e-Governance Academy

Global Information Society Initiative

Krüptoraha – võimalused, ohud, riskid

Tallinn, veebruar-mai 2014

Sisukord

Kokkuvõte

Töö eesmärk on anda informatsiooni Eesti seisukoha kujundamiseks krüptoraha kohta. Töö põhiformaadiks oli seotud valdkondade ekspertidega tehtud intervjuud ja ajurünnakud.

Kogutud, süstematiseeritud ja analüüsitud informatsiooni põhjal koostatud ettepanekud on kindlasti heaks aluseks järgmistele analüüsidele. On oluline rõhutada, et iga teema ja ettepanek vajab süvaanalüüsi. Selle töö puhul on tegemist suhteliselt laia spektrisse kuuluvate eksperthinnangute kogumiga.

Eksperdid olid üsna ühisel seisukohal, et tegemist on uue paradigmaga, mis on oma arengutee alguses ja hetkel on pea võimatu prognoosida isegi lähitulevikus toimuvat. Krüptoraha turule tuleku aeg – krüptoraha startis süveneva pangakriisi tingimustes – viitab traditsioonilisele rahasüsteemile alternatiivi otsimist. Krüptoraha loomist on nimetatud lausa protestiks poliitikute ja pankurite omavoli vastu (Davis).

Avalikult krüptorahaga tegelev kogukond ei ole Eestis suur – pigem tegelevad entusiastid igaüks omaette. Sellist käitumist põhjendatakse nii riigi kui ka avaliku arvamuse pigem negatiivse hoiakuga. Samas, nagu näitavad arvud, tunnevad Eesti elanikud suurt huvi krüptoraha vastu. Google Trendsi kohaselt on maailmas *bitcoin*'i vastu kõige rohkem huvi tundnud eestlased (Google Trends).

Krüptoraha on „mahutatud" olemasolevasse õigusruumi, kuhu see ei sobi oma tunnuste tõttu. Eksperdid arvasid, et juba sõna „raha" on kohati eksitav, sest tegemist on palju enamaga kui raha. Oleks kasulik, kui terminoloogiliselt eristuks krüptoraha süsteem ning selles kasutatav vahetusühik. Hetkel kasutatakse sõna „krüptoraha" või „*bitcoin*" nii avaliku raamatupidamise, vahetusühiku kui ka süsteemi peale ehitatavate uute teenuste kohta.

Krüptovaldkonna areng on sõna otseses mõttes tormiline ning uudiste ja muu informatsiooni allikate hulk kasvab hüppeliselt.

Eksperdid olid ühisel seisukohal, et krüptoraha vajaks Eesti riigi professionaalset käsitlust, samas pooldati tasakaalukat lähenemist teemale. Eesti elanikke ei tule õhutada krüptoraha kasutama, küll aga tuleks neile anda sellest teadmisi. Aega, mil toimub krüptoraha „metsik" arendamine, tuleb kasutada selleks, et õigusruumi ja muud keskkonda, samuti elanikke, krüptoraha ajastu jaoks ette valmistada.

Uuringu tegemist juhtinud e-Riigi Akadeemia ekspert Mari Pedak tänab kõiki, kes aitasid krüptoraha teemas selgust luua ja seisukohti kujundada.

Sissejuhatus

Eesti e-riik on tänaseks rahvusvaheliselt tunnustatud edulugu. Eesti riigi infosüsteemi ainulaadsele arhitektuurile on peale ehitatud tuhandeid e-teenuseid. Alates 28. jaanuarist 2002 välja antud isikutunnistusi kasutades on antud peaaegu 160 miljonit digitaalallkirja ning oma isikut on tuvastatud üle 250 miljoni korra (ID). X-tee andmevahetuskiht on e-maailmas saanud Eesti e-riigi tunnussõnaks. E-teenused on tulevikus üha enam piiriülesed. Eesti eestvedamisel on kavas luua Põhjamaade e-valitsemise baastaristu innovatsiooniinstituut – rahvusvaheline arenduskeskus, mille eesmärk on X-teed, e-identiteeti, digiallkirja ja muid baastaristu komponente ühiselt arendada.

E-maailm jälgib hoolega Eesti e-riigiga seotuid arenguid, mida siseriigis alati ei tunnetata. Näiteks jõudis Eesti Panga hoiatus krüptoraha kohta (Eesti Panga kommentaar) rahvusvahelisse meediasse ja seda on laialt tsiteeritud.

Krüpto- ehk digiraha, nagu seda nimetatakse, on laiema avalikkuse silmis ka üks e-lahendusi, kuna näiteks füüsilises maailmas me *bitcoin*'e puudutada ei saa.

Seetõttu on krüptoraha suhtes sisulise ja põhjendatud seisukoha kujundamine ülima tähtsusega Eesti kui eduka e-riigi rahvusvahelise kuvandi tagamisel.

Nagu juba kokkuvõttes öeldud, näitavad Google Trendsi andmed eestlaste suurt huvi teema vastu (Google Trends).

On palju kaevandajaid ja üksiküritajaid, kes toimetavad rohkem omaette. Kuna avalikku arvamust ja riigi tuge tajutakse kas olematuna või pigem negatiivsena[1], siis ei söandata väga avalikult asjaga tegeleda. Aktiivsem osa krüptoraha kogukonnast on kas välismaalased või väliseestlased, keda see pole häirinud või pole nad sellest teadlikud olnud. Eeltoodud väide kehtib näiteks nii ainsa *bitcoin*'i ATM-i omaniku kui ka Mälla mõisa värske omaniku (Eestis osteti *bitcoin*'ide tulu eest mõis) kohta.

Korduvalt on kaalutud kogukonda liitva krüptoraha liidu loomist, kuid siiani pole see idee veel piisavalt entusiastlikke tegijaid suutnud koondada. Kogukonna eestvedajad korraldasid 21. mail k.a Tallinnas hariva eesmärgiga *bitcoin*'i-teemalise konverentsi (Konverents). Järgmisena on kavas korraldada suvel Mälla mõisas ülemaailmne (Ameerika, Venemaa, Hiina, Soome, Taani jt riikide) entusiastide kokkusaamine.

Eksperdid on seisukohal, et Eesti pole krüptoraha suhtes seisukohta (mitte) kujundades oma IKT ja/või e-riigi potentsiaali seni veel piisavalt kasutanud.

[1] Ka meedias ilmuvad artiklid riigi tegevuse kohta on hoiatavad. Vt Hans Lõugas „Ettevaatust: *bitcoin*'idega kaubitsemine võib teile kraesse tuua kriminaalasja". Eesti Päevaleht, 07.05.2014.

Uuringu metoodika

Uuring korraldati järgnevalt kirjeldatud metoodika alusel.

Algne töö allikatega toimus sellises ulatuses, mis oli vajalik intervjuude ettevalmistamiseks ja tegemiseks. Seejärel alustati intervjuude tegemist.

Intervjuude ja täiendava allikate läbitöötamise tulemusena valmistati ette ajurünnak, millest kutsuti osa võtma Arengufondi, ASi Cybernetica, Eesti Panga, Guardtime'i, LHV, e-Riigi Akadeemia, ASi Datel, Majandus- ja Kommunikatsiooniministeeriumi, Politsei- ja Piirivalveameti Rahapesu Andmebüroo, Rahandusministeeriumi, Riigi Infosüsteemi Ameti (edaspidi: RIA), ASi Tavid, TransferWise'i ja vabakutselised eksperdid. Kokku osales kaksteist eksperti.

Ajurünnakule järgnes selle tulemuste analüüs ning täiendav allikate läbitöötamine. Samuti jätkusid intervjuud ja kokku küsitleti 15 eksperti.

Seejärel vormistati lõpparuanne ning koguti ekspertidelt ettepanekuid.

Ühiselt otsustati esitada aruanne asjasse puutuvatele riigiasutustele, teha aruanne veebis nähtavaks ja kättesaadavaks ning anda välja pressiteade. 15. mail 2014 saadeti aruanne adressaatidele.

Intervjuude, ajurünnakute või kommentaaride vormis andsid oma arvamuse 22 eksperti (tähestiku järjekorras): Agu Leinfeld (Datel), Ahto Truu (Guardtime), Andres Kitter (LHV), Andres Kütt (RIA), Arvo Ott (eGA), Asse Sauga, Henri Laupmaa, Jan Villemson (Cybernetica), Kristiina Kaljurand (Rahandusministeerium), Kurmet Ojamaa (Rahandusministeerium), Mari Pedak (eGA), Mihkel Nõmmela (Eesti Pank), Monika Paukštite (Rahapesu Andmebüroo), Rainer Olt (Eesti Pank), Sören Meius (Rahandusministeerium), Taavi Kotka (Majandus- ja Kommunikatsiooniministeerium), Veljo Otsason (Mobi), Veronika Mets (Rahandusministeerium).

1 Krüptoraha teke

Avalikkus ei tea, kes peitub(vad) nime Satoshi Nakamoto taga.

Legendi järgi alustas Satoshi Nakamoto (alles) 2007. aastal tööd krüptoraha loomiseks (vt History of Bitcoin). Satoshi Nakamoto isik ei ole vaatamata paljudele selgitamiskatsetele ja spekulatsioonidele[2] teada. Arvatakse ka, et tegemist on kollektiivse nimega.

Satoshi Nakamoto kirjeldab oma loodud süsteemi tööpõhimõtteid 31. oktoobril 2008. aastal (metzdowd.com[3] kaudu) avaldatud artiklis "Bitcoin: A Peer-to-Peer Electronic Cash System". Enne seda, 18. augustil 2008 registreeriti Helsingis asuva teenusepakkuja juures bitcoin.org. Eelnimetatud artikkel on n.ö krüptoraha maailma piibel, milles on kirjeldatud ka Bitcoini protokoll. *Bitcoin*'i koguemissiooni väärtus on 21 miljonit *bitcoin*'i (BTC), mis realiseeritakse 2140. aastaks.

