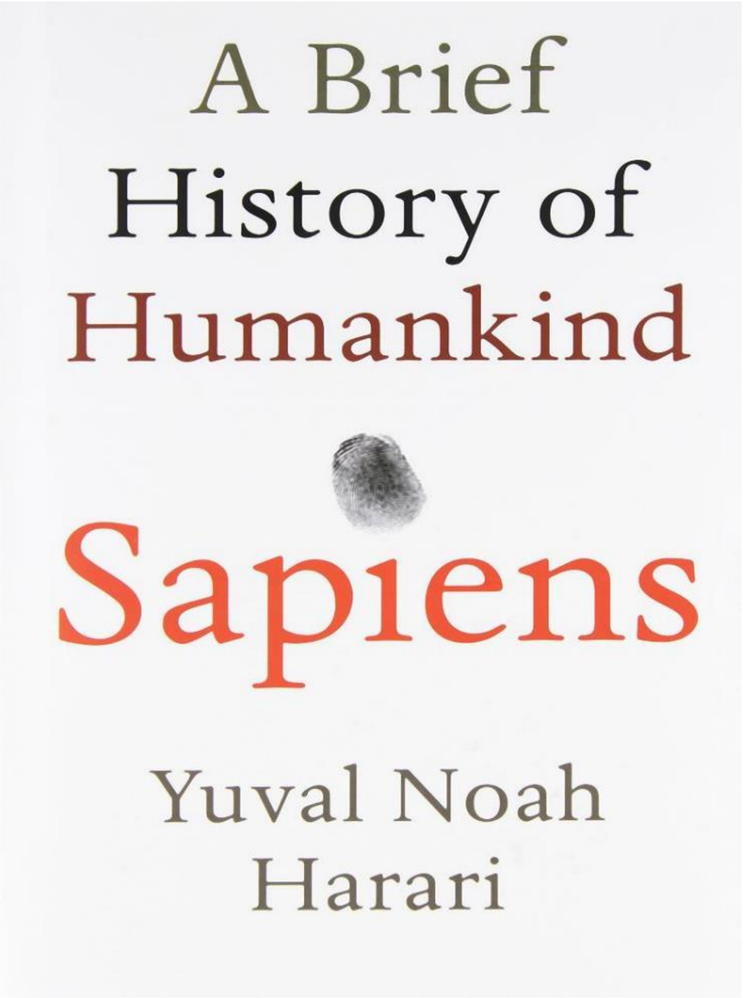
Ihmiset, verkostot ja kryptoekonomia

2018

alvarmahlberg
@alvarmahlberg

TARINAT JA VERKOSTOT

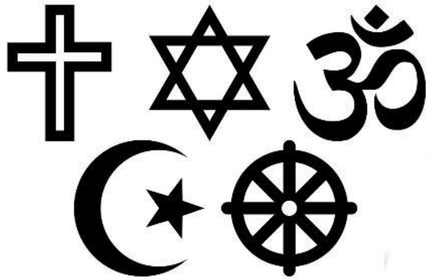


TARINAT JA VERKOSTOT

YRITYKSET

NOKIA

USKONNOT



RAHA

HUOM: Osa kuvista poistettu

TARINAT JA VERKOSTOT

Yhteiskuntamme muodostuu valtavasta määrästä erilaisia päällekkäisiä verkostoja.

Verkostoille ominaista on verkostovaikutukset.

HAASTEENA: VERKOSTOT TULEE JÄRJESTÄÄ SÄÄNTÖJEN MUKAAN!

HUOM: Osa kuvista poistettu

TARINAT JA VERKOSTOT

Mihin tarvitaan järjestystä ja sääntöjä?

Yksilöt tarvitsevat rakenteita, jotta he kykenevät toimimaan. Tarvitaan jonkinlaista ennustettavuutta siitä, mitä seurauksia tietyllä toiminnalla on. Rakenteiden ja ennustettavuuden avulla voidaan toimia kohti tiettyä tavoitetta yksin tai yhdessä.

HAASTEENA: KUKA VALVOO SÄÄNTÖJÄ JA JÄRJESTYSTÄ?

