Vaasan yliopisto 5.6.2018
Tuotantotalouden ja tietojärjestelmätieteen kandidaattiohjelma
Valintakoe - VASTAUKSET

Tehtävä 3. Kerro mitä tarkoittaa lohkoketju? (4 p)

Vastauksesta tulisi käydä ilmi seuraavat asiat:

- Alkuperäinen idea: dokumenttien muokkaushistorian säilytys ja turvaaminen dokumenteista muodostettavilla tiivisteillä ja näiden tiivisteiden varmentamisesta aikaleimalla, tiivisteistä muodostuva järjestetty ketju, jonka järjestystä ei voi muuttaa (1 p)
- Lohkoketjun perustana on ajatus jaetusta tilikirjasta, johon kaikki tapahtumat kirjataan aikajärjestyksessä. Kaikki kirjataan ja mitään ei poisteta. Tilikirjan paikkansapitävyys varmistetaan monimutkaisilla laskutoimituksilla, joita niin kutsutut louhijat ratkaisevat tehokkailla tietokoneillaan. Kun louhija saa laskutehtävän ratkaistua, muut louhijat varmistavat sen ja tapahtumat tiivistetään lohkoksi, joka liitetään edellisen lohkon perään. Ympäri internetiä jaettua tilikirjaa on mahdoton väärentää, koska tässä onnistuakseen kaikki kopiot tilikirjasta pitäisi väärentää. Poikkeavat tilikirjat hylätään automaattisesti. (2p)
- Avoimet lohkoketjut ovat järjestelmiä, joihin kuka tahansa voi osallistua. Kuka tahansa voi osallistua avoimen lohkoketjun varmistamiseen, ja lohkoketjussa tapahtuvat transaktiot ovat kaikkien nähtävillä. Suljetut lohkoketjut ovat rajatulle porukalle, joka yleensä tuntee toisensa. Suljetussa lohkoketjussa tapahtuvien transaktioiden tarkasteleminen vaatii luvan. (0,5 p)
- Haarautuvat ketjut: Soft fork – protokollapäivityksestä aiheutuva haarautuminen. Hard fork luodaan tietoisesti uusi ketju, jolla sama historia kuin alkuperäisellä. Mutta se ei synkronoidu alkuperäisen ketjun kanssa. (0,5 p)

Tehtävä 4. Pohdi mitä hyviä ja huonoja puolia lohkoketjuteknologian käyttöön voi liittyä? (4 p)

Vastauksesta tulisi käydä ilmi muun muassa seuraavat asiat:

Hyviä puolia (2 p)

- Lohkoketjuun perustuvan hajautetun tietokannan merkittävin etu on korkea vikasietokyky. Järjestelmä ei kaadu, vaikka osa siitä joutuisi esimerkiksi verkkohyökkäyksen kohteeksi.
- Hajautettu järjestelmä: kriittisen infran suojaaminen kyberhyökkäyksiltä
- luotettava: vaikea väärentää
- omien henkilötietojen omistaminen
- muutokset liiketoiminnassa:
    - välittäjät (kuten Amazon) poistuvat ja tämä kilpailumahdollisuuksia pienemmille yrittäjille
    - varmentajien poistuminen (kuten pankit) kuluttajat voivat käydä kauppaa luotettavasti ilman välikäsiä

    - arvon välittäminen, säilyttäminen ja turvaaminen, perustuu älykkäisiin sopimuksiin
- viranomaistoiminnan avoimuus
- välikädettömyys lisää luottamusta etenkin kehittyvissä maissa, joissa on esimerkiksi korruptiota, kehittyvissä maissa voi mahdollistaa rahan tallettamisen turvallisesti älypuhelimen avulla

Huonoja puolia (2 p)

- skaalautuvuus, mitä tapahtuu kun käyttäjämäärät kasvavat
- käsiteltävien tapahtumien (transaktioiden) pieni määrä vrt. Visa 4000 tapahtumaa per sekunti
- teknologian keskeneräisyys: esimerkiksi varmistusprosessi vaatii paljon laskutehoa ja sähköä
- avoimuuden takia ei vielä sovellu esim. henkilötietojen käsittelyyn

*Hyvistä ja huonoista puolista **perustellusti** kootusta kokonaisuudesta max. 4 pistettä. Pelkkä luettelo ei siis riitä, kyse on esseevastauksesta. Kyseessä on laaja kysymys, joten täysiin pisteisiin vaaditaan kattava, perusteltu kokonaisuus.*