Santeri Tani

TIEA100: Lohkoketjuteknologiat ja sovellutukset

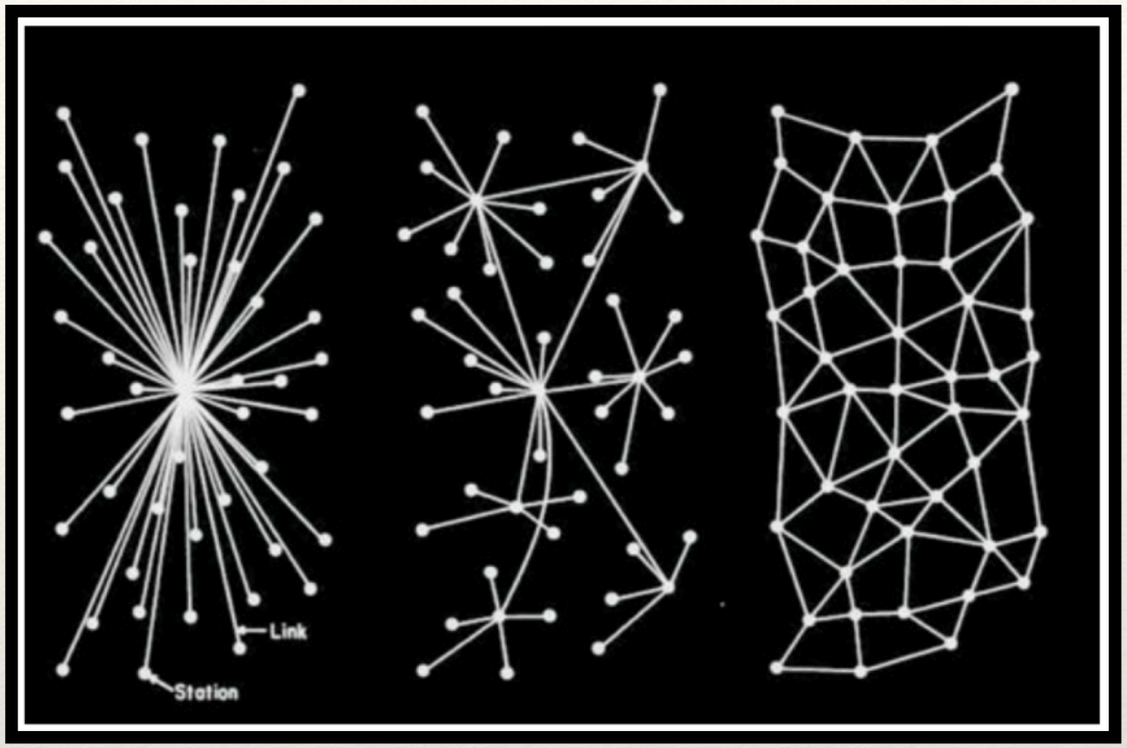
Luento 1

Esityksessä hyödynnetty materiaalia sitaattilain turvaamana seuraavilta tahoilta: IBM, Solteq, NSA (Paul Baran), JYU (Santeri Tani, Henrik Korhonen, Erkka Nurmi)

Mikä lohkoketju?

Lohkoketjut yksinkertaisesti

- Lohkoketju on Bitcoinin tunnetuksi tekemä hajautettu (distributed) tietokanta, joka koostuu järjestyksessä toisiinsa linkitetyistä, muuttumattomista lohkoista
- Lohkoketjuun tallennettu tieto fyysisesti ja digitaalisesti samaan aikaan useissa eri paikassa verkon solmukohtina toimivissa tietokoneissa



Paul Baranin (1964) kaavioita havainnollistamaan keskitettyjen ja hajautettujen verkkojen rakennetta

- Lohkoketju on

hajautettu
luottamukseton
sisällöllisesti validoitu
tarvittaessa anonyymi
tarvittaessa salattu
muuttumaton
massalukukelvoton
vahvan tunnistautumisen mahdollistava
no-single-point-of-failure

tapa tallentaa tietoa

Historiaa

- Juuret 1991 Stuart Haberin ja W. Scott Stornettan työssä aikaleimauksen saralla
- 1997 Nick Szabo (BitGold, älysopimus-termi), Wei Dan (b-money), Zooko Wilcoxin kirjoitelmat (200x-2009)
- Satoshi Nakamoton Bitcoin 2009 ja Proof-of-Work
  - 2017 Bitcoin market cap 122 miljardia, kryptovaluutat yhteensä 201 miljardia
- Ethereum 2015, älysopimukset
  - The DAO 2016, 150 000 000 USD, 50 000 000 USD krakkerille
- Älysopimukset ja hajautetut verkkoratkaisut —> Web 3.0

Miksi lohkoketju?