HUOM: Osa kuvista poistettu

TARINAT JA VERKOSTOT

Koska verkostot tulee organisoida sääntöjen puitteissa, tarvitaan joku taho varmistamaan että näitä sääntöjä noudatetaan.

Perinteisesti verkostoja ovat hallinneet kuninkaat, papisto, yritykset ja valtiot.

He ketkä vastaavat sääntöjen noudattamisesta, myös hallitsevat verkostoja.

Miten tämä liittyy lohkoketjuteknologiaan?

Lohkoketjut
mahdollistavat verkostojen
luomisen ja **ylläpitämisen**,
ilman hallitsijaa ja
ilman rahaa.

LOHKOKETJUTEKNOLOGIA MAHDOLLISTAA SEURAAVANLAISTA LIIKEHDINTÄÄ:

Keskitetty -> Hajautettu

Kansalaisuus -> Yksilönvapaus

Koordinoidusti -> Yhteistyössä

Läpinäkymätön -> Läpinäkyvä

HUOM: Osa kuvista poistettu

LOHKOKETJUTEKNOLOGIAN MÄÄRITTELYÄ

Catalini & Gans (2017) mukaan lohkoketjuteknologia mahdollistaa taloudellisten toimijoiden verkoston olla yhtä mieltä jaettujen tietojen todellisesta tilasta tasaisin väliajoin. Joustavuus siitä, mitä jaetut tiedostot edustavat, tekee lohkoketjuteknologiasta yleiskäyttöisen teknologian.

Yleiskäyttöisille teknologioille on ominaista, että niitä voidaan soveltaa monelle eri toimialalle ja yleistyessään ne lisäävät tuottavuutta eri toimialoilla, sekä parantavat talouskasvua yleisemminkin.

Yleiskäyttöisiä teknologioita ovat höyryvoima, sähkövoima ja tieto- ja viestintätekniikka.

HUOM: Osa kuvista poistettu

LOHKOKETJUTEKNOLOGIAN MÄÄRITTELYÄ

Pilkington (2015) kuvaa lohkoketjuteknologiaa on murroksellisena (disruptive) teknologiana.

Lansiti ja Lakhani (2017) mukaan lohkoketju ei ole murroksellinen teknologia vaan se voidaan nähdä ennemmin perustavana (foundational) teknologiana.

HUOM: Mikään ei ole helpompaa kuin ennustusten tekeminen!

KRYPTOEKONOMIA

Kryptoekonomia on metodologia siitä, kuinka pyritään rakentamaan hajautettuja järjestelmiä, joilla on tietyt tietoturvaominaisuudet.

Kryptoekonomiassa yhdistetään **kryptografiaa** ja **taloutta**, jotta voidaan luoda vahvoja hajautettuja vertaisverkkoja, jotka menestyvät ajan myötä, vaikka vastustajat yrittävät häiritä verkkoa.

HAJAUTETUT JÄRJESTELMÄT

HUOM: Osa kuvista poistettu

KRYPTOEKONOMIAN KAKSI OSA-ALUETTA

1. **Kryptografiaa** käytetään todentamaan sellaisia viesteihin liittyviä ominaisuuksia, jotka ovat tapahtuneet aikaisemmin

2. **Taloudelliset kannustimet** on järjestelmän sisällä määriteltyjä kannustimia, joiden avulla tietyt järjestelmän ominaisuudet säilyvät myös tulevaisuudessa.

HUOM: Osa kuvista poistettu

KRYPTOEKONOMIA

Järjestelmää suunnitellessa halutaan, että sillä on jotain tiettyjä ominaisuuksia, sekä toiminallisuuksia.

Esimerkkejä Bitcoin lohkoketjun ominaisuuksista:

- Uusien lohkojen lisääminen ketjuun
- Lohkoja ei voi poistaa ketjusta
- Luoda ketju lohkokoista
- Sisällyttää transaktioita jokaiseen lohkoon
- Lähettää vain oikeellisia transaktioita
- Ylläpitää oikeaa tilaa omistuksista
- Tietojen saatavuus
- Aikaleimaus

KRYPTOGRAFIA

Kryptografiaa on perinteisesti pidetty armeijan ja tiedustelu organisaatioiden toteuttamana tapana lähettää ja purkaa salattuja viestejä.

