BITCOINI JA ALTCOINIDE TULEVIK VALUUTA, PLOKKAHELAPÕHISTE PROTOKOLLIDE KOMMUNIKATSIOONI TOKENITENA NING FINANTSEERIMISELEMENTIDENA (IOC-D): MÕNED KRIITILISED ANALÜÜSID PLOKKAHELA KASUTUSTE KOHTA[1]

Wolfgang Eibner
Kurt Rätzsch, Antonio Schulz, André Rolapp
Ernst-Abbe-Hochschule Jena [2]

1 Krüptovaluutad

1.1 Visioon ja tööhüpoteesid

Digitaalse valuuta idee, mis võimaldab anonüümseid rahatehinguid, ei ole midagi uut. Juba 1999. aastal oli Milton Friedmanil ettekujutus internetis raha ülekandmise kohta punktist A punkti B, ilma et tehingupartnerid teineteist tunneksid või et tehingust jääks järele dokumentatsioon selle kohta, kust raha tuleb. [5, intervjuu, tsitaat ajal 14:40 jj.] 2008. aastal avalikustas Satoshi Nakamoto pseudonüümi all tänaseni tundmatu autor lühiülevaate „Bitcoin: A Peer-to-Peer Electronic Cash System" [10, Ik1], mida loetakse virtuaalse valuuta „bitcoin" alusdokumendiks. Nakamoto kirjeldab maksesüsteemi, kus pole vahendajaid, kes toimiksid usaldusväärsete töötlusasutustena. See kirjeldab süsteemi, mis asendab usalduse krüptograafilise tõendiga ning võimaldab kahel partneril vahetult ning vahelülideta teineteisega kaubelda.

Tänu krüptograafilisele tõendile ja võrgus osalejate konsensusele ei ole finantsasutusi enam vaja. Kõigil osalejatel on võrdsed õigused, mistõttu on neil samad andmekogud. Selline jaotatud võrk on maksimaalselt detsentraliseeritud erinedes tsentraliseeritud võrgust, mis on olemas näiteks andmebaasil, või detsentraliseeritud võrgust, mida realiseeritakse näiteks pilves erinevate andmetöötluskeskuste kaudu.

Erinevalt harilikest nn fiat-valuutadest ei käi krüptograafiliselt krüptitud krüptovaluutad kesksete asutuste (nt keskpanga) reguleerimise ja kontrolli alla, vaid neid väljastavad harilikult ainult juriidilised isikud teatud raamides. [Ladinakeelsest sõnast „fiat" (= saagu) tuletatud mõistega fiat-valuutad tähistatakse kõiki moodsaid, katteta valuutasid, mis alluvad keskpanga või kommertspankade väärtusloomele.]

Kuid harilikel valuutadel ja krüptovaluutadel on oluline ühine omadus: nende väärtuse määrab nn kasutusväärtus või usaldus, mis antakse asjakohasele (makse)vahendile. Seda

[1] Artikli täistekst „On the Future of Bitcoin and Altcoins as Currencies, Tokens for Smart Contracts, and Instruments of Commitment (IOCs): Some Considerations Regarding Blockchain Applications" asub publikatsiooni CD-l.

[2] Prof. Dr. rer. pol. Wolfgang Eibner, FB Wirtschaftsingenieurwesen – Department of Industrial Engineering, Ernst-Abbe-ülikool Jena, Carl-Zeiss-Promenade 2, 07745 Jena, Saksamaa, Wolfgang.Eibner@eah-jena.de.

Ettekande koostamisele aitasid kaasa candes. M.Sc. majandusinsener Kurt Rätzsch, Antonio Schulz, André Rolapp ning stud. B.Sc. majandusinsener Marie-Therese Kiontke.

usaldust võimaldav krüptovaluutade tehnoloogia on plokkahel. Seetõttu vaadeldakse seda alljärgnevalt lähemalt.