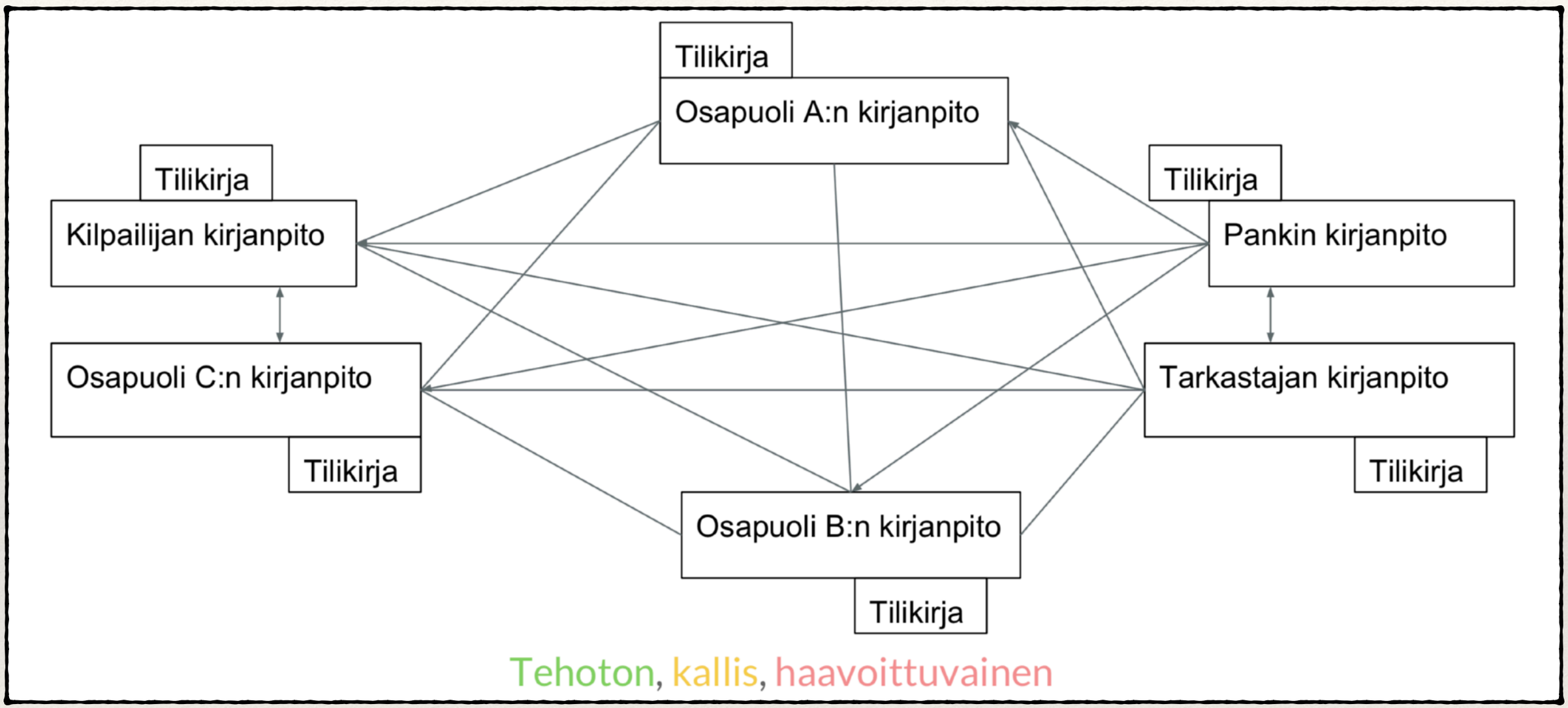
1. Säästää aikaa
2. Vähentää kuluja
3. Vähentää riskejä
4. Lisää luottamusta

- Jokaisella osapuolella omat referenssidatat, joista nähdään luotettavasti tapahtuneet transaktiot
- Yksittäinen kokonaisnäkymä datakokonaisuuteen
- Sisäinen auditointi helppoa
- Varmistaa osapuolien kompliansin ja sopimusten noudattamisen
- Osapuolienvälisen tarkkailun tarve vähenee

“Lohkoketjut ovat parhaimmillaan useiden keskenään luottamuksettomien osapuolien keskustellessaan keskenään.”

