Kryptovaluuttoista ja lohkoketjuista – osa 1

Jyväskylä 17.4.2018

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

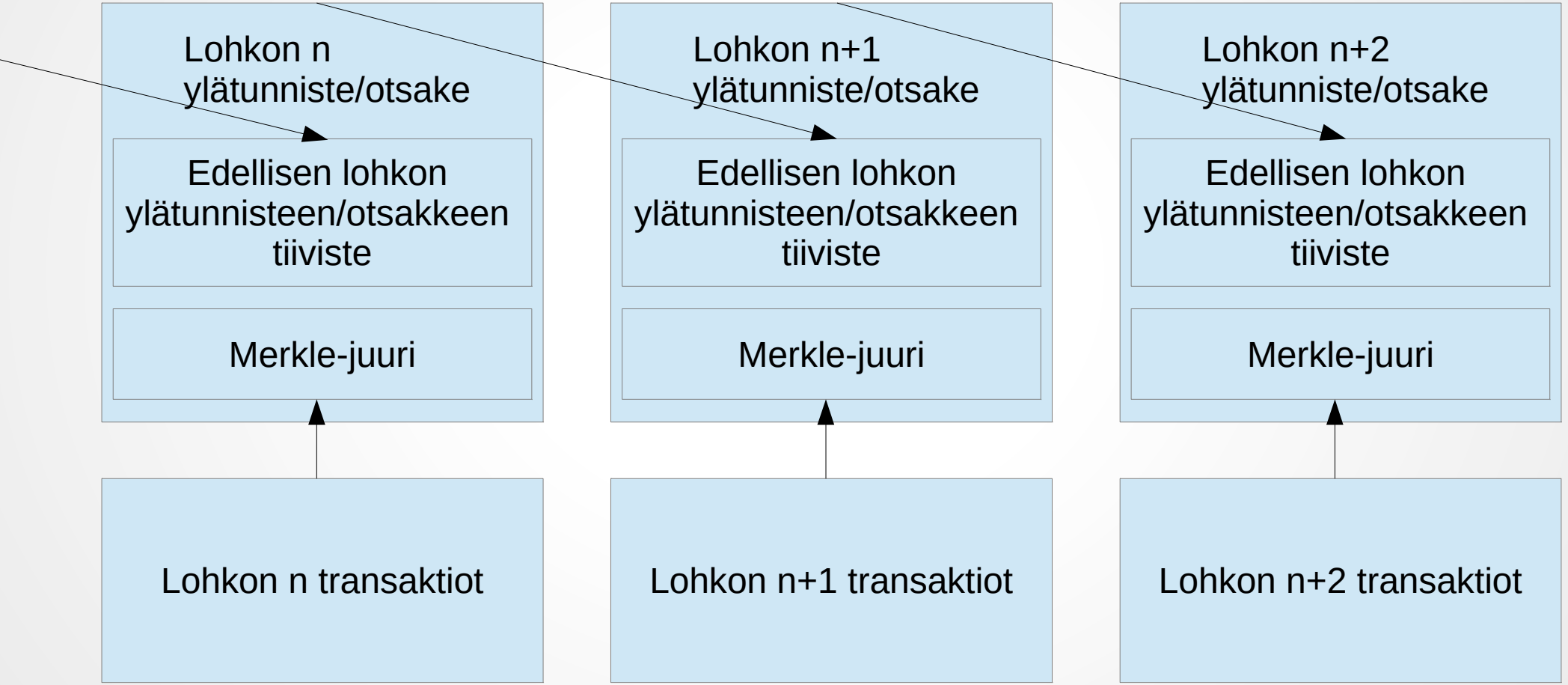
Mikä on lohkoketju?

- BitTorrent on kuuluisa esimerkki vertaisverkkopohjaisesta (P2P, peer-to-peer) ratkaisusta.
- BitTorrent mahdollistaa tiedostojen jakamisen ilman keskuspalvelinta siten, että jokainen verkon käyttäjä toimii tavallaan sekä asiakkaana että palvelimena.
- Vertaisverkot tekevät tiedostojen jakamisen halvaksi ja nopeaksi, koska ei tarvita enää keskuspalvelinta nopean Internet-yhteyden päähän.

