Liite lausuntoon HE 167/2018 vp

BITCOIN-SANAKIRJA

Altcoin: Altcoin-nimityksellä viitataan kaikkiin niihin virtuaalivaluuttoihin, jotka ovat vaihtoehtoja Bitcoinille ja joilla on oma lohkoketjunsa.

Fork, suom. haara, haarauma: Virtuaalivaluutalle tehty ohjelmistopäivitys, jonka lopputuloksena syntyy uusi valuutta vanhan pohjalta. Uusi valuutta voi olla yhteensopiva vanhan valuutan kanssa (soft fork) tai täysin uusi valuutta (hard fork). Esimerkki Bitcoinista on haarautunut Bitcoin Cash.

(Virtuaalivaluutta)lompakko: Virtuaalivaluutan säilytystapa, joka voi olla esim. online- , desktop-, hardware- ja paperilompakko. Kylmä lompakosta / kylmävarastosta puhutaan silloin, kun virtuaalivaluutan kuluttamiseen tarvittava yksityinen avain on “offline” eli ei ole millään internettiin kytketyllä tietokoneella.

Konsensusmekanismi: Mekanismi, jonka avulla kaikki lohkoketjun käyttäjät hyväksyvät transaktion oikeellisuuden ja lohkoketjun sisällön. Bitcoin-lohkoketjun käyttämä konsensusprotokolla tarkoittaa, että lohkon validointiin sitoutuu paljon energiaa.

Lohko (block): lohko koostuu määrätyin väliajoin yhteen niputetuista transaktioista, joita kutsutaan lohkoiksi.

Lohkoketju (blockchain): Lohkoketju on hajautetussa verkossa toimiva, avoimeen lähdekoodiin perustuva kirjanpitojärjestelmä, joka on matemaattisesti varmennettu ja sen tiedot ovat muuttumattomia. Kaikki transaktiot ovat aikajärjestyksessä, kaikkien osapuolten vahvistamia ja tallennettu niin, että mitään ei voida muuttaa tai väärentää.

Louhinta, eng mining: Lohkoketjujen ylläpitoa ja niissä tapahtuvien transaktioiden vahvistamista yleensä luovuttamalla tietokoneen resurssit verkon käyttöön. Vastineeksi lohkoketjujen ylläpitoon osallistuville koneille maksetaan palkkiona pieniä määriä ylläpidettyä virtuaalivaluuttaa.

Node: Lohkoketjun ylläpitoon osallistuva tietokone. Katso louhinta.

Salamaverkko, eng Lightning Network: Bitcoinin lohkoketjun päälle toteutettu siirtoverkko, joka mahdollistaa teoriassa huomattavasti aiempaa nopeammat ja edullisemmat transaktiot, ja jonka avulla lohkoketjun skaalautuvuuden rajoitteet voidaan kiertää.

Satoshi Nakamoto: Bitcoinin kehittäjän käyttämä pseudonyymi. Satoshi Nakamoto nimellä esiintynyt henkilö tai taho loi bitcoinin ja jättäytyi tuntemattomaksi.

Solmu (Node): jokainen lohkoketjun ylläpitoon osallistuva tietokone tai palvelin toimii solmuna, ja jokaisessa solmussa on yhdenmukainen kopio jaetusta tietokannasta eli lohkoketjusta. Kaikilla osallistujilla ja solmuilla ei tarvitse olla täydellistä kopiota

TXID (Transaction Identifier): Bitcoin-siirron tunniste, jonka avulla lohkoketjusta voi tarkastella siirron tilaa ja perustietoja. TXID voidaan syöttää erilaisiin lohkoketju explorer -ohjelmiin, esimerkiksi blockchain.info

Älysopimus, eng. smart contract: Järjestelmä lohkoketjussa, jolla on mahdollista solmia ja toteuttaa sopimuksia itsenäisesti. Lisäksi älysopimuksen on mahdollista valvoa sopimuksen noudattamista sekä asettaa sanktioita, jos toinen osapuoli ei noudata sopimusta. Hyvin laaditulla älysopimuksella tehty kauppa ei tarvitse kaupanvahvistajaa tai muuta ulkopuolista tahoa.