameznikov in podjetij, zagotavlja univerzalen dostop do pametnih pogodb. Analiza platforme je narejena na podlagi informacij s spletne strani platforme Bitshare (Bitshare, 2016).

Bitshares je platforma z vgrajenimi visoko zmogljivimi pametnimi pogodbami za finančni trg (Slika 11). Visoko zmogljiva veriga blokov za digitalne valute in pametne pogodbe je alternativa obstoječim finančnim platformam za fiat valute. Bitshares je v osnovi

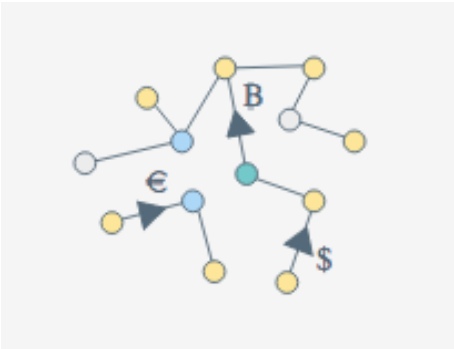
zasnovana tako, da trenutno procesira več transakcij kot Visa in Mastercard skupaj. S pomočjo sistema »Proof of Stake« so transakcije potrjene povprečno v eni sekundi, kar je bistveno hitreje od obstoječih bančnih ali kartičnih transakcijskih sistemov, ki za mednarodne transakcije potrebujejo še vedno nekaj dni ali več.

Slika 11: Grafični prikaz visoke zmogljivosti platforme

Vir: Bitshares, Industrial Performance and Scalability, 2016.

Bitshares omogoča tudi decentralizirano borzo (angl. *Decentralized Exchange – DEX*) brez tveganj zaradi posredovanja tretje strani. Decentralizana borza Bitshares poleg trgovanja digitalnih valut in sredstev ponuja tudi tradicionalne finančne instrumente in vrednostne papirje. Grafični shema decentralizirane borze je prikazana na Slika 12.

Slika 12: Grafični shema decentralizirane borze



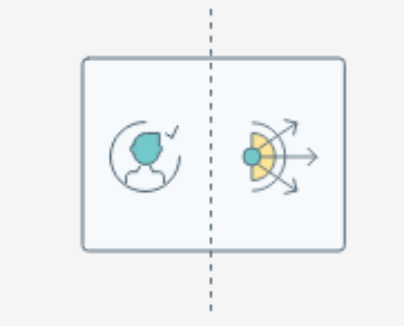
Vir: Bitshares, Decentralized Asset Exchange, 2016.

Omogočeni so tudi imenski računi, da si jih uporabniki lažje zapomnijo, in so zato uporabniku bolj prijazni kot druge digitalne valute, ki uporabljajo daljše nize znakov kot imena računov, kar je primerno za računalnike, ne pa za ljudi. Shema storitve je prikazana na Sliki 13.

Platforma ponuja možnost ustvarjanja tržno vezanih sredstev (angl. *Market Pegged Assets - MPA*), kot je na primer bitUSD, in uporabniško izdanih sredstev (angl. *User Issued*

Assets – UIA), kar je prikazano na Sliki 14. Primer prvega je digitalna valuta, ki zadrži vse lastnosti digitalnih valut, pri čemer njena vrednost ne more pasti pod prednost fiat valute USD (1 bitUSD je minimalno 1 USD). Primer drugega pa je digitalna delnica, ki jo izda podjetje na tej platformi za svoje potrebe ali potrebe projektov.

Slika 13: Grafični prikaz imenskih računov



Vir: Bitshares, Transferable Named Accounts, 2016.

Slika 14: Grafični prikaz tržno vezanih sredstev

Vir: Bitshares, Price-Stable Cryptocurrencies, 2016.

Bitshares omogoča tudi decentralizirano anonimno podjetje, ki omogoča lastnikom podjetja sprejemanje odločitev o bodočih usmeritvah oz. produktih. Prav tako omogoča dinamično podeljevanje pravic na računih, kar je zelo primerno za upravljanje z računi pri korporacijah in finančnih ustanovah, saj se pravice vežejo na osebe. Vsak račun se lahko upravlja s kakršno koli uravnoteženo kombinacijo drugih računov ali privatnih ključev, s čemer se da postaviti hierarhijo, ki odseva potrebe po strukturi pravic v poslovnem svetu in tako vzpostavi več uporabniško arhitekturo (MacDonald, Allen & Potts, 2016).

Kot prva platforma ima vgrajen tudi sistem za ponavljajoča se in časovno načrtovana bodoča plačila na osnovi pametnih pogodb (Slika 15). Omogoča tudi, da lahko uporabnik pooblasti tretjo osebo, da naredi izplačilo iz njegovega računa z nekaterimi omejitvami. Na tak način se lahko zelo preprosto izvajajo aplikacije po metodi nastavi in pozabi, saj se

lahko transakcije izvršijo po vnaprej določenem urniku ali pogojih kot neke vrste bančni trajnik ali plačilo obrokov.

Bitshares ima v protokol vgrajen tudi sistem priporočil (Slika 16), saj se nagradi vsakega, ki pridobi nove uporabnike sistema, in avtomatsko razdeli nagrade, ki se zbirajo za ta namen.

Slika 15: Grafični prikaz avtomatizacije plačil

Vir: Bitshares, Recurring & Scheduled Payments, 2016.

Slika 16: Grafični prikaz sistema priporočil

Vir: Bitshares, User-Issued Assets, 2016.

Poleg drugih finančnih storitev, Bitshares omogoča tudi, da uporabniki izdajajo lastna finančna sredstva (deleže, delnice, obveznice, …) na platformi (angl. *User Issued Assets*) in tako omogoča vzpostavitev dobičkonosnih poslovnih modelov za nekatere tipe storitev. To pomeni, da lahko uporabnik ustvari namenski žeton, valuto ali sredstvo, ki ga drugi uporabniki lahko držijo ali z njim trgujejo znotraj nekaterih omejitvenih okvirov.

Izdajatelj takega javnega instrumenta lahko določi pogoje, kot so na primer: vnaprej določeni računi, ki lahko hranijo ta instrument, trgovalna ali prenosna provizija. Shematski prikaz storitve je razviden iz Slike 17.

Slika 17: Grafični prikaz izdaje lastnih finančnih sredstev

Vir: Bitshares, User-Issued Assets, 2016.

Platforma Bitshares omogoča tudi samostojni model množičnega zbiranja sredstev, o katerih odločajo deležniki projekta (Slika 18). Deležniki pri takem projektu lahko odločijo, za kateri namen se bodo porabila zbrana sredstva.

Za lastne namene ima Bitshare vzpostavljen sklad v višini 1,2 milijarde BTS (kar znaša ca. 8 milijonov USD), ki se avtomatsko polni iz transakcijskih provizij. Vsak dan se sme porabiti 432.000 BTS (kar znaša 77.000 USD na mesec), kar je dovolj za potrebe vzdrževanja platforme ali omrežja.

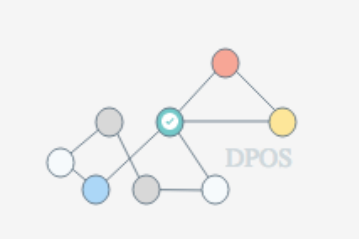
Slika 18: Grafični prikaz samostojnega množičnega zbiranja sredstev

Vir: Bitshares, Stakeholder-Approved Project Funding, 2016.

Bitshares uporablja konsenzni protokol za hitro, učinkovito, decentralizirano in fleksibilno potrjevanje transakcij (angl. *Delegated Proof of Stake,* v nadaljevanju DPOS), kot je razvidno s Slike 19. DPOS sloni na glasovalni moči deležnikov, ki demokratično s konsenzom potrjujejo transakcije.

Vse parametre omrežja kot so urnik, intervali blokov, velikost transakcij itd. se lahko spreminjajo s pomočjo izvoljenih delegatov. Deterministična izbira procedur verige blokov pa omogoča, da se transakcije potrjujejo povprečno vsako sekundo. Protokol sam po sebi je zasnovan tako, da varuje vse udeležence pred neželenimi regulatornimi vplivi.

Slika 19: Grafični prikaz DPOS



Vir: Bitshares, Delegated Proof-of-Stake Consensus, 2016.

1.3.4 Druge platforme - Rootstock - prva bitcoinska odprto kodna platforma

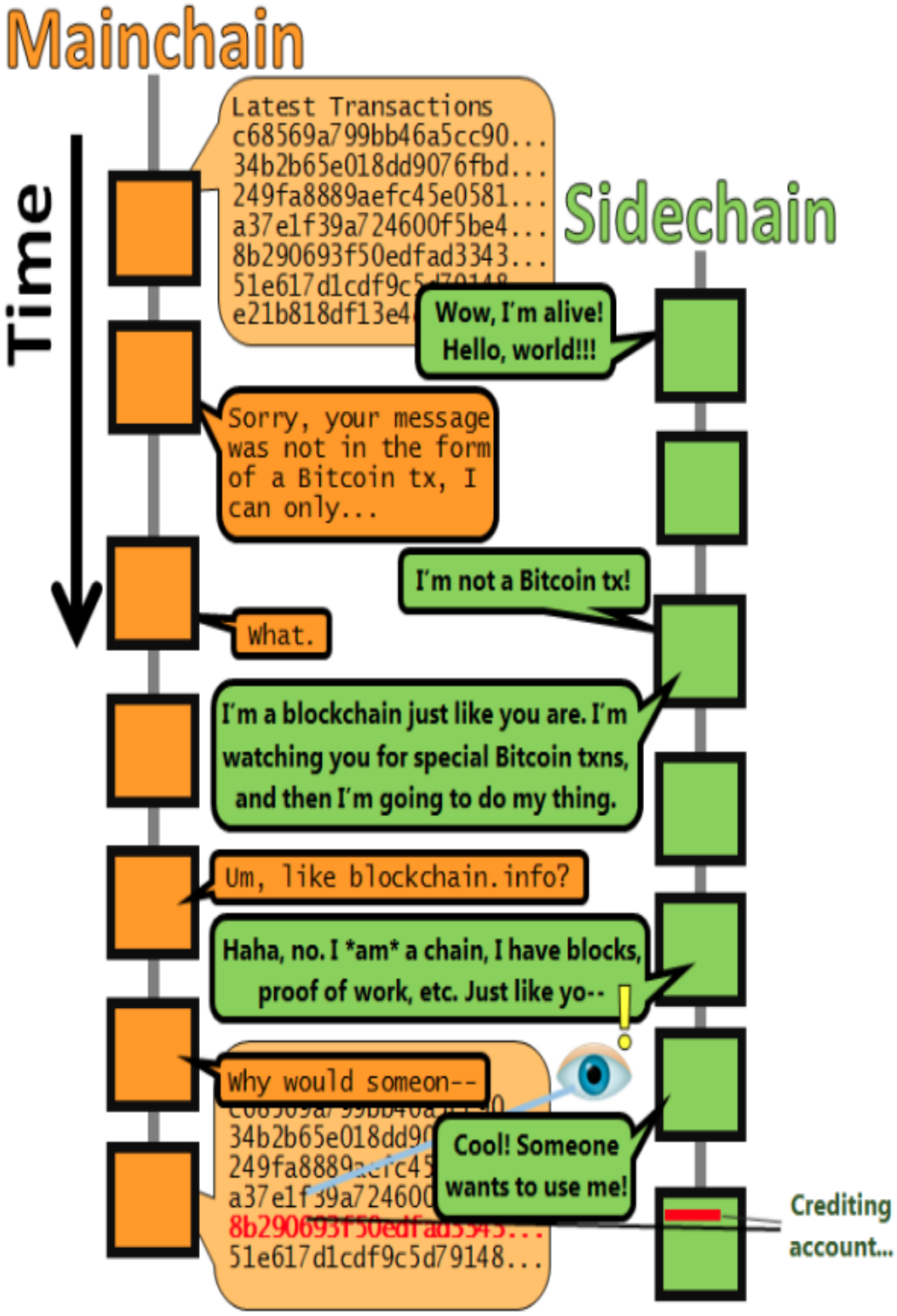
Rootstock (v nadaljevanju RSK) je prva odprtokodna platforma (Rootstock, 2016), ki podpira pametne pogodbe in dvosmerni prehod med glavno in stranskimi verigami (angl. *2-way peg*) (Künnapas, 2016). Prednost platforme Rootstock je dodajanje pametnih pogodb, skoraj takojšnja plačila in kompatibilnost z Bitcoin. RSK podpira možnost prehoda iz glavne verige (angl. *Mainchain*) v stransko verigo (angl. *Sidechain*) blokov (Croman et.al, 2015), ki je zasnovana na način, da podpira funkcionalnosti verig blokov druge generacije. Za spreminjanje glavne, obstoječe verige blokov Bitcoin ni bilo soglasja, zato RSK uvaja možnost prehoda na stransko in seveda nazaj (Garrod, 2016). Mehaniziem dvosmernega prehoda je prikazan na Sliki 20. RSK deluje kot stranska veriga Bitcoina. Ko BTC preidejo v verigo blokov RSK, postanejo Rootcoins (RTC). RTC lahko kadarkoli preidejo nazaj v glavno verigo in postanejo nazaj BTC brez dodatnih stroškov, razen standardnega stroška transakcije v RSK.

RSK izboljšuje Bitcoin na naslednjih področjih:

- Uvedba »Turing complete« navideznega stroja (angl. *Rootstock Virtual Machine – RVM*);
- Potrditev prve transakcije v povprečno 10 sekundah;
- Rudarjenje po principu »Proof of Work« združeno z »Treshold Signature« podpisovanjem (Shoup, b.l.);
- Vgradnja nizko zakasnitvenega hrbteničnega omrežja v točka točka omrežje Gossip (Shah, b.l.);
- Uvedba mehanizma dvosmernega prehoda med glavno in stranskimi verigami blokov.

Če primerjamo trenutno glavna kripto valutna omrežja, katera delujejo in smo jih opisali v nalogi, lahko opazimo nekatere bistvene razlike med njimi, ki jih podajamo v Tabeli 7.

Slika 20: Prikaz prehoda podatkov iz glavne v stransko verigo



Vir:Truthcoin, Drivechain, 2016.

Tabela 7: Razlike med glavnimi kripto verigami blokov

	Bitcoin	**Ethereum**	**BitShares**	**RootStock**
Povprečni čas med dvema blokoma	600 s	12 s	1 s	10
Uporaba »Turing Complete« izvrševanja programske kode	Ne	Da	Ne	Da
Zgoščevalna funkcija	SHA256D	Ethash	SHA-512	SHA256D
Omejevanje centralizacije rudarjenja s hash algoritmom	Ne	Da	Ne	Ne
Prepolovitev nagrade blokov rudarjem	Vsake 4 leta	Nikoli	/	/
Plačilo transakcij	Provizija	Plin	Provizija	Provizija
Cena transakcije odvisna od zahtevnosti, omrežja in spomina	Ne	Da	Status	Ne
Množično financiran	Ne	Da	Da	Da
Količina kovancev ob izdaji	Večina	50 % v petih letih	47 % PTS 47 % AGS 6 % rezerv. sklad	/
Varnostni prag zaradi sebičnosti rudarjev	ca. 30 %	30 % -50 %	/	50 %
Dodana vrednost za Bitcoin	/	Ne	Ne	DA
Integriran z Bitcoinom	/	Ne	Ne	DA
Strojno nezahtevna integracija denarnice	Ne	Da	Da	Da
Zaupnost transakcij	Ne	Preko pogodbo	Ne	Planirana integracija AppleCoin protokola
Skalabilnost transakcij na sekundo	3-24	Neomejeno	100.000	300
Lastna valuta	BTC	ETH	BTS	Uporablja BTC

Vir: Rootstock, 2016.

1.4 Verige blokov tretje generacije

Verige blokov tretje generacije v praksi še niso zaživele, se pa pripravljajo projekti, ki naj bi jih še v letošnjem letu postavili na trg. Gre za kriptografske platforme, ki odpravljajo omejitve verig blokov prve in druge generacije. Verige blokov tretje generacije bodo izboljšale predvsem pretočnost verig blokov in povečale velikost podatkovnih zbirk verig blokov, ki se trenutno hranijo na vsakem vozlišču posebej.

Eno takih rešitev je na svoji spletni strani predstavilo podjetje HEAT Ledger Ltd (HEAT Ledger, 2016), ki je uspešno množično zbralo sredstva s prodajo žetonov (angl. *Initial Token Offerring – ICO*). HEAT Ledger (angl. *Heuristically Enhanced Asynchronous Transactions Ledger*, v nadaljevaju HEAT) je platforma, ki je narejena po zgledu

aplikacijske platforme NXT1 in verige blokov. Za potrjevanje blokov uporablja konsenzusni algoritem »Proof of Stake«. Potrjevanje se predvideva na 25 sekund. Aplikativna pretočnost verige blokov, ki je lahko tudi veriga verig blokov, pa je načrtovana 15 do 30 milijonov zapisov na sekundo.

Glavni tehnični poudarki platforme HEAT (Klerk & Lehtinen, 2016) so:

- V celoti je napisana v programskem jeziku Java;
- Osnovana je na varni MIT licencirani kriptografiji NXT in točka točka konsenzualni kodi;
- Arhitektura je načrtovana z zmožnostmi za uporabo v zasebnih verigah blokov;
- Optimizirana je za velike hitrosti in nizko potrebo po diskovnem spominu;
- Načrtovana je za masovno uporabo verig blokov;
- Med aplikacijami so vključene vse dosedanje funkcionalnosti verig blokov druge generacije, poleg tega pa še lasten trgovalni sistem z dobrinami (angl. *Asset to Asset Trading*), distribuirane aplikacije in točka točka kodiran sporočilni sistem.

HEAT uporablja povsem nov pristop kreiranja verige blokov, saj bo popolnoma odstranil lokalno kopijo verige blokov. Konsenzusna veriga blokov ne bo shranjena v eni datoteki, ampak v več oštevilčenih datotekah omejene velikosti z dodanim majhnimi datotekami zapisanega stanja.

Zaradi teh inovativnih rešitev bodo vozlišča povezana v verigo blokov HEAT procesorsko in spominsko nezahtevna, s čemer se odpirajo vrata za široko masovno uporabo in cenovno dostopno rešitve.

HEAT uvaja tudi novo tehniko distribuirane arhitekture storitev (angl. *Distributed Service Architecture - DSA*), pri kateri uporabniki za svoje aplikacije lahko uporabijo enostavno programsko kodo napisano v Javi ali JavaScriptu. Slednje uporabnikom zagotavljajo interaktivne storitve z uporabo verig blokov, kot kodirano in distribuirano stanje spomina. DSA temelji na lastniškem interaktivnem komunikacijskem protokolu, podobnem kot je protokol http. HEAT bo omogočal izgradnjo širokega spektra digitalnih valut in točka točka podatkovnih storitev. Storitve bodo ponujene na decentraliziran in anonimen način, pri čemer bodo ponudniki storitev lahko zagotovili korektnost. Vsakdo bo lahko na svojem vozlišču, povezanem v verigo blokov HEAT (HEAT Ledger, 2016), objavil in zastonj ponudil svoje avtomatizirane storitve. DSA je v osnovi podobna pametnim pogodbam, je pa v primerjavi z njimi nadgrajena. V Tabeli 8 so opisane podobnosti in razlike med DSA in pametnimi pogodbami.