Ennen 2000-lukua sen käyttö on ollut rajoittunutta ja se on perustunut koodien tekemiseen ja purkamisen sitä taitavien henkilöiden luovuuden ja henkilökohtaisten taitojen pohjalta. (Katz & Lindell, 2015)

KRYPTOGRAFIA

Kryptografian avulla pyritään saavuttamaan seuraavia **ominaisuuksia:**

Aitous: Viesti on todella peräsin ilmoitetulta lähettäjältä

Luottamuksellisuus: Yksityiset tiedot pysyvät yksityisinä siirron aikana

Eheys: Tiedot pysyvät muuttumattomina

HUOM: Osa kuvista poistettu

KRYPTOGRAFIA

Käytännössä kryptografiaa hyödynnetään lohkoketjuissa:

Tiivisteet = varmistetaan ketjun yhteneväisyys ja transaktioiden järjestys.

Digitaaliset allekirjoitukset = tiedetään kuka on lähettänyt transaktion, muttei välttämättä henkilön oikeaa identiteettiä.

Konsensus menetelmät = varmistetaan, että konsensuksen ylläpitoon osallistuvilla on esimerkiksi tarpeeksi laskentateho.

TALOUDELLISET KANNUSTIMET

Taloudelliset kannustimet voidaan jakaa kahteen ryhmään:

1. **Tokenit:** kannustetaan toimijoita toimimaan määritellyn protokollan mukaan antamalla heille järjestelmän omaa kryptovaluuttaa eli tokeneita.

2. **Etuoikeudet:** toimijoille voidaan antaa etuoikeuksia. Esimerkiksi louhija, joka louhii uuden lohkon on hetkellisesti sen lohkon yksinhaltija. Louhijalla on silloin etuoikeus periä transaktiokustannuksia.

(Buterin, 2017)

TALOUDELLISET KANNUSTIMET

Taloudelliset kannustimet voidaan jaotella myös **toisella tavalla** kahteen ryhmään:

1. **Palkkiot:** toimijoita voidaan palkita tokeneilla, tai antaa heille etuoikeuksia, jos he tekevät jotain hyvää.

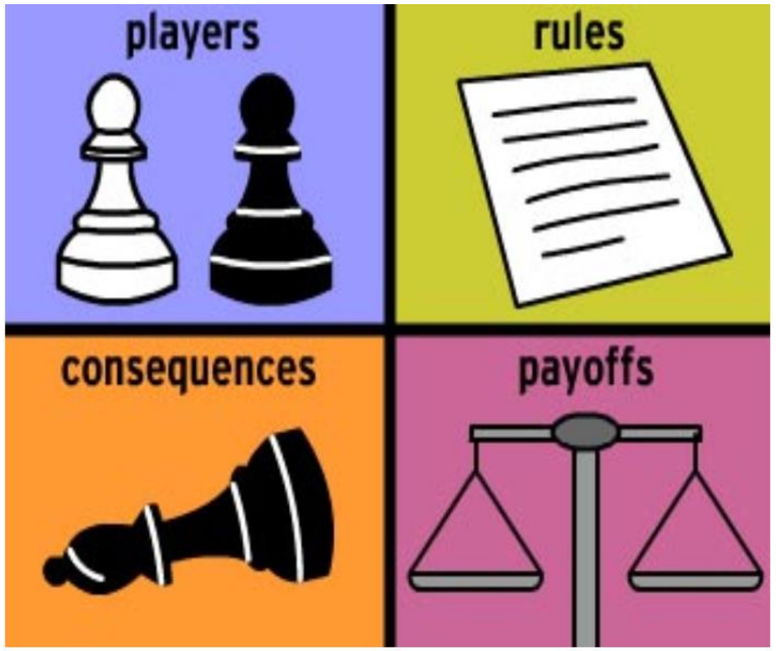
2. **Rangaistukset:** toimijoilta voidaan vähentää tokeneita, tai rajoittaa heidän etuoikeuksia, jos he tekevät jotain pahaa.

Miten luodaan toimivia kannustimia?

(Buterin, 2017)

PELITEORIA

”Kiteytettynä peliteoria on oppi strategisesta vuorovaikutuksesta sellaisten omaa etuaan ajavien agenttien välillä, jotka pyrkivät toimintansa avulla tuottamaan sellaisia lopputuloksia, joista seuraa heille itselleen suurin mahdollinen hyöty.” (Honkanen, 2015.)