Nagu Hausse seda nn krüptoturul, eriti just ajavahemikus 2017. aasta septembrist kuni detsembrini, demonstreeris, on plokkahel ja sellest genereeritud maksevahenditega seotud uuendused paljude, eriti just noorte inimeste jaoks unistuseks detsentraliseeritud otsuste ja riigist ning pankadest sõltumatute väärtustehingute kohta.
Alljärgnev analüüs baseerub kahel kesksel tööhüpoteesil, mida alljärgnevalt kontrollitakse.

Tees 1: „Privaatsete krüptovaluutade kasutamine alternatiivse maksevahendina ei ole lähemas tulevikus veel mõeldav."

Tees 2: „ICO-d muutuvad järjest enam alternatiiviks traditsioonilistele riskikapitalirahastustele ning tokenitest saavad ajendid, millele tuginedes ehitatakse üles nutikate lepingutega detsentraliseeritud infrastruktuur."

1.2 Plokkahel ja plokkahelapõhiste protokollide kommunikatsioon

Plokkahel on uuenduslik teooria andmetehingute verifitseerimiseks. Selles toimub tehingu infot sisaldavate andmeplokkide lineaarne, kronoloogiline järjestamine.
Plokkahela tehnoloogiat tajutakse turvalise ja eriliselt veakindlana. Sellel on potentsiaal lahendada usaldusprobleem üksikute väärtust loovate partnerite vahel seoses rahalise väärtusega tehingute, andmevahetuse ja lepingute sõlmimisega.

Bitcoini või altcoini ühikute kandmiseks erinevate nn „rahakottide" vahel tuleb esmalt luua tehingusõnum. See tehinguteade jõuab nüüd bitcoini võrgustiku aktiivsete osalejateni, kes kontrollivad sissetulevaid tehinguteateid krüptograafiliste algoritmidega ning koondavad need andmeplokki.

Aktiivsete võrgus osalejate edasiseks funktsiooniks on tehingute andmeplokiks koondamise järel lahendada arvutusülesanne „katse-eksituse-meetodil". Õnnestumise korral kontrollivad osalejad vastava aktiivse osaleja värskelt loodud plokki, nn „Miner", uuesti kehtivuse suhtes ning see ühendatakse viimaks uusima plokkahela versiooniga nii, et summa hüvitamine toimub juba mõni minut pärast esimest kinnitust.

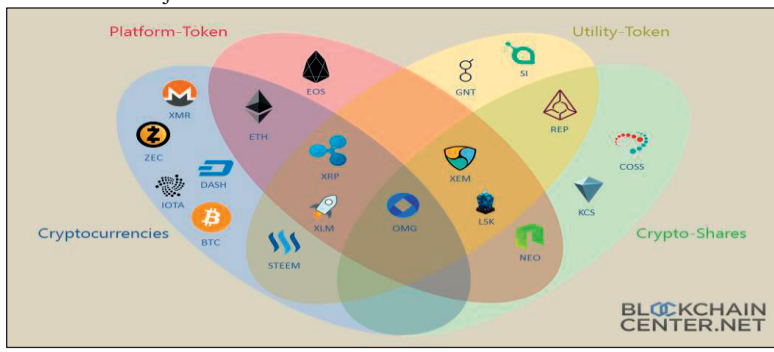
Plokkahela struktuur muudab tehnoloogia harilikest krüptimistehnoloogiatest oluliselt turvalisemaks. Selleks on protokolli lülitatud mitmeid turvamehhanisme.
Omavaheline üksikutele andmeplokkidele *viitamine* takistab minevikus olevate võrgutehingute hilisemat märkamatut manipuleerimist. Avaliku plokkahela kõigi tehingudetailide takistamatu ja täiemahulise *läbipaistvuse* omadus, nt ka saldo või „kontoseisud", ning teave ringluses oleva rahakoguse või bitcoinide arvu kohta tekitab võrgustiku suhtes usaldust ning võimaldab oma tehinguid pidevalt jälgida ja jälitada ning seda tänu *pseudonüümide kasutamisele* ilma, et neid oleks siiski võimalik konkreetsetele identiteetidele omistada. Võrgu *detsentraliseeritus*, mis tagab tehingute kontrolli ning hõlmab bitcoini puhul tuhandeid globaalselt jaotatud võrgustikusõlmi, tänu millele ei ole vaja kasutada usaldusväärset vahendajat. [12, lk 59 jj]