Mikä on lohkoketju?

- Lohkoketju on vertaisverkossa jaettava tietokanta/tilikirja.
- Lohkot sisältävät tyypillisesti transaktioita ja otsake-/ylätunnistetietoja.
- Lohkoja syntyy tasaisin väliajoin.
- Ketjutus syntyy siitä, että jokainen lohko viittaa edelliseen lohkoon tiivisteosoittimen (hash pointer) avulla. Poikkeuksena on alkulohko (genesis block), jotka ennen ei ollut mitään.

Mikä on lohkoketju?



Miten lohkoja lisätään lohkoketjuun?

- Vertaisverkossa oleva laite lähettää dataa (transaktion) verkkoon lisättäväksi uuteen lohkoon: esimerkiksi bitcoin-lompakon käyttäjä lähettää bitcoineja kaverilleen.
- Louhintasolmut saavat tämän transaktion ja monta muuta transaktiota, ja järjestävät eräänlaisen arpapelin päättäkseen, kenen lohko lisätään lohkoketjuun.
- Palkinnoksi lohkon lisännyt louhija saa lohkon sisältämän lohkopalkkion (Bitcoin vuonna 2018: 12,5 BTC) + siirtokulut, jotka tule transaktion lähettäjältä.

  Lähde: Chainfrog Blockchain Lecture part 1: https://www.youtube.com/watch?v=TyZBV_w4MHg

Miten lohkoja lisätään lohkoketjuun?

Muutamia käytössä olevia konsensusalgoritmeja:

- Työtodistus (proof-of-work): Bitcoin, Litecoin, Ethereum...
- Varantotodistus (proof-of-stake): Peercoin, Ethereum (tulevaisuudessa)…
- Käytännöllinen Bysantin vikasietoisuus (practical Byzantine fault tolerance): Hyperledger Fabric.
- Todistus kuluneesta ajasta (proof of elapsed time): Hyperledger Sawtooth.

Lähde: Chainfrog Blockchain Lecture part 1: https://www.youtube.com/watch?v=TyZBV_w4MHg

Työtodistus

- Bitcoinin työtodistuksen (Proof-of-Work) juuret ovat Adam Backin vuonna 1997 luomassa Hashcash-järjestelmässä, jonka tarkoituksena oli tehdä sähköpostin lähettämisestä sen verran laskennallisesti vaikeaa, että spämmääjien toiminta vaikeutuu.
- Ota data ja lisää siihen nonce: data + nonce.
- Tiivistä se kahdesti: SHA256d(data + nonce) eli SHA256(SHA256(data + nonce)).
- Tarkista, onko saatu tiiviste pienempi kuin verkon vaikeustason (difficulty) määrittelemä kohde (target). (Tarkista siis, että tiivisteessä on riittävän monta peräkkäistä nollaa.)
- Jos ei, tee sama uudelleen arvolla: nonce = nonce + 1.

Lähteet: ”Chainfrog Blockchain Lecture part 3” https://www.youtube.com/watch?v=peckb7295fk, https://en.bitcoin.it/wiki/Difficulty, https://en.bitcoin.it/wiki/Target

Mikä on Bitcoin?