Z vzpostavitvijo verige blokov HEAT lahko pričakujemo veliko novih storitev, saj verige blokov HEAT izkorišča prednosti vseh obstoječih in delujočih verig blokov. Veriga blokov HEAT je veriga verig, v kateri se zapisujejo podatki o lokaciji zapisa originalne verige

blokov, ki je primarni nosilec podatkov. S takim konceptom praktično nima omejitev ustvarjanja novih storitev. Relativno hitro potrjevanje transakcij v blokih prinaša še dodatne ugodnosti, saj bo veriga blokov veliko bolj pretočna in sposobna velikega števila transakcij v sekundi. To odpira možnost tudi trgovalnim in finančnim storitvam oz. storitvam, ki so časovno vnaprej predvidene.

Tabela 8: Razlike med DSA in pametnimi pogodbami

	DSA	**Pametne pogodbe**
Se proži na osnovi dogodka v verigi blokov	Da	Da
Prejmejo vhodne podatke preko verige blokov	Da	Da
Vrne rezultat v verigo blokov	Da	Da
Deluje v velikem obsegu, posamezne storitve ne delujejo na vsa vozlišča v omrežju	Da	Ne
Avtor ostane anonimen	Da	Da
Arhitekturno vključuje vgrajen zmogljiv plačilni sistem	Da	Da
Lahko dostopa do vhodnih podatkov izven verige blokov	Da	Ne
Lahko kliče zunanje storitve ali izvaja opravila izven verige blokov	Da	Ne
Se lahko verižijo storitve s sklicevanje druga na drugo	Da	Da
Se lahko povezuje z drugimi verigami blokov	Da	Ne
Zaganjanje storitev/pogodb je zastonj	Da	Ne

Vir: HEAT Ledger, Difference between DSA and Smart contracts, 2016.

Za boljše razumevanje novih možnosti so v nadaljevanju na kratko opisani nekateri primeri novih storitev, ki jih omogoča platforma HEAT in ki bodo po vzpostavitvi platforme HEAT gotovo ustvarjene:

- Oracle storitve, ki zapišejo zunanji podatek v verigo blokov. Na tak način se lahko vzpostavi storitev, ki opravi transakcijo pod pogojem, da so izpolnjeni pogoji izven verige blokov HEAT;
- Poveriteljske storitve, ki se vežejo lahko tudi na zunanje, recimo Oracle storitve ali na vnaprej določene pogoje za izvršitev;
- Časovno tempirane dekodirne podatkovne storitve;
- Sopodpisniške storitve;
- »Gateway Bot« trgovalne storitve;
- Enostavne spletne trgovine.

3 INFORMATIKA V ENERGETIKI

3.1 Delovanje elektroenergetskih omrežij

3.1.1 Povezovanje in upravljanje elektroenergetskega omrežja v Evropi

Elektroenergetski sistem je skupek elektroenergetskih objektov, ki v harmoničnem in usklajenem delovanju izkazujejo sinergijske učinke; v doseganju visoke stopnje zanesljivosti delovanja in v doseganju visoke stopnje kvalitete dobave električne energije (Hrovatin, 2009). Elektroenergetski sistemi se združujejo v večje sisteme – interkonekcije, katerih odlika je izredna obratovalna zanesljivost, odpornost proti motnjam in vzajemna pomoč, če posamezen elektroenergetski sistem zaide v težave.

Delovanje elektroenergetskega sistema omogočajo proizvodna, distribucijska in prenosna podjetja. Za nemoteno in visoko kakovostno delovanje elektroenergetskega sistema je potrebno njihovo sodelovanje in usklajenost ter povezovanje matičnega sistema s sosednjimi državami. Povezave s sosednjimi in oddaljenejšimi sistemi omogočajo uvoz in izvoz električne energije in s tem racionalnejše pokrivanje obremenilnega diagrama matičnega sistema. Interkonekcija omogoča manjše rezerve proizvodnih kapacitet, visoko kvaliteto frekvence, visoko kontinuiranost napetosti idr.

Delovanje elektroenergetskih omrežij pogojujejo politični, tehnični in prostorski vplivi in pogoji. Omrežja v večini primerov presegajo meje držav, omejena pa so s kontinentalnimi oz. fizičnimi mejami. Kontinentalni sistemi se težje povezujejo med seboj zaradi velikih razdalj. Omejitve interkonekcij so tudi elektrotehnične narave, saj morajo elektromagnetno povezani sistemi delovati v istih okvirih, predvsem frekvenčnih, da je možno stabilno delovanje. V nasprotnem primeru se lahko taki sistemi povezujejo preko visoko napetostnih enosmernih povezav.

V Evropi imamo med seboj povezano elektroenergetsko omrežje od Norveške na severu do Grčije na jugu in od baltskih držav in Ukrajine na vzhodu do Portugalske na zahodu (Slika 21). V to omrežje, ki deluje na isti frekvenci, nista elektromagnetno sklenjeni Velika Britanija in Irska. Za sinhrono, skupno delovanje v evropski interkonekciji veljajo enotni, trdno določeni, medsebojno dogovorjeni tehnični standardi in priporočila glede vodenja proizvodnje, nadzora kakovosti obratovanja, poročanja rezerv, sigurnostnih kriterijev in posebnih obratovalnih ukrepov (Derganc, 2007).

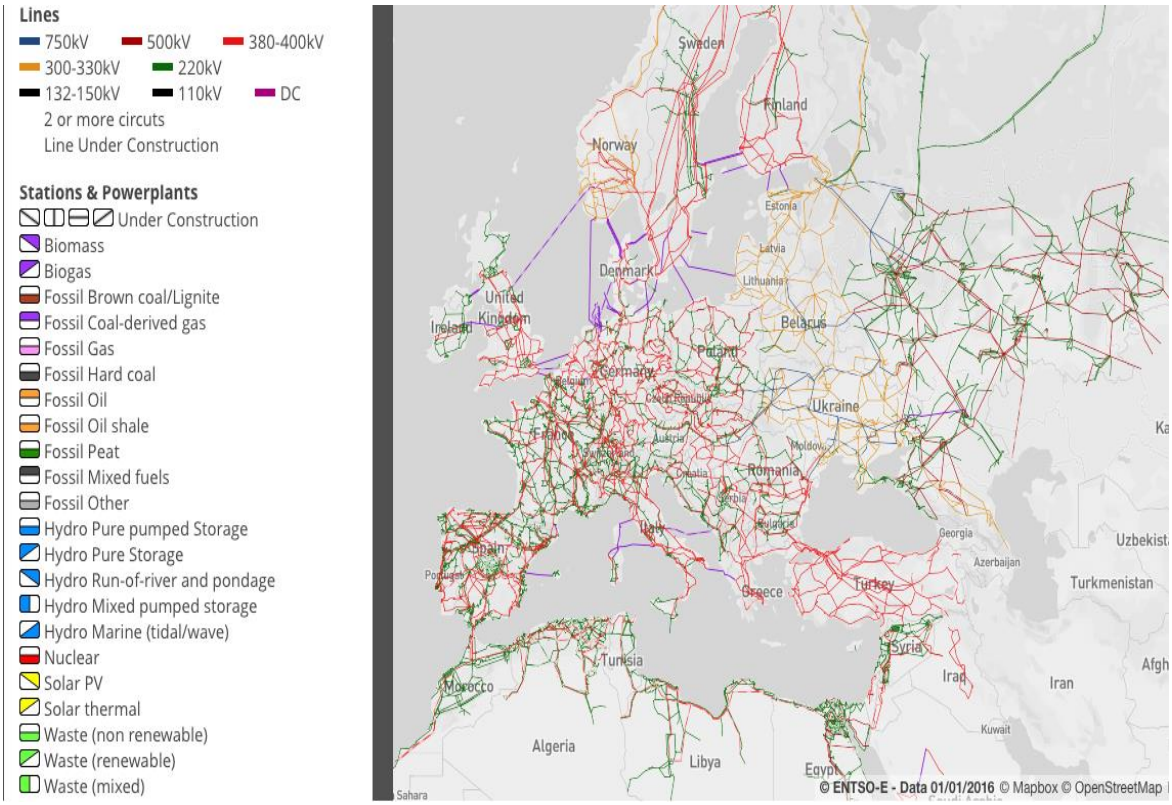
Za povezovanje nacionalnih elektroenergetskih omrežij in delovanje evropske interkonekcije v skladu s pravili je pristojen ENTSO-E (angl. *European Network of Transmission System Operators for Electricity*). ENTSO-E (prej UCTE) je neprofitna organizacija, ki skrbi za sodelovanje evropskih operaterjev prenosnih omrežij (angl.

Transmission System Operators -TSO) na panevropski in regionalni ravni. ENTSO-E koordinira aktivnosti TSO na področju:

- prenosa električne energije,
- razvoja prenosnih sistemov,
- razvoja trgov in drugih raziskav.

Cilj sodelovanja v okviru ENTSO-E je zagotavljanje delovanja notranjega in čezmejnega trgovanja z električno energijo ter usklajevanje pravil delovanja v skladu z evropsko zakonodajo.

Slika 21: Zemljevid prenosa omrežij ENTSO-E



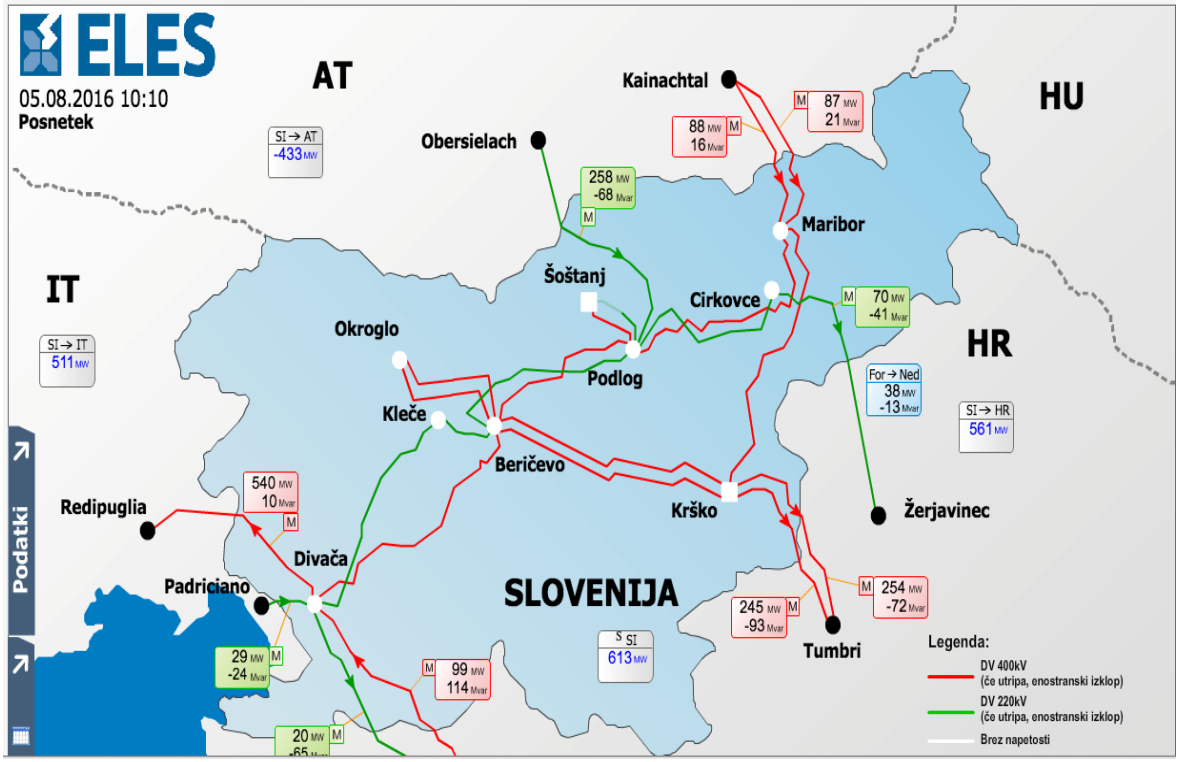
Vir: ENTSOE, ENTSO-E Transmission System Map, b.l.

Za koordinacijo obratovanja in izmenjavo podatkov med posameznimi reguliranimi območji sta zadolžena centra Brauweiler v Nemčiji in Laufenburg v Švici. Centra dnevno izdelujeta tako imenovane vozne rede, ki predstavljajo plan proizvodnje, porabe in čezmejnega prenosa električne energije po urnih produktih za en dan ali nekaj dni vnaprej. Koordinacijski center dobi podatke s strani regionalnih ali nacionalnih centrov, ki morajo imeti znotraj svojega regulacijskega območja usklajen vozni red. Z združenim voznim redom za celotno območje ENTSO-E je potrjen tudi plan proizvodnje in porabe na urni postavki za celotno elektroenergetsko povezano območje za dan v naprej. Plan proizvodnje

in porabe po urah mora v skupnem seštevku znašati nič, da je pravilen in usklajen. Vsota nič pomeni, da sta poraba in proizvodnja za vsako uro posebej enaki. Za uspešno sistemsko obratovanje je potrebno rešiti problem, ki se pojavlja zaradi osnovne značilnosti preskrbe z električno energijo: energija mora biti proizvedena v istem trenutku, ko naključni odjemalec priključi porabnika na napetost (Hrovatin, 2009).

Slovenski elektroenergetski sistem že dolgo vrsto let deluje v evropski interkonekciji ENTSO-E. Sistemski operater prenosnega elektroenergetskega omrežja v Sloveniji (Slika 22) je ELES, ki nenehno skrbi za uravnovešenje proizvodnje, odjema in čezmejnih pretokov energije. Za zagotavljanje varnega in neprekinjenega obratovanja elektroenergetskega sistema mora operater v vsakem trenutku zagotoviti ustrezen nivo sistemskih storitev. Ponudniki sistemskih storitev so proizvajalci elektrike, v določenih primerih pa tudi odjemalci. Prav slednji z razvojem tehnologij pridobivajo na pomenu pri primarni regulaciji sistema. Optimiziranje primarne, sekundarne in terciarne regulacije tako iz tehničnega kot tudi ekonomskega vidika je pomembno za delovanje elektroenergetskih omrežij na visokem kakovostnem nivoju.

Slika 22: Prenosno omrežje v Sloveniji



Vir: Eles, Prenosno omrežje, b.l.

3.1.2 Skupna energetska politika EU

Zanesljiva oskrba z energijo je glavni pogoj za uspešno gospodarsko rast in socialno varnost. Pri zagotavljanju kakovostne oskrbe z energijo se EU sooča z mnogimi izzivi. Zaloge energentov so skoncentrirane v posameznih državah, ki so v večini politično nestabilne, kar pomeni politična in gospodarska tveganja. Ob tem pa je EU čedalje bolj odvisna od uvoza energije iz tretjih držav. Izzivi, s katerimi se Evropa sooča na področju energetike, so na primer:

- vse večja odvisnost od uvoza,
- majhna diverzifikacija,
- visoke in nestabilne cene energije,
- rastoče svetovno povpraševanje po energiji,
- varnostna tveganja v državah proizvajalkah in tranzitnih državah,
- vse večje grožnje podnebnih sprememb,
- počasen napredek na področju energetske učinkovitosti,
- izzivi, ki jih prinaša vse večji delež obnovljivih virov energije,
- potreba po večji preglednosti in nadaljnjem povezovanju ter medsebojni povezanosti energetskih trgov.

Energetska politika EU je tako zasnovana za uresničevanje treh glavnih ciljev, ki so opredeljeni v Zeleni knjigi - Evropska strategija za trajnostno, konkurenčno in varno energijo (2006). Namen energetske politike je zagotoviti zanesljivo, cenovno dostopno in okolju prijazno energijo. V EU so v skladu z Lizbonsko pogodbo postavljeni tudi glavni cilji skupne energetske politike, ki so:

- zagotoviti delovanje energetskega trga,
- zagotoviti zanesljivost oskrbe z energijo v EU,
- spodbujati energetsko učinkovitost in varčevanje z energijo ter razvijanje novih in obnovljivih virov energije,
- spodbujati medsebojno povezovanje energetskih omrežij.

Zanesljivost oskrbe z energijo se povečuje z diverzifikacijo energetskih virov, z zmanjšanjem odvisnosti od uvoza energentov in z razvojem domačih virov. Liberalizacija energetskih trgov in s tem tehnično-upravna členitev na proizvodnjo, prenos in distribucijo naj bi pripomogli k boljši transparentnosti, ekonomski učinkovitosti in s tem k večji konkurenčnosti. Pri soočenjih z okoljskimi problemi imajo pomembno vlogo obnovljivi viri energije in energetska učinkovitost. Obnovljivi viri poleg neposrednega vpliva na izpolnjevanje cilja varovanja okolja pripomorejo tudi k uresničevanju cilja zanesljive oskrbe energije v smislu večje raznovrstnosti energetskih virov in manjše odvisnosti od uvoza energentov.

Aktualni program energetske politike temelji na celostni, povezani, podnebni in energetski politiki, ki jo je Evropski svet sprejel marca 2007 in ki do leta 2020 predvideva uresničitev naslednjih ciljev:

- najmanj 20 % zmanjšanje emisij toplogrednih plinov v primerjavi z ravnmi iz leta 1990,
- povečanje deleža obnovljivih virov v porabi energije na 20 % in
- 20 % izboljšanje energetske učinkovitosti.

3.1.3 Vpliv energetike na okolje in pomen obnovljivih virov

Iz vsebine znanstvenih prispevkov, analiz in sprememb, ki jih beležimo v zadnjih 50 letih, ko bolj sistematično beležimo spremembe v okolju, lahko vidimo, da je energetika eden bistvenih onesnaževalce okolja, sledi pa ji transport. S pravočasnim prehodom na obnovljive vire, bi se lahko trend onesnaževanja okolja zmanjšal in omejil na nivo, ki ga naš planet še prenese (Evropska komisija, 2015).

Globalno segrevanje in podnebne spremembe ter s tem nujnost prehoda na uporabo čistih, obnovljivih virov energije so bili tema Pariške konference 2015, ki se jo je udeležilo 195 držav. Decembra 2015 se je tako v Parizu zgodil zgodovinski podnebni dogovor, s katerim so sodelujoče države sprejele pravno zavezujoče sklepe s ciljem omejitve globalnega ogrevanja pod 2°C.

Ambiciozen in uravnotežen sporazum, ki je prvi pomemben večstranski dogovor 21. stoletja, določa globalni akcijski načrt, s katerim naj bi se preprečile nevarne podnebne spremembe in omejilo globalno segrevanja pod 2°C.

Dogovor je rezultat dolgoletnih prizadevanj mednarodne skupnosti, ki je želela doseči univerzalen večstranski sporazum o podnebnih spremembah. Po omejenem sodelovanju pri Kjotskem protokolu (kot predhodniku Pariškega) in nesoglasjih v Kobenhavnu leta 2009 je EU začela sestavljati široko koalicijo razvitih držav in držav v razvoju v imenu visoko zastavljenega cilja, ki se odraža v uspešnem izidu konference v Parizu. Ta sporazum je jasen znak vlagateljem, podjetjem in oblikovalcem politik, da je svetovni prehod na čiste energije trajnega značaja in da je treba fosilna goriva, ki onesnažujejo, nadomestiti z drugimi viri.

