Kryptovaluuttoista ja lohkoketjuista – osa 2

Jyväskylä 18.4.2018

Henri Heinonen (henri.t.heinonen@jyu.fi)

Louhiminen

- Mikä on motivaatio ”louhimiselle”?
- Se on ratkaisu Bysantin kenraalien ongelmaan, jos oletetaan, että ainakin yli puolet verkon laskentatehosta on ”hyväntahtoista”.
- Se on suhteellisen yksinkertainen, mutta ei ainoa mahdollinen, tapa saavuttaa konsensus (yhteisymmärrys) hajautetussa järjestelmässä.

Louhiminen

- Bitcoinin lohkoja suojelee työtodistuskonsensusalgoritmi (PoW), joka käyttää kryptografisia tiivisteitä.
- Millä todennäköisyydellä löytyy tiiviste, jossa on viisi etunollaa (0x00000ABCDEF…)?
- Heksoja on 16 erilaista.
- Ensimmäinen merkki on 0, todennäköisyydellä 1/16.
- Toinen merkki on 0, todennäköisyydellä 1/16. jne.
- Vastaus: $(1/16)^5 = 1 / 1\,048\,576$.

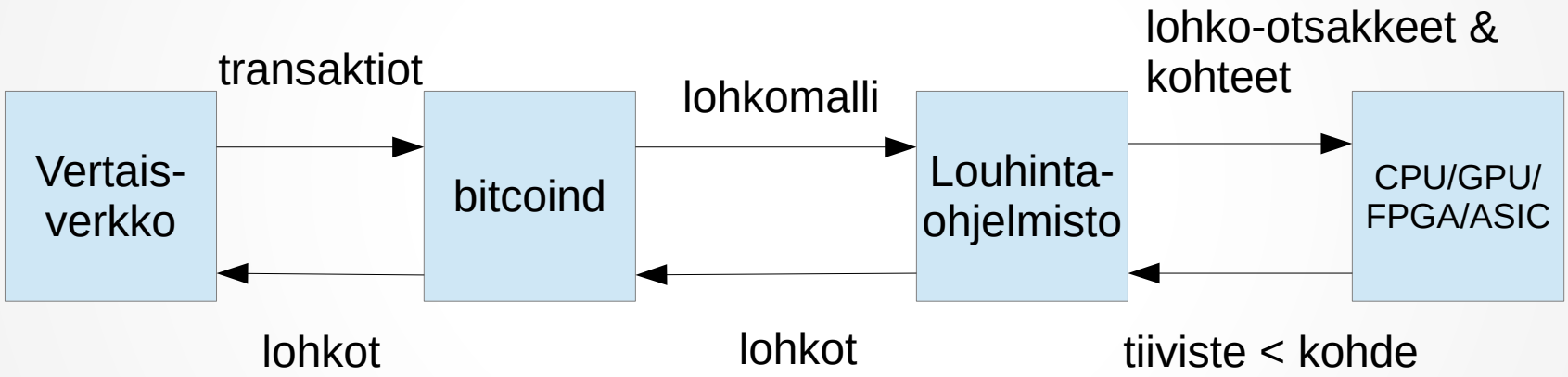
Louhiminen

```
while(nonce < MAX):
    if sha256(sha256(block+nonce)) < target:
        return nonce
    nonce += 1
```

Louhiminen soolona

- Kun Bitcoin aloitti, louhiminen tapahtui soolona. Tämä oli mahdollista, koska louhijoita oli melko vähän ja tuolloin käytettiin louhimiseen tietokoneen CPU:ta, joten louhiminen oli melko tasaväkistä. Esimerkiksi: Jos koko maailmassa oli vain noin 1000 CPU:ta louhimassa, oli hyvä todennäköisyys voittaa itsekin tässä lottopelissä.
- Nykyään soolona louhiminen on vaikeaa, koska on epätodennäköistä, että sillä ansaitsee bitcoineja ilman mittavia laitteistohankintoja.
- Louhintaohjelmisto saa lohkomalleja (block template) bitcoind-ohjelmalta.
- Jos pitkän yrittämisen (yleensä pitää kokeilla miljardeja nonce-arvoja) jälkeen lohko lopulta löytyy, louhintaohjelmisto lähettää lohkon bitcoind-ohjelmalle, joka puolestaan lähettää sen vertaisverkkoon.