3. jaanuari 2009. aasta õhtul kell 18:15:05 keskmise päikeseaja (GMT) järgi kaevandas Satoshi Nakamoto esimesed 50 *bitcoin*'i, kusjuures 1 *bitcoin*'i väärtus oli alla 1 penni[4]. Esimene ülekanne Satoshi Nakamoto ja krüptograafia-entusiasti Hal Finney vahel toimus 12. jaanuaril 2009. aastal.

18. veebruaril 2010 publitseeriti krüptograafiaalane patent, millel *bitcoin* põhineb ja mida taotlesid juba 15. augustil 2008 Neal Kin, Vladimir Oksman ja Charles Bry[5].

Esimene reaalne tehing tehti 22. mail 2010 Jacksonvilles, kui Florida programmeerija Laszlo Hanyecz ostis 10 000 *bitcoin*'i eest pitsa, kusjuures pitsa hinnaks kujunes umbes 25 USA dollarit. Ühe *bitcoin*'i hind oli sel ajal 0,07 USA senti, arvutatuna kaevandamisele kuluva elektri hinna järgi.

Tasapisi tekkis kaupmeeste huvi ja usaldus ning 2010. aasta lõpus hakkas *bitcoin*'i väärtus järsult kasvama ja 2011. aasta juunikuu lõpus maksis üks *bitcoin* 29 dollarit. Siis õnn pöördus ja septembrikuu lõpus anti *bitcoin*'i eest

[2] Adam L. Penenberg. The Bitcoin Crypto-Currency Mystery Reopened; Joshua Davis. The Crypto-Currency; Rob Wile. Still Nobody Knows Who Created Bitcoin - But There Are A Few Bif Theories.
[3] Metzdowd.
[4] *Bitcoin*'il pole garanteeritud väärtust. *Bitcoin*'i väärtus tekib turul klassikaliselt nõudluse ja pakkumise vahekorra kaudu. Esimene väärtus anti *bitcoin*'ile 5. oktoobril 2009 kaevandamise energiakulu hindamise kaudu [*New Liberty Standard publishes a Bitcoin exchange rate that establishes the value of a Bitcoin at US$1 = 1,309.03 BTC, using an equation that includes the cost of electricity to run a computer that generated Bitcoins.*].
[5] Siiani spekuleeritakse, et need 3 krüptograafi varjuvad Satoshi Nagamoto varjunime taha.

5 dollarit[6]. Samas oli ringluses juba üle 7 miljoni *bitcoin*'i ja Nakamoto tulu oli selleks hetkeks 35 miljonit dollarit.

Aprillis 2011 saatis Nakamoto viimase sõnumi, et hakkab tegelema uute valdkondadega, pärast seda temast kuuldud ei ole.

27. septembril 2012 registreeriti USA-s Bitcoini Sihtasutus (Bitcoin Foundation), mille eesmärgiks on üle maailma kasutajate huvides standardiseerida, kaitsta ja arendada krüptoraha.

Bitcoini Sihtasutuse esimene (iga-aastane) konverents toimus 2013. aastal Silicon Valley's, millest võttis osa 1200 inimest. Teine konverents „Bitcoin 2014: Building the Digital Economy" toimus 15.–17. mail 2014 Amsterdamis[7].

Parima tegutsemiskeskkonna otsingul kavatseb Bitcoini Sihtasutus kolida Londonisse[8].

2 Bitcoini süsteem

Bitcoini süsteem on Bitcoini protokolli alusel loodud avatud lähtekoodiga tarkvara ja keskse osapooleta P2P-võrgustik, mille võrgusõlmed peavad koos andmebaasi, mis kajastab kõiki tehinguid ja *bitcoin*'ide kuuluvust adressaatidele ehk omanikele. P2P-võrgustiku võrgusõlmedes asuvad arvutid osalevad kaevandamisel ning tehingute tegemisel. *Bitcoin* ehk krüptograafiline valuuta on selle süsteemi arveldusühik.

Andmebaas ehk avalik raamatupidamisregister ehk tehinguplokkide ahel kajastab kogu ringluses olevat ehk kaevandatud raha ja sellega tehtud tehinguid, aga samuti infot kõigi kontode kohta, millega on krüptoraha olnud seotud. Kui raharingluses ei ole võimalik jälgida konkreetsete pangatähtede liikumist, siis Bitcoini süsteem võimaldab jälgida iga *bitcoin*'i liikumist algusest lõpuni. Tavapäraselt rõhutatakse krüptorahaga seotud anonüümsust, kuid kuna kõikide transaktsioonide ajalugu on nähtav, on mõnes mõttes tegemist palju avatuma süsteemiga kui tavapärane pangasüsteem.

Kaevandamine on protsess, mille käigus kaevandajad moodustavad juba kontrollitud tehingutest ülimat ressurssi nõudva arvutuse abil tehinguplokke ja saavad selle eest preemiaks ringlusesse lastavaid uusi *bitcoin*'e[9]. Kaevandaja kasutab spetsiaalset riist- ja tarkvara, kusjuures selle keerukuse

[6] Volatiilsust loetakse krüptoraha suurimaks puuduseks, mille suhtes mingeid lahendusi seni välja pakutud ei ole.
[7] Bitcoin 2014.
[8] Bitcoin Foundation Record Straight UK Office.
[9] Uute *bitcoin*'ide ringlusesse laskmisega kompenseeritakse kaevandajate panust süsteemi tööshoidmisel. Arvestades, et tehinguplokkide eest saadavate *bitcoin*'ide arv väheneb, tuleb ühel hetkel hakata kaevandajate panust kompenseerima teenustasudega.

juures kasutatakse üldjuhul ASIC (*application specific integrated circuit*) riistvara ja koos sellega tarnitavat vabavaralist CGmining tarkvara. Kaevandamiseks vajaliku arvutusressursi suurenemine on esile kutsunud kaevandajate ühistegevuse, mille eesmärgiks on arvutusressursside koondamise teel suurendada uute *bitcoin*'ide teenimise võimalusi.

Kõigepealt kaevandatakse krüptoraha tekke- ehk esmaplokk. *Bitcoin*'ide loomine toimub tsüklitena, kus igas tsüklis kinnitatakse 210 000 tehinguplokki ja kokku väljastatakse X arv *bitcoin*'e. Esimeses tsüklis väljastati iga plokiga 50 *bitcoin*'i, kokku 10,5 miljonit. Pärast igat tsüklit väheneb iga tehinguploki kohta loodavate uute *bitcoin*'ide arv poole võrra. Praegu käib teine tsükkel ning iga ploki eest on võimalik saada 25 *bitcoin*'i, mis kehtib, kuni ringlusesse on lastud kokku 15,75 miljonit *bitcoin*'i. Järgmises tsüklis on iga ploki eest võimalik saada 12,5 bitcoin'i. Kokku lastakse ringlusesse 21 miljonit bitcoin'i, protokolli kohaselt lõpeb emissioon 2140. aastal.

Tehinguplokk moodustatakse võrgu poolt kontrollitud, aga seni veel tehinguplokkidesse lülitamata tehingute andmetest. Tehinguploki õigsuse kinnituseks ja võltsimiskindluse tagamiseks arvutatakse tehingute andmete põhjal krüptograafiline räsi, mis saab ploki osaks ja mis peab vastama Bitcoini protokolliga etteantud reeglitele. See arvutus peab kogu kaevandajate võrgustikul võtma aega umbes 10 minutit. Kui ilmneb, et kaevandamine võtab rohkem aega, vähendab protokoll automaatselt arvutuse keerukust. Vastupidisel juhul arvutuse keerukus suureneb. Tehinguplokki võib erinevatel ajahetkedel kuuluda väga erinev arv tehinguid (vt Number of Transactions per Block).

Krüptorahaga tehingute tegemiseks on lisaks riist- ja tarkvarale vaja **rahakotti**, mis moodustub krüptoraha omaniku identifitseerimist võimaldavatest digitaalsetest tõenditest, mida kasutades omanik pääseb oma rahale ligi ja saab sellega teha tehinguid. Omanikul võib olla mitu rahakotti. Muus osas võrdlust füüsilise rahakotiga kasutada ei saa – *bitcoin*'i rahakotis ei hoita raha.

Bitcoini süsteemis kasutatakse avaliku võtme krüptograafiat. Iga andmebaasi kirje omistab mingi koguse krüptoraha kindlale aadressile, kusjuures aadressiks on krüptograafilise võtmepaari avaliku poole kontrollsumma (*hash*-väärtus). Võtmepaari privaatset poolt teab vaid selle omanik ning privaatvõti on vajalik raha ülekandmiseks teisele omanikule. Tehingukirjed koondatakse eespool kirjeldatud tehinguplokkideks, millest igaühel on unikaalne plokiräsi (*hash*), mis genereeritakse mingi krüptograafilise räsialgoritmiga. *Bitcoin*'i räsialgoritm on SHA-256, *litecoin*'il *scrypt* jne.

Krüptoraha aadresside inimloetav kuju on 33-täheline tekstijupp, näiteks "1rYK1YzEGa59pI314159KUF2Za4jAYYTd". Krüptoraha aadressi esimene täht on igal rahal erinev (*bitcoin* – 1, *litecoin* – L jne). Igaüks võib luua niipalju erinevaid aadresse kui vaid hallata jaksab, aadresside loomine on hetkeline ning ei vaja suhtlust võrguga. Ühekordsete ja sihtotstarbeliste aadresside kasutamine võimaldab hoida anonüümsust.