3.1.4 Pomen informatike za delovanje energetike in prenos električne energije

Predvideva se, da bodo v EU do leta 2050 potrebe po električni energiji podvojile (Hrovatin, 2008). Tako velika rast porabe električne energije bo zahtevala izjemne strateške usmeritve in velika vlaganja. Informatika pridobiva vse večjo veljavo v

energetiki, saj je količina podatkov izjemno velika, njihova izmenjava pa vse pogostejša in kompleksnejša (Novak, 2007).
Za soočanje z izzivi kot so rast povpraševanja po energiji na eni strani in uresničevanje ambicioznih načrtov o energetski neodvisnosti in prehodu na čisto energijo na drugi strani, je pomembno usklajeno delovanje energetike, informatike in financ.
Energetika se nahaja pred pomembnimi strateškimi odločitvami, ki so povezane z uvajanjem informacijske podpore, predvsem na področju optimizacije poslovnih procesov in s tem elektroenergetskih sistemov.

Vključevanje razpršenih virov proizvodnje iz obnovljivih virov ter vse glasnejše zahteve po učinkovitejši rabi energije in aktivnejši vlogi odjemalcev postavljajo v ospredje pametna omrežja. Vloga informacijskih tehnologij ima pomembno vlogo pri implementaciji koncepta pametnih omrežij, ki so skupek tehnologij, storitev in konceptov (napredno merjenje, prilagajanje proizvodnje in porabe, aktivna omrežja, shranjevanje energije…).

Razvoj pametnih omrežij bo imel velik vpliv na način reguliranja elektroenergetskih trgov, njihovo prilagodljivost, zanesljivost in ekonomičnost.

Razvoj informacijskih tehnologij in rešitev bo omogočal učinkovito izmenjevanje podatkov med napravami, informacijskimi sistemi in podjetji znotraj elektroenergetskega omrežja. Poleg tega informacijski sistemi predstavljajo podporo sprotnim odločitvami v obratovanju elektroenergetskega sistema, omogočajo vizualno predstavitev množice podatkov za boljšo preglednost in hitrejše odzivanje, razvoj aplikaciji in sistemov za enostavno upravljanje idr.

Pomembno vlogo pa ima tudi varnost informacijskih sistemov, saj je potencialna škoda vdorov v informacijske sisteme v energetiki lahko velika za celotno družbo in gospodarstvo.

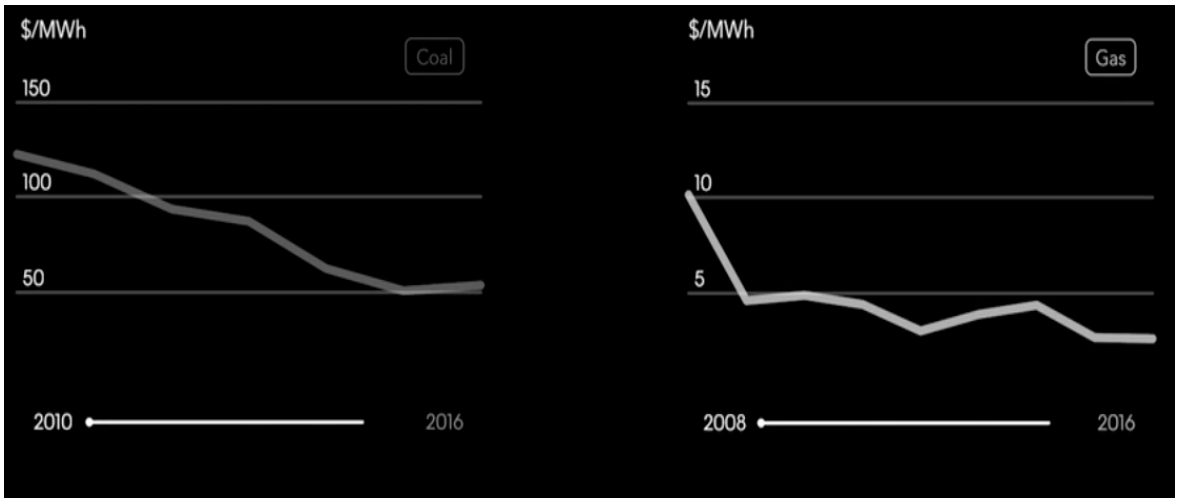
3.2 Monitoring obnovljivih virov energije

Monitoring obnovljivih virov energije je pomemben s strateško-ekonomskega in tehničnega vidika. Spremljanje razvoja energetike in njenega prehoda na obnovljive vire je pomembno zaradi prilagajanja ukrepov in politik za doseganje strateško zastavljenih ciljev. S tehničnega vidika je monitoring obnovljivih virov pomemben za usklajeno delovanje energetskih trgov. Oba pogleda sta lahko izziv za ustvarjanje novih poslovnih modelov, ki bodo lahko pomembno vplivali na globalni delež obnovljivih virov v skupni porabi energije. Prehod v energetiko, ki temelji na čisti energiji, je infrastrukturni, investicijski in organizacijski zalogaj, ki zahteva sodelovanje različnih deležnikov in podporo informacijskih tehnologij.

3.2.1 Strateško-ekonomski vidik obnovljivih virov energije

Napovedi deležev posameznih virov energije do leta 2040, ki smo jih analizirali v nadaljevanju, kažejo pričakovana najbolj potencialna področja, področja, na katerih se bo izvajala večina investicij, ceno posameznih tehnologij in delež obnovljivih virov.
Glede na dosedanje izkušnje ugotavljamo, da kljub znižanju cen premoga in plina v obdobju 2010 - 2016 (Slika 23) ta dva energenta ne bosta mogla konkurenčno slediti proizvodnji energije iz vetra in sonca, kar razlagamo s predvidenimi investicijami v obnovljive vire energije.

Slika 23: Gibanje cene premoga in zemeljskega plina

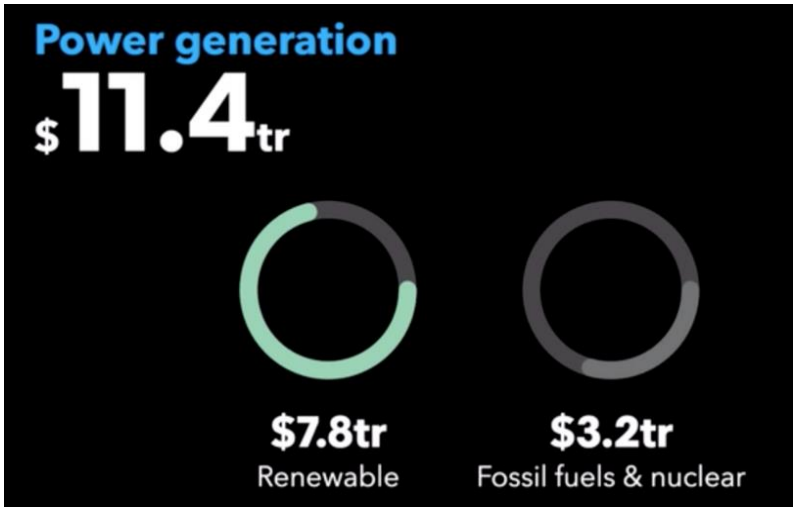


Vir: Bloomberg New Energy Finance, Evolution of coal and gal prices, 2016.

Predvideva se, da se bo do leta 2040 na področju proizvodnje energije porabilo 11,4 trilijona USD za investicije, od tega 7,8 trilijona za investicije v obnovljive vire in 3,2 trilijona za investicije v proizvodnjo električne energije iz premoga in jedrske energije, kar je prikazano na Slika 24. To pomeni, da bo leta 2040 že 60 % globalne inštalirane moči v obnovljivih virih.

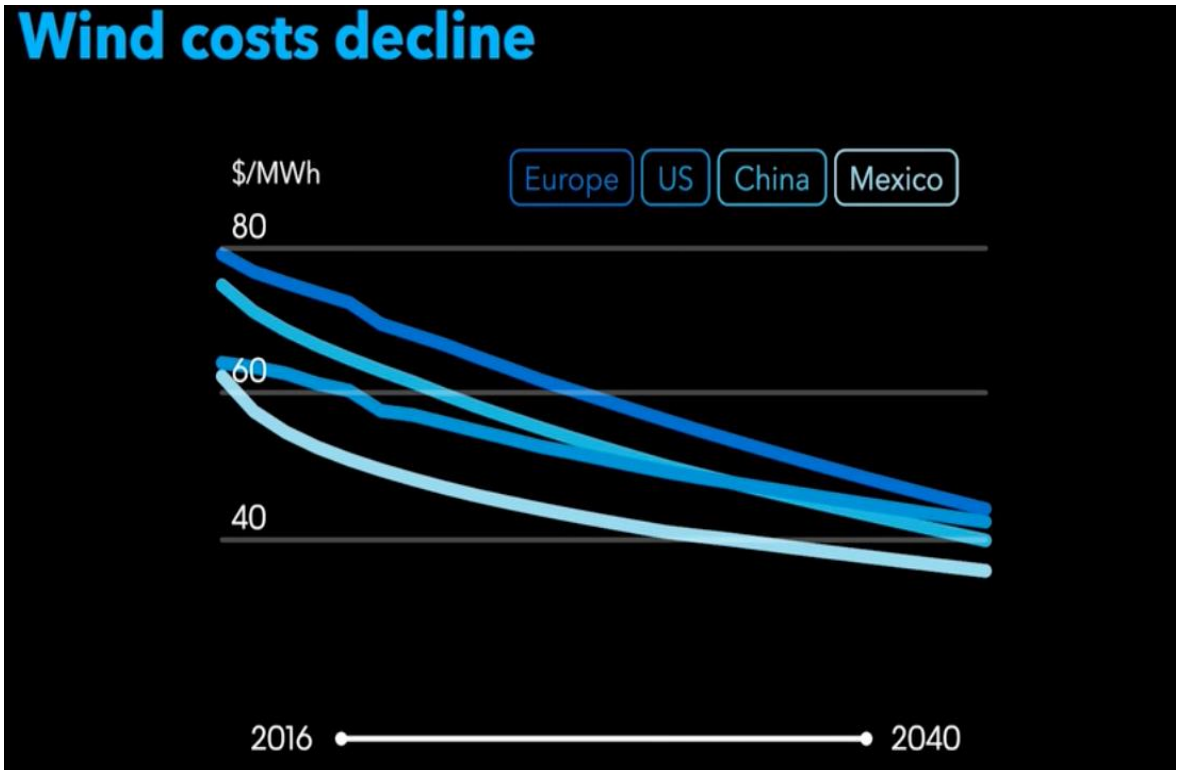
Predvideva se, da se bo do leta 2040 najbolj pocenila električna energija pridobljene iz vetrne in solarne energije. Strošek instalirane moči vetra se bo do leta 2040 zmanjšal za 41 %, sončne pa za 60 %. Nižanje cene energije iz vetrnih in sončnih elektrarn prikazujeta Slika 25 in Slika 26. To pa pomeni, da bosta omenjeni tehnologiji cenovno nepremagljivi na trgu, v nekaterih deželah že leta 2020, v večini dežel pa gotovo leta 2040.

Slika 24: Predvidene investicije v nove proizvodnje vire do leta 2040



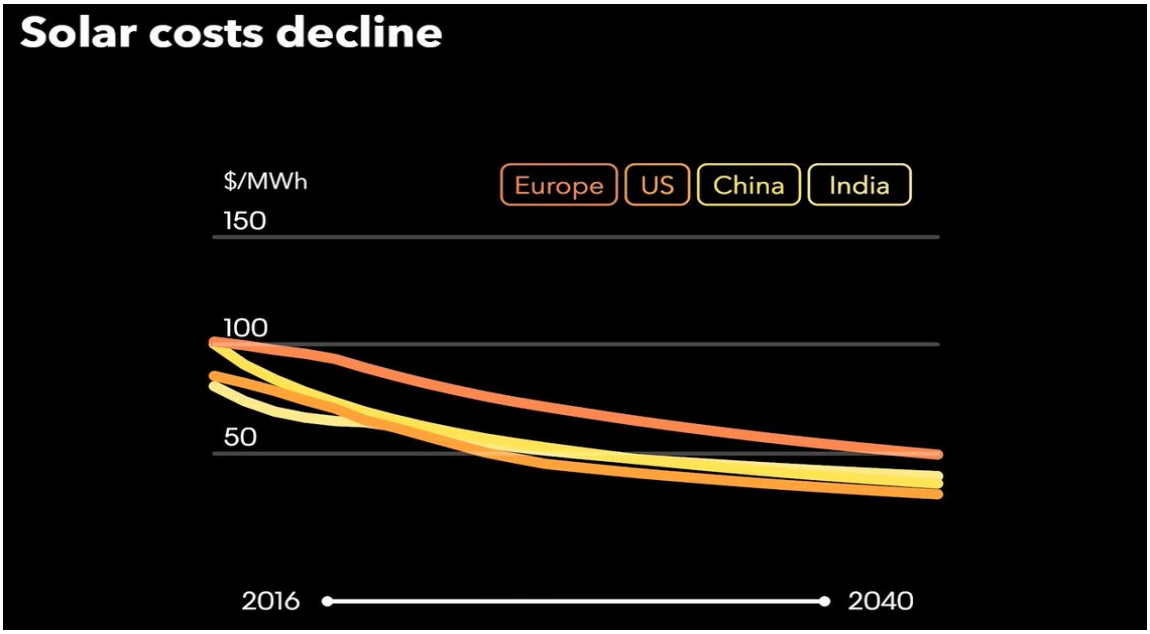
Vir: Bloomberg New Energy Finance, Total investment in power generation to 2040, 2016.

Slika 25: Predvidena proizvodnja cena energije iz vetrnih elektrarn do leta 2040



Vir: Bloomberg New Energy Finance, Wind costs to 2040 , 2016.

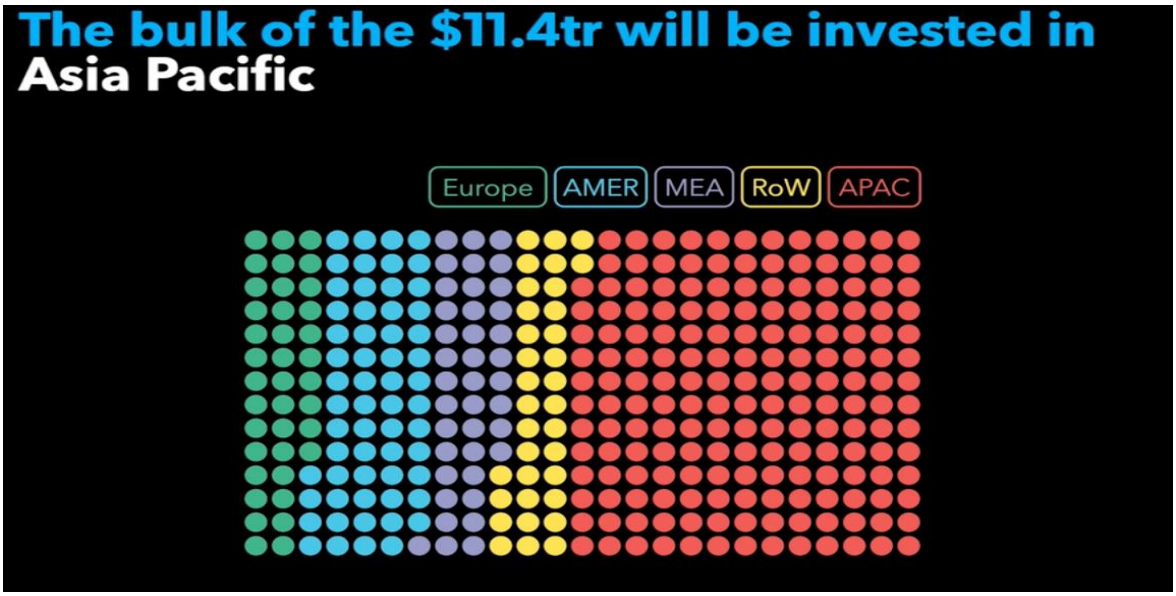
Slika 26: Predvidena proizvodna cena energije iz sončnih elektrarn do leta 2040



Vir: Bloomberg New Energy Finance, Solar PV costs to 2040, 2016.

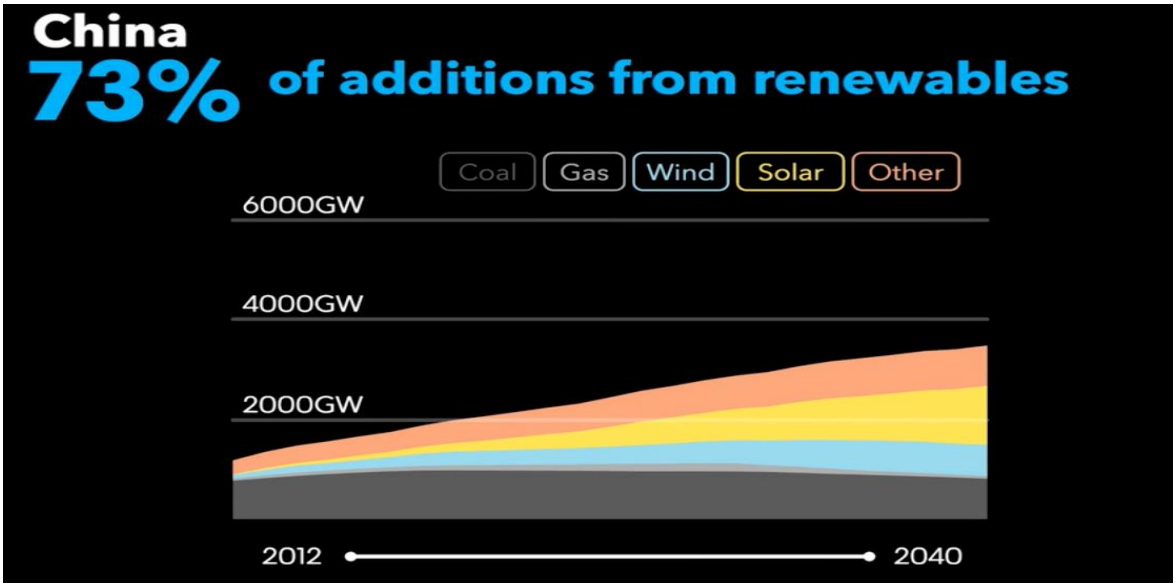
Večina investicij v obnovljive vire bo izvedena v azijsko pacifiški regiji, kjer bo izvedenih več investicij kot na preostalem delu sveta skupaj. Grafično predstavitev predvidenih investicij prikazuje Slika 27. Polovica investicij v azijsko pacifiški regiji bo na Kitajskem, kjer se bo investiralo 2,3 trilijona USD, kar bo zagotovilo, da bo Kitajska leta 2040 73 % preskrbovana iz obnovljivih virov (Slika 28).

Slika 27: Predvidene nove investicije po regijah



Vir: Bloomberg New Energy Finance, Cumulative capacity additions by region, 2016.