Vitalik Buterin laiendas 2004. aastal Nakamoto seisukohta ning lõi Ethereumiga plokkahelal baseeruva platvormi, mis võimaldab **plokkahelapõhiste protokollide kommunikatsiooni** (ka „nutikad lepingud“) detsentraliseeritud käsitlemist, mis moodustab omakorda nn „hajutatud rakenduste“ aluse.

Plokkahelapõhiste protokollide kommunikatsioon on kõige elementaarsemal tasemel programm, mis sisaldab analoogselt kirjalikult fikseeritud lepingutele teatud lepingutingimusi kõigi osalenud poolte kohta ning mis võivad käivitada (nt kliendipoolse) teenuse täitmisega lepingu täitmise. Niinimetatud tokenitega saab siis tasuda plokkahelapõhiste protokollide kommunikatsiooni raames turuteenuste eest ning nt ka masinatevaheliste teenuste kasutamise eest automaatselt, ilma inimliku juhtimiseta.

1.3 Krüptovaluutade vormid ja turukapitalisatsioon

Krüptovaluutade klassifitseerimine, nagu näiteks joonisel 1 toodu, on keeruline, kuna senini pole juurdunud ja üldtunnustatud terminoloogiat ning ühest tokenist võib piisata ka mitme nõude jaoks.



Joonis 1. Oluliste krüptovaluutade ülevaade [1]

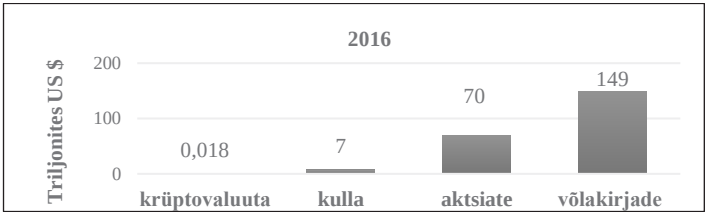
Platvormi tokenite kaudu luuakse lähtuvalt ühest olemasolevast infrastruktuurist, nagu näiteks Ethereum, uusi krüptovaluutasid näiteks plokkahelapõhiste protokollide kommunikatsiooni elluviimiseks.
Utiliidi-tokenite kasutusotstarve on seevastu leitav DApp-platvormil programmeeritud rakendustel. Neil on olemas eelnevalt selgelt defineeritud suvalise rakenduskeskkonna funktsioon, nt usalduspunktid.

Krüptoaktsiad, mida nimetakse ka security või equity tokeniks, esindavad teatud määral osa ettevõttest, võrgust või üksikust projektist, mis müüakse näiteks krüptorahal põhineval osakute esmapakkumisel (ICO) omakapitali loomiseks. **ICO-d** ei esinda aktsiatest erinevalt kaasomandit ning seega ka mitte hääleõigust ega õigust dividendidele.
Krüptorahal põhinevate osakute esmapakkumine toob endaga siiski kaasa keskseid eeliseid.