Enamik krüptorahasid baseeruvad Bitcoini protokollil, on selle mingis osas muudetud variandid. Näiteks varieeruvad järgmised parameetrid:

- võrgu ülalhoidmise põhimõte: *proof-of-work* (*bitcoin*, *litecoin*, *auroracoin*), *proof-of-work/proof-of-stake* hübriidsed süsteemid (*peercoin*, NXT);
- ploki räsialgoritm: SHA-256 (*bitcoin, peercoin*), *scrypt* (*litecoin, dogecoin, auroracoin, 42coin*), Primechain (*primecoin*), Quark (*quark coin*);
- plokkide genereerimise aeg: *bitcoin* – 10 min, *litecoin* – 2,5 min;
- emissiooni kogumaht: *bitcoin* – 21 miljonit, *litecoin* – 82 miljonit;
- eelkaevandatud kogus (jaotus- ja tekkeskeem): *bitcoin, litecoin* 0%, *auroracoin* 50%[10].

Proof-of-work protokolli kasutavate krüptorahade süsteemide toimimiseks vajalik arvutiressurss on väga suur ja kasvab pidevalt vastavalt kaevandamise keerukuse kasvule. 14. aprilli 2014 seisuga on *bitcoin*'i kaevandamisvõimsus 55PH/s[11] ($55x10^{15}$ *hash*'i sekundis), sellele kuluva elektri hind oli 2013. aasta lõpus 15 miljonit dollarit päevas[12], praegu oletatavalt 10 korda suurem. Bitcoini süsteemi üleval hoidmiseks kasutatakse hinnanguliselt arvutiressurssi, mis on 1400 korda suurem kui 500 maailma parima superarvuti ressurss kokku.

Krüptoraha soetamine

Lisaks kaevandamisele on võimalik *bitcoin*'e soetada erinevate vahetusplatvormide kaudu või osta inimestelt otse. Variant on ka müüa oma tooteid/teenuseid, aktsepteerides makseid *bitcoin*'ides. Üle maailma eksisteerib umbes sadakond erinevat vahetusplatvormi, kus on võimalik vahetuskursi alusel osta ja müüa *bitcoin'*e.

Praktikad on erinevad. Paljud vahetusplatvormid nõuavad inimestelt üsna põhjalikku informatsiooni enne, kui konto aktiveeritakse ning on võimalik hakata *bitcoin*'e ostma. Mis viitab „tunne oma klienti" ja rahapesu nõuete täitmisele (näiteks USA-s). Sellistel juhtudel on tegelikult *bitcoin*'e kasutav inimene tuvastatav.

Bitcoin'i omanikku on keerulisem tuvastada, kui *bitcoin*'e ostetakse sularaha eest teiselt inimeselt või *bitcoin*'i ATM-ist. Niipea kui *bitcoin*'i kontoga on vahetusplatvormi kaudu seotud pangakonto, on inimest juba lihtsam tuvastada.

Tuleb välja tuua, et vahetusplatvormid võtavad *bitcoin*'i ostu-müügitehingute eest teenustasu, mis jääb umbes poole protsendi juurde. Täiendavalt tuleb välja tuua, et eri platvormide lõikes on võimalik *bitcoin*'e osta erineva hinnaga. Hindade erinevust näitavad ka erinevate turgude graafikud.

[10] Eelkaevandamist oma riigi kõigi elanike jaoks on lisaks *auroracoin*'ile (23.02.2014) lubanud ka *spaincoin*'i (Hispaania, 12.03.14), *ukrainecoin*'i (Ukraina, 15.03.14), *PLNcoin*'i (Poola, 17.03.14), *aphroditecoin*'i (Küpros, 22.03.14) ja *cataloniacoin*'i (Kataloonia/Hispaania, 30.03.14) käibele laskjad.
[11] Blockchain.
[12] Forbes - Bitcoin Mining Uses Electricity.

Maksete tegemine

Maksete tegemine toimub süsteemis järgnevalt:

1. Raha omanik vormistab ja allkirjastab rahakoti vahendusel ja avaliku võtme infrastruktuuri kasutades tehingu.
2. Iga tehing saadetakse töötlemiseks kõigile kaevandajatele ehk süsteemi ühendatud arvutitele.
3. Tehingud koondatakse üheks plokiks ja kontrollitakse vastu avalikku raamatupidamisregistrit.
4. Tehinguteploki kinnitamiseks hakkavad kõik süsteemi ühendatud arvutid lahendama matemaatilist probleemi, et leida tehinguplokkide kinnitus. Esimene, kes leiab õige lahenduse, saab vaevatasuks praeguses tsüklis 25 *bitcoin*'i.
5. Lahenduse leidmisel saadetakse kinnitatud plokk kõigile kaevandajatele täiendavaks kontrollimiseks.
6. Teised kaevandajad aktsepteerivad ploki, kui kõik selles sisalduvad tehingud on korrektsed ning kõnealuseid *bitcoin*'e ei ole kulutatud mujal.
7. Peale aktsepteerimist hakatakse arvutama kõnealusele jadale järgnevat plokki, kasutades kogu infokogumit (ehk arvestades kõiki varasemalt *bitcoin*'idega tehtud tehinguid), mis on plokkide jadaga kaasa tulnud. Iga järgneva ploki lisandumist saab võtta kui maksetehingu täiendavat kinnitust.

Kui kontrollimisele saadetakse üheaegselt kaks plokki (võrdse pikkusega jada), hakkab kaevandaja kontrollima seda, mis jõudis temani esimesena, samas igaks juhuks salvestatakse ka paralleelne jada. Lõpuks loetakse õigeks jada, millele lisandub esimesena järgnev plokk.

Makse kiirus on u 10 minutit ehk ploki kinnitamiseks vajamineva matemaatilise probleemi lahendamiseks kulunud aeg. Iga lisanduv plokk kinnitab makse veelkord üle ja **makset pole võimalik enam tagasi kutsuda**.

Kuna tehing loetakse piisava usaldusväärsusega kinnitatuks, kui see asub 6 ploki sügavusel, siis tagab 10 minuti reegel usaldusväärse kinnituse u 1 tunni jooksul. Samas võib tehingu osapool tehingut aktsepteerida ka pärast selle tehinguploki moodustamist, millesse konkreetne tehing kuulub, ja mitte oodata järgnevaid kinnitusi.

Samuti näeb algoritm ette, millised tehingud on kõrgema prioriteediga ja mis tuleb tehinguplokkidesse kaasata eelisjärjekorras. Näiteks on kõrgema prioriteediga suuremate summadega tehtavad tehingud ja tehingud *bitcoin*'idega, millega pole pikemat aega tehinguid tehtud. Väikesed, vahendustasuta tehingud võivad pikka aega tehinguplokkidesse lülitamist oodata.

Krüptoraha turg

Erinevate krüptorahade arv ulatub sadadesse. Näiteks kajastab veebileht Map of Coins (Map of Coins) 3. mai 2014 seisuga 379 krüptoraha. Veebileht Coin Calender (Coin Calender) vahendab infot uute rahade turule tuleku

kohta. Veebileht Com-HTTP (Com-HTTP) on 3. mai 2014 seisuga indekseerinud 430 krüptoraha.

Need veebilehed toidavad üldlevinud müüti, et krüptoraha on laialt levinud või kasutusel. Eesti Panga info alusel tehakse kogu maailmas krüptorahaga u 70 000 tehingut päevas, mis tähendab, et krüptoraha osa rahaturul on marginaalne. Praeguses arengufaasis on tegemist alles nõudluse loomisega, tarbimist pole veel näha.

Suurim väljakutse on hoopis krüptoraha kasutajakeskkonna tekitamine, sest raha väärtus tekib teenuste pakkumise kaudu. Krüptoraha emiteerimine on lihtne võrreldes nõudluse tekitamisega. Teadaolevad *bitcoin*'iga seotud kõige suuremad investeeringud on tehtud just turundusse. Tõenäoliselt ei konkureeri seetõttu ükski teine krüptoraha turul *bitcoin*'iga – *bitcoin*'i turuosa on u 80%.

Krüptoraha turu-ülevaadet vahendav veebileht Crypto-Currency Market Capitalization (Crypto-Currency Market Capitalizations) kajastab 2. mai 2014 seisuga 257 krüptoraha turumahuga 6.028.004.773 $, millest *bitcoin* moodustab u 80% ja *litecoin* u 10 %. Sama veebileht annab hea visuaalse ülevaate ka turukõikumistest.

Vaatamata suurele volatiilsusele, mis on krüptorahaga kauplemise suurim risk, on *bitcoin*'i investeerimine siiski väga ahvatlev, sest ennustatakse, et hinnatõusud jätkuvad (vt Bitcoin Price Prediction 2014).

3 Riikide, sh Eesti seisukohad

Praeguseks ajaks ei ole välja kujunenud (ühtegi) ühtset ametlikku käsitlust selle kohta, mis on *bitcoin* või krüptoraha kui selline. Euroopa Keskpank ja Financial Action Task Force (FATF) on oma analüüsi tulemusel asunud seisukohale, et *bitcoin*'i puhul on tegemist detsentraliseeritud digitaalse käibevahendi ehk virtuaalrahaga (*decentralized virtual currency*)[13]. Krüptoraha ei väljasta ükski konkreetne emitent ning selle väärtus ja vahetuskurss sõltub täielikult nõudlusest, mitte aga alusvarast või fikseeritud kursist mõne muu valuuta suhtes. Krüptorahaga maksekohustuste täitmine on võimalik ainult osapoolte vabatahtlikul nõusolekul.

Veebisait BitLegal (BitLegal) hoiab aktuaalsena ülevaate riikide seisukohtadest krüptoraha suhtes (roheline värv tähistab riikide lubavat, kollane vaidlustavat ja punane vaenulikku hoiakut, musta värviga on tähistatud riigid, mille seisukoht ei ole teada.

