Kryptovaluuttoista ja lohkoketjuista – osa 4

Jyväskylä 25.4.2018

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

Mitä bitcoinilta/kryptovaluutalta vaaditaan ollakseen toimiva maksujärjestelmä?

- Volatiliteetin vähentäminen
- Konsensusalgoritmin vaihtaminen
- Skaalautuvuuden parantaminen
- Lohkoketjun sirpalointi (sharding)
- Atomiset vaihdot
- Siirtyminen kvanttitietokoneturvallisiin algoritmeihin
- Anonymiteetin parantaminen

Volatiliteetin vähentäminen

Volatiliteetin vähentäminen

- Bitcoinin kurssivaihtelua kutsutaan volatiliteetiksi.
- Puolen vuoden sisällä (lokakuu 2017...huhtikuu 2018) bitcoinin arvo on vaihdellut Bitstamp-pörssissä välillä 4602 EUR/BTC...16457 EUR/BTC.
- Ero on ollut puolen vuoden sisällä siis suurimmillaan 3,5-kertainen.
- Bitcoinin volatiliteettia selitetään sääntelyn epävarmuudella, pienellä likviditeetillä, pienellä markkina-arvolla, rajatulla markkinakäytöllä, kapealla omaksumisella, jne.
- Suuri volatiliteetti tekee bitcoinista varmasti kiinnostavan sijoituskohteen, mutta vähemmän houkuttelevan vaihdannan välineen: ”Jos taulutelkkari maksaisi nyt puoli bitcoinia, entäs, jos parin kuukauden odottamisen jälkeen saan samalla määrällä bitcoineja kolme yhtä arvokasta taulutelkkaria?”

Volatiliteetin vähentäminen

- On ehdotettu muutoksia Bitcoinin protokollaan siten, että bitcoineja syntyisi enemmän silloin, kun bitcoinin hinta on korkealla, ja vastaavasti bitcoineja syntyisi vähemmän silloin, kun bitcoinin hinta on matalalla. Vaikeuksia tuottaa kuitenkin bitcoinin rehellisen hintatiedon hakeminen ”ulkomaailmasta” ja syöttäminen lohkoketjuun.
- On ehdotettu, että lompakossa olevien bitcoinien määrän pitäisi vaihdella bitcoinin ostovoiman perusteella. Tässäkin vaikeuksia tuottaa rehellisen hintatiedon hakeminen ja syöttäminen.
- On ehdotettu, että jonkinlainen keskuspankki voisi hallinoida bitcoinin rahapolitiikkaa.

Konsensusalgoritmin vaihtaminen

- Bitcoinin konsensusalgoritmina toimii SHA-256-tiivistefunktiota hyödyntävä työtodistus (Proof-of-Work), joka toimii siten, että eniten työtä (raskain ketju) sisältävä ketjuhaara on se, jota louhijat yrittävät työstää eteenpäin.
- Louhinta on siirtynyt aikojen saatosta tietokoneiden keskussuorittimilta (CPU) näytönohjaimille (GPU), ja lopulta erikoisvalmisteisiin FPGA- ja ASIC-piireihin. Tavallaan ASIC-piirit ovat energiatehokas tapa louhia bitcoineja, koska ne on suunniteltu pelkkään SHA-256-laskentaan.
- Louhimisesta on kuitenkin tullut FPGA:n ja ASIC:in myötä hyvin keskitettyä, koska on parempi ostaa suuri määrä ASIC-laitteita ja viedä ne paikkaan, jossa on halpaa sähköä ja mahdollisesti luonnollinen jäähdytysmekanismi (merivettä, kylmä ilmasto). Tavallinen käyttäjä ei ehkä hanki ASIC:ia, koska sillä voi tehdä vain SHA-256-laskentaa. Vertaa: CPU ja GPU, joilla voi tehdä hyvin yleiskäyttöistä laskentaa.