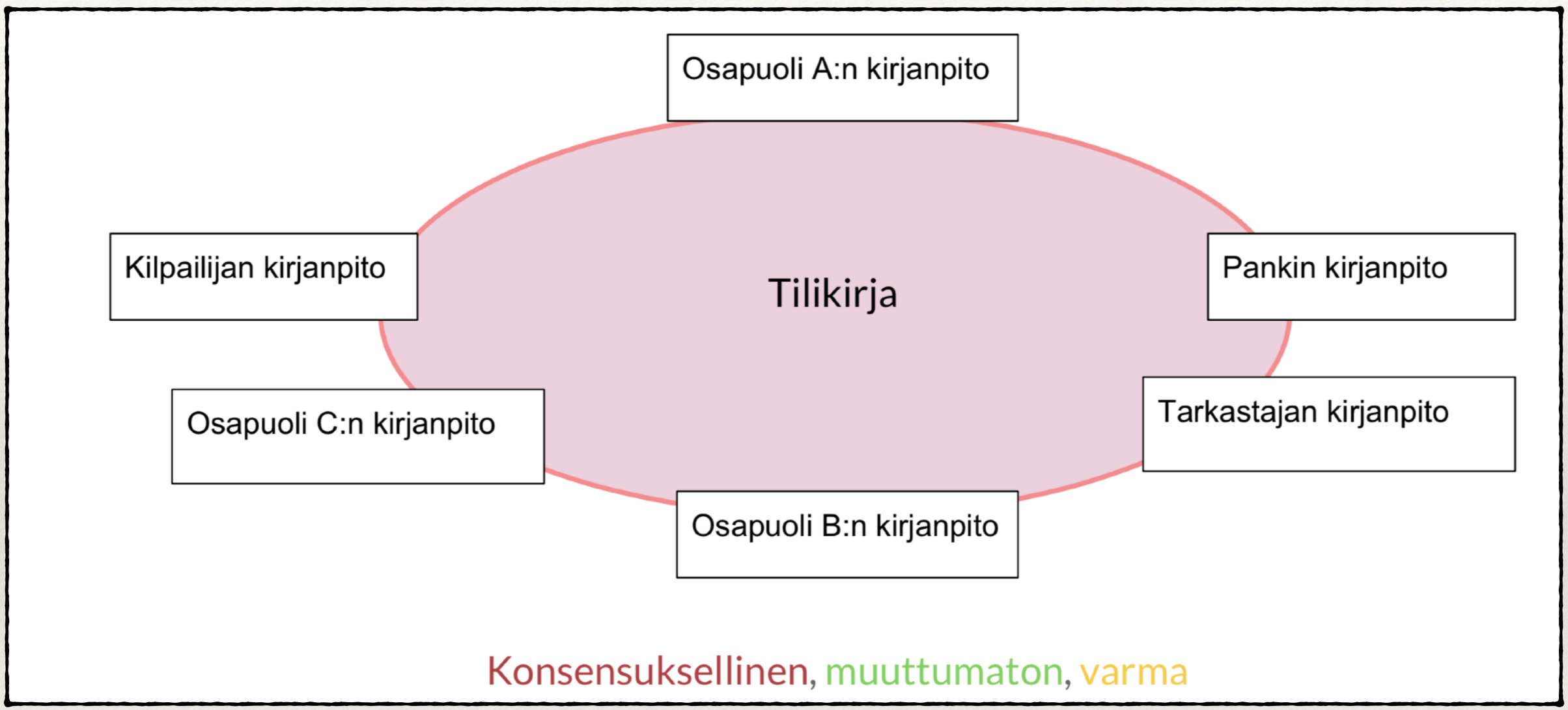
–Tuntematon

Ongelma: nykyisen mallin kirjanpito



Tehoton, kallis, haavoittuvainen

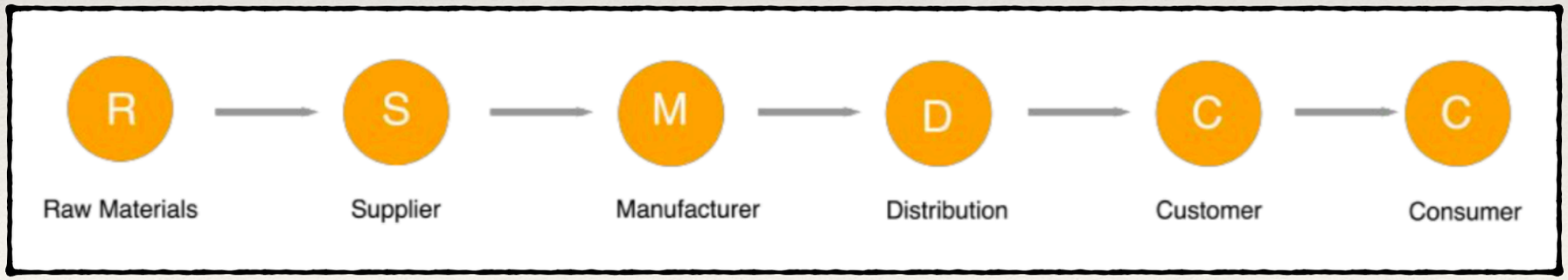
Ratkaisu: hajautettu kirjanpito



Konsensuksellinen, muuttumaton, varma

Esimerkki: tuotantoketjunseuranta

- Eliminoisi vuosittain satojen miljoonien häviöt
- Luottokirjeet (letters of credit)
- Reimburssit



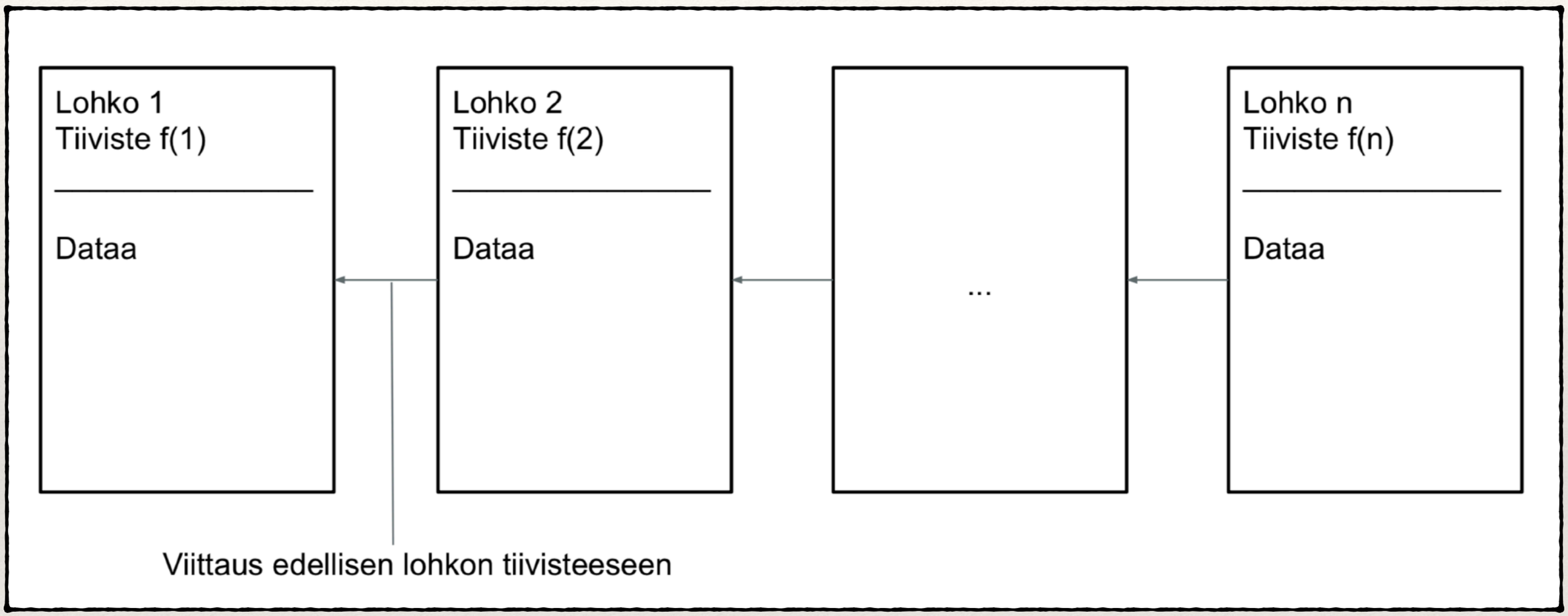
Esimerkki: SOTE

- Kokonaisarkkitehtuurin korvaaminen älysopimuskudoksella
- Arvonsiirto
- Lääkintälaitteiden resurssiviisas kiertotalous
- Automatisoitu maksuverkko

- Vahvuudet:
  - Laajennettavuus
  - Autonomisuus
  - Luottamuksettomuus
  - Muuttumattomuus
  - Hajautettuneisuus

- Heikkoudet:
  - Massaluettavuus
  - Konsensusmekanismit
  - Lainsäädäntö
  - Hype

Kuinka lohko rakentuu?