[13] ECB. Virtual Currency Schemes. October 2012

Riikide seisukohad krüptoraha kohta on seinast seina. Krüptoraha peetakse nii kaubaks/teenuseks (Skandinaaviamaad), arvestusühikuks (Saksamaa), alternatiivseks maksevahendiks kui ka rahaks/valuutaks. Kohati tunnistatakse, et krüptoraha kui uue paradigma suhtes ei osata seisukohta võtta või igaks juhuks ignoreeritakse teemat.

Huvi ja surve riikide valitsustele kujundada seisukoht krüptoraha suhtes on suur, mis kohati sunnib riikide valitsusi ka varem välja öeldud seisukohti revideerima.

Nii näiteks oli Suurbritannia seisukoht veel jaanuaris 2014, et krüptoraha on reguleerimata valdkond, mille kohta rakendatakse 10–20 % käibemaksu (Regulation of Bitcoin in Selected Jurisdictions). Märtsis 2014 avaldatud uudise kohaselt ei maksustata *bitcoin*'i tehinguid enam käibemaksuga (Britain to scrap VAT on Bitcoin trades)

Väga positiivse seisukoha võttis 9. mail k.a USA Föderaalreservi Nõukoda (FAC). Nõukoda arutas, kas krüptoraha kujutab ohtu traditsioonilisele pangandusele ja jõudis seisukohale, et "*Bitcoin does not present a threat to economic activity by disrupting traditional channels of commerce; rather, it could serve as a boon*."[14](Federal-reserve-bitcoin-potential-boon). *Bitcoin* annab kaubandusinnovatsioonile uue hoo: avab uusi turge, suunab kapitalivooge arenevatesse maadesse ja suurendab globaalset tarbimist.

Euroopa keskpangad on siiani võtnud ja hoidnud hoiatavat seisukohta[15]. Euroopa Keskpanga hoiatuse on edastanud ka Eesti Pank (vt lisaks Eesti Pank. Kommentaar *bitcoin*'i kohta).

Eestis on krüptoraha kohta seisukoha avaldanud ka Rahandusministeerium, Maksu- ja Tolliamet ning Rahapesu andmebüroo[16].

Bitcoin ei ole Eestis seaduslik vääring[17] ja sellel ei ole küllaldaselt rahale (pidades selle all silmas pangatähti, münte, füüsilisel kujul eksisteerivat raha ning elektroonilisel kujul edastatavat raha) omaseid tunnuseid.

Bitcoin ei ole Eesti õigusruumis ka e-raha[18], sest *bitcoin*'is väljenduv väärtus ei ole ranges mõttes rahaline, see ei loo nõuet *bitcoin*'ide väljaandja vastu ja *bitcoin*'e ei väljastata „rahalise sissemakse eest saadud summa nimiväärtuses".

[14] *Bitcoin* ei kujuta endast majandustegevusele ohtu, lõhkudes traditsioonilisi kaubanduskanaleid, pigem on tegemist õnnistusega.
[15] European Central Bank warns of virtual currency risks; ECB. Virtual Currency Schemes. October 2012, Warning to consumers on virtual currencies; EBA Consumer Trends. Report 2014.
[16] Rahandusministeeriumi 04.03.2014 vastus AS Tavid teabenõudele, Maksu- ja Tolliameti seisukoht „Maksustamine Bitcoin'idega kauplemisel" ja „Rahapesu andmebüroo juht Aivar Paul bitcoinidega seonduvast".
[17] *Bitcoin*'il puuduvad avalik-õiguslik staatus, käibe regulatsioon, identifitseeritav emiteerija, kursi reguleerimiseks või *bitcoin*'ide käibelt kadumisel nende ümber vahetamiseks kohustatud isik, tehingutes vastu võtmise kohustus ja finantsjärelevalve.
[18] MERAS § 6 lõike 1 kohaselt on e-raha elektroonilisel kandjal säilitatav rahaline väärtus, mis väljendab rahalist nõuet selle väljaandja vastu ja mis vastab kõigile järgmistele tingimustele: (i) seda väljastatakse rahalise sissemakse eest saadud summa nimiväärtuses; (ii) seda kasutatakse maksevahendina maksetehingute tegemiseks võlaõigusseaduse § 709 lõike 6 tähenduses; (iii) seda aktsepteerib maksevahendina vähemalt üks isik, kes ise ei ole selle e-raha väljastaja.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse (rahaPTS) mõistes on *bitcoin*'ide ostul, müügil, vahendamisel alternatiivsete maksevahendite teenuse pakkumise tunnused[19].

Bitcoin'idega kauplemisel tekkiv käive maksustatakse tavapärase 20protsendilise käibemaksumääraga. Käibemaksuseadus (KMS) tugineb Euroopa Liidu käibemaksuregulatsioonile, mis ei näe ette alternatiivsete maksevahendite teenuste käsitlemist finantsteenustena ja mis seetõttu ei kuulu finantsteenusele kohaldatava maksuvabastuse alla. 18. juulil 2011 jõustunud Käibemaksuseaduse § 16 lõike 21 punkt 6 kohaselt e-raha käivet ei maksustata, aga, nagu eespool öeldud, ei vasta *bitcoin* Eesti õigusruumis e-raha tunnustele[20].

Tulumaksuseaduse (TuMS) kontekstis käsitletakse *bitcoin*'i varana ja tulumaksuga maksustatakse vara võõrandamisest, sh vahetamisest saadud kasu, samuti maksustatakse teenitud tulu ettevõtlustuluna, sh sotsiaalmaksuga.[21]

Toodud käsitluses on krüptoraha „mahutatud" olemasolevasse õigusruumi, kusjuures riigiasutused peavadki ainult kehtivatest õigusaktidest lähtuma. Selline mõnevõrra lihtsustatud käsitlus on Eesti *bitcoin*'i kogukonnas tekitanud arusaamise, et Eesti riik on krüptoraha suhtes võtnud eitava seisukoha.

Ekspertide hinnangu kohaselt on krüptoraha näol tegemist täiesti **uue paradigmaga**, mida ei saa n.ö eraldi tükkidena käsitleda, vähemalt mitte enne, kui on loodud krüptoraha ja sellega seotud keskkonna kohta tervikkäsitlus ja vastav õigusruum. **Krüptoraha kannab endas nii panga, raha kui ka rahaturu tunnuseid** ja katsed hinnata või reguleerida krüptoraha süsteemi üksikuid osi kehtiva õigusruumi raames ei saa seetõttu olla edukad.

Krüptoraha valdkond vajaks õiguslikku süvaanalüüsi ja sellele tuginevat regulatsiooni. Suure tõenäosusega tähendaks see olemasoleva õigusruumi täiendamist[22].

[19] RahaPTS § 6 lõike 4 kohaselt on alternatiivsete maksevahendite teenuse pakkuja isik, kes oma majandus- või kutsetegevuse käigus ostab, müüb või vahendab side-, ülekande- või kliiringsüsteemi kaudu rahalist väärtust omavaid vahendeid, mille abil on võimalik täita rahalisi kohustusi või mida saab vahetada kehtiva vääringu vastu, kuid kes ei ole lõikes 1 nimetatud isik ega finantseerimisasutus krediidiasutuste seaduse tähenduses.

[20] KMS 18.07.2011 jõustunud § 16 lõike 21 punkt 6 kohaselt ei maksustata mittesularahaliste maksevahendite, näiteks elektrooniliste maksevahendite, e-raha, reisitšekkide ja vekslite väljastamist ja haldamist.

[21] TuMS tähenduses on *bitcoin* vara ja maksustamine toimub TuMS § 15 lõike 1 ja § 37 lõike 1 kohaselt.

[22] Kahtlemata kaasnevad uut tüüpi virtuaalraha kasutamisega ka uued riskid, mille analüüsimisega on juba Euroopa Liidus tegelema asutud. Muu hulgas kaalutakse, kas ja kuidas tuleks virtuaalraha reguleerida, kuidas kehtivaid regulatsioone täpsustada või kas oleks vajalik teatud tunnustega virtuaalraha hoopiski keelustada. Eeldatakse, et edaspidi täpsustub Euroopa Liidu õigus virtuaalrahade osas, mis omakorda võib kaasa tuua Eesti õigusaktide muutmise.

4 Krüptoraha tugevused ja nõrkused

Krüptoraha usaldusel põhinev süsteem on ühtlasi selle suurimaks tugevuseks ja nõrkuseks.

Intervjuudes toodi kõige rohkem positiivsena välja transaktsioonide kiirust ning ülekandetasude madalat hinda.

Enamik nõrkusi, mida krüptorahaga seoses välja tuuakse, on (on olnud) ühtlasi ka tavarahaga seostatavad: parim näide on võimalus, et rahakott varastatakse.

Tugevused

Krüptoraha detsentraliseeritud ja usaldusel põhinev olemus on tema suurim tugevus.

Krüptoraha on nimetatud ka protestirahaks, mis tekkis vastukaaluks kehtivale rahasüsteemile: kellelgi (sh mitte ühelgi pangal ega poliitikul) ei ole võimalust oma otsusega krüptoraha olemust ja aluspõhimõtteid muuta. Ühtlasi puudub neil võimalus (ka kaudselt) tekitada näiteks panganduskriise. Ei ole ilmselt juhus krüptoraha turule tuleku aeg, mis langes kokku ülemaailmse panganduskriisiga. Inimesed ei tahtnud enam usaldada pankasid ega poliitikuid ja olid väga vastuvõtlikud igale uuele lahendusele, mis seda vältida võimaldas.

Andmebaas ehk avalik raamatupidamisregister ehk tehinguplokkide ahel kajastab kogu ringluses olevat ehk kaevandatud raha ja sellega tehtud tehinguid, aga samuti infot kõigi kontode kohta, millega krüptoraha on olnud seotud. Kui raharingluses ei ole võimalik jälgida konkreetsete pangatähtede liikumist, siis *bitcoin*'i süsteem võimaldab jälgida iga *bitcoin*'i liikumist algusest lõpuni.