Konsensusalgoritmin vaihtaminen

- Bitcoinin konsensusalgoritmina toimii SHA-256-tiivistefunktiota hyödyntävä työtodistus (Proof-of-Work), joka toimii siten, että eniten työtä (raskain ketju) sisältävä ketjuhaara on se, jota louhijat yrittävät työstää eteenpäin.
- Louhinta on siirtynyt aikojen saatosta tietokoneiden keskussuorittimilta (CPU) näytönohjaimille (GPU), ja lopulta erikoisvalmisteisiin FPGA- ja ASIC-piireihin. Tavallaan ASIC-piirit ovat energiatehokas tapa louhia bitcoineja, koska ne on suunniteltu pelkkään SHA-256-laskentaan.
- Louhimisesta on kuitenkin tullut FPGA:n ja ASIC:in myötä hyvin keskitettyä, koska on parempi ostaa suuri määrä ASIC-laitteita ja viedä ne paikkaan, jossa on halpaa sähköä ja mahdollisesti luonnollinen jäähdytysmekanismi (merivettä, kylmä ilmasto). Tavallinen käyttäjä ei ehkä hanki ASIC:ia, koska sillä voi tehdä vain SHA-256-laskentaa. Vertaa: CPU ja GPU, joilla voi tehdä hyvin yleiskäyttöistä laskentaa.
- Ethereumin Ethash-algoritmi on PoW, josta on tarkoituksellisesti rakennettu ASIC-resistentti eli on vaikeaa luoda ASIC-piiriä, jota voisi käyttää Ethash-laskemiseen. Toinen esimerkki on Litecoinin Scrypt-algoritmi, jolle tosin on jo osattu kehittää ASIC-piirejä.

Konsensusalgoritmin vaihtaminen

- Bitcoinin louhiminen kuluttaa pienehkön valtion verran sähköä.
- Vähemmän energiaa tarvitseva konsensusalgoritmi on varantotodistus (Proof-of-Stake). Tässä konsensusta pääsee muodostamaan, jos omistaa kyseisen lohkoketjun rahaketta ja pitää niitä hallussaan tietyn ajan.
- Ethereum on siirtymässä Casper-nimiseen varantotodistusalgoritmiin.
- Peercoin käyttää varantotodistusta.

Skaalautuvuuden parantaminen

- Bitcoinin yhden megatavun lohkoon mahtuu tyypillisesti muutama tuhat transaktiota.
- Uusia lohkoja syntyy keskimäärin 10 minuutin välein.
- Siispä bitcoin-transaktioita voi olla vain muutama kappale sekunnissa, maailmanlaajuisesti.
- Jotta bitcoin olisi oikeasti miljardien ihmisten käytettävissä, pitäisi pystyä käsittelemään tuhansia transaktioita joka sekunti.
- Tämä taas tarkoittaisi, että lohkoketju kasvaisi jopa useita gigatavuja tunnissa. Vertailun vuoksi: 9 vuoden aikana Bitcoinin lohkoketju on kasvanut nollasta noin 150 gigatavuun.

Skaalautuvuuden parantaminen

- Lohkokoon kasvattaminen yhdestä megatavusta esimerkiksi kahdeksaan megatavuun on vain väliaikainen ratkaisu.
- Samalla tavoin lohkojen välillä kuluvan ajan pienentäminen 10 minuutista esimerkiksi 2,5 minuuttiin (kuten Litecoinilla) tai noin 15 sekuntiin (kuten Ethereumilla), olisi vain osaratkaisu skaalautuvuusongelmaan.
- Entäs, jos kaikkia transaktioita ei edes talletettaisi lohkoketjuun? Salamaverkkoa (Lightning Network) on jo onnistuneesti testattu.
- Salamaverkko toimii siten, että avataan maksukanava ostajan ja myyjän välille, tehdään vaikkapa muutamia kymmeniä tai satoja maksusuorituksia esimerkiksi kuukauden aikana (ostetaan joka aamu kupillinen kahvia), ja lopulta suljetaan maksukanava. Ainoastaan maksukanavan avaamiseen ja sulkemiseen liittyvät transaktiot talletetaan lohkoketjuun. Järjestelmä on rakennettu siten, että huijaamismahdollisuutta ei ole, ja lisäksi verkko osaa itse etsiä parhaan (siirtokulujen suhteen halvimman) reitin transaktioille.