MEKANISMIN SUUNNITTELU

Taloustieteen osa-alue, jolla sovelletaan peliteorian menetelmiä. Luodaan säännöt pelille, jotta päästään tiettyyn lopputulokseen.

Mekanismin suunnittelun ideana on luoda järjestelmä, joka luo pelaajille kannustimet toimia suunnittelijan tavoitteiden mukaan.

LOHKOKETJUTEKNOLOGIAN VAIKUTUKSIA

- Lohkoketjut korvaa verkostoja markkinoilla
- Lohkoketjuteknologian avulla voimme helpottaa arvonsiirtoa sellaisilla alustoilla, joilla se olisi muutoin mahdotonta.
- Lohkoketjuteknologian avulla voidaan avata valtavasti potentiaalista taloudellista arvoa.
- Lohkoketjut muokkaavat nykyisiä liiketoimintamalleja
- Kryptoekonomiset järjestelmät ovat pohjimmiltaan uusia tapoja kannustaa ihmiskäyttäytymistä

LOHKOKETJUTEKNOLOGIAN NYKYTILA

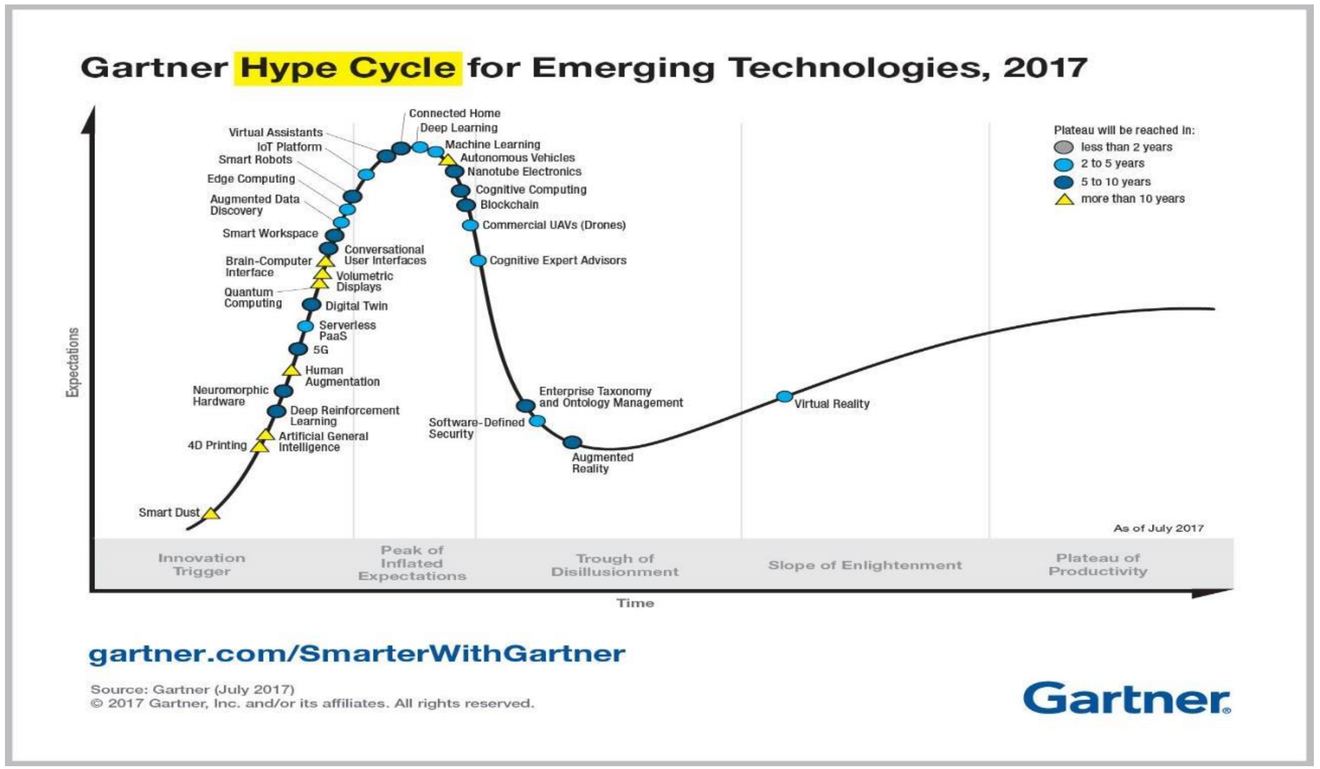
IBM (2016) julkaiseman tutkimuksen mukaan pankit ja finanssiala ovat ottaneet lohkoketjuteknologiaa käyttöön huomattavasti nopeammin kuin alun perin on ajateltu.