Konsensus julkisissa lohkoketjuissa

- Määrittävät mitkä lohkot lisätään lohkoketjuun ja mikä lohkoketjun senhetkinen tila on
- Kriittinen osa luottamuksetonta verkkoratkaisua
- Ilman toimivaa konsensusmekanismia tulee olla keskitettyä järjestelmää muistuttava luottamussuhde joidenkin toimijoiden välillä (hajautettuneisuuden pienempi aste)
- Useat älysopimusalustat ratkaisevat tämän ongelman erottamalla ns. maailman tilan (world state) ja transaktiolohkoketjun toisistaan erillisiksi kokonaisuuksiksi

Proof-of-Work (PoW)

- Suosii ongelmatapauksissa niitä lohkoja, joiden louhinnassa on käytetty eniten laskentatehoja
- Lohkonmuodostus tietyn raja-arvon alittavia tiivistefunktioita laskemalla
- Vaikeustaso skaalautuu laskentatehon mukaan Äärimmäisen epäedullinen energiatehokkuudeltaan
- Esimerkiksi Bitcoin käyttää tätä

Proof-of-Stake (PoS)

- Suosii ongelmatapauksissa niitä lohkoja, joiden louhinnan takana on eniten panostettua krypto-omaisuuseriä
- Erittäin hankala toteuttaa laaja-alaisesti skaalautuvasti
- Vaatii erittäin pienen määrän laskentatehoa
- Ethereum on siirtymässä tähän

Ei-julkiset lohkoketjut

- Yksityiset lohkoketjut sekä hybridi/-konsortiolohkoketjut
  - Älysopimukset, yksityisyys, luottamus
- Luottamuksettomuuden aste pienempi — konsensusmetodit yksinkertaisempia
- Välitön siirtymä täysin julkisiin lohkoketjuihin yrityksille harvoin kiinnostavaa
- Hyötyjinä finanssi- sekä julkinen sektori, jälleenmyynti, vakuutusyhtiöt, valmistajat…
- Byzantine Fault Tolerance y/n
- Esim. Hyperledger, Corda (R3)

Älysopimukset

- Lohkoketjuteknologian viimeisimpiä merkittäviä kehitysaskelia
- Arvon- tai datansiirron automatisoiva ohjelma, protokolla tai skripti
- Toiminta varmennettavissa
- Turing-täydellisesti ohjelmoitavissa
- Autonomisesti aktivoitavissa (esimerkiksi transaktioiden yhteydessä); tiettyjen ehtojen täytyttyä suoritetaan operaatio x
- Kryptografisesti allekirjoitettuja

Älysopimukset: esimerkkejä

- Toimijoidenvälisen kirjanpidon automatisointi
- Valuutan- ja tiedonsiirrot tiettyjen ehtojen tai funktioiden täytyttyä
- Yritystoiminnot toteuttava hajautettu autonominen organisaatio (DAO)
- Myös esimerkiksi verkkotunnusten rekisteröintijärjestelmät ja äänestystoiminnot

Esimerkki: kellokortti

- Kellokortin leimaamisesta aktivoidaan älysopimus
- Älysopimus siirtää henkilölle automaattisesti tämän tuntipalkkaa vastaavan rahamäärän kryptovaluuttana x
- Koska valuutan siirtyminen julkistetaan lohkoketjuun, on mahdotonta esimerkiksi kavaltaa tai väärentää siirrettyjä varoja
- Myös kirjanpito on näin automatisoitu — kaikki siirtynyt varallisuus on tarkasteltavissa lohkoketjun sisällä
- Älysopimusten avulla voidaan paremmin varmentaa siirretyn rahan oikeellisuus, sekä säästää kirjanpidollisissa kuluissa

Hajautetut sovellukset (Đapps)