Tavapäraselt krüptoraha nõrkusena nimetatav anonüümsus ei ole ainult nõrkus. Kuna kõikide transaktsioonide ajalugu on nähtav, on mõnes mõttes tegemist palju avatuma süsteemiga kui tavapärane pangasüsteem. Anonüümsus selles süsteemis on ainult näiline. Analüüsides tehingute mustreid, saab hinnata tehingute tegijate motiive ja neid vajaduse korral ka tuvastada. Samuti kaotavad krüptorahaga tehingute tegijad anonüümsuse sidudes ostu-müügi korral oma isiku mingi pangakontoga.

Kui raharingluses ei ole võimalik jälgida konkreetsete pangatähtede liikumist, siis Bitcoini süsteem võimaldab jälgida iga *bitcoin*'i liikumist algusest lõpuni.

Krüptoraha ülekandeid iseloomustab suur kiirus. Ülekanne ise toimub n.ö momentaalselt, sellele lisandub ülekande kinnitamine ehk usalduse tekitamine tehinguploki moodustamise (*proof of work*) kaudu, mis võtab *bitcoin*'i puhul aega u 10 minutit. Iga lisanduv plokk kinnitab makse veelkord üle ja makset pole võimalik enam tagasi kutsuda. Tehing loetakse kokkuleppeliselt piisava usaldusväärsusega kinnitatuks, kui see asub 6 ploki sügavusel, seega tagab 10 minuti reegel usaldusväärse kinnituse u 1 tunni jooksul. Samas võib tehingu osapool tehingut aktsepteerida ka pärast selle

tehinguploki moodustamist, millesse konkreetne tehing kuulub, ja mitte oodata järgnevaid kinnitusi.

Samuti näeb algoritm ette, millised tehingud on kõrgema prioriteediga ja mis tuleb tehinguplokkidesse kaasata eelisjärjekorras. Näiteks on kõrgema prioriteediga suuremate summadega tehtavad tehingud ja tehingud *bitcoin*'idega, millega pole pikemat aega tehinguid tehtud. Väikesed, vahendustasuta tehingud võivad pikka aega tehinguplokkidesse lülitamist oodata.

Krüptoraha ülekanded on praegu tasuta või väga väikese ülekandetasuga. Näiteks maksab iga järgmise 1 kB[23] suuruse andmemahuga transaktsioon 10 000 *satoshi*'t ehk 5 USA senti. Selline väike ülekandetasu on võimalik, kuna kaevandajaid saab veel premeerida uute *bitcoin*'idega. Mida edasi, seda väiksemaks jääb selline premeerimisvõimalus ning tekib vajadus ülekandetasude kehtestamiseks. Praegu ei ole ülekandetasude maksmine kohustuslik, aga see kiirendab tehingu kinnitamisprotseduuri.

Nõrkused

Tegemist on detsentraliseeritud emissiooniga, mistõttu puudub keskne vastutav osapool ning krüptoraha kasutamine maksevahendina toimub inimeste endi riisikol. Võrdluseks: kasutades mõne panga või muu makseasutuse teenuseid e-ostu tegemiseks internetis, on petturluse korral võimalik tehingut tagasi pöörata ehk inimese raha on kaitstud. Krüptoraha puhul ei ole inimesel petturluse korral kellegi poole pöörduda: kuna keskset makseteenuse pakkujat ei eksisteeri, siis pole ka kellegi vastu võimalik nõuet esitada. Isegi kui leidub abivalmis riigiasutus – näiteks politsei poole võib inimene alati pöörduda – peab arvestama, et selle saaja tuvastamine ja raha tagasi nõudmine võib osutuda üsna ebarealistlikuks ning võimatuks väljakutseks.

Kuna krüptoraha on klassikalise turustiihia reguleerida, on tema suurimaks nõrkuseks suur volatiilsus (vt Crypto-Currency Market Capitalizations). Vaatamata sellele on *bitcoin*'i investeerimine siiski väga ahvatlev, sest ennustatakse, et hinnatõusud jätkuvad (vt Bitcoin Price Prediction 2014). Viimane omakorda süvendab krüptorahaga spekuleerimist. *Bitcoin*'i tavapärase kasutamise mõjutamine (hinnaga spekuleerimine, suure tootluse lubamine või kunstlikult suurema nõudluse tekitamine) võib lõpuks realiseeruda *bitcoin*'i kasutajate huve kahjustavalt. Näiteks Coinbase'i põhjal võiks öelda, et spekulantide ja n.ö igapäevaste maksete tegijate osakaalud on vastavalt 80% ja 20%.

Krüptoraha süsteemi üheks nõrgimaks lüliks on siiani peetud nn vahetusplatvorme ehk börse. Börside turvanõrkused kahjustavad teenuse kasutajate ning kokkuvõttes kogu *bitcoin*'i süsteemi huve. Tuntuim näide on Mt.Gox nimelise vahetusplatvormi sulgemine (sisuliselt pankrot) Jaapanis, mille legendi järgi põhjustas ülekannete mõjutatavus (*transaction malleability*). Valdkonda pikaajaliselt uurinud Austria teadlased aga

[23] Ühe sisendi maht on u 200 baiti ja 1 väljundi maht u 50 baiti. Näiteks 3 allikast pärineva raha, mis omakorda kantakse 3 adressaadile, ülekandmine maksaks selle arvutuse kohaselt 5 USA senti (kogumaht alla 1 kB).

väidavad, et ülekannete mõjutatavusest võis kaduma minna kuni 400 *bitcoin*'i[24], mitte 850 000, nagu Mt.Gox teavitas. Vahetusplatvormide tööd halvavad oluliselt ka DDoS rünnakud (*distributed denial of service attacks).* Lisaks tuuakse börsidega seoses välja probleeme nende juhtimise ja klienditeenindusega. Börsid ei ole lihtsalt võimelised haldama kogu kliendimassi, mis on viimase aastaga tekkinud. Kuna krüptorahabörsid pole õiguslikult reguleeritud ega allu finantsjärelevalvele, on börsiomanike taust sageli hägune või nad on lausa anonüümsed.

Olulise nõrkusena nimetatakse sageli ka rahakoti lahendusi. Rahakotiga on seotud privaatvõtmete ehk turvakoodide haldamine, mille turvalisusele peavad tähelepanu pöörama nii vastavate lahenduste arendajad kui ka kasutajad. Eelkõige kasutatakse pahavara, mis otsib inimeste arvutitest *bitcoin*'i rahakotte ning turvakoode, mille abil *bitcoin*'id „rahakotist ära varastada". Kõige rohkem on ohustatud võrguühendusega rahakotid – näiteks koduarvutis, tahvelarvutis või mobiiltelefonis asuvad rahakotid. Kaspersky avaldatud hinnangute kohaselt tehti 2013. aastal rahakottidele 6 miljonit rünnet ja tuvastati 1 miljon kannatanut (2012. aastal kandis 600 000 rahakotiomanikku kahju) (6-million-bitcoin-wallets-attacked-2013). Samas ei saa kindlalt väita, et veebilahenduste puhul on kasutusel kõikjal vajaliku tasemega kaitsemeetmed, nagu näitas meile inputs.io lugu (inputs.io). Kõige turvalisem on hoida oma *bitcoin*'i aadressi privaatset võtit *offline* seadmel või isegi paberil.

Suurim diskussioon toimub anonüümsuse teemadel. Ka palju eksperte on seisukohal, et süsteemi kasutavate klientide identifitseerimine ja AML (*anti-money laundering*) nõuete täitmine aitaks vähendada riske. *Bitcoin*'i süsteemile peale ehitatavate teenuste puhul võib klientide identifitseerimine muutuda kriitiliseks vajaduseks. Samas ei ole anonüümsust kasutatud ainult pahatahtlikel eesmärkidel, näiteks on inimesed suutnud krüptoraha tehingute anonüümsuse abil oma raha totalitaarsete riikide kontrolli alt välja tuua.

Unustada ei saa ka kogu Bitcoini süsteemi pahatahtliku ümberkorraldamise võimalusi. Eksisteerib reaalne risk, et keegi saavutab kontrolli rohkem kui 50 % arvutusvõimsuse üle ja korraldab nn „51% rünnaku" ehk muudab ühepoolselt kogu süsteemi toimimist. Suurema tõenäosusega võivad sellise võimekuseni jõuda ühiskaevandajad ning nende koordineerijatel tekib võimalus soovi korral muuta kogu Bitcoini süsteemi avalikku raamatupidamisregistrit. Samas seab aga see koheselt ohtu kogu süsteemi usaldusväärsuse kasutajate ees ning see on nagu saagida oksa, millel ise istutakse.

Bitcoini süsteemi enda nõrkustest tulenevatele riskidele lisanduvad välise keskkonna tekitatud riskid. Bitcoini süsteemist arusaamine eeldab sügavaid teadmini krüptograafias, mis paljudel kriitikutel kahjuks puuduvad. Üks

[24] Malleability' attacks not to blame for Mt. Gox's missing bitcoins, study says; Breaking: Evidence That Transaction Malleability Did Not Bankrupt Mt. Gox. *However, while MtGox claimed to have lost 850,000 bitcoins due to malleability attacks, we merely observed a total of 302,000 bitcoins ever being involved in malleability attacks. Of these, only 1,811 bitcoins were in attacks before MtGox stopped users from withdrawing bitcoins. Even more, 78.64% of these attacks were ineffective. As such, barely 386 bitcoins could have been stolen using malleability attacks from MtGox or from other businesses. Even if all of these attacks were targeted against MtGox, MtGox needs to explain the whereabouts of 849,600 bitcoins.*

enamlevinud on Bitcoini süsteemi kahtlustamine nn Ponzi skeemi kasutamises[25], mis kahtlemata ei ole tõene väide. Kuna pangad on üldjuhul Bitcoini süsteemi suhtes skeptilised kui mitte tõrjuvad, on krüptoraha tavavaluutaks vahetamine kohati keeruline ning pole haruldane, et pangad blokeerivad ülekandeid krüptosaitidele. Eelnevale saab lisada sageli esineva riikide tõrjuva või vaenuliku seisukoha või seisukoha puudumise. Eriti oluline on riikide seisukoht tehingute maksustamise suhtes.