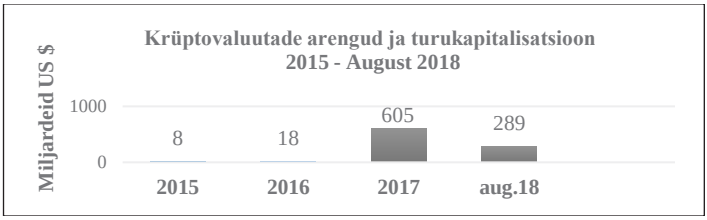
1. *Kapitali hankimisprotsessi lihtsustatakse võrreldes avaliku pakkumisega olulisel määral.*

2. *Enam ei ole vajadust mahuka oskusteabe järgi:* moodsad, intuitiivsed tööriistad ja veebirakendused võimaldavad projektil baseeruvate ICO-de rakendamist IT-alaste põhiteadmistega.
3. *Plokkahelal ja seega ka sellesse salvestatud plokkahelapõhiste protokollide kommunikatsioonil on muudetamatu, läbipaistev karakter:* alguses defineeritud pakkumus tokenile on muudetamatu ning ICO kogu lähtekoodiga nähtavalt kindlaks määratud.
4. *Laiem ligipääs investeeringuvõimalustele* tänu omakapitali soodsale hankimisele ICO-dega.

Joonisel 2 võrreldakse krüptovaluuta kapitaliseerimist turul kulla, aktsiate ja laenude puhul aastal 2016: joonisel 3 kujutatakse krüptovaluutade kapitaliseerimist turul aastast 2015 kuni 2018. aasta augustini.



Joonis 2. Ülevaade krüptovaluuta, kulla, aktsiate ja võlakirjade turu kapitaliseerumisest aastal 2016 [4,14]



Joonis 3. Krüptovaluutade arengud ja turukapitalisatsioon [2]

2 Kasutusalad

Plokkahela praegused peamised praktilised kasutusjuhud paiknevad finantssektoris. Ülevaade konkreetsetest plokkahelalahendustest teeb selgeks, et erinevad projektid jaotuvad järgmiste rakendusalade vahel.

1. Krüptovaluutad: plokkahelarakendust kasutatakse tehinguprotokollina erinevate krüptovaluutade puhul, nagu näiteks bitcoin (BTC), Ethereum (ETH) või Monero (XMR).
2. Ärivõrgustikud: plokkahelat kasutati plokkahelapõhiste protokollide kommunikatsiooni ja andmevahetuse puhul. Siinkohal kasutatakse Ethereumi eriti just nutikate lepingute rakendusena. Edasised näited on Hyperledger ja MultiChain.
3. Plokkahelapõhiste protokollide kommunikatsioon Asjade Interneti osalejate vahel, kes ei ole inimesed. Siin on edukaks tehnoloogiaks nt IOTA.

4. Pangandus: plokkahelat kasutatakse finantstehingute valdkonnas. Kõige tuntum kasutusviis on Ripple.

Plokkahela erinevate rakendusvaldkondade (lisaks finantssektori ja ühisrahastusele valdkonnas Asjade Internet, tarneahela haldus, riiklik haldus, keskkonnakaitse [9]) ning eriti just plokkahelapõhiste protokollide kommunikatsiooni põhjaliku kirjelduse leiate selle ettekande põhjalikust digitaalsest versioonist.

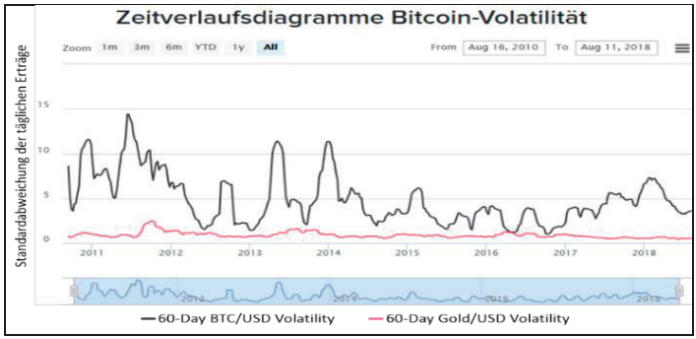
3 Krüptovaluutade kasutamisega seotud riskid

Krüptovaluutade kasutusriskid on mitmekülgsed ning neid jaotatakse selle ettekande digitaalses versioonis põhjalikumalt tehnilisteks, rahva- ja ärimajanduslikeks riskideks. Selles kokkuvõttes võetakse vaid kesksed rahva- ja ärialased aspektid lühidalt kokku.