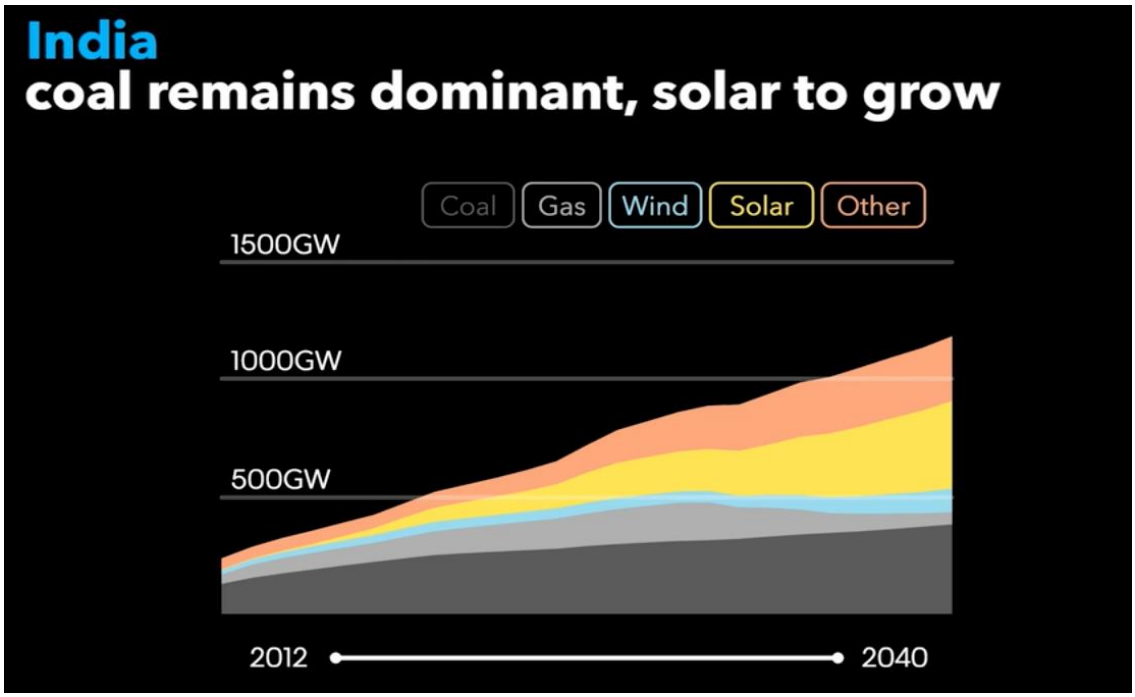
Slika 28: Struktura predvidenih investicij na Kitajskem do leta 2040



Vir: Bloomberg New Energy Finance, China total installed capacity by technology, 2016.

Druga najbolj dominantna država v Aziji bo Indija, v kateri se bo zaradi demografskih in razvojnih trendov povečala poraba energije. V Indiji bo premog ostal največji energent, kot obnovljiv vir pa bo sonce precej dominantno (Slika 29).

Slika 29: Struktura predvidenih investicij v Indiji do leta 2040



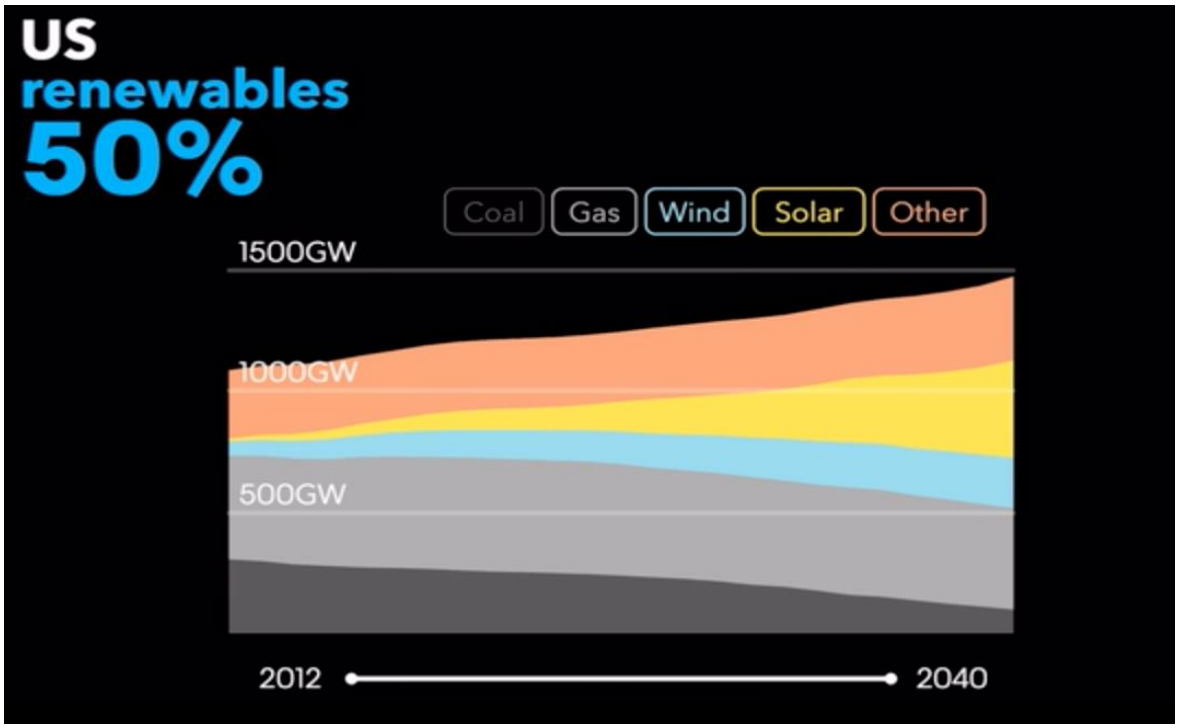
Vir: Bloomberg New Energy Finance, India total installed capacity by technology, 2016.

Pričakuje se, da bodo v ZDA leta 2040 50 % energije pridobili iz obnovljivih virov. Od primarnih virov pa bo ostal glavni vir zemeljski plin. Struktura predvidenih investicij je prikazana na Sliki 30.

V Evropi bo delež obnovljivih virov leta 2040 70 %. Največji delež bo predstavljala sončna energija. Iz Slike 31 lahko razberemo, da se v Evropi pričakuje drastično zmanjšanje porabe premoga in plina.

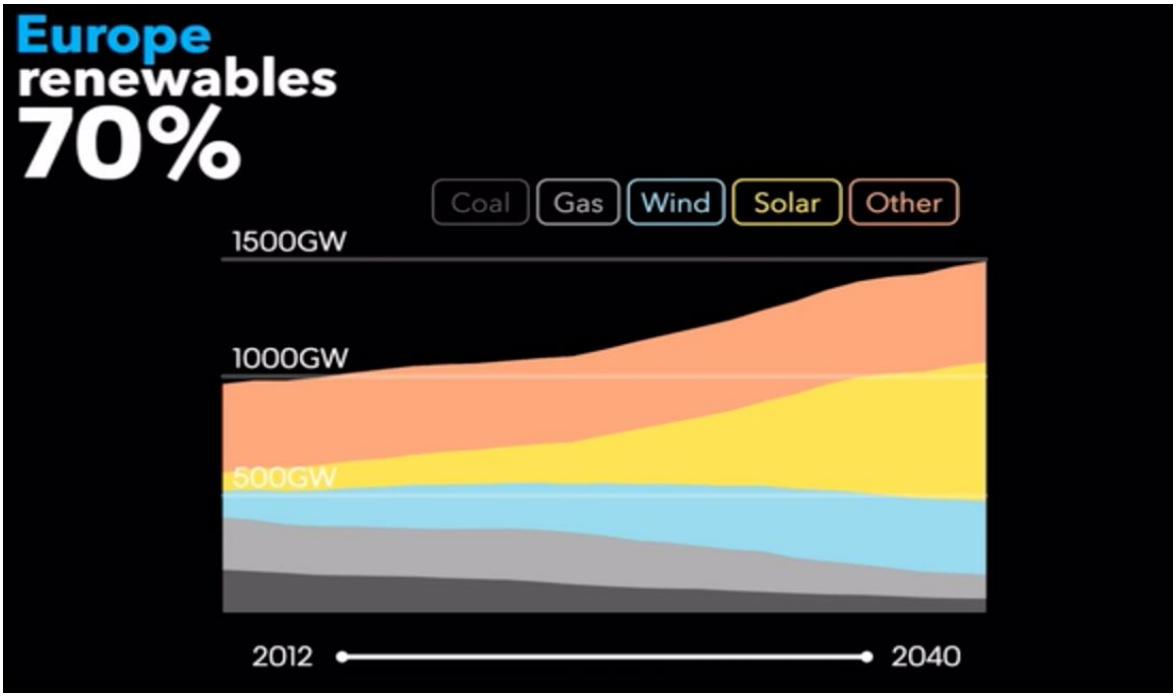
Kot izredno pomemben segment, ki je trenutno izredno majhen, je elektrifikacija transporta oz. električna vozila. To je sektor, ki bo do leta 2040 naredil revolucionarne premike in dosegel 8 % delež porabe električne energije. Trend rasti je razviden iz Slike 32. Zaradi veliko vlaganj v razvoj novih ali izboljšanje obstoječih baterij se bo bistveno povečala tudi kapaciteta baterij na enoto. Z masovno proizvodnjo, kakšno je že lansko leto v ZDA začel Tesla Motors s postavitvijo Gigafactory, se bo postopoma zniževala tudi cena baterij in do leta 2040 bo padla za 76 %.

Slika 30: Struktura predvidenih investicij v ZDA do leta 2040



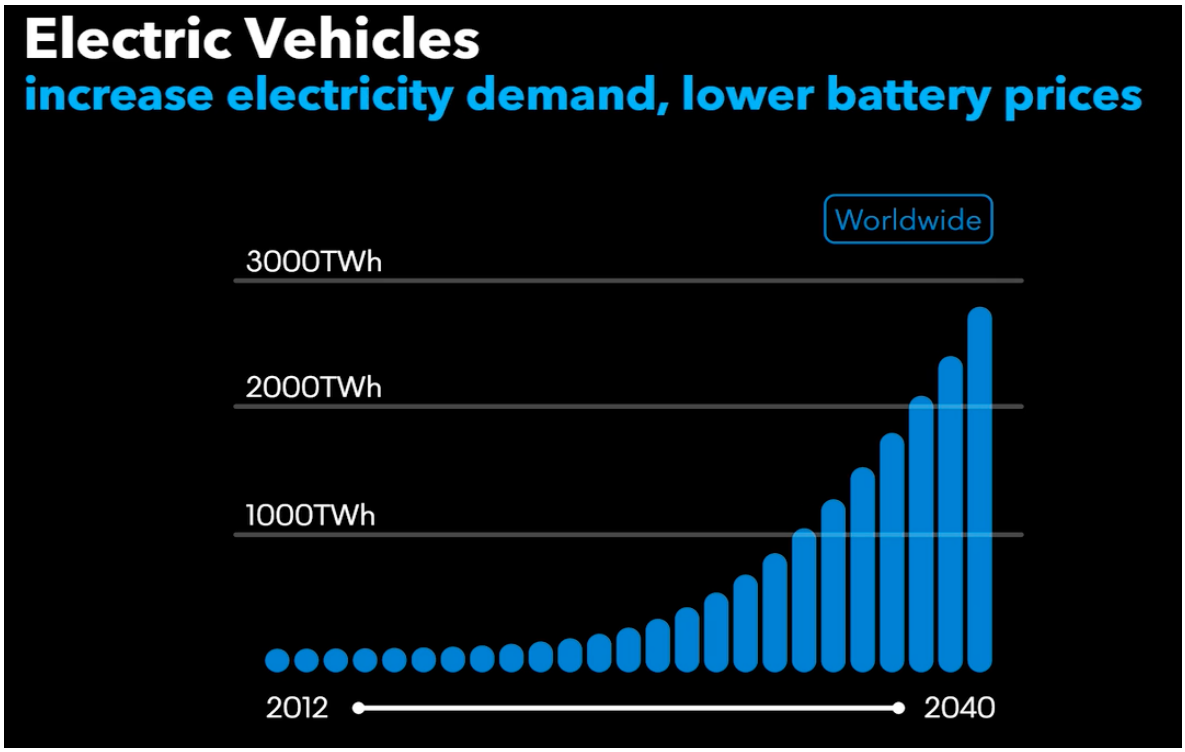
Vir: Bloomberg New Energy Finance, US total installed capacity by technology, 2016.

Slika 31: Struktura predvidenih investicij do leta 2040 v Evropi



Vir: Bloomberg New Energy Finance, Europe total installed capacity by technology, 2016.

Slika 32: Predvidena rast kapacitet baterij v transportu



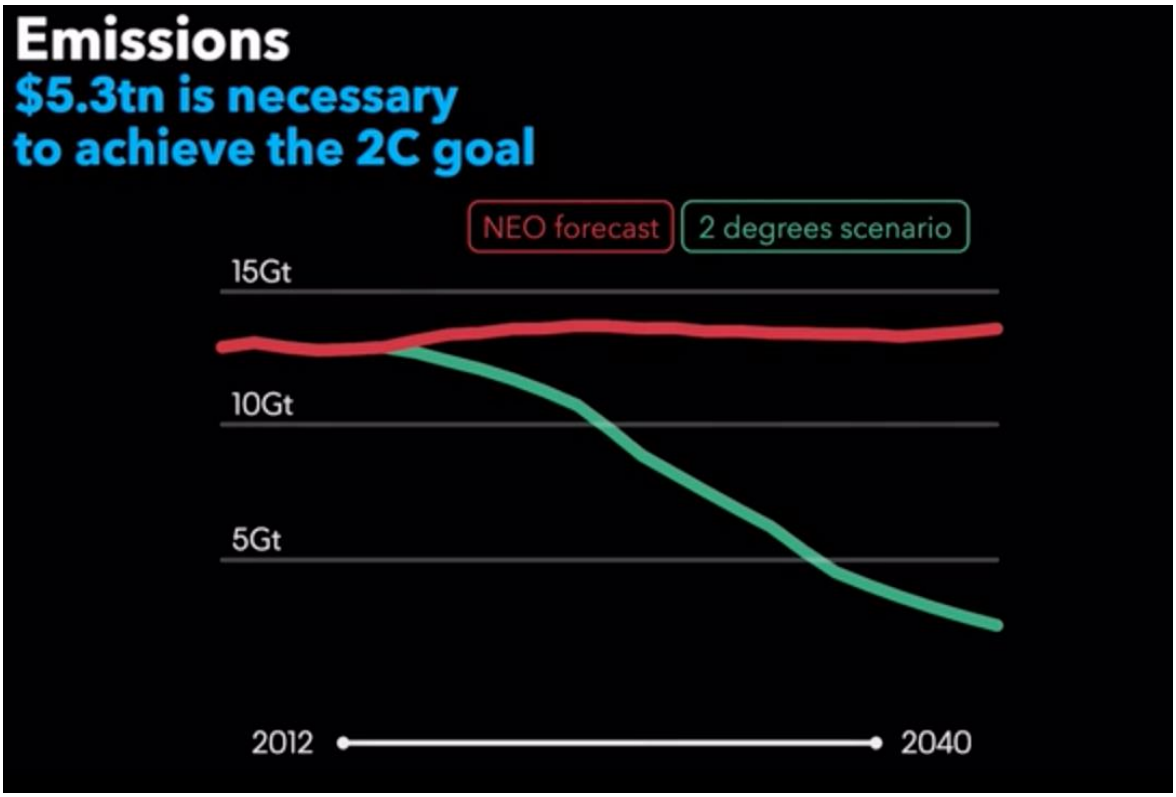
Vir: Bloomberg New Energy Finance, Power demand from EVs to 2040, 2016.

Kljub izjemnemu povečanju proizvodnih kapacitet do leta 2040, bodo fosilna goriva obdržala 44 % vse proizvodnje energije (leta 2015 je njihov delež znašal 66 %). Globalno gledano bodo emisije toplogrednih plinov kljub povečanju proizvodnje energije iz obnovljivih virov še vedno 5 % nad današnjo vrednostjo (Slika 33). Če bi želeli doseči zavezo s pariške konference in omejiti globalno segrevanje pod 2 ºC, potem bi do leta 2040 potrebovali še dodatnih 5,3 trilijona USD investicij v čiste vire energije. Trenutne napovedi investicij v obnovljive vire dosegajo le 59 % od investicij, s katerimi bi uspeli omejiti globalno segrevanje pod 2 ºC, kar je zelo zaskrbljujoče.

2.2.2 Tehnični vidik monitoringa obnovljivih virov energije

Monitoring obnovljivih virov je skupek strojne, programske opreme in storitev, ki omogočajo upravljavcu, lastniku ali distributerju vpogled v posamezen segment delovanja vira. Tehnični pogled monitoringa obnovljivih virov energije, ki smo ga izvedli, je pokazal, da ne obstaja nobena tehnična platforma ali standard, ki bi združevala večino ali vse obnovljive vire energije. Taka tehnična platforma bi vlagateljem prinesla več transparentnosti, primerljivost in boljši pregled. Tako pa vsak proizvajalec opreme in izvajalec projektov poskrbi za svoje rešitve, ki jih razvije sam ali kupi na trgu.

Slika 33: Predviden izpust CO2 v okolje do leta 2040



Vir: Bloomberg New Energy Finance, Power sector CO2 emission trajectories to 2040, 2016.

Sistem za monitoring vključuje strojno in namensko programsko opremo za nadziranje več parametrov in produkcijskih vrednosti celotnega nadzorovanega sistema, kakor tudi status sistema ali njegovega dela. Preko sistema za monitoring se praviloma lahko spremlja podatke, ne da pa se jih spreminjati ali konfigurirati. Napredni sistemi za monitoring vključujejo tudi obveščanje in alarmiranje. Sistem primerja dobljene vrednosti z idealnimi ali pričakovanimi vrednostmi in sporoča odstopanja od pričakovanj. V primeru odstopanj od nastavljenih vrednosti sistem javi, obvešča ali sproži določene druge aktivnosti.

Daljinski nadzor pa omogoča, da uporabnik lahko do podatkov dostopa na daljavo, iz pisarne, iz nadzornega centra, od doma ali kjerkoli, če je povezan na splet. Uporabnik lahko daljinsko tudi nastavlja kontrolne parametre, kot je čas delovanja, točke alarmiranja, način obveščanja, torej vse podatke, ki bi jih sicer lahko nastavljal lokalno na zaslonu naprave. Ta storitev je še posebej koristna, ko uporabnik ali vzdrževalec upravlja večje število dislociranih proizvodnih enot in na tak način zagotovi kakovostnejšo in predvsem ažurnejšo storitev z bistveno manj stroški, kot če bi to zagotavljal fizično na lokacijah samih. V primeru večjih in bolj zahtevnih sistemov ponavadi govorimo o inteligentnem daljinskem nadzoru z monitoringom. Sistemi vsebujejo kontrolne enote, ki lokalno upravljajo, optimizirajo in nadzirajo vsak posamezen proizvodni postroj. Vse naprave pa se povezujejo v centralni sistem, kjer lahko operater sistemov sproža nekatere daljinske ukaze za potrebe vzdrževanja, preizkusov ali optimizacije. Taki sistemi so večinoma že vnaprej programirani za delovanje. Preko monitoringa lahko hranijo podatke o stanjih oz. zgodovino ter kažejo trende, odstopanja od pričakovanih vrednosti, primerjavo med posameznimi komponentami, polji, lokacijami itd. Zgodovinski podatki se tudi analizirajo za potrebe navzkrižnih kontrol pričakovane in realizirane proizvodnje in optimizacije porabe (Carel, 2016). Na trgu lahko vidimo več poslovnih modelov ponudbe sistemov za monitoring:

- neodvisni proizvajalci programske opreme (angl. *Independent Software Providers*),
- proizvajalci razsmernikov, ki ponujajo programsko opremo ali storitev kot del njihove rešitve,
- ponudniki storitev na ključ ali ponudniki vzdrževanja.