Arvestades, et krüptorahal on väärtus ainult niikaua, kuni inimesed seda usaldavad ja selle järele on nõudlus, peab süsteem olema usaldusväärne. Protokollis ja tarkvaras tuleb kõik avastatavad vead kiiresti kõrvaldada. Samuti tuleb otsida lahendusi vahetuskursi stabiilsemaks muutmiseks. Täiendavalt tuleks tegeleda riskidega, mis tulenevad sellest, et *bitcoin*'i atraktiivsus muudab aktiivseks kurjategijad, kes tahavad ära kasutada inimeste usaldust (ostu-müügi ja spekuleerimise kaudu) või selle üldist anonüümsust (rahapesu kaudu).

5 Krüptoraha näited ja seotud teenused

Krüptoraha näited

Esimene krüptoraha – *bitcoin* – on jätkuvalt suurima kasutajaskonna ja turuväärtusega krüptoraha.

Kasutajaskonnalt ja turuväärtuselt teine[26] – *litecoin* – kasutab tehinguploki moodustamisel mitte SHA-256 algoritmi nagu *bitcoin*, vaid *scrypt* algoritmi.

Turul 6. kohal olev NXT (varem ka *nextcoin*) krüptoraha (Nextcoin; NXT Community) kasutab tehinguploki moodustamisel *proof of work* asemel *proof of stake* meetodit.

Turul 7. kohal oleva, *bitcoin*'i plokiahela peale ehitatud *mastercoin*'i protokoll võimaldab igasuguse vara haldust ja sellega seotud tehinguid, hajuslepingute sõlmimist ja haldamist (Distributed Contracts), samuti (alates 15. märtsist 2014) detsentraliseeritud börsiteenust (Mastercoin).

Uudse kontseptsiooniga toodi turule *litecoin*'i kloon *auroracoin*, mille kogumahust 50% oli eelkaevandatud jagamiseks Islandi kodanikele.

Auroracoin'i väljakuulutamisele 2014. aasta veebruaris järgnes riigikesksete krüptorahade väljakuulutamise buum: *spaincoin* (Hispaania), *PLNcoin* (Poola), *cataloniacoin* (Kataloonia), *aphroditecoin* (Küpros), *ukracoin* (Ukraina). Nendest ainsatena on praeguseks jõudnud krüptoraha emissioonini *auroracoin* ja *spaincoin*.

Auroracoin'i jagamine Islandi elanikele algas 25. märtsil 2014. Esialgu pälvis *auroracoin* oma uudse lähenemisega suurt huvi, mida näitas ka börsihinna

[25] Näiteks süüdistas U.S. Securities and Exchange Commission 2013. aasta suvel üht *bitcoin*'e vahendavat ettevõtet Ponzi skeemis (SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme).
[26] *Litecoin*'i turuväärtus on 19 korda väiksem *bitcoin*'i turuväärtusest.

30-kordne tõus 3,2 dollarilt 97 dollarini 5 päeva jooksul pärast kauplemise algust 27. veebruaril 2014, sealt alates on aga hind olnud pidevas languses, olles hetkel vaid 0,5 dollarit.

Spaincoin startis 12. märtsil 2014 ja selle kogumahust 50% jagatakse etapiviisiliselt Hispaania kodanikele. Börsil on *spaincoin* käitunud sarnaselt *auroracoin*'ile: hind on kukkunud 500 korda. *Spaincoin*'i praeguse turuhinna juures saab iga Hispaania kodanik *spaincoin*'e 0,15 eurosendi väärtuses. Islandi elanikel on läinud paremini – praeguse turuhinna juures on nad saanud *auroracoin*'e 10,6 euro väärtuses.

Tundub, et teised *auroracoin*'i jäljendajad on hetkel kas ootel või on projekt lõpetatud.

Seotud teenuste areng

Järgnevalt käsitletakse mõningaid krüptoraha süsteemi toimimisega seotud teenuseid, samuti on toodud mõned näited, milliseid teenuseid on ehitatud krüptoraha süsteemi peale ehk teiste sõnadega: milliseid uusi teenuseid krüptoraha süsteem võimaldab arendada.

Kõige stabiilsemaks ja kasumlikumaks peetakse riistvara tootjate äri. Juba praegu ei ole tavaarvuti arvutusvõimsusega üldjuhul võimalik krüptoraha kaevandada. Nõudlus spetsiifiliste kaevandamistööriistade järele suureneb[27].

Krüptoraha genereerimise teenus on kergesti kättesaadav[28]. Saab võtta *bitcoin*'i, *litecoin*'i vm krüptoraha avaliku netis kättesaadava lähtekoodi, seda soovitud parameetrite osas modifitseerida, lähtekood kompileerida, genereerida tekkeplokk – ja krüptoraha ongi valmis. Seejärel tuleb raskem osa: tekitada kaevandajate, börside, kasutajate ja kaupmeeste huvi.

Suur nõudlus on ka krüptoraha soetamist võimaldavate teenuste – kaevandamise ja ostmise järele. Seejärel vajatakse kohe krüptoraha hoidmise ehk rahakoti teenust. Kasutusel on mitut tüüpi rahakotte, näiteks spetsiaaltarkvara abil arvuti kõvakettale installeeritud rahakotid, mobiilirakendused ja veebipõhised teenused, samuti on turvavõtmest võimalik teha koopiaid, mida saab endale e-kirjaga saata, salvestada teisele seadmele või paberile trükkida.

Kaupmeeste arv, kes *bitcoin*'e aktsepteerivad, on tasapisi kasvamas. Näiteks pakub veebilehe UseBitcoins vahendusel teenust 2551 *bitcoin*'iga seotud äri (Use Bitcoins). Tehniliselt on *bitcoin*'iga maksmine võrdlemisi lihtne – eriti Eesti elanikele, kes on harjunud avatud võtme infrastruktuuri kasutades digitaalallkirja andma.

Kaupmeestele omakorda pakutakse *bitcoin*'ide aktsepteerimiseks erinevaid võimalusi nii internetis kui ka poes kohapeal maksete vastuvõtmiseks. Arvestades *bitcoin*'i väärtuse (vahetuskursi) volatiilsust, võimaldatakse lahendusi, kus ostu hetkel vahetatakse *bitcoin*'id koheselt näiteks eurodeks. Nagu juba öeldud, ei saa tulevikus välistada tavapäraseid vahendustasusid,

[27] Ka ajaloos tuntud kullapalaviku ajal oli parim äri "labidate müük".
[28] Näiteks Coingen (hind 0.05BTC = 30USD) ja Coincreator (hind 0.075BTC = 45USD), mille kaudu 17.03.2014 kell 23.15 seisuga oli tehtud 299 uut raha.

kuid esialgu vahendustasud kas puuduvad või on minimaalsed. Näiteks Coinbase pakub kuni miljoni dollari ülekandmisel 0 %-st vahendustasu, edasi oleks ülekandetasu kuni 1 % (Coinbase Merchants).

Kaasatud ekspertide arvates on – arvestades maksete kiirust ja ülekandetasude puudumist või väiksust – kõige perspektiivikam arendada krüptoraha süsteemil põhinevaid **mikromakseid**.

Bitcoini süsteemi kasutavatest teenustest on levinum oksjoniteenus[29]. Müüdavate kaupade valik on lai.

Mitmete teenuste puhul võib klientide identifitseerimine muutuda kriitiliseks vajaduseks.

Mõned näited Bitcoini protokolli kasutavatest või selle edasiarendustega tekkivatest teenustest:

- Ethereum – *bitcoin*'i-rahaga kaudselt seotud, oma plokiahela peale ehitatud tarkvaraarenduse platvorm, mis võimaldab realiseerida rakendusi nagu digitaalsed lepingud, detsentraliseeritud börsid ja detsentraliseeritud domeeninimede haldus (Ethereum);
- BitID – detsentraliseeritud kasutajate autentimislahendus (Secure Bitcoin Alternative);
- BTProof - ajatemplirakendus, mis võimaldab näiteks loodud loomingu andmestruktuurile peale panna ajalise kinnituse, et see asi on sellel ajahetkel loodud (Btproof).

6 Krüptoraha areng

Tehnoloogiline: Bitcoin 2.0

Bitcoin'i nurgakivi – plokiahel – on kohandatav ja rakendatav igat tüüpi vahetuseks, sõltumata sellest, kas see on seotud rahaga või mitte (Bitcoin 2.0).

Bitcoini protokoll võimaldab emiteerida igat sorti väärtpabereid (aktsiad, võlakirjad, uued valuutad), teha nendega tehinguid ja kaubelda igasuguse muu varaga, mille omandisuhe on registreeritud plokiahelas (*smart property*). Plokiahelas omandi registreerimine ja tehingute tegemine vähendab pettusi, vahendustasusid ja võimaldab tehinguid, mida muidu oleks raske teha. Näiteks võivad üksteisele võõrad inimesed laenata omavahel raha, andes tagatiseks plokiahelas registreeritud vara.

Mastercoin ja ColoredCoins on projektid, mille eesmärgiks on kasutada *bitcoin*'i plokiahelat igasuguse vara halduseks ja sellega seotud tehingute tegemiseks, nende protokollidesse sisseehitatud detsentraliseeritud börsiteenuse ning hajuslepingute sõlmimise võimaldamiseks.

[29] Näiteks: Bitcoin Forum Auctions; Blockrun Bitcoin Auctions; CryptoThrift.