3.1 Finantsturgude stabiilsus

Krüptovaluutad on spekulatsiooniriskide suhtes äärmiselt tundlikud, kuna siinkohal ei ole pakkumine ja nõudlus vähemalt senini enamasti kasutusega määratud, vaid on suunatud valdavalt investorite spekulatiivsetel tingimustel tõusvale või langevale huvile. Sellistest spekulatsioonilainetest tulenevad mõjud rahanduslikule stabiilsusele on seda tugevamad, mida kõrgemale tõuseb turu kapitaliseerimine ning seda tugevamalt on krüptoturud teiste finants- ja kapitalituru segmentidega seotud.
Hetkel on krüptovaluuta finantsturgude stabiilsuse jaoks pigem ebaoluline, nagu seda on näha joonisel 2 toodud turu kapitaliseerimise graafikult. See võib muuta ka krüptoväärtuste tähendust finantsturgudel. Finantsturu stabiilsuse puhul olulise rolli mängimine kujutab endast ka krüptovaluuta kõrget volatiilsust.

Joonisel 4 torkab selgelt silma bitcoini kursi tugev kõikumine USA dollari suhtes, vastupidiselt kulla ja USA dollari võrdlemisi stabiilsele kursile. Seda saab muuhulgas seletada üpris uue tehnoloogiaga seotud õhinaga. Jätkuv meediahuvi tõmbab ligi investoreid – mida tugevamini kurss tõuseb, seda suurem on huvi. Kasumivõtmisel läheb vaimustus üle, ning aset leiavad liiga suuremahulised ostud (kaasajooksikute poolt). Sealjuures võimendab krüptovaluuta puhul seda turukriisi suur hulk kogenematuid (väike)investeerijaid.



Joonis 4. USA dollari ja bitcoini ning USA dollari ja kulla volatiilsusindeks [16]

Lisaks on krüptovaluutaturud endiselt haavatavad massiivsete rünnakute suhtes, mh turu- ja kursimanipulatsioonid, nagu näiteks *double-spend*-rünnakud või *spoofing* ja *washtrade*-strateegia. Siinkohal tuleb viidata selle ettekande täielikule versioonile, mis käsitleb arvutusvõimsuse (hash rate) probleemi: nii on kuue suurima ühiskaevanduse (Mining Pool) osakaal kogu arvutusvõimsusest 78,7%, mis võimaldab ühelt poolt *double-spend*-rünnakuid; teisalt, kuna suurem arvutusvõimsus langeb Hiinale, võivad tulevikus tekkida poliitilise olemusega probleemid.

3.2 Rahvamajanduslikud – majanduslangusega seotud – riskid

Ka rahvamajanduslikud riskid on suured. Krüptovaluutade suur eelis, et nende väärtust ei saa omavoliliselt suurendada ega vähendada, on moodsa raha- ning majanduspoliitika raames oluliseks probleemiks.
Juhul kui loobutakse võimalusest intresside- või rahakogusepoliitika kaudu aktiivset konjunktuuripoliitikat teha, viiakse maailmamajandus Keynesi vaatenurgast nähtuna uusklassitsistlikku majanduslikku kiviaega: konjunktuurilised kriisid tooksid vältimatult kaasa tugeva majanduslanguse ning tugeva deflatsiooni, mis omakorda paneks rahvastiku silmitsi suurte raskustega.

Krüptovaluutade suur eelis – nendega ei saa (vähemalt mahupiiranguga plokkahela valuutade puhul, nagu näiteks bitcoin) tekitada riiklikult manipuleeritud või tekitatud inflatsiooni või hüperinflatsiooni –, ei käi kahjuks käsikäes deflatsiooni võimaluse välistamisega. Pigemini tõuseb deflatsioonirisk võrreldes fiat-valuutade režiimidega hüppeliselt. (Mahupiiranguta krüptovaluutade, nt Ripple'i puhul ei kehti ka see inflatsiooni välistusvahend, kuna (teoreetiliselt!) saaks lühiajaliselt suurtes kogustes Ripple'isid turule paisata.)