Monitoring lahko razdelimo na naslednje segmente:

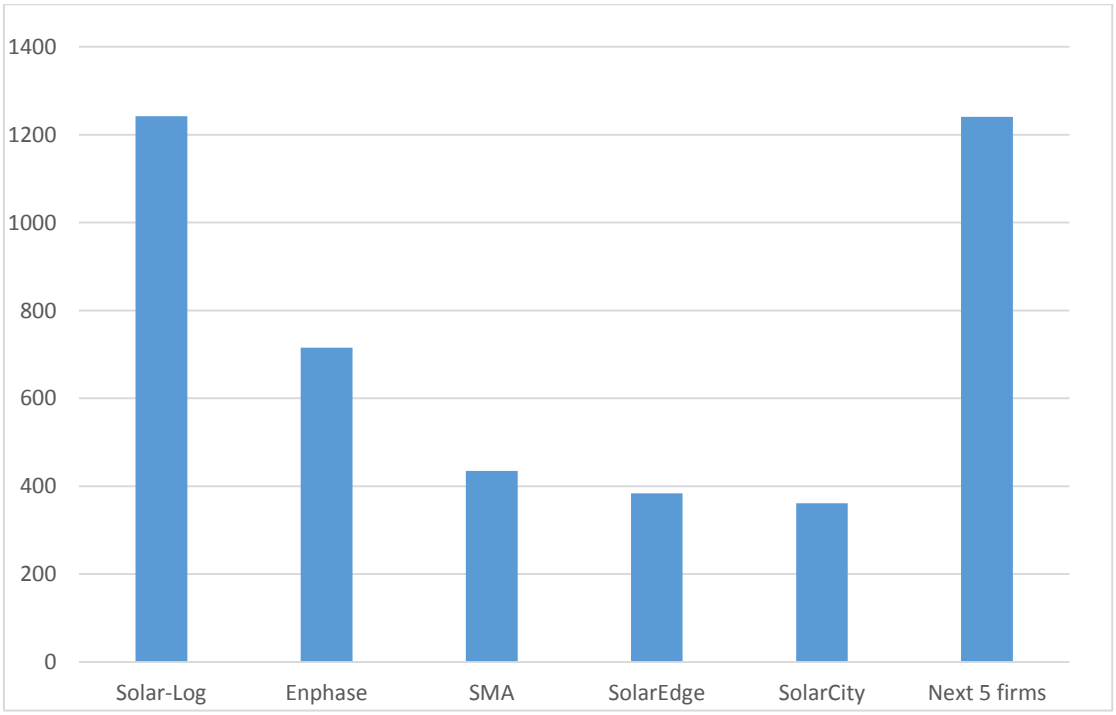
- rezidenčni – projekti do 20 kW,
- komercialni – projekti od 20 kW do 1 MW,
- industrijski – od 1 MW do 5 MW,
- komunalni ali distribucijski – nad 5 MW.

Na rezidenčnem trgu v Nemčiji in Italiji ima največji delež trga podjetje Solar-log (prikazano na Sliki 34), v domači Nemčiji kar tri četrtine. Sledi mu ameriški Enphase in nemški SMA, ki je tudi največji proizvajalec razsmernikov na svetu. Četrti je izraelski

SolarEdge in peti ameriški neodvisni ponudnik energetskih storitev SolarCity. Vsi ti ponudniki delujejo na področju fotovoltaike. Največji kitajski ponudnik je SolarMan, ki je v zadnjem času podvojil proizvodnjo sistemov za monitoring. Za monitoring in daljinsko vodenje in upravljanje postrojitve komercialne, industrijske ali distribucijske velikosti pa na trgu obstajajo različne rešitve in proizvajalci kot na primer:

- Asoenergy – SCADA in monitoring;
- Egauge Systems – monitoring, proizvodnja, poraba in dobava v javno omrežje;
- Enphase Energy – nadzor proizvodnje in hranilnika energije kompatibilno s komunikacijo z distribucijo;
- Locus Energy – dostop do podatkov o proizvodnji preko preglednic v programu Excel, enostavno za poročanje in izdelovanje poročil;
- Skytron Energy – prednost pri velikih podatkovnih zbirkah;
- Solar-Log – omogoča monitoring preko spletnega centralnega portala, GSM komunikacijo vseh naprav na lokacijah, manegeriranje naprav na daljavo, v povezavi s števcem tudi proizvodnjo in porabo in optimizacijo le te, priklop vremenske postaje;
- Sunverge Energy – optimizator PV energije v povezavi s hranilnikom energije;
- Trimark Associates – portalska rešitev za monitoring in daljinski nadzor PV postrojenj;
- Campbel Scientific – univerzalne rešitve za samostoječe vremenske postaje;
- Itron – celovita rešitev za solarne postroje vključujoč monitoring, upravljanje s sredstvi, napoved bodoče proizvodnje, primerna za vzdrževanje, upravljanje in nadzor.

Slika 34: Globalni rezidenčni monitoring po vodilnih podjetjih



Vir: M. Munsell, Who leads the Residential PV Monitoring Market?, 2016.

3 ANALIZA UPORABE VERIG BLOKOV IN PAMETNIH POGODB V ENERGETIKI

Analiza prednosti in slabosti ter priložnosti in nevarnosti (PSPN) se uporablja pri strateškem načrtovanju in odločitvah. Smiselnost vpeljave verig blokov v energetiko je gotovo potrebna strateškega razmisleka za posamezno podjetje ali celotno branžo. Zaradi tega smo izdelali PSPN analizo, da smo lažje razumeli vpliv tehnologij verig blokov na energetiko in obratno. V analizi najprej razmejimo prednosti/slabosti in nato še priložnosti/nevarnosti. Prva dva aspekta se nanašata na notranje dejavnike, druga dva na zunanje dejavnike. Na notranje dejavnike imamo vpliv mi, na zunanje pa nimamo direktnega vpliva. Zunanjim zahtevam se moramo prilagoditi, saj že beseda pove, da so zunanje, to pomeni izven našega dosega. Predvsem je pomembno, da smo pri zunanjih dejavnikih lahko hitro odzivni oz. prilagodljivi (Kos, 2010).

3.1 Vpeljava verig blokov v energetiko (analiza PSPN)

Na prvi pogled energetika in verige blokov izgledata ravno kontradiktorni. V energetiki je vse centralizirano, regulirano z lokalnimi mehanizmi nacionalnih ali regionalnih neodvisnih agencij, ki predpisujejo pravila tako na tehničnem kakor tudi komercialnem področju, verige blokov pa temeljijo na decentralizaciji.

V energetiki imamo tehnično gledano prenosni in distribucijski nivo. Nivo prenosnega omrežja se stika z drugimi državnimi prenosnimi omrežji. Nivo prenosnega omrežja se vodi iz enega ali več centrov, je vsekakor centraliziran in nič ni prepuščeno naključju ali komu izven ustanov, ki imajo za izvajanje dejavnosti posebno koncesijo, podeljeno s strani države. Na nivoju prenosnega omrežja sta tehnično zanesljivi del in komercialni del razmejena. V komercialni del spada meddržavno trgovanje z električno energijo, avkcijsko določanje cen prenosnih kapacitet, bilateralne pogodbe za nakup električne energije, katere sklepajo trgovci, porabniki ali proizvajalci ter trgovanje na borzi električne energije. Temu operaterji prenosnih omrežij dodajo še svoje regulacijske storitve, gre za sekundarno regulacijo, terciarno regulacijo, uravnavanje odstopanj in še kako drugo sistemsko storitev.

Posledica teh kompliciranih meddržavnih pogodb in regionalnih regulacij je, da je prenosni energetski nivo na državni in meddržavni ravni izredno kompliciran, nepregleden in vsekakor zelo drag za končnega uporabnika, ki mora na koncu plačati vse razkrite, skrite, optimalne in ne optimalne stroške. Predvsem se vidi odraz tega v razmerju med ceno električne energije in ostalimi dajatvami, ki jih države predpišejo po zakonu, določijo z raznimi pravilniki, uredbami itd. Pri rezidenčnih uporabnikih se te ostale dajatve vključno z DDV gibljejo od 60 % in več, glede na celoten strošek električne energije, ki se zaračuna končnemu odjemalcu, kar je samo po sebi postalo absurd.

Na distribucijskemu nivoju pa sistemski operater distribucijskega omrežja poskrbi, da se energija iz prenosnega omrežja prenese do končnega uporabnika. Tudi distribucijsko omrežje je bilo zasnovano zgolj za enosmerno razdeljevanje energije v smeri proti uporabnikom, zato je tudi centralno upravljano in zelo statično in nefleksibilno umeščeno v prostor.

Za razliko od energetike, tehnologije na osnovi verig blokov omogočajo transparentnost, ne potrebujejo posrednikov pri potrjevanju poslov, temveč potrjujejo posle drug drugemu, torej omogočajo točka točka poslovanje (Christidis & Devetsikiotis, 2016). Na prvi pogled verige blokov predstavljajo prijetno poenostavitev, kako pa jo resnično udejanjiti, pa je v okviru obstoječih regulativ resno vprašanje, nekateri bi rekli misija nemogoče, ali pač?
Vsekakor je potrebno tehnologije prilagoditi potrebam uporabnikov, ki so lahko rezidenčni, komercialni, industrijski ali še večji, saj so uporabniki osnovni element energetskega sistema in zanje je infrastruktura tudi zgrajena. Za uporabnike pa je bistveno, da so tehnologije, ki podpirajo energetiko uporabnikom prijazne, čim cenejše, fleksibilne in predvsem enostavne.

3.1.1 Prednosti

Prednost uporabe verig blokov v energetiki lahko najdemo na več področjih. Elektroenergetika je specifična v primeru hrambe električne energije za energetske potrebe, kar za enkrat še ni mogoče. To je razlog, da morata proizvodnja in poraba v vsakem trenutku biti enaki. Veriga blokov bi se lahko uporabila kot glavna knjiga elektroenergetike, v katero bi se sproti beležili in uravnavali proizvodnja in poraba. Tako bi lahko držali ravnovesje, hkrati bi oboje postalo popolnoma transparentno na vseh nivojih od proizvajalca do porabnika. Takšen vpogled v energetiko bi sam po sebi prinesel ogromne prihranke, saj se zaradi nejasnih in nejavnih sistemov izgubi tudi do 20 % energije na poti od proizvajalca do porabnika, kar ni skladno s projektiranimi izgubami, ki nastajajo na tranzitnih poteh.

Vpeljava verige blokov bi pripomogla tudi k bistveni poenostavitvi načrtovanja in napovedi proizvodnje in porabe električne energije. Trenutno tako imenovani vodje bilančnih skupin v energetiki dnevno za dan v naprej (včasih tudi do 5 dni vnaprej zaradi koncev tedna in praznikov) planirajo proizvodnjo in porabo za svojo skupino. Te podatke v posebnih formatih pošljejo zbirateljem bilančnih podatkov (v Sloveniji to delo opravlja podjetje Borzen). Ti zbrane podatke nato pošljejo sistemskemu operaterju, ki doda še svoje plane koriščenja sistemskih rezerv, zakupljene količine z avkcij čezmejnih pretokov moči in nekatere druge podatke in tako oblikuje nacionalni vozni red električne energije. Nato se vozni red uskladi še znotraj bloka regulacije (v našem primeru je to poleg Slovenije še Hrvaška in del BiH) in odpošlje v center v Švico ali Nemčijo. V celoten proces je vpletenih veliko ljudi, aplikacij, posebej v primeru napak (ko vsota vseh planov v voznem redu ni nič) pa tudi veliko usklajevanj in velika poraba časa.

Veriga blokov je tudi idealen instrument za trgovanje z električno in tudi drugo energijo. Borzni zapisi trgovanja v knjigo blokov bi lahko poenostavili trgovanje do te mere, da bi trgovanje na borzi lahko sprostili tudi za manjše porabnike, kar v sedanjem sistemu ni mogoče. Vključitev na trg električne energije bi lahko omogočili vsakomur, ki prodaja, kupuje ali preprodaja električno energijo na transparenten, enostaven in poceni način. Tako bi postala električna energija resnično tržno blago, kar bi znižalo končno ceno energije. Predvsem pa bi sredstva, s katerimi sedaj bogatijo trgovci, porazdelili med proizvajalce, skrbnike omrežij in porabnike. Te tri entitete so realne entitete v energetiki, ki opravljajo svoje storitve, da sektor funkcionira. Vse ostale storitve pa so v primeru uporabe knjige blokov nepotrebne in se jih lahko minimizira ali izloči. Ta transparenten, decentraliziran in cenovno optimiziran pristop bi omogočil boljšo porazdelitev dobrin med prebivalci in podjetji in tako zvišal konkurenčnost in pravičnost v družbi in s tem prispeval k večji blaginji vseh in varnosti na splošno.

Enostavna in transparentna uporaba verig blokov v energetiki bi imela veliko dodano vrednost tudi pri razumevanju in odzivanju končnih uporabnikov, rezidentov in podjetij za skrb za okolje. V primeru transparentne porabe, proizvodnje in cene, bi zemljani bolj začutili svoj osebni prispevek, ki ga lahko dajo, za ohranjanje našega planeta. Vsaka generacija je odgovorna tudi za bodoče rodove, kar se v našem času pozablja in ravna skrajno neodgovorno. Transparentnost v energetiki bi spodbudila in pokazala, da resnično vsak Zemljan lahko pripomore k ohranjanju planeta na način, da tudi sam prispeva k investicijam v obnovljive in čiste vire energije, da po nepotrebnem ne porablja energije in da ima od svojih trenutnih skrbnih dejanj tudi trenutne in dolgoročne koristi. Gre za možnost, da se ob transparentni politiki s pomočjo verige blokov, vzpostavi množično zbiranje sredstev za čisto energijo ali učinkovito rabo le te. Na tak način bi lahko posamezniki zbrali potrebni primanjkljaj za investicije, ki glede na napovedi še manjka, da bi obdržali naš planet pod v Parizu določeno maksimalno vrednostjo segrevanja (Johnson, Gogerty, & Zitoli, 2015). Ker manjka še ogromno sredstev, jih brez drastičnih ukrepov ne bo mogoče zbrati. Ena bistvenih možnosti takega ukrepa je, da se Zemljani samoorganizirajo in samo prispevajo k zmanjšanju emisij preko investicij v obnovljive vire. To bi bilo veliko lažje, če bi ljudje zaupali, da se bodo investicije upravljale, vodile in izplačevale preko javne infrastrukture, ki ne glede na barvo, politiko, raso ali drugo prepričanje z matematično natančnostjo skrbi za pravilnost podatkov in prenos podatkov in vrednosti.

Pogoj za zaupanje v takšne projekte je tudi prehod monitoringa v vseh njegovih razsežnostih in presežnostih na javno kriptografsko strukturo verige blokov. Na način, da veriga blokov in njena skupnost za vsako vas, mesto, državo, regijo, podeli pooblastilo nekomu, ki ima njeno zaupanje in skrbi za vhodno izhodne naprave ali števce, ki bi avtomatsko zapisovali podatke o porabi in proizvodnji v in iz javnega omrežja. Na tak način bi skupnost sama demokratično odločala o zaupanja vrednih zastopnikih, ki svoje zaupanje potrjujejo z izvajanjem nalog in skrbijo za pravilno delovanje tehničnih naprav,

ki bi povezovale električni svet z verigo blokov. Na ta način bi odpravili ogromno korupcijo, neekonomičnost javnih podjetij, ki izkoriščajo državno pridobljene koncesije, za interese nekaterih posameznikov in tako širijo nezaupanje in nepravičnost porazdelitve dobrin med ljudmi, hkrati pa zaradi svoje požrešnosti in grabežljivosti še ovirajo hiter prehod energetike na obnovljive vire energije.

Tudi plačila v energetiki bi se lahko avtomatizirala in izvedla s pomočjo tehnologij verig blokov. Za te potrebe obstaja že vsa infrastruktura, manjka pa le pripravljenost državnih politik, da bi omogočila in spodbudila uporabo digitalnih valut, deležev, obveznic ali drugih digitalnih sredstev kot normalen del ekonomije. S tem bi prispevali tudi k prenovi drugega zelo pomembnega področja, to je področja financ in z njimi rigidnega bančnega sistema, ki je zgubil zaupanje in se pokazal kot nedorasel in neprimeren za trenutek časa.
Prehod energetike na tehnologije verig blokov v tehničnem in ekonomskem pomenu, bi bil tako velik, da bi naredil tektonske premike na celem svetu, v energetiki in financah, s čemer bi se spremenila tudi strateška geopolitična slika sveta.

Velika prednost uporabe verig blokov v energetiki je, da je ta tehnologija zaradi svoje fleksibilnosti prenosljiva globalno, saj se digitalno sredstvo zapisano v verigo blokov lahko uporabi enostavneje, hitreje in bolj univerzalno, kakor trenutni tehnični in finančni mehanizmi.

3.1.2 Slabosti

Glavna slabost verig blokov je, da je uporaba za povprečnega uporabnika relativno zahtevna. Uvaja nov način razmišljanja, zahteva informacijske veščine in znanje ter razumevanje delovanja digitalnega sveta. Za potrebe v široki potrošnji bo potrebna še tehnološka poenostavitev in odprava teh slabosti.

Trenutna slabost verige blokov je tudi njena transparentnost, saj so transakcije javno dostopne. Zaradi strateškega pomena energetike so gotovo pomisleki, da bi bile te informacije javne in tako na voljo nepridipravom.

Velika količina podatkov zapisanih v obstoječe verige blokov bi pomenila njihovo ekstremno rast in neobvladovanje le teh, zato bi vsak uporabnik moral razpolagati z veliko količino statičnega spomina, kar pa v tem trenutku ni primerno.

3.1.3 Priložnosti

Vpeljava verig blokov v energetiko odpira veliko novih poslovnih priložnosti in storitev (Czepluch, Lollike & Malone, 2015). Poleg storitev, ki bi omogočale uporabnikom bolj neposredni stik in koristi od energetskih poslov, do enostavnejšega dostopa do podatkov za analitične in raziskovalne namene.