NXT on krüptoraha, mille protokolli on sisse ehitatud võimalused luua detsentraliseeritud börs, hääletussüsteem, detsentraliseeritud domeeni-nimede süsteem (DNS). NXT kasutab plokkide loomisel *proof of stake* algoritmi – plokke ei kaevandata, vaid kasutatakse olemasolevaid kasutajakontosid plokkide tekitamisel.

Bitshares X, detsentraliseeritud pank ja börs, võimaldab kasutajal hoiustada, laenata ja kaubelda raha ning muude finantsinstrumentidega ilma selliste vahendajateta nagu pank või maaklerfirma. Transaktsioonid tehakse kasutajate arvutite võrgus ja verifitseeritakse avalikult, tehes varguse ja pettuse võimatuks. Bitshares X debüteerib 2014. aasta teises kvartalis.

Sotsiaalse suunitlusega projektid

Tavapäraselt, lisaks teaduslike ja majanduslike huvide realiseerimisele ning spekuleerimisele, on tekkinud ka sotsiaalse suunitlusega projektid.

Kuigi pikemas vaates on ilmselt tegemist majanduslike huvide realiseerimisega, võib sotsiaalse suunitlusega projektide hulka lugeda ka riigi elanike kasuks eelkaevandamise, mis algas (eelkirjeldatud) *auroracoin*'i turule tulekuga. Eesmärgiks on suurendada krüptoraha kasutajate hulka, mis suurendab nõudlust turul, samal ajal ei saa alahinnata sellega kaasnevat elanike teadlikkuse tõusu nii krüptoraha olemasolu kui ka selle kasutamisvõimaluste ning turvariskide kohta.

Krüptoraha *ripple* koguemissioonist 55% jagatakse heategevusorganisatsioonidele ja Ripple'i heategevusprojektides osalejatele. Kuni 1. maini 2014 oli Ripple'i heategevusprojektiks Computing for Good (Computing for Good), milles osalejad jagasid oma arvutiressurssi vähiuuringuteks (Mapping Cancer Markers) ja puhta energia projektile (The Clean Energy Project) ning said vastutasuks krüptoraha *ripple*.

H2Ocoin on heategevuslik krüptoraha, mille eesmärk on toetada arengumaades puhta vee tagamise projekte Charity Water (Charity Water), The Water Project (The Water Project) jt.

Massachusettsi Tehnoloogiainstituudi (MIT) üliõpilastele jagatakse 2014. aasta sügissemestril igaühele 100 dollari väärtuses *bitcoin*'e. Projekti algatas MIT-i Bitcoiniklubi, mis on kogunud selleks otstarbeks juba 500 000 dollarit.

7 Mida võiks Eesti riik teha?

Kuigi ekspertide hinnangud selles osas jagunesid seinast seina alates riigiemissioonist[30] (esimesena maailmas) ja lõpetades soovitusega „käed eemale" (riik loogu ainult keskkond) oldi ühel meelel, et riik peaks krüptoraha valdkonnaga professionaalselt ja tasakaalustatult tegelema.

[30] Näiteks: Valuutakomitee süsteemil fikseeritud kursiga krüptoraha, mille garandiks on riik. Kristo Käärmann.

Krüptoraha on seni „mahutatud" olemaolevasse õigusruumi, kuhu see ei sobi oma uute tunnuste tõttu. Eksperdid arvasid, et juba sõna „raha" on kohati eksitav, sest tegemist on palju enamaga kui raha. Oleks kasulik, kui terminoloogiliselt eristuksid krüptoraha süsteem ning selles kasutatav vahetusühik. Hetkel kasutatakse sõnu „krüptoraha" või „*bitcoin*" nii avaliku raamatupidamise, vahetusühiku kui ka süsteemi peale ehitatavate uute teenuste kohta.

Krüptoraha kogukonna (kiired) ootused

Krüptoraha kogukonna jaoks on (!) oluline sõnum, mida riik teadlikult või mitteteadlikult edastab. Nagu eespool öeldud, tajub kogukond riigi seisukohta pigem negatiivsena. Entusiastid loodavad, et rahvusvaheliselt tuntud Eesti e-tiiger võtab innovaatilise krüptoraha suhtes toetava seisukoha.

Samas on entusiastide ootused „riigiabi" suhtes kohati – pehmelt öeldes – ebarealistlikud. Esialgu kaasneb krüptoraha süsteemiga, nagu iga innovatsiooniga, äririsk, mille riigi poolt täies mahus maandamine ei ole realistlik või lihtsalt võimalik. Majandus- ja Kommunikatsiooniministeeriumi asekantsler Taavi Kotka väljendas ministeeriumi ootusi, et ettevõtjad muutuvad ise ka selles ärivaldkonnas aktiivsemaks, väljendades valmisolekut panustada vastava tegevuskeskkonna arendamisse.

Kogukonna suurim ootus on läbimõeldud maksustamine. Suurbritannia eeskujul loodetakse, et enne põhjalikke analüüse ja diskussioone vabastatakse ka krüptoraha ülekanded käibemaksust.

Kogukonna suurim ootus on läbimõeldud maksustamine. Suurbritannia eeskujul loodetakse, et enne põhjalikke analüüse ja diskussioone, mis võivad väärtuslikku aega võtta, vabastatakse ka krüptoraha tehingud käibemaksust. Teine kiiret lahendust vajav regulatsioon on rahapesu ja terrorismi rahastamise tõkestamise seaduses olev alternatiivsete maksevahendite definitsioon, kus tuleb krüptoraha eraldi ära määratleda ning defineerida. Praeguse seaduse järgi on mõistlikul, heatahtlikul ja ausal viisil krüptorahadega majandamine kriminaalkorras karistatav.

Vaadates tulevikku

Iga uue innovatsiooni rakendamine igapäevaellu nõuab elanike teadlikkuse tõstmist.

Eesti elanikke ei tule õhutada krüptoraha kasutama, küll aga tuleks neile anda sellest teadmisi. Aega, mil toimub krüptoraha „metsik" arendamine, tuleb kasutada selleks, et õigusruumi jm keskkonda, samuti elanikke, krüptoraha ajastu jaoks ette valmistada.

Nii nagu Eesti on aktiivne ja üks eestvedajaid internetivabaduse säilitamisel ja rahvusvahelise koostöö tagamisel, nii võiks Eesti kaaluda aktiivsemat rolli ka rahvusvahelises ulatuses. Krüptoraha kogukonna üks liidreid Asse Sauga, kes on ka eestikeelse krüptoraha veebilehe asutaja, omanik ja haldaja,

esitas Arengufondi ideedekonkursile ettepaneku arendada Eesti krüptoraha eestvedajaks maailmas (Arenguidee). Tulevikus – miks ka mitte?

Kui 90ndatel aastatel alustati „Tiigrihüpet" koolidest, siis krüptoraha „Krüptohüpe" võiks toimuda kõrgkoolide tasemel. Tulevikule mõeldes ja eespool kirjeldatud Massachusettsi Tehnoloogiainstituudi (MIT) Bitcoiniklubi eeskujul võiks Eesti riik toetada üliõpilaste *bitcoin*'i-klubi loomist ja tegutsemist.

Tulevikule mõeldes on kõige tähtsam Eesti ettevõtjate toetamine krüptoraha valdkonnaga seotud teenuste arendamisel. Tuleb esitada küsimus, miks krüptoraha turule toodi ehk mida sellega lahendada taheti. Protestivaimuga põhjendamisest jääb sellise uue ja suure fenomeni kirjeldamisel väheks.

Ärisektorile on omane liikuda kulude optimeerimise suunas. Selliseid väljakutseid on krüptoraha valdkonnas palju. Toome siinkohal ainult ühe olulise näite – rahaülekannete tasu optimeerimine. Oleme Eestis harjunud, et suur osa makseid toimub ühe panga piires ja on seetõttu tasuta või marginaalse hinnaga. Suuremates riikides ja suurte firmade puhul, kus ülekanded toimuvad paljude pankade osalusel, annavad tasuta (või marginaalse tasuga) ülekanded märkimisväärse kokkuhoiu.

Kaugemale ette vaadates tuleks riigil kindlasti läbi mõelda ka võimalused ressursihalduse või sotsiaalse suunitlusega projektide käivitamiseks.

Lõppsõna

Nii nagu küsitletud Eesti ekspertidel oli erinevaid seisukohti, valitseb arvamuste paljusus ka arvamusliidrite hulgas ülemaailmses meedias (Is it Too Late to Get Involved in Bitcoin?).

Analoogselt Eesti infoühiskonna arengukavas aastateni 2020 ette nähtud infoühiskonnaalase seadusandluse korrastamisele ja täiendamisele (pidades samal ajal silmas, et seadusandlus peab innovatsiooni toetama, mitte seda liigse reguleeritusega pidurdama), peaks Eesti riik analüüsima ja täiendama krüptorahaga seotud õigusruumi, mis muuhulgas peab tagama nii andmekaitse kui ka intellektuaalomandi seadusandluse vastavuse infoühiskonna võimalustele ja vajadustele[31].

Selleks et säilitada Eesti e-riigi ja riigirahanduse head rahvusvahelist mainet, peaks Eesti riik valmistuma (kindlasti eelnevalt mitmeid transformatsioone läbi tegeva) krüptoraha ajastuks.

On muutunud lööklauseks, et krüptoraha on tulnud, et jääda. Kuna sellega on olnud nõus kõik uuringu käigus küsitletud eksperdid, on sobilik selle seisukohaga lõpetada.

[31] Eesti Infoühiskonna arengukava 2020.

Kasutatud mõisted ja lühendid

AML (Anti-Money Laundering) nõuded on rahapesu tõkestavad nõuded (vt FATF ja RahaPTS).