Krujiff & Weigand (2017) toteavat terminologian kehityksen vaativan tavallisten internet käyttäjien ja yritysjohtajien perustavanlaatuista ymmärrystä lohkoketjuteknologian toiminnasta ja vaikutuksista.

LOHKOKETJUTEKNOLOGIAN NYKYTILA

Gartner (2017) arvio lohkoketjuteknologian olevan siirtymässä ”Peak of Inflated Expectations” –vaiheesta kohti ”Through of Disillusioment” -vaihetta.

Tämän arvion pohjalta lohkoketjuteknologiaan kohdistuneen innostuksen huippu olisi juuri nähty ja olisimme matkalla kohti vaihetta jossa investoinnit teknologiaan jatkuvat vain, jos tekniikkaa onnistutaan parantamaan.



HUOM: Osa kuvista poistettu

LOHKOKETJUTEKNOLOGIAN HAASTEET

Skaalautuvuus

Louhinta

Kryptopörssit

HUOM: Osa kuvista poistettu

ICO

- ICO eli ”initial coin offering” on uusi tapa kerätä riskirahoitusta, yleensä startup-yritykselle
- Käytännössä oman kryptovaluutan liikkeelle laskemista
- Tavallaan sekoitus listautumisantia ja joukkorahoitusta
- ”Helppo” tapa kerätä rahoitusta
- Harvoin minkäänlaisia vakuuksia, mutta tuottopotentiaali voi olla valtava

HUOM: Osa kuvista poistettu

ICO

Valtavasti avoimia kysymyksiä!

- Minkälainen sijoitus kyseessä? Pääoma, lahjoitus, tulo?
- Mikä on tulosta vähennyskelpoinen meno?
- Kansainvälisen verotuksen ulottuvuudet?

”Kyse on täysin siitä, miten järjestely (ICO) toteutetaan ja mitä tokeneilla on tarkoitus tehdä, eli käyttää vai myydä (onko kyse enemmän ennakkomaksun luonteisesta utility-tokenista vai tuottoa synnyttävästä ”arvopaperista”) ja miten tokeniin liittyvät tulovirrat on rakennettu.” (PWC, 2018)

YHTEENVETO

1. Lohkoketjut
mahdollistavat verkostojen
luomisen ja **ylläpitämisen**,
ilman hallitsijaa ja
ilman rahaa.

2. **Kryptoekonomiassa** yhdistetään **kryptografiaa** ja **taloutta**,
jotta voidaan luoda vahvoja hajautettuja vertaisverkkoja, jotka menestyvät ajan myötä, vaikka vastustajat yrittävät häiritä verkkoa.

3. Lohkoketjuteknologian avulla voidaan avata valtavasti potentiaalista **taloudellista arvoa**.

LÄHTEET

Catalini, C & Gans, J. (2017) Some simple economics of the blockchain. Technical report, National Bureau of Economic Research.

Katz, J. & Lindell, Y, (2015). Introduction to modern cryptography. Chapman & Hall.

Pilkington, M. (2015) Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations.

Lansiti, M & Lakhani, K. (2017) “The Truth About Blockchain”, Harvard Business Review, January-February 2017.

Buterin, V. (2017) Introduction to Cryptoeconomics.

Honkanen, V. (2015) Kokeellinen peliteoria ja rahalliset palkkiot (Pro gradu –tutkielma) Tampereen yliopisto.

Kruijff, J & Weigand, H. (2017) Understanding the Blockchain using Enterprise ontology. Advanced Information Systems Engineering.

IBM, (2016). Leading the pack in blockchain banking: Trailblazers set the pace.