Storitev Odziv na povpraševanje (angl. *Demand Response*) bi bila lahko čudovito rešena s pomočjo verige blokov. Sprotno zapisovanje stanja ravnovesja sistema ali tako imenovane sekundarne regulacije, bi bila enostavno lahko identificirana iz same verige blokov in to v intervalih na 1 ali 5 minut. Zaradi velikega navora energije v energetskih sistemih, je najbrž 5 minutni interval dovolj dober odziv na stanje in bistveno izboljšan glede na sedanje stanje, kjer se uporablja 15 minutni ali urni interval.

Podobno kot se dela za rudarjenje in razporejanje moči hashov bi se s pomočjo verige blokov lahko avtomatsko z algoritemsko izbiro aktiviral bazen, ki bi lokacijsko in časovno določil, katere naprave se lahko vključijo v storitev,. Tako bi energetika dobila optimizirano, na verigi blokov temelječo sekundarno regulacijo, ki bi bistveno pocenila in izboljšala obstoječe rešitve. Omenjena rešitev bi doprinesla tudi k varnosti in stabilnosti delovanja energetskega sistema na mikro, regionalni, nacionalni, in kontinentalni ravni.

Verige blokov bi se lahko uporabile tudi za urno, 15 minutno, 5 minutno ali 1 minutno načrtovanje proizvodnje in porabe električne energije, saj je veriga blokov javno dostopna, odprta in hitra, poleg tega pa ima lastnost, da se podatkov zapisanih v verigo blokov, ne da spreminjati za nazaj (Lemieux 2016), kar jim daje konsistentnost in zaupanje.

Vsak uporabnik bi glede na svoje potrebe lahko predvidel porabo ali proizvodnjo za naslednje obdobje in to s svojimi priključnimi podatki zapisal v verigo blokov. Iz teh zapisov bi potem skrbniki bilančnih skupin, nacionalni izdelovalci voznih redov, blokovni ali regionalni izdelovalci voznih redov in generalni izdelovalec voznega reda za celotno skupino ENTSO-E avtomatsko pridobili podatke o planih za dan ali več dni vnaprej. Izdelovanje voznih redov bi lahko avtomatizirali za vsak mikro ali makro sistem in tako prihranili ogromno časa, energije in možnosti zlorab in izločili napake, ki pri tem nastajajo.

Uporaba verig blokov v energetiki bi zagotovo zelo pospešila prehod na obnovljive vire energije in učinkovito rabo le te, zato bi se potrebe po uporabi surove nafte, zemeljskega plina in premoga bistveno zmanjšale, s tem pa bi se sredstva, ki se namenjajo za nakup teh energentov, porazdelila med proizvajalce čiste energije, ki pa so praviloma ali v večini lokalni. Ta ukrep bi geostrateško prispeval tudi k svetovnemu miru, saj bi razbremenil boj za strateške lokacije in trgovske poti, predvsem za potrebe energetike. Na tak način bi planet Zemlja lažje preživela tudi demografsko večanje prebivalstva, tudi čez 10 milijard, če bodo prebivalci živeli med seboj bolj strpno in racionalno.

3.1.4 Nevarnosti

Pomanjkljivost uporabe verig blokov je, da verige blokov v splošni javni uporabi še niso dovolj uveljavljene. Če omenimo verigo blokov, večina ljudi sploh ne ve, kaj je to, ali pa pomisli na Bitcoin. Naslednja nevarnost je ta, da ljudje mislijo, da so verige blokov za

računalničarje in zato nevarne. Ker večina ljudi ne loči med Bitcoinom in med pomenom verige blokov, to smatra kot nekaj nevarnega, nestabilnega ali zahtevnega za uporabo.

Nevarnost uporabe verig blokov v energetiki je lahko tudi to, da se finančni sektor ustraši prevlade verig blokov in z njo povezanih javnih decentraliziranih infrastruktur, zato lahko preko državnih in zakonodajnih vzvodov zelo zavre ali prepove verige blokov na več nivojih ali pa jih zakonsko tako zakomplicira, da bodo postale neuporabne. Pričakujemo lahko tudi argument nekaterih v energetiki, da je energetika preveč pomembna, da bi podatke o delovanju lahko zaupali javni knjigi verigi blokov; čeravno ta argument gotovo nima tehnične osnove. Da si v energetiki ne želijo transparentnosti, sicer ne bomo direktno slišali, bo pa nasprotovanje gotovo utemeljeno z varnostjo in zanesljivostjo delovanja. Zaradi javne infrastrukture imajo ljudje občutek, da je le ta bolj izpostavljena hekerskim napadom, ki lahko onemogočijo posamezno storitev in tudi delovanje energetike. Nestanovitnost cene digitalnih valut je velika in to je za sektor, kot je energetika, lahko velika težava. Energetika je nizko donosna branža z velikim navorom sredstev v obtoku, zato sama po sebi zahteva ogromno stabilnost tudi v finančnem smislu.

Na Sliki 35 je analiza PSPN predstavljena še grafično. V njej so prikazane bistvene prednosti, slabosti, priložnosti in nevarnosti.

Slika 35: Vpeljava verig blokov v energetiko - analiza PSPN

3.2 Uporaba pametnih pogodb v energetiki (analiza PSPN)

Pogodbe poznamo že zelo dolgo, saj je pogodba v bistvu vsak dogovor med dvema stranema, kjer ena stran da ponudbo, druga stran pa to ponudbo sprejeme. Pogodbe so ustne, pisne ali oboje. Pogodbe pišemo z razlogom, da je bolj jasno, kakšen je bil dogovor, in da se tak dogovor skozi čas ne pozabi. Pod pogodbo se podpišemo, včasih je bilo v modi tudi žigosanje, vsekakor zabeležimo pogodbo na način, da je čim bolj nedvoumno, kaj, kdo in kdaj je bilo dogovorjeno.

Pogodbe so se skozi zgodovino pisale na različne materiale kot so kamen, glina, les, kovina in kasneje papir, ki še danes ostaja glavni fizični medij. Zaradi počasnosti prenosa pogodb po svetu, pa so pogodbe postale vse bolj digitalne. Pogodba je lahko popolnoma digitalna in nato podpisana z elektronskim podpisom. V primeru, da je pogodba oz. nosilni dokument pravilno kreiran in njemu pripet veljaven elektronski podpis, je taka pogodba tudi pravno formalno veljavna.

Smo v obdobju, v katerem se vse več aktivnosti avtomatizira in v katerem smo z Bitcoinom dobili tudi verige blokov, zato je pametna pogodba logično nadaljevanje klasičnih pogodb, ki se lahko avtomatizirajo, še več, se lahko izvajajo na decentraliziranem omrežju brez posredovanja tretje osebe, postanejo zaupanja vredne brez fizičnega ali elektronskega podpisa. Za obstoječo miselnost, prakso in način delovanja poslovanja so pametne pogodbe temelječe na verigi blokov prava mala revolucija, saj pametne pogodbe omogočajo nadgradnjo finančnih verižno bločnih protokolov.

Pametne pogodbe (angl. *Smart Contracts*) so v bistvu del programske kode (Heires, 2016) in ne klasične pogodbe, ki jih poznamo iz pravno obligacijskih razmerij, ki nadgrajujejo verigo blokov. Nadgradnja je v tem, da veriga blokov ni več zbirka transakcij, kot v Bitcoinu ali zbirka stanj denarnic, kot pri Ethereumu, temveč avtomatska implementacija pravil in pogojev večstranskih pogodb.

Pametne pogodbe se izvajajo na vozliščih, računalnikih, povezanih v verigo blokov na osnovi protokola, ki deluje na osnovi konsenza in ki izvede zaporedje ukazov v pogodbi, kodi sami. Rezultat je metoda, s katero se stranke ali strani dogovorijo o pravilih in pogojih in zaupajo, da se bo pogodba izvedla avtomatsko, kar zmanjšuje možne človeške napake ali manipulacije.

S pametno pogodbe se lahko stranke dogovorijo in izvedejo, da bodo proti plačilu dobile digitalna sredstva, žetone, delnice, deleže, valuto, obveznice ali kaj tretjega in to avtomatsko z nakazilom prenosa digitalne valute v namensko kreirano denarnico. Za izvedbo takega dogovora je dovolj le kratka koda pametne pogodbe, ki se izvrši na verigi blokov in se je ne da spreminjati za nazaj, popravljati ali ustaviti.

Kot drug primer uporabe pametne pogodbe je, da stranke z njo potrjujejo upravičenosti posojila za izvršitev sporazumov transfernih cen med odvisnimi družbami. Pametne pogodbe so lahko smiselne tudi v primeru ko se nekatere transakcije večkrat ponavljajo med istimi strankami. Stranke ročno obdelujejo pogodbe, pri čemer se podvajajo operacije v fazi potrjevanja, podpisovanja ali izvedbe. Veriga blokov pa v takih primerih deluje kot podatkovna zbirka v skupni rabi, ki zagotavlja varno, nedvoumno in avtomatsko potrjevanje pametnih pogodb, izračunov in drugih transakcijskih aktivnosti, ki zmanjšujejo možnosti napak in pospešijo delovanje.

Podjetja bi morala pogledati prednosti, slabosti priložnosti in nevarnosti pametnih pogodb in premisliti, kje se lahko le te uporabijo oz. doprinesejo k večji učinkovitosti ali novim poslovnim priložnostim. Podjetja bi lahko pogledala svoje poslovne procese in ugotavljala, kje bi bila vpeljava smiselna. (Ream, Chu & Schatsky, 2016)

3.2.1 Prednosti

Pametne pogodbe temelječe na verigi blokov lahko prinesejo veliko prednosti potencialnim aplikacijam. Te prednosti so gotovo v hitrosti izvedbe, saj se pametne pogodbe izvajajo avtomatsko za razliko od klasičnih pogodb, ki se pišejo in podpisujejo ročno.

Pametne pogodbe pripomorejo tudi k zmanjšanju človeških napak in morebitnih manipulacij, saj se izvajajo na nivoju verige blokov, decentralizirano in avtomatsko.

Takšen način sklepanja pogodb pripomore tudi k odpravi potrebe po prisotnosti, verifikaciji ali zaupanju tretjim osebam. Na tak način se izloči nepotrebne tretje osebe zaradi potrebe zaupanja, saj niso več potrebne, kajti zaupanje in verodostojnost daje veriga blokov.

Zaradi vseh naštetih poenostavitev, procesi temelječi na pametnih pogodbah prinašajo cenejše poslovanje, kar je bistvenega pomena za konkurenčnost na trgu.

3.2.2 Slabosti

Pametne pogodbe niso smiselne v kompliciranih medsebojnih dogovorih med strankami, ki jih je zelo težko vnesti nedvoumno v programsko kodo ali se izvajajo le enkrat ali redko.

Slabost pametnih pogodb je tudi, da so neberljive za »normalnega človeka« brez programerskega znanja, zato potrebujejo splošno verzijo ali razlago pogodbe, razumljivo za povprečnega človeka brez računalniškega predznanja.

Pametne pogodbe so omejene na delovanje znotraj verige blokov. Izvajajo se samo v verigi blokov, ne znajo direktno prejemati in pisati podatkov ali sprožiti funkcij izven verige blokov.

Slabost pametnih pogodb vidimo tudi v tem, da se te pogodbe, ko je naložena v verigo blokov, ne da več ustaviti ali spremeniti. To pomeni, da morajo biti 100 % pravilno napisane vnaprej. Takšna natančnost pisanja programske kode je možna za enostavne funkcije ali metode, kompleksne funkcije pa vedno vsebujejo napake in možnost zlorab.

3.2.3 Priložnosti

Glavne priložnosti pametnih pogodb vidimo v novih poslovnih modelih. Ker prinašajo boljše, hitrejše in kakovostnejše storitve brez potrebe interakcije tretje osebe, so zelo primerne za uporabo v novih poslovnih modelih, ki postanejo konkurenčni ali konkurenčnejši le na tak način.

Zaradi nižje cene pametne pogodbe odpirajo vrata, ki jih s klasičnimi pogodbami cenovno ne bi bilo možno odpreti. To so novi točka točka poslovni modeli, model trgovanja, dobave in proizvodnje električne energije, storitve Odziv na povpraševanje in druge, ki so možne na osnovi pametnih pogodb, saj tako odpade vrsta birokratskih, trgovskih in drugih posrednikov (Fairfield, 2014).

Poslovne modele povezani v smislu točka točka, ki direktno povezujejo proizvajalca in porabnika, ali ki direktno povezujejo prodajalca in kupca, zmanjšajo čas, stroške in vso potrebno pravno in informacijsko infrastrukturo, ki je povezana s tem.

Pametne pogodbe prinašajo tudi novitete v finančni sektor in ga spreminjajo. Do sedaj smo morali verjeti bankam in finančnim inštitucijam, sedaj pa jih v veliki meri lahko nadomestijo pametne pogodbe, ki temeljijo na konsenzu verig blokov in ne potrebujejo birokratskega aparata za sklepanje poslov.

Pametne pogodbe se lahko uporabijo tudi za nove načine upravljanja podjetij ali skupnosti, saj omogočajo tudi glasovanje na osnovi pravic z naslova digitalnih sredstev, deležev, delnic... Omogočajo decentralizirano upravljanje, odločanje ali glasovanje.

Pametne pogodbe prinašajo nov pogled tudi na informacijsko tehnologijo, saj omogočajo distribuirano procesiranje funkcij in virtualizirajo računalniški procesor na distribuiran način. Iz centralnega procesorja so naredile distribuiran operacijski sistem ali globalni verižno blokovni računalnik, ki je brez omejitev izvajanja funkcij.

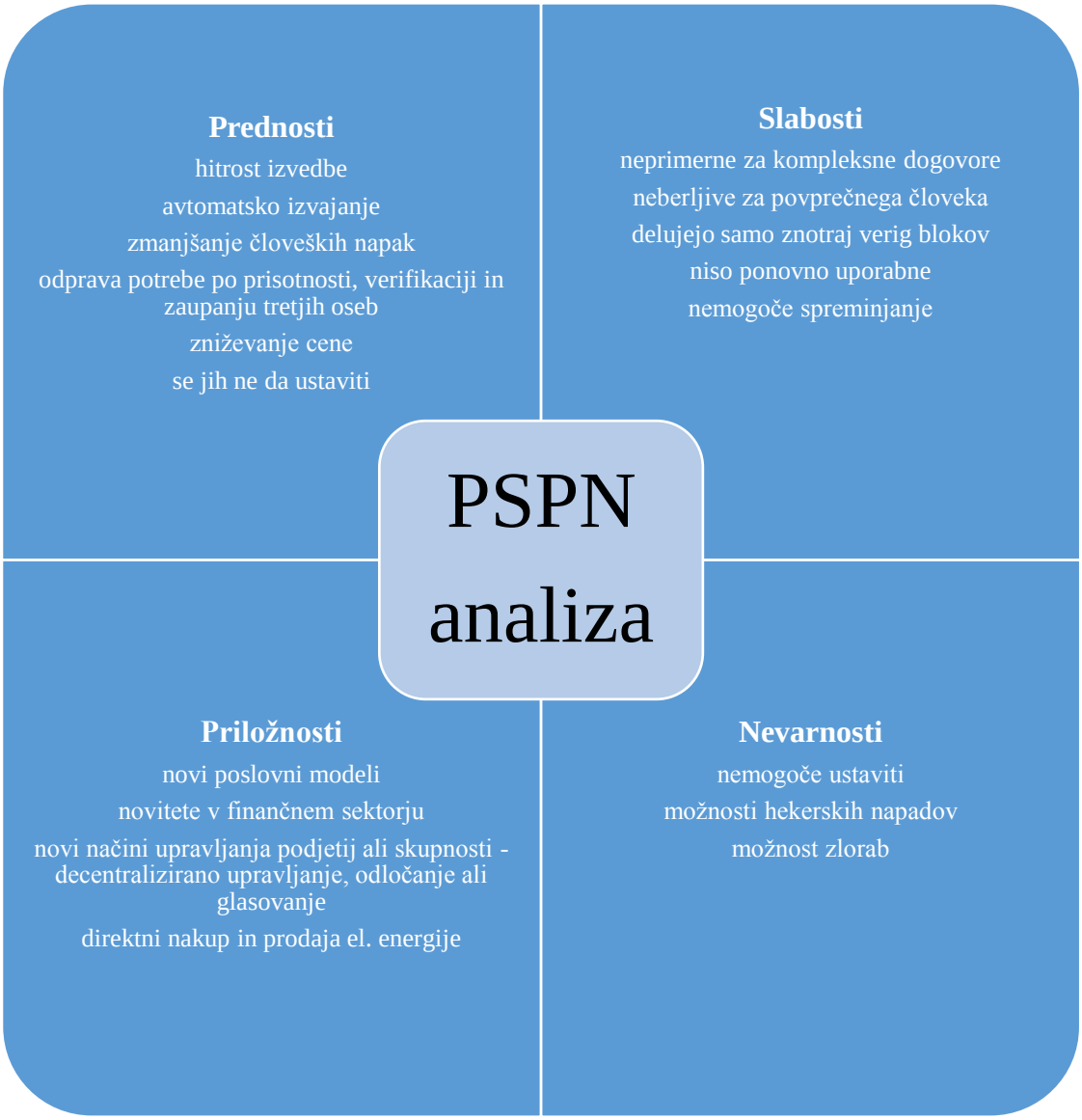
V energetiki je vidna priložnost predvsem na področju direktnega nakupa in prodaje električne energije po principu točka točka, kjer bodo končni kupci in prodajalci direktno

izvedli posle brez provizij, birokracije in tako še izboljšali ponudbo in povpraševanje na trgu in ga tako uravnali.

Prav tako v energetiki vidimo veliko možnost na področju storitev kot so Odziv na povpraševanje, kjer se spet lahko direktno povežeta ponudnik in prejemnik storitve na osnovi pametnih pogodb.

Hrambi energije, ki je osnova za storitev Odziv na povpraševanje in bistvena v električnem transportu, ki šele prihaja, bo zagotovo koristila storitev pametnih pogodb na osnovi verige blokov.

Slika 36: Uporaba pametnih pogodb v energetiki - analiza PSPN



Tudi financiranje projektov v energetiki ima veliko priložnost z uporabo pametnih pogodb, saj lahko na tak način zaobide bančni sektor in lobijsko povezane finančne in politične strukture, ki usmerjajo ali zavirajo določene projekte na področju obnovljivih virov energije in energetske učinkovitosti. Množično zbiranje financiranja za katero koli branžo, tudi energetiko, je izredno primerno, saj ga veriga blokov in pametne pogodbe naredijo dostopnega tudi majhnim vlagateljem, globalno in brez finančnih svetovalcev.

Tako vidimo takojšnjo možnost implementacije pametnih pogodb na energetskem področju: trgovanja, izvajanja plačil in poravnav, kreditiranja, dajanja garancij, dobave energije, financiranja, optimizacije itd. Pri tem bo potrebno pametne pogodbe nadgraditi vsaj z aplikacijami Oracle, ki povezujejo zunanji svet z verigo blokov ali pa z uporabo DSA, ki je v svoji osnovi že storitev, ki povezuje zunanji svet in svet verig blokov ali ponovno uporabo že vzpostavljenih storitev kjerkoli na internetu.