- Älysopimuksilla rakennetut hajautetut sovellukset
- Perinteinen frontend ja backend lohkoketju
- Suurimmat alustat Ethereum ja IPFS
- Đapp melko löyhästi määritelty konsepti

Đapps

- Factom Foundationin johtaja David Johnston (ynnä Yilmaz, Kandah, Bentenitis, Hashemi, Gross, Wilkinson & Mason 2015) asettaa Đappille seuraavat kriteerit:

    1. Sovelluksen tulee olla vapaa ja avointa lähdekoodia, autonominen, eikä yksikään yksittäinen entiteetti saa kontrolloida enemmistöä siihen liitetyistä tokeneista. Kaikki sovelluksen protokollan muutokset tulee tapahtua käyttäjien yksimielisestä päätöksestä
    2. Sovelluksen data sekä logit tulee olla kryptografisesti säilötty julkiseen ja hajautettuun lohkoketjuun keskitetyn verkkomallin heikkouksien välttämiseksi
    3. Sovelluksen tulee käyttää kryptotokenia. Se mahdollistaa sovellukseen käsiksipääsyn, ja sillä voidaan palkita merkittävää toiminnallisuutta tuottavia käyttäjiä
    4. Sovelluksen tulee generoida käyttämänsä tokenit standardoitua kryptografista algoritmia käyttäen, jonka avulla voidaan todistaa tokeneiden arvo (proof of value)

Määritelmä on hieman puutteellinen, sillä kaikki Ethereumin ja muiden hajautettujen alustojen sovellukset eivät täytä näitä vaatimuksia. Johnston jakaa Đappit kolmeen tyyppiin sen mukaan, käyttävätkö ne omia lohkoketjujaan.

- **Tyypin I** sovellukset käyttävät omia lohkoketjujaan
- **Tyypin II** sovellukset käyttävät tyypin I lohkoketjuja
- **Tyypin III** sovellukset ovat tokenisoituja protokollaratkaisuja, ja käyttävät tyypin II protokollaa toimintaansa

Hajautettujen sovelluksien avulla voidaan laskea merkittävästi yksittäisten tietokoneiden tehotarvetta, nopeuttaa verkon toimintaa, ja rakentaa todellisen muuntumattoman (immutable) verkon.

Hajautetut, autonomiset organisaatiot (DAO)

- Yksi älysopimusalustojen suurimmista myyntivalteista
- DAO:ssa älysopimukset aktivoidaan autonomisesti ennalta ohjelmoitujen sääntöjen täytyttyä
  - Kryptovaluuttojen ja -tokeneiden omistajuus
  - Aloitteiden vapaa äänestäminen
  - Joukkorahoituskampanjat (esim. ICO-rahoitukset)

Miksi DAO?

Ethereum määrittelee esim. DAO-pankkijärjestelmän mahdollistavan seuraavat:

- Stabiilin universaalin kryptovaluutan luomisen. Kontrolloimalla liikenteessä olevien valuuttayksiköiden määrää, osakkaat voivat estää äkkinäiset hintavaihtelut
- Seritifioitujen arvopääoman liikkeellelaskun. Valuuttayksikkö vastaa sertifioitua arvopääomaa, ja valuuttayksiköllä voidaan todistaa arvopääoman omistajuussuhde. Valuuttayksikkö on generoitavissa ja "poltettavissa" (burn) siten, että niiden määrä vastaa arvopääoman määrää
- Digitaalisesti varmennetut arvopaperit. DAO pystyy laskemaan liikkeelle kryptovaluuttoja joiden arvo on sidottu muihin liikkeellä oleviin valuuttoihin. Nämä kaikki ovat toteutettu ja käytössä erinäisissä projekteissa paraikaa (Van de Sande 2015-2.)

2017 seitsemän kymmenestä suurimmasta krypto-omaisuuseräyksiköstä on rakennettu ohjelmoitavien älysopimusalustojen avulla. Näihin lukeutuu ennustealusta Augur (Augur Team 2017), sijoitusrahasto ja -alusta Iconomi (Iconomi 2017-1), kryptografisesti sertifioitu, krypto-omaisuuseräyksiköllä todennettava kultakauppa Digix DAO (Digix Global 2017) sekä hajatutettu supertietokone Golem (Golem Team 2017)

Luento 1: kysymyksiä?

Seuraavalla luennolla: älysopimusten liittäminen lohkoketjuun sekä älysopimusohjelmointi