Lohkoketjun sirpalointi (sharding)

- Tietokannan sirpalointi eli horisontaalinen osittaminen tarkoittaa suunnitteluratkaisua, jossa tietokantataulun rivit pidetään erillään.
- Tämä tarkoittaa sitä, että jokaisen yksittäisen sirpaleen ei tarvitse sisältää kaikkea tietokannan sisältämää dataa.
- Bitcoinin lohkoketju on tällä hetkellä noin 150 gigatavua. Tämän verran dataa on jokaisen täyssolmun (full-node) ladattava Bitcoinin vertaisverkosta.
- Bitcoin-sovellukset mahdollistavat kyllä lohkoketjun karsimisen (pruning), mutta täyssolmun on kuitenkin ladattava koko lohkoketju ennen karsimista.
- Olisi tärkeää saada lohkoketju sirpaloitua vaikkapa siten, että älypuhelimeen voisi ladata gigatavun verran sirpaloitua lohkoketjua.

Atomiset vaihdot

- Entä, jos omistan bitcoineja, mutta haluan vaihtaa osan niistä litecoineiksi? Litecoineja (ja useimpia kryptovaluuttoja) on vaikeaa ostaa fiat-rahalla.
- Melkein ainoa mahdollisuus on siis vaihtaa bitcoineja halutuksi kryptovaluutaksi kolmannen osapuolen ylläpitämässä pörssissä. Tämä on kuitenkin hyvin keskitetty ratkaisu, jossa välikäsi ottaa pienen siivun vaihtokaupoista. Lisäksi monet pörssit toimivat harmaalla alueella lainsäädännön suhteen.

Atomiset vaihdot

- Atomiset vaihdot (atomic swaps) on kokeiluvaiheessa olevaa tekniikkaa, joka mahdollistaa eri lohkoketjuissa olevien rahakkeiden keskinäiset vaihdot ilman kolmatta osapuolta. Lisäksi vaihdot tapahtuvat atomisesti eli joko ne tapahtuvat kokonaan (100%) tai eivät ollenkaan. Vertailun vuoksi: Kolmannen osapuolen ylläpitämässä pörssissä pitää ensin lähettää bitcoineja pörssisivuston ylläpitämään lompakkoon, ja vasta pitkähkön odottelun (minuutteja/tunteja) jälkeen pääsee tekemään osto- ja myyntitarjouksia pörssisivuston muiden käyttäjien kanssa.

Siirtyminen kvanttitietokoneturvallisiin algoritmeihin

- Kvanttitietokoneille suunniteltu Shorin algoritmi soveltuu kokonaislukujen tekijöihinjakoon polynomiaalisessa ajassa.
- Muutama vuosi sitten Shorin algoritmilla saatiin jaettua tekijöihin luku 21. (21 = 7 * 3.)
- Toinen kvanttitietokoneille suunniteltu algoritmi on Groverin algoritmi, joka on yleiskäyttöisempi eli sillä voisi yrittää murtaa myös SHA-256- ja RIPEMD-160-tiivistefunktioita.
- Groverin algoritmi ei kuitenkaan nopeuta murtamisyrityksiä yhtä dramaattisesti kuin Shorin algoritmi.
- Käytetty bitcoin-osoite (josta on joskus siirretty bitcoineja) on paljastanut julkisen avaimen. Elliptisen käyrän kryptografiaa voidaan yrittää murtaa Shorin algoritmilla.
- Käyttämätön bitcoin-osoite (josta ei ole siirretty bitcoineja) on paremmassa turvassa, koska RIPEMD-160 olisi Groverin algoritmista huolimatta melko turvallinen.

Siirtyminen kvanttitietokoneturvallisiin algoritmeihin

- Vuonna 1979 kehitetty Lamportin allekirjoitusjärjestelmä voisi tehdä Bitcoinista kvanttitietokoneturvallisen.
- https://en.wikipedia.org/wiki/Lamport_signature
- https://web.archive.org/web/20160116115057/https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/
- http://www.bitcoinnotbombs.com/bitcoin-vs-the-nsas-quantum-computer/