Tsentraalne deflatsioonirisk seisneb selles, et raha väärtus tõuseb pidevalt, mis on võlgnike jaoks probleemiks. Ka võlgadeta majandussubjektide puhul mõjub deflatsioon majanduslangust pidurdavalt: kuna hinnad langevad, vähendatakse tarbimis- ja investeerimisotsuseid, kuna „kõik muutub veel soodsamaks“. Majanduses valitseb langus. Edasine oht seisneb selles, et krüptovaluutad toovad kaasa automaatse deflatsiooni. Hiljemalt hetkel, mil viimane võimalik bitcoin on loodud, toimuks bitcoinil baseeruvas majanduses ka majanduskasvust hoolimata langus – aina enam kaubateenuseid tuleb katta sama rahasummaga – Bitcoini väärtus tõuseks tugevalt, hinnad ja palgad peaksid sellele vastavalt langema. (Bitcoin on piiratud väärtusele 20.999.999,9769 BTC. Viimane bitcoini ploki number on 6.929.999 ning see võidakse luua aastal 2140. [7])

Idee asendada fiat-süsteemid täielikult detsentraliseeritud krüptovaluutaga on seega täiesti ebarealistlik. Võimalik tundub aga senise „analoogse“ fiat-raha väljavahetamine riikliku krüptovaluuta vastu või raha nendega täiendamine. Siinkohal juhiks krüptovaluutat keskselt keskpank, mis suudaks vältida ülalmainitud deflatsiooni-stsenaariume (ühe piiramatu riikliku krüptovaluutaga). Nõnda oleks võimalik plokkahela suuri eeliseid rakendada ka riiklikul ja rahvusvahelisel tasandil ametlikus raha- ja maksetehingutes.

Sellisel viisil oleksid krüptovaluutad (võttes arvesse edasised uuringud) rahvamajanduslikult rakendatavad ning mitmed keskpangad kontrollivad juba praegu isikliku krüptovaluuta loomise võimalusi. Eesti võib olla esimene riik, mis ei tee tööd vaid kontseptsiooni kallal, vaid viib esimese riigina sisse „Estcoini“ [6].

3.3 Ökoloogilised riskid

Krüptovaluuta suureks probleemiks on nende tekkes sisalduv kõrge energiavajadus. 90% voolutarbest kasutatakse hetkel uute bitcoinide loomiseks ning umbes 10% tehingute valideerimiseks. [13]
Kogu kaevandamisele kuluv energiatarve ei kasva mitte ainult bitcoini puhul aasta-aastalt olulisel määral, vaid ka plokkahela aluseks olevad algoritmid nõuavad arvutitelt järgmise (bit)coini loomiseks aina enam arvutusvõimsust: Ainuüksi 2018. aastaks prognoositakse bitcoinide voolutarbeks 70 TWh, mis vastab sellise tööstusriigi nagu Austria voolutarbele [15, lk 3]. Sellest lähtuvalt mõjutavad krüptovaluutad kliimamuutust siiski omajagu, kuna suur hulk kaevandustehingutest leiab aset Hiinas ning seal on taastuvenergia teadupärast veel tulevikumuusika ning enamik elektrivoolust toodetakse põlevkivitehastes.

4 Kokkuvõte

Plokkahela tehnoloogiaga sündis uus makseinstrument: krüptovaluutad. Neist tuntuim, bitcoin, ei sobi „vana“ plokkahela ülesehituse ja pikkade tehinguaegade tõttu juba praegu maksetehingute funktsionaalsuses kasutamiseks, seetõttu kuulub tulevik kiirematele, „moodsatele“ krüptorahadele. Seevastu investeeringmündiks sobib bitcoin hetkel tänu oma tuntusele kõigist krüptovaluutadest kõige paremini, kuna see on piiratud vaid 21 miljardi mündiga. Sellest hoolimata räägib selle väärtuse säilitamise vahendina kasutamise mõttekuse vastu äärmuslik volatiilsus, mis nullib selle kasutatavuse väärtuse säilitamise vahendina. Lisaks on aktiivne kursiga manipuleerimine hõivatud ning tehniliselt raskesti takistatav.