Louhiminen soolona



Louhiminen altaassa

- Nykyään louhiminen tapahtuu altaissa eli palvelimissa, joihin monet käyttäjät ottavat yhteyttä. Yleensä käytetään nykyään ASIC-louhimia, joita voi ostaa muutamalla sadalla tai tuhannella eurolla.
- Uuden Bitcoin-lohkon voi löytää siis allas, jonka laskentateho on sen käyttäjien louhimien laskentatehojen summa.
- Käyttäjät saavat altaalta bitcoin-louhittavaksi lohkomallin (block template) sijasta prototyyppilohkoja (prototype block).
- Allas puolestaan saa käyttäjiltä lohkojen sijasta osuuksia (shares).
- Allas saa löydetystä lohkosta palkinnoksi lohkopalkkion ja siirtokulut.
- Palkkiot jaetaan käyttäjien kesken; on olemassa lukuisia erilaisia palkkionjakostrategioita. Allas ottaa usein pienen osuuden itselleen ylläpitokustannusten kattamiseksi.
- Voi olla vaarallista konsensuksen kannalta, jos vihamielinen allas saa haltuunsa puolet tai enemmän koko verkon laskentakapasiteetista: ”51% hyökkäys”

”51% hyökkäys”

Hyökkääjä voisi:

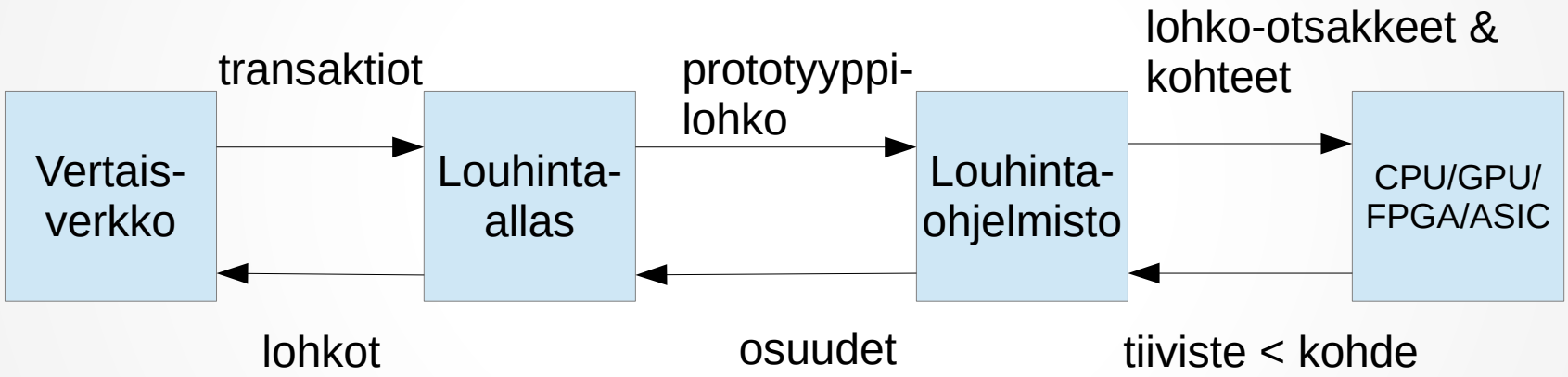
- Kumota transaktioitaan eli lähettää ensin rahaa jollekulle, ja ottaa ne sitten takaisin itselleen.
- Estää joitain tai jopa kaikkia transaktioita saamasta varmistuksia.
- Estää joitain tai jopa kaikkia muita louhijoita louhimasta valideja lohkoja.

Hyökkääjä **ei** voisi:

- Kumota muiden ihmisten transaktioita ilman heidän suostumustaan.
- Estää transaktioita lähtemästä lainkaan (näkyisi 0 varmistusta).
- Muuttaa lohkopalkkiota.
- Luoda kolikoita tyhjästä.
- Lähettää kolikoita, jotka eivät koskaan kuuluneet hänelle.

Lähde: https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

Louhiminen altaassa



Miksei louhimisessa lasketa jotain ”hyödyllistä”?

- Usein tulee esille idea tiivistelaskennan hyödyttömyydestä: tiivisteillä ei ole varsinaista tieteellistä käyttöarvoa.
- Olisi vaikea tehdä desentralisoitu ratkaisu, jossa laskettaisiin vaikkapa lääkeainesimulointia: a) mistä data tulisi?, b) kuka varmistaa, että tulokset ovat valideja?, c) miten säätää laskennan vaikeutta?, d) entäs laskennasta päättävän tahon etulyöntiasema? Voisi tehdä laskentaa, jossa juuri he ovat kaikkia muita parempia.
- On olemassa joitakin mielenkiintoisia yrityksiä: a) PrimeCoin etsii louhinnan aikana uusia alkulukuja, b) GridCoin ajaa taustaa BOINC-laskentaa ja myöntää palkkioksi gridcoineja.