3.2.4 Nevarnosti

Nevarnost vidimo pri uporabi denarnic, ki vsebujejo večje količine sredstev, za izvajanje pametnih pogodb. Po našem mnenju je smiselno, da pametna pogodba izvede naloge, ki so bile dogovorjene in predpisane, ni pa to instrument hranjenja večje količine digitalnih sredstev na katerem koli segmentu. Pametna pogodba je namreč izvedena na osnovi programske kode, ki je ves čas dostopna na internetu in tako podvržena možnosti zlorab s strani nepridipravov, hekerjev ali druge zainteresirane skupine.

Na Sliki 36 je analiza PSPN predstavljena še grafično. V njej so prikazane bistvene prednosti, slabosti, priložnosti in nevarnosti.

4 POSLOVNE PRILOŽNOSTI UPORABE VERIG BLOKOV IN PAMETNIH POGODB V ENERGETIKI

4.1 Močnostne verige blokov

Energetika je strateška panoga vsake države in sveta kot celote, saj bo od nje odvisna dostopnost do vode, pridelava hrane, transport in funkcioniranje tega sveta. Vpeljava namenskih verig blokov za potrebe energetike je samo še vprašanje časa, saj lahko tako imenovane močnostne verige blokov združijo rudarjenje za potrebe delovanja verige blokov kakor tudi dejansko nastajanje energetskega digitalnega sredstva. Namenske vpeljave energetskih ali močnostnih verig blokov bodo potrebne predvsem zaradi zahtev energetike po bolj pogostem posredovanju podatkov v verigo blokov, količini podatkov in stroškov, ki se rudarjem plačujejo v primeru koncepta »Proof of Work«. Energetske verige blokov bodo verjetno kombinacija koncepta pred rudarjenja in delno rudarjenja, predvsem zaradi uravnavanja stroškov potrjevanja in določitve algoritma izračuna zahtevnosti za ta

namen. Prav tako bodo verjetno tudi kombinacija javnih in zasebnih verig blokov, saj nekatere podatke energetske družbe ne bodo želele ali smele razkrivat.

4.2 Pametne bilančne skupine

Velika priložnost za nove poslovne modele je združitev koncepta samooskrbe in verig blokov na osnovi pametnih pogodb. Ta združitev lahko kreira poslovni model Pametnih bilančnih skupin, ki na osnovi verige blokov in pametnih pogodb samozadostno uravnavajo potrebe svojih članov in skrbijo za proizvodnjo, porabo, odstopanja, plačila in plačilno poravnavo, garancije, depozite, kredite, solidarno odgovornost, odločanje in druge potrebne parametre, da so v ravnovesju in cenovno konkurenčni. Pametne bilančne skupine se lahko tvorijo na teritoriju enega sistemskega upravljavca. Pametne bilančne skupine se lahko s pametnimi pogodbami povezujejo tudi z drugimi bilančnimi skupinami in tako tvorijo širšo virtualno energetsko skupnost. Taka skupnost uporablja večinoma čiste vire energije, je konkurenčna obstoječim poslovnim modelom, je fleksibilna in hitrorastoča. V skupnost se enostavno vključujejo novi člani. Skupnost je višji nivo povezovanja, ki ga določajo državne energetske norme, zakoni in pravila in je predpogoj za popolno neodvisnost državljanov od državnih energetskih infrastruktur. Pogoj za tako neodvisnost je cenovno dostopno hranjenje energije. Baterijski hranilniki in konverzija »Power to Gas«, ki je lahko najhitreje uporabljena glede na trenutno tehnološko stanje infrastrukturo, se hitro razvijajo in bodo v perspektivi 4 do 10 let popolnoma konkurenčni. Takrat bo lahko pametna bilančna skupina kot samostojna neformalna skupnost proizvajalcev, porabnikov, hranilnikov in pretvornikov energije postala ena samozadostna in konkurenčna celota, ki bo priklop na obstoječo elektroenergetsko infrastrukturo koristila le še kot rezervo (angl. *Backup*) za svoje neprekinjeno poslovanje.

4.3 Pametno blok trgovanje

Trenutno trgovanje v elektroenergetiki sloni na urnih produktih. Trguje se vsaj za dan v naprej, lahko tudi za več dni v naprej. Trguje se lahko na sprotnem ali avkcijskem trgu. Trguje se tudi z izvedenimi finančnimi instrumenti v energetiki. Poleg trgovanja z energijo, pa se v energetiki pojavljajo prostori trgovanja tudi s prenosnimi kapacitetami. Prenosne kapacitete se po navadi ponujajo na avkcijah, s posamezno mejno prenosno pot in njeno smer. Avkcije se izvajajo za daljše časovno obdobje. Zaradi razhajanj med napovedmi proizvodnje in porabe energije za vnaprej, vedno pride do odstopanj, katere strošek se spet deli med deležnike, ki so ta odstopanja povzročili.

Z uvedbo pametnega blok trgovanja, le to lahko poteka sproti. Gre za sprotno trgovanje in izvedbo plačil med deležniki na trgu. Za izvedbo takšnega dejanskega trgovanja je potrebna nadgradnja informacijske energetske infrastrukture oz. prehod na verigo blokov. Nujna je tudi uvedba digitalne valute za izvedbo finančnih poravnav, ki se dogajajo sproti s trgovanjem.

Smiselna je uvedba sistema decentralizirane borze s centraliziranim trgovalnim mehanizmom. Pri decentraliziranih sistemih deležnikom pri trgovanju ni potrebno finančnih sredstev prenašati na tretjo osebo, temveč jih hranijo v svoji digitalni denarnici ves čas. Na tak način je zagotovljena varnost sredstev, saj le ta niso izpostavljena tretji osebi in zato ni potrebno dodatno zaupanje med vsemi deležniki. Decentraliziran sistem trgovanja je z vidika zaupanja bistveno boljši od klasičnih centraliziranih, kar poznamo sedaj v finančni in energetski industriji, pa tudi v digitalni industriji verig blokov.
Decentraliziran sistem ima tudi slabosti, saj ni toliko učinkovit kot centraliziran, ker težko sprejema hitre in nedvoumne odločitve. Predvsem gre za mehanizem trgovanja, ki mora biti za vsak primer izbran skrbno in smiselno s potrebami deležnikov na trgu. Gre v bistvu za različne mehanizme trgovanja kot je na primer trgovanje za energijo, trgovanje za kapacitete, trgovanje s storitvami Odziv na povpraševanje, trgovanje s storitvami hranjenja energije in še katerimi drugimi.

Primerno rešitev vidimo pot, da združimo prednosti decentraliziranega in centraliziranega sistema v en sistem. Ta je centralizirano upravljan le na področju kreiranja storitev trgovanja in pri izgradnji algoritmov trgovanja, samo trgovanje pa se izvede na decentralizirani energetski borzi kot sprotno ali avkcijsko trgovanje. Vsi udeleženci na borzi nastopajo avtomatsko po principu točka točka.

4.4 Pametni blok števec

Pametni blok števec (angl. *Smart Power Meter*) bo z vpeljavo energetskih verig blokov eden od stebrov delovanja elektroenergetskih sistemov, temelječih na osnovi verig blokov in pametnih pogodb. Specifika pametnega blok števca je v tem, da zna beležiti in zapisovati podatke iz energetskih naprav in sistemov v verigo blokov in tako omogočiti avtomatsko obravnavo vnesenih parametrov za potrebe drugih storitev. Pametni blok meter bo upravljal pooblaščenec Pametne bilančne skupine, ki ga člani skupine pooblastijo in plačajo za skrb pravilnega in korektnega beleženja delovanja energetskih sistemov in posredovanja teh podatkov v verigo blokov.

Pooblastila in izbira pooblaščenca se tudi izvede s pomočjo pametnih pogodb znotraj bilančne skupine. V primeru, da gre za večje bilančne skupine, ki teritorialno pokrivajo večje področje, pa se lahko pooblasti tudi več pooblaščencev, da sprotno opravijo svoje delo. Pooblaščenci lahko svoje pooblastilo tudi izgubijo, če delo ni opravljeno profesionalno, korektno in prijazno do strank.

Pametni blok števec bo zapisoval električne veličine in skupke le teh v verigo blokov skupaj s podatki o članu, lokaciji in drugimi potrebnimi informacijami, kar bo osnova za optimizacijo in obračun znotraj pametne bilančne skupine ali na drugačen način priklopljene naprave ali sistema na verigo blokov.

4.5 Odziv na povpraševanje v medsebojno povezanih omrežjih

Odziv na povpraševanje (angl. *Demand Response*) je odlična storitev, ki s pomočjo verig blokov in pametnih pogodb, lahko konkurenčno in kompetentno zaživi in rešuje veliko energetskih problemov pretakanja, pomanjkanja ali presežkov električne energije znotraj bilančnih skupin, mikro omrežij ali širših omrežij oz. sistemov le-teh. Ker je bila do sedaj v vseh državah storitev pogojena s pravno regulacijo, v večini držav te storitve ne morejo ponujati rezidenčni uporabniki, manjše skupine uporabnikov ali drugi zainteresirani uporabniki, čeprav imajo za to tehnične možnosti. S pomočjo pametnih bilančnih skupin pa se taka storitev lahko uporablja najprej na navideznem nivoju. V državah, kot so Švica, Nemčija in Avstrija, pa se lahko že sedaj storitev, Odziv na povpraševanje, razvije v zagotavljanje sistemske storitve za upravljavce prenosnega omrežja (angl. *Transmission System Operators, TSOs*), ki jo praviloma kupujejo od več energetskih sistemov, proizvajalcev ali trgovcev.

Storitev Odziv na povpraševanje temelji večinoma na osnovi pametnih pogodb, ki uravnavajo ponudbo storitve, izbirajo primerne energetske uporabnike za zagotavljanje storitve, proizvajalce glede na interne parametre in medsebojne pametne dogovore, vklopijo in izklopijo uporabnike, izvajajo plačila z uporabo digitalnih valut itd. Storitev Odziv na povpraševanje je optimalna tako za implementacijo verig blokov in pametnih pogodb, kakor za energetsko optimizacijo, brez enormnih stroškov manageriranja, upravljanja, poračunavanja, papirologije in birokracije. Poleg tega pa storitev na osnovi verig blokov prinaša koristi članom, saj se stroške poračunavajo na dnevni ravni avtomatizirano preko verig blokov. Administracija v tem primeru ni potrebna, saj se preko pametnih blok števcev storitve izvajajo same po sebi in po v naprej določenem korektnem postopku. Plačilo storitev je pavšalno glede na sredstva, ki jih je vsak član pripravljen deliti z drugimi, kot v primeru delovanja v skupnih bazenih rudarjenja.

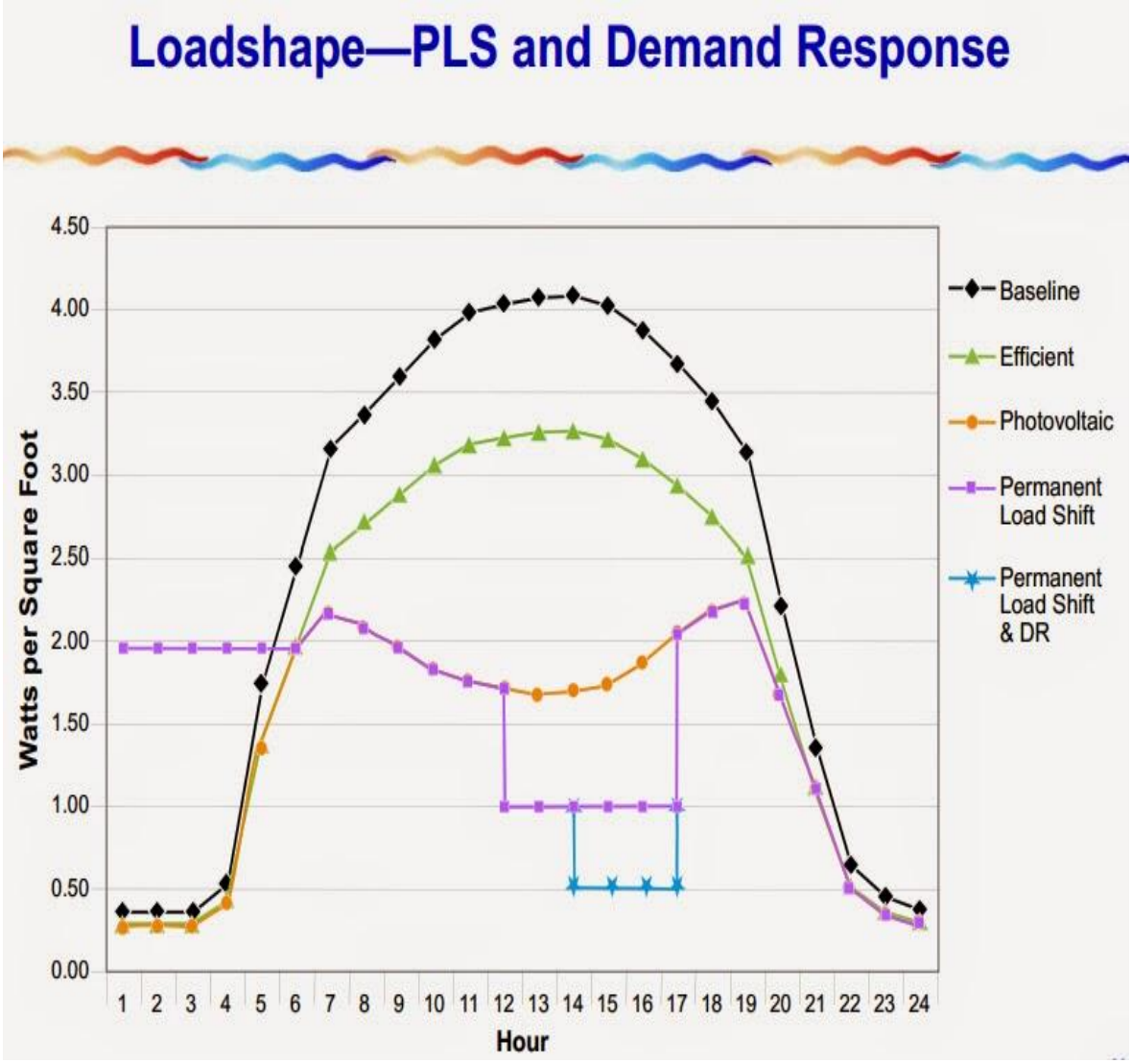
4.6 Razpoložljivost storitve

Razpoložljivost storitve je sistemska storitev znotraj pametne bilančne skupine in zagotavlja optimizacijo oz. ravnovesje med dobavo oz. proizvodnjo in porabo. Za to storitev, se določi tipičen parameter MWh/h, ki je osnova za izračun, poračun in porabo energije znotraj storitve. Razpoložljivost, ki je na voljo za koriščenje znotraj dogovorjenega bazena članov, mora biti določena v verigi blokov s pomočjo razpoložljivega parametra. Veriga blokov s pomočjo pametne pogodbe izbira primere proste razpoložljive kapacitete na dovoljeni lokaciji in jih uporablja dovoljen čas.

Algoritem v verigi blokov tudi računa porazdelitev uporabe razpoložljivih storitev in na osnovi zgodovinskih podatkov, kot je na primer prikazano na Sliki 37, in vnesenih potreb po storitvi, za vsak blok posebej izračunava oz. optimizira njeno enakomerno porazdelitev med člani ponudniki storitve. Sistem deluje kot pri rudarjenju digitalnih valut v skupnih

bazenih, kjer se izračuna skupen doprinos vsakega člana glede na moč heshov, ki jih vsak naredi in se pridobljena nagrada enakomerno porazdeli med vse rudarje v istem bazenu.

Slika 37: Krivulja obremenitve in razpoložljivosti storitve



Vir: Neuralenergy, Loadshape PLS and Demand Response, 2016.

4.7 Uporaba verig blokov za transparentno in decentralizirano financiranje za obnovljive vire in učinkovito rabo energije

Možnost investiranja, financiranja ali posojanja sredstev globalno, decentralizirano in z možnostjo odločanja o projektih, kamor se sredstva namenijo, se lahko realizira s pomočjo Pametnega množičnega zbiranja sredstev. Globalne verige blokov že sedaj omogočajo, da se sredstva za investicije v projekte, razvoj, financiranje kapitala, kredite, itd. zbirajo brez posebnih dovoljenj, lahko v manjših vrednostih, na krajši ali daljši rok in z zanemarljivimi stroški transakcij. Govorimo o Finance 2.0, ki se bodo s pomočjo verig blokov gotovo

spremenile v samem svojem bistvu. Če govorimo o podpori projektom za obnovljive vire, za to že obstajajo platforme za množično financiranje s fiat valuto. Vlaganje v projekte pa je klasično in omejeno na vpogled investitorja. Predvsem pa se plačila in vračanja denarja po navadi zgodijo enkrat letno, vmes pa ni podatkov, kaj se dogaja s projekti.

Z uporabo Množičnega zbiranja 2.0, ki temelji na verigi blokov in pametnih pogodbah, pa se interakcija med investitorjem, financerjem in projektom dogaja na dnevni, lahko tudi urni ali minutni osnovi. Investitor ima vpogled v delovanje projekta, vidi tehnične podatke, vidi njegova dnevna izplačila in se lažje odloča, v kateri projekt bo namenil svoja sredstva. Poleg tega digitalna sredstva, kot so deleži, ki jih investitor pridobi pri investiciji, lahko likvidno proda na borzi digitalnih valut brez stroškov za odpiranje računov, najemanja borznih hiš ali kaj podobnega. S pomočjo pametnih pogodb namreč vsak projekt ali skupina projektov že pri nakupu deležev izda digitalno sredstvo, ki kotira na digitalni borzi in je zamenljivo za drugo digitalno valuto ali fiat valuto. Tako investiran denar postane takoj likviden, kar je velika prednost pred klasičnimi investicijskimi modeli.

SKLEP

Pri odgovoru na temeljno vprašanje, ali obstajajo poslovne priložnosti uporabe verig blokov in pametnih pogodb v energetiki, smo prišli do pomembnih spoznaj, ki potrjujejo našo domnevo, da nove kriptografske tehnologije verig blokov in nadgradnje le teh s pametnimi pogodbami odpirajo popolnoma nov horizon z mnogo novimi priložnostmi tudi za energetiko.

Ugotovili smo, da smo v nalogi soočili več področij in morali multi disciplinarno presojati energetske potrebe posameznika skozi prizmo možnosti, ki jo ponuja informatika in hiter razvoj znotraj le-te, in finančne in okoljske koristi, ki jih ima posamezni porabnik energetskih storitev. Pri tem se nismo omejili samo na kratkoročne tehnične ali finančne koristi, temveč smo imeli v mislih tudi naš planet kot celoto, ki prav na energetskem področju nujno potrebuje spremembe. Zmanjšanje izpustov toplogrednih plinov, kjer energetika prispeva levji delež, nakazuje alternativno smer uporabe obnovljivih virov energije, da bodo tudi bodoči rodovi lahko koristili Zemljino gostoljubnost.

Naše ugotovitve kažejo, da nove informacijske tehnologije, temelječe na verigah blokov in pametnih pogodbah, ponujajo energetiki odprta vrata izboljšav in novitet na več področjih. Ugotovili smo, da je uvedba verig blokov smiselna tam, kjer se nekatere storitve velikokrat ponavljajo in so enostavno dogovorljive.