Vahetus- ja maksevahend peab täitma põhilisi funktsioone ja omadusi, et seda võidaks aktsepteerida usaldusväärse valuutana [3, peatükk 1.2]. Elementaarseks eelduseks on eriti just see, et suurem osa ühiskonnast aktsepteerib seda maksevahendit, mis ei ole aga ilma piiramatu väärtuse säilitamise funktsioonita, mis on raha funktsionaalsuse põhitingimuseks [11, lk 7], veel realistlik. Just seda väärtuse säilitamise funktsiooni krüptovaluutal (veel) ei ole. Lisaks on krüptovaluutad spekulatsiooniriskide suhtes äärmiselt tundlikud, kuna siinkohal ei ole pakkumine ja nõudlus vähemalt senini enamasti kasutusega määratud, vaid on suunatud valdavalt investorite spekulatiivsetel tingimustel tõusvale või langevale huvile.
Sellega on selgelt kinnitatud esimene tööhüpotees:

Tees 1: „Privaatsete krüptovaluutade kasutamine alternatiivse maksevahendina ei ole lähemas tulevikus veel mõeldav.“

Siinkohal toome ära analüütiku ja GMO-strateegi James Montieri drastilise tsitaadi: „Bitcoin on jama. Need krüptovaluutad on põnevad, kuid need ei ole raha. Need ei täida ühtegi klassikalist funktsiooni, ei ole ehtne maksevahend, ei sobi väärtuse säilitamiseks ega ole arvutusühikuks. Need on pigem võrreldavad kirjamarkide või veiniga – kuigi

veini saab vähemalt ära juua.“ [8] Sellega saab selgeks, et krüptovaluutadel puudub olemuslik väärtus, v.a juhul, kui seda kasutatakse kas ICO-de või plokkahelapõhiste protokollide kommunikatsiooni tokenina.
Mis käsitleb teist tööhüpoteesi:

Tees 2: „ICO-d muutuvad järjest enam alternatiiviks traditsioonilistele riskikapitalirahastustele ning tokenitest saavad ajendid, millele tuginedes ehitatakse üles nutikate lepingutega detsentraliseeritud infrastruktuur.“

Krüptovaluutade kasutamise kõrval on plokkahelaga võimalik ellu viia just selliseid programme, mis võimaldavad plokkahelapõhiste protokollide kommunikatsiooni (smart contracts) – see saab tulevikus olema krüptovaluutade peamine sihipärane kasutusalternatiiv.

ICO-d on ühelt poolt huvipakkuvad iduettevõtete, projektide või ettevõtete ühisrahastamiseks, mille puhul toimub kapitali hankimine asjakohaste tokenite väljastamise teel. Eelkõige nõuab plokkahelapõhiste protokollide kommunikatsioon tulevikus peamiselt Asjade Internetis tokeneid või krüptovaluutat. Jätkuva küpsemisprotsessi ja läbimõeldud käivitamise korral on ICO-del potentsiaal asendada riskikapitalide investorid mitmetel juhtudel esmase või varajase finantseerimisfaasi käigus.

Sellega ning eriti tänu mitmetele (siinkohal ruumi kokkuhoidmiseks väljajäetud) tokenite kasutusvõimalustele võib ülalnimetatud teise tööhüpoteesi lugeda tõestatuks: plokkahelatehnoloogia tulevik võib seetõttu pigem peituda igapäevase elu või Asjade Interneti digitaalses revolutsioonis ja mitte nii väga raha aseaine loomise