Avalik raamatupidamisregister (*public ledger*) ehk **tehinguplokkide ahel** *(block chain)* on krüptoraha tehinguplokkide kogum, mis kajastab kogu ringluses olevat ehk kaevandatud raha ja sellega tehtud tehinguid, aga samuti infot kõigi kontode kohta, millega krüptoraha on olnud seotud.

Bitcoin ehk krüptograafiline valuuta on Bitcoini süsteemi arveldusühik. *Bitcoin* omakorda jaguneb 10^8 *satoshi*'ks.

Bitcoini süsteem on B**itcoini protokolli** alusel loodud avatud lähtekoodiga tarkvara ja keskse osapooleta P2P-võrgustik, mille võrgusõlmed peavad koos andmebaasi, mis kajastab kõiki tehinguid ja *bitcoin*'ide kuuluvust adressaatidele ehk omanikele. Kui raharingluses ei ole võimalik jälgida konkreetsete pangatähtede liikumist, siis Bitcoini süsteem võimaldab jälgida iga *bitcoin*'i liikumist algusest lõpuni.

BTC on *bitcoin*'i tähis.

FATF (Financial Action Task Force) on valitsustevaheline rahapesuvastane töökond, mis arendab rahapesu ja terrorismi rahastamise vastast poliitikat ja tegevusi.

Kaevandaja (*miner*) on mistahes võrgukohas asuv isik, kes spetsiaalset riist- ja tarkvara kasutades moodustab mingite tunnuste alusel tehinguplokke. Selle keerukuse tõttu kasutatakse üldjuhul ASIC (*application specific integrated circuit*) riistvara ja avatud lähtekoodiga CGminer tarkvara.

Kaevandamine (*mining*) on protsess, mille käigus kaevandajad moodustavad juba kontrollitud tehingutest ülimat ressurssi nõudva arvutuse abil tehinguplokke ja saavad selle eest preemiaks ringlusesse lastavaid uusi *bitcoin*'e.

KMS on käibemaksuseadus.

Krüptoraha tekke- ehk esmaplokk *(genesis block)* on mistahes krüptoraha kõige esimene kaevandatud plokk.

LTC on *litecoin*'i tähis.

Peer-to-peer network **ehk P2P**. P2P-võrgustik ehk partnervõrk ehk võrdõigusvõrk, mille all infotehnoloogias ja sidetehnikas mõistetakse võrdsete õiguste ja võimalustega võrgusõlmede kogumit, milles iga osaline võib algatada sideseansi ning milles töö või ülesanded jaotatakse osalejate vahel ära.

Rahakott moodustub krüptoraha omaniku identifitseerimist võimaldavatest digitaalsetest tõenditest, mida kasutades omanik pääseb oma rahale ligi ja saab sellega teha tehinguid. Omanikul võib olla mitu rahakotti. Muus osas võrdlust füüsilise rahakotiga kasutada ei saa – *bitcoin*'i rahakotis ei hoita raha.

Bitcoini süsteemis kasutatakse avaliku võtme krüptograafiat. Omaniku iga rahakotis oleva aadressiga seostub nii avalik kui ka privaatvõti (turvavõti). Avalikust võtmest tuletatud aadressi võib mõista kui konto numbrit ja see

pole salajane. Iga konkreetne *bitcoin* kuulub mingile aadressile. Privaatvõti on pikk numbrite ja tähtede jada, mida peab teadma ainult rahakoti omanik. Kui omanik unustab või kaotab privaatvõtme, kaotab ta võimaluse oma raha kasutada, samuti ei saa seda raha kasutada keegi teine. Privaatvõtit tuleb hoida turvaliselt ja kaitsta varguse eest, et selle abil ei oleks võimalik krüptoraha varastada.

Kasutusel on mitut tüüpi rahakotte, näiteks spetsiaaltarkvara abil arvuti kõvakettale installeeritud rahakotid, mobiilirakendused ja veebipõhised teenused, samuti on turvavõtmest võimalik teha koopiaid, mida saab endale e-kirjaga saata, salvestada teisele seadmele või paberile trükkida.

MERAS on 22. jaanuaril 2010 jõustunud makseasutuste ja e-raha asutuste seadus, mis reguleerib makseteenuste ja e-raha teenuste osutamist, makseasutuste ja e-raha asutuste tegevust ja vastutust ning järelevalvet nende asutuste üle.

RahaPTS on 28. jaanuaril 2008 jõustunud rahapesu ja terrorismi rahastamise tõkestamise seadus, mille eesmärk on tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks.

Tehinguplokk on kontrollitud ja kinnitatud tehingute kogum.

Tehinguploki moodustamine (*proof of work*) on kontrollitud, aga seni veel tehinguplokki lülitamata tehtud tehingute andmetega läbi viidud krüptograafilisel algoritmil põhineva arvutuse tulemus (räsi), mis peab vastama Bitcoini protokolliga etteantud reeglitele. See arvutus peab kogu kaevandajate võrgustikul võtma aega u 10 minutit. Kui ilmneb, et kaevandamine võtab rohkem aega, vähendab protokoll automaatselt arvutuse keerukust. Vastupidisel juhul toimub arvutuse keerukuse suurendamine. Kuna tehing loetakse piisava usaldusväärsusega kinnitatuks, kui see asub 6 ploki sügavusel, siis tagab 10 minuti reegel usaldusväärse kinnituse u 1 tunni jooksul. Samuti näeb algoritm ette, millised tehingud on kõrgema prioriteediga ja mis tuleb tehinguplokkidesse kaasata eelisjärjekorras. Näiteks on kõrgema prioriteediga suuremate summadega tehtavad tehingud ja tehingud *bitcoin*'idega, millega pole pikemat aega tehinguid tehtud. Väikesed, tehingutasuta tehingud võivad pikka aega tehinguplokkidesse lülitamist oodata.

TuMS on tulumaksuseadus.

Võrgusõlm (*node, network node) on* arvuti, mis on võrgus ja mis osaleb kaevandamisel ja/või tehingute tegemisel.

Ühiskaevandamine (*mining pool*) on kaevandamisel toimuv kaevandajate ühistegevus, mille eesmärgiks on arvutusressursside koondamise teel suurendada uute *bitcoin*'ide teenimise võimalusi, mis omavahel jagatakse vastavalt kokkulepetele[32]. Ühiskaevandamiseks on loodud ka pilvelahendusi, mis võimaldavad inimestel osta kaevandusettevõttelt arvutusressurssi, mis hakkab talle *bitcoin*'e teenima[33].

[32] Näiteks eligius
[33] Näiteks cex.io, ghash.io/

Allikad

Davis

Google Trends

ID

Eesti Panga kommentaar

Hans Lõugas. Ettevaatust: bitcoiniga kaubitsemine võib teile kraesse tuua kriminaalasja. Eesti Päevaleht, 07.05.2014.

Eestis osteti Bitcoinide tulu eest mõis

Konverents

I

History of Bitcoin

Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

Adam L.Penenberg. The Bitcoin Crypto-Currency Mystery Reopened

Joshua Davis. The Crypto-Currency

Rob Wile. Still Nobody Knows Who Created Bitcoin - But There Are A Few Bif Theories

Bitcoin.org

Bitcoin Foundation.org

Bitcoin 2014

Pete Rizzo. Bitcoin Foundation Sets record Straight on New UK Office

II

Number of Transactions per Block

Blockchain

Forbes - Bitcoin Mining Uses Electricity

Map of Coins

Coin Calender

Com-HTTP

Crypto-Currency Market Capitalizations

Bitcoin Price Prediction 2014

III

ECB. Virtual Currency Schemes. October 2012

BitLegal

Regulation of Bitcoin in Selected Jurisdictions

Britain to scrap VAT on Bitcoin trades

Federal-reserve-bitcoin-potential-boon

European Central Bank warns of virtual currency risks
ECB. Virtual Currency Schemes. October 2012,
Warning to consumers on virtual currencies
EBA Consumer Trends. Report 2014
Eesti Panga kommentaar
Rahandusministeeriumi 04.03.2014 vastus AS Tavid teabenõudele
Maksu- ja Tolliamet. Maksustamine Bitcoin'dega kauplemisel
Rahapesu andmebüroo juht Aivar Paul bitcoinidega seonduvast
Makseasutuste ja e-raha asutuste seadus
Rahapesu ja terrorismi rahastamise tõkestamise seadus
Käibemaksuseadus
Tulumaksuseadus
IV
Bitcoin Price Prediction 2014
Crypto-Currency Market Capitalizations
Malleability' attacks not to blame for Mt. Gox's missing bitcoins, study says
Breaking: Evidence That Transaction Malleability Did Not Bankrupt Mt. Gox
SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme
V
Bitcoin
Bitcoin wiki
Wikipedia: History of Bitcoin
Wikipedia: Bitcoin
Bitcoin Cryptocurrency Crash Course with Andreas Antonopoulos
Byron Gibson. Bitcoin & the Byzantine Generals Problem 22.03.13
Top of Mind. All about Bitcoin 11.03.14
BTC.ee - Your source of Bitcoins in Tallinn, Estonia
Bitcoin 2.0
6-million-bitcoin-wallets-attacked-2013
inputs.io
Nextcoin
NXT Community
Distributed Contracts
Mastercoin
Ripple

Litecoin
Auroracoin
Spaincoin (spaincoin.org)
Coingen
Coincreator
Use Bitcoins
Coinbase Merchants
Bitcoin Forum Auctions
Blockrun Bitcoin Auctions
CryptoThrift
Ethereum
Secure Bitcoin Alternative
Btproof
VI
Bitcoin 2.0
VII
Arenguidee
Eesti Infoühiskonna arengukava 2020
Is it Too Late to Get Involved in Bitcoin?
Wikipedia
Wikipedia: Cryptocurrency
Wikipedia: History_of_Bitcoin
Wikipedia: Bitcoin
Wikipedia: Ripple_(payment_protocol)
Wikipedia: Litecoin