Prvo področje je trgovanje z električno energijo, kjer se s pomočjo pametnih pogodb in verig blokov, le to da v večini avtomatizirati, tako v tehnično nadzornem kakor tudi finančnem smislu. Veriga blokov, ki zagotavlja nedvoumnost, transparentnost in se je ne da spreminjati za nazaj, lahko zagotovi, da se ponudnik in porabnik energije pogodbeno

dogovorita brez posrednika in tako uskladita ceno in birokratski postopek, pri čemer je tretja stran, ki potrjuje transakcije, kar veriga blokov.

Kot nadgradnjo trgovanja smo videli priložnost participacije posameznih porabnikov energetskih storitev tudi pri omogočanju Razpoložljivosti storitve vsem uporabnikom. Ta storitev bo vse bolj pomembna za operaterje prenosnih omrežij, saj povečan delež obnovljivih virov energije povečuje tudi energetska nihanja energetskega sistema. Uporaba verige blokov in preko nje optimizacija porabe in proizvodnje, omogočanje participacije vseh uporabnikov pri tej storitvi, pa prinaša korenite spremembe v energetskem sektorju. To je preskok v miselnosti, ki iz Pametnih omrežij naredi Pametno energetiko, ki bo lahko s pomočjo verig blokov na najcenejši in končnemu uporabniku dostopen način omogočila optimizacijo pretokov moči in delovanje energetskega sistema. V analizi smo ugotovili, da ima storitev Razpoložljivost storitve prav vse elemente primernosti za prehod na verigo blokov.

Ekonomika v energetiki je tudi področje, ki se mu je treba posvetiti. Boljša ekonomska učinkovitost temelji na boljši organiziranosti in transparentnosti vrednosti skozi verigo posrednikov od proizvajalca do porabnika. V energetiki je dodana vrednost proizvajalca skoraj nič, končna cena energije pa je nesorazmerno visoka glede na delež proizvodnih stroškov. Temu botruje kompliciran birokratski aparat, ki upravlja z nepregledno množico regulativ in inštitucij in splošna nepreglednost dodane vrednoti v procesu. Z uporabo tehnologij verig blokov v sistem lahko vnesemo visoko mero transparentnosti in izločimo posrednike, inštitucije nadzora, finančne posrednike itd., torej energetsko storitev lahko naredimo transparentno in cenejšo za končnega uporabnika, kar doprinese tudi k splošni blaginji vseh prebivalcev planeta.

Z vključitvijo posameznikov v energetske projekte veriga blokov in na njej temelječe rešitve prinašajo tudi posredne učinke pripadnosti in možnosti spreminjanja sveta. Prav sončna energija je skozi tehnologije fotovoltaike namreč pokazala, da v energetiko lahko vlagajo vsi udeleženci branže, to je vsi uporabniki energije, in to v aktivnem smislu investicij v proizvodne vire in ne samo pri učinkoviti rabi. Občutek pripadnosti in možnosti, ki jih sončna in vetrna energija, kot najbolj perspektivni in konkurenčni obnovljivi viri energije v naslednjih desetletjih, dajeta vsakemu posamezniku zavest, da tudi sam lahko nekaj prispeva k ohranjanju tega planeta in hkrati še prihrani, kar je pomemben in morebiti rešilen trenutek, da se bodo investicije v obnovljive vire povečale do te mere, da se segrevanje ozračja na planetu ne bo povečalo več kot za 2 stopinji Celzija. Ugotovili smo, da so vse trenutne napovedi investicij do leta 2040, konzervativne ali ambiciozne, vsekakor premalo ambiciozne, da bi planet obvarovali katastrofalnega povečanja temperatur in s tem povezanih radikalnih sprememb življenjskih pogojev na Zemlji. Prav vključitev vsakega posameznika v skupen energetski projekt daje upanje in možnosti, da uspemo v tej bitki s časom.

Za uspeh pa so potrebne tudi zadostne finančne možnosti. Tudi na tem področju ima tehnologija verig blokov s pametnimi pogodbami možnost, da prenovi finančni sektor in tako omogoči točka točka poslovne modele na področju energetike in financ, ki bodo odprli možnosti globalnega množičnega investiranja in financiranja v obnovljive vire energije. Veriga blokov in na njej temelječe storitve omogočajo decentralizano, avtonomno upravljanje sredstev, storitev ali organizacij, omogočajo decentralizirane borze, decentralizirano odločanje ali vodenje podjetij, investiranje itd. Tehnologije omogočajo, da se zaradi izjemno nizkih stroškov transakcij in hitrosti le teh energetski uporabniki med seboj direktno povežejo tudi pri naložbah v energetske projekte kjerkoli na svetu.

V nalogi smo ugotovili, da je bilo temeljno vprašanje zastavljeno pravilno in da smo dobili nanj zelo jasen odgovor, ki ni samo pritrdilen, ampak pokaže na nujnost uporabe verig blokov in pametnih pogodb v energetiki, v informatiki in financah. Namreč vsa tri področja dajejo posameznikom ali podjetjem tisto celoto, s katero lahko naredimo svet in življenje na njem kakovostnejše, bolj varno, transparentno in tudi boj pravično. Verige blokov namreč omogočajo prenos informacij, sredstev, denarja ali odločitev direktno med uporabniki in tako izločajo nepotrebne posrednike v tem procesu, zaradi česar proces izboljšajo, pospešijo, pocenijo in naredijo bolj pravičen, saj bistvena dodana vrednost ostane pri tistemu, ki jo direktno ustvarja in ne zgolj pri posrednikih.

LITERATURA IN VIRI

1. *Altcoin*. Najdeno 25. julija 2016 na spletnem naslovu http://altcoins.com/
2. Andersen, C. B. K., & Bjornskov, C. (2016). *The potential and future of the cryptocurrencies market* (magistrsko delo). Aarhus: Aarhus University, Business and Social Sciences Department of Economics and Business.
3. Aron, J. (2015). Automatic world. *New Scientist*, *227*(3038), 18-19.
4. Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). *Blockchain–the Gateway to Trust-free Cryptographic Transactions*. Istanbul: ECIS.
5. Becker, G. (2008). Merkle signature schemes, merkle trees and their cryptanalysis. Najdeno 25. julija 2016 na spletnem naslovu http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf
6. Birch, D. G. W. (2015). What Does Cryptocurrency Mean for the New Economy? V Chuen, D. L. K. (ur.), *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data* (str. 505-517). London: Academic Press.
7. *Bitcoin*. Najdeno 25. julija 2016 na spletnem naslovu https://bitcoin.org/
8. *Bitcoin difficulty*. Najdeno 25. julija 2016 na spletnem naslovu http://bitcoin-difficulty.com/
9. Bitcoin help. (2014). *Bitcoin price chart with historc events*. Najdeno 25. julija 2016 na spletnem naslovu https://bitcoinhelp.net/know/more/price-chart-history
10. *Bitcoinblockhalf*. Najdeno 25. junija 2016 na spletnem naslovu http://www.bitcoinblockhalf.com/
11. *Bitshares*. Najdeno 19. avgusta 2016 na spletnem naslovu https://bitshares.org
12. *Bitstamp.* Najdeno 25. julija 2016 na spletnem naslovu https://www.bitstamp.net/
13. Bitstamp. (b.l.). *Bitstamp to become first nationally licensed bitcoin exchange and launches BTC/EUR trading.* Najdeno 25. julija 2016 na spletnem naslovu https://www.bitstamp.net/article/bitstamp-first-nationally-licensed-btc-exchange/
14. Block. (b.l.). *Block Parsers: How to Read the Bitcoin Block Chain*. Najdeno 25. julija 2016 na spletnem naslovu https://www.cryptocoinsnews.com/block-parser-how-read-bitcoin-block-chain/
15. *Blockchain.* Najdeno 20. avgusta 2016 na spletnem naslovu https://blockchain.info/
16. Bloomberg New Energy Finance. (2016). *New Energy Outlook 2016.* Najdeno 20. junija 2016 na spletnem naslovu http://about.bnef.com/video/new-energy-outlook-2016-watch-the-story-unfold
17. Buterin, V. (2013). *A next-generation smart contract and decentralized application platform* (white paper). Najdeno 20. avgusta 2016 na spletnem naslovu https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
18. Carel. (b.l.). *Difference between monitoring, remote management and supervision*. Najdeno 31. julija 2016 na spletnem naslovu http://www.carel.com/what-is-the-difference-between-monitoring-remote-management-and-supervision-

19. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Jurnals and Magazines*, *4*, 2292-2303.
20. Coinmarketcap. (b.l.a). *Total Market Capitalization*. Najdeno 27. julija 2016 na spletnem naslovu https://coinmarketcap.com/charts/
21. Coinmarketcap. (b.l.b). *Bitcoin Percentage of Total Market Capitalization*. Najdeno 27. julija 2016 na spletnem naslovu https://coinmarketcap.com/charts/
22. Coinmarketcap. (b.l.c). *Crypto-Currency Market Capitalizations*. Najdeno 27. julija 2016 na spletnem naslovu https://coinmarketcap.com/
23. Cointelegraph. (b.l.). *What are crptocurrencie*s. Najdeno 25. julija 2016 na spletnem naslovu https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies
24. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A. & Gün, E. (2016). On scaling decentralized blockchains (A Position Paper). V *Proc. 3rd Workshop on Bitcoin and Blockchain Research.*
25. CyptoBond. (2016, 29. februar). *Why is Ethereum different to Bitcoin?* Najdeno 25. julija 2016 na spletnem naslovu https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin/
26. Czepluch, J. S., Lollike, N. Z., & Malone, S. O. (2015). *The Use of Block Chain Technology in Different Application Domains* (diplomsko delo). Copenhagen: IT University.
27. de Klerk, D.M. & Lehtinen, S. (2016). *HEAT Ledger White Paper*. Najdeno 20. avgusta 2016 na spletnem naslovu http://heatledger.fi/HEATWhitepaper.pdf
28. Decker, C., & Wattenhofer, R. (2014). Bitcoin transaction malleability and MtGox. V *European Symposium on Research in Computer Security* (str. 313-326). Zurich: Springer International Publishing.
29. Derganc, B. (2007). *Bodoče delovanje slovenskega EES v interkonekciji UCTE: napoved osnovnih trendov, značilnosti in obratovalnih problemov za obdobje od 2007 do 2030.* Čatež: 8. Konferenca slovenskih elektroenergetikov. Najdeno 16. julija 2016 na spletnem naslovu http://www.cigre-cired.si/Images/files/documents/8_konferenca_Catez_2007/2007-CIGREC2-10.pdf
30. Difficulty. (b.l.). *What is Bitcoin Mining Difficulty*. Najdeno 5. avgusta 2016 na spletnem naslovu https://www.bitcoinmining.com/what-is-bitcoin-mining-difficulty/
31. Eles. (b.l.). *Prenosno omrežje v Sloveniji*. Najdeno 25. julija 2016 na spletnem naslovu http://www.eles.si/
32. ENTSOE. (b.l.). *ENTSO-e Transmission System Map*. Najdeno 25. julija 2016 na spletnem naslovu https://www.entsoe.eu/map/Pages/default.aspx
33. Etherscan. (b.l.). *Ethereum mining calculator*. Najdeno 25. julija 2016 na spletnem naslovu https://etherscan.io/ether-mining-calculator
34. Ethdocs. (b.l.). *What is Ethereum?* Najdeno 25. julija 2016 na spletnem naslovu http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

35. Evropska komisija. (2015). *Zgodovinski podnebni dogovor v Parizu: Evropska unija na čelu svetovnih prizadevanj*. Evropska komisija – sporočilo za medije. Najdeno 25. julija 2016 na spletnem naslovu http://europa.eu/rapid/press-release_IP-15-6308_sl.pdf
36. Fairfield, J. (2014). Smart contracts, Bitcoin bots, and consumer protection. *Wash. & Lee L. Rev. Online*, *71*, 35-299.
37. Garrod, J. Z. (2016). The Real World of the Decentralized Autonomous Society. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *14*(1), 62-77.
38. Github. (b.l.). *Mining.* Najdeno 25. julija 2016 na spletnem naslovu https://github.com/ethereum/wiki/wiki/Mining
39. *HEAT Ledger*. Najdeno 20. avgusta 2016 na spletnem naslovu http://heatledger.fi
40. Heires, K. (2016). The Risks and Rewards of Blockchain Technology. *Risk Management*, *63*(2), 4.
41. Higgins, S. (2015, 5. januar). *Bitstamp claims $5 million lost in hot wallet hack.* Najdeno 25. julija na spletnem naslovu http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/
42. Hrovatin, J. (2008). Izbrane značilnosti slovenskega elektrogospodarstva. *Elektrotehniški vestnik 75*(1): 7-11. Najdeno 17. avgusta na spletnem naslovu http://ev.fe.uni-lj.si/1-2-2008/Hrovatin.pdf
43. Hrovatin, J. (2009). *Vodenje elektroenergetskih sistemov*. Najdeno 20. avgust 2016 na spletnem naslovu http://www.impletum.zavod-irc.si/docs/Skriti_dokumenti/Vodenje_elektroenergetskih_sistemov-_Hrovatin_NU.pdf
44. *Jaxx.* Najdeno 20. avgusta 2016 na spletnem naslovu https://jaxx.io/
45. Johnson, L. P., Gogerty, N. & Zitoli, J. (2015). *Connecting the Blockchain to the Sun to Save the Planet*. Najdeno 29. julija 2016 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2702639
46. Karldiab. (b.l.). *Ethereim Mining Calculator.* Najdeno 21. avgusta 2016 na spletnem naslovu http://karldiab.com/EthereumMiningCalculator/
47. Kaye, R. (2000). *Infinite versions of minesweeper are Turing-complete* (Manuscript). Birmingham: University of Birmingham.
48. Khaliq, A. (b.l.). 10 *Exchanges to buy and sell Bitcoins*. Najdeno 25. julija 2016 na spletnem naslovu http://www.hongkiat.com/blog/exchanges-buy-sell-bitcoins/
49. Komisija Evropskih skupnosti (2006). *Zelena knjiga - Evropska strategija za trajnostno,konkurenčno in varno energijo*. Bruselj: Komisija evropskih skupnosti, 2006. Najdeno 12. julija 2016 na spletnem naslovu http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0105:FIN:SL:PDF
50. Korošec, P. (2016). *Varnost in anonimnost pri plačevanju s spletno valuto Bitcoin* (doktorska disertacija). Ljubljana: Ekonomska fakulteta.
51. Kos, B. (2010). *SWOT analiza.* Najdeno 25. julija 2016 na spletnem naslovu http://www.blazkos.com/swot-analiza.php

52. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2015). *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. Cryptology ePrint Archive, Report 2015/675, 2015.
53. Künnapas, K. (2016). From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?. *The Future of Law and eTechnologies*, 111-131.
54. Lemieux, V. L. (2016). Trusting Records: Is Blockchain Technology the Answer? *Records Management Journal*, *26*, 2.
55. MacDonald, T. J., Allen, D., & Potts, J. (2016). *Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking.* Najdeno 15. julija 2016 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2749514
56. Miller, R., Tripathi, A. (2003). *Primitives and Mechanisms of the Guardian Model for Exception Handling in Distributed Systems.* Najdeno 25. julija 2016 na spletnem naslovu http://homepages.cs.ncl.ac.uk/alexander.romanovsky/home.formal/Anand-talk.pdf
57. Minergate. (b.l.). *Mining profitability calculator.* Najdeno 25. julija 2016 na spletnem naslovu https://minergate.com/calculator/ethereum
58. Munsell, M. (2014). *Who leads the Residential PV Monitoring Market?* Najdeno 25. julija 2016 na spletnem naslovu http://www.greentechmedia.com/articles/read/Who-Leads-the-Residential-PV-Monitoring-Market
59. *Nanopool*. Najdeno 19. avgusta 2016 na spletnem naslovu https://eth.nanopool.org/stats
60. *Neuralenrgy.* Najdeno 22. avgusta 2016 na spletnem naslovu http://www.neuralenergy.info
61. Novak, G. (2007). *Vpeljava SOA v informacijski sistem Eles.* Čatež: 8. Konferenca slovenskih elektroenergetikov.
62. Odom, C. (2015). *Open-Transactions: Secure Contracts between Untrusted Parties*. Najdeno 11. avgusta 2016 na spletnem naslovu http://www.opentransactions.org/open-transactions.pdf
63. O'Dwyer, R. (2015). The Revolution will (not) be decentralised: Blockchains. *Commons Transition.* Najdeno 11. julija 2016 na spletnem naslovu http://commonstransition.org/
the-revolution-will-not-be-decentralised-blockchains/
64. Omohundro, S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. *AI matters*. New York: ACM.
65. *Radeon*. Najdeno 22. avgusta 2016 na spletnem naslovu http://www.amd.com/en-us/products/graphics/radeon-rx-series/radeon-rx-480
66. Ream, J., Chu, Y. & Schatsky, D. (2016). Upgrading blockchains: Smart contract use cases in industry. *Deloitte University Press.* Najdeno 14. avgusta 2016 na spletnem naslovu http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2016/06/DUP_2833_Smart-contracts_vFINAL.pdf

67. Riveret, F. I. G. G. R., Sartor, G. (b.l.). *Evaluation of Logic-Based Smart Contracts for Blockchain Systems*. Najdeno 30. junija 2016 na spletnem naslovu https://www.researchgate.net/publication/303679677_Evaluation_of_Logic-Based_Smart_Contracts_for_Blockchain_Systems
68. Roth, N. (2015). An Architectural Assessment of Bitcoin: Using the Systems Modeling Language. *Procedia Computer Science*. (str. 527-536).
69. *Rootstock*. Najdeno 18. avgust 2016 na spletnem naslovu http://www.rsk.co
70. Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE.
71. Shah, D. (b.l.). *Gossip Algorithms*. Najdeno 3. avgusta 2016 na spletnem naslovu http://web.mit.edu/vdb/www/6.977/l-shah.pdf
72. Shoup, V. (b.l.). *Practical Threshold Signature*. Najdeno 20. avgusta 2016 na spletnem naslovu http://www.iacr.org/archive/eurocrypt2000/1807/18070209-new.pdf
73. Spaven, E. (2014). *Bitstamp wins best virtual currenxy startup awars at the Europas*. Najdeno 25. julija na spletnem naslovu http://www.coindesk.com/bitstamp-wins-best-virtual-currency-startup-award-europas/
74. *Truthcoin*. Najdeno 18. avgusta 2016 na spletnem naslovu http://www.truthcoin.info/blog/drivechain
75. Wagner, K. (2013). *World's First Bitcoin ATM Opens In Vancouver, Canada*. Najdeno 25. julija 2016 na spletnem naslovu http://mashable.com/2013/10/30/bitcoin-atm-2/#p1yuVS7l_5qX
76. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*. Najdeno 1. avgusta 2016 na spletnem naslovu http://gavwood.com/paper.pdf
77. Wright, A., & De Filippi, P. (2015). *Decentralized blockchain technology and the rise of lex cryptographia*. Najdeno 1. avgusta 2016 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664
78. Zevnik, R. (2012). *Od tržnega denarja do fiat valut* (doktorska disertacija). Maribor: Pravna fakulteta.