- Bitcoin on kryptovaluutta ja ensimmäinen lohkoketjutekniikoiden sovellus.
- Bitcoin oli alun perin tarkoitettu maksujärjestelmäksi, koska kaikilla ei ole mahdollisuuksia saada pankkitiliä ja/tai luottokorttia.
- Bitcoin on suunniteltu siten, että uusia lohkoja syntyy keskimäärin 10 minuutin välein.
- Bitcoiniin on rakennettu oma rahake: bitcoin. Tämän valuuttayksikkönä on BTC tai virallisemmin XBT. Symbolina on Unicoden koodipaikkaan U+20BF hyväksytty merkki: ₿
- Bitcoin-transaktioiden (siirtojen) varmentaminen vaatii laskentatyötä, joka kuluttaa runsaasti sähköä. Tätä louhimista kannustaa jatkamaan uuden lohkon louhimisen myötä saatava lohkopalkkio ja transaktioiden sisältämät siirtokulut.
- Jokaisen uuden lohkon myötä syntyi alkuvaiheessa 50 uutta bitcoinia järjestelmään. Vuonna 2018 lohkopalkkio on 12,5 BTC/lohko. Lohkopalkkio puolittuu neljän vuoden välein.
- Bitcoinin markkina-arvo on alle vuosikymmenessä kasvanut nollasta liki 117 miljardiin euroon.

Sähköisten valuuttojen historiaa

- David Chaumin paperi vuodelta 1983 ”Blind signatures for untraceable payments” toi esille ajatuksen anonyymistä sähkörahasta.
- DigiCash
- Ecash (Suomessa Meritan kokeilu)
- b-money
- Älysopimukset 1990-luvun alkupuolella

Sähköisten valuuttojen historiaa

- Lokakuussa 2009 Internet-pörssi myi 5050 bitcoinia hintaan 5,02 Yhdysvaltain dollaria. Tästä saadaan vaihtokurssiksi 0,000994 USD/BTC. Hinta laskettiin bitcoinien tuottamiseen käytetyn sähkön arvon perusteella. Tämä lienee ensimmäinen kerta, kun bitcoinille määriteltiin hinta. Lähde: The Bitcoin Standard: The Decentralized Alternative to Central Banking.
- Bitcoinia käytettiin vaihdon välineenä tiettävästi ensimmäistä kertaa 22. toukokuuta 2010; kahden pitsan hinnaksi tuli 25 Yhdysvaltain dollaria eli 10 000 bitcoinia. Lähde: The Bitcoin Standard: The Decentralized Alternative to Central Banking.

Sähköisten valuuttojen historiaa

- Pseudonyymi Satoshi Nakamoto kirjoitti koodipunkkarien (cypherpunks) sähköpostilistalle 1. marraskuuta 2008 ilmoittaakseen, että hän on kehittänyt ”uuden sähköisen käteisjärjestelmän, joka on kokonaan vertaisverkkoon pohjautuva”. Lähde: The Bitcoin Standard: The Decentralized Alternative to Central Banking.
- Bitcoinin alkulohko louhittiin 3. tammikuuta 2009 tai hieman sen jälkeen. Alkulohkossa on viittaus tuoreeseen The Times -sanomalehden otsikkoon: ”The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” eli ”The Times 3. tammikuuta 2009 Valtiovarainministeri pankkien toisen pelastuspaketin kannalla (?).”

Bitcoinin niukkuus

- Myös puhtaasti digitaaliset resurssit voivat olla niukkoja.
- Bitcoin on suunniteltu siten, että niitä tulee olemaan noin 21 miljoonaa kappaletta.
- Tämä raja saavutettaneen noin vuoden 2140 paikkeilla.
- Reilu enemmistö bitcoineista on louhittu jo 10 ensimmäisen vuoden aikana. Tämä on sinänsä ymmärrettävää, koska alussa bitcoinin arvo oli lähellä nollaa, joten niitä oli kätevä saada 50 BTC per lohko. Koska lohkoja syntyy noin 10 minuutin välein, tunnin aika maailmaan syntyi siis 300 uutta bitcoinia.

Mitä bitcoin tarkoittaa?

Bitcoin tarkoittaa oikeastaan montaa eri asiaa.

- **Protokolla**: Määrittely, joka kertoo, miten rakentaa hajautettu tietokanta (lohkoketju), kuinka jäsentää sitä, miten transaktiot pitäisi koota, millainen on validi transaktio, jne.
- **Verkko**: Tämä on vertaisverkko (P2P), johon solmut yhdistyvät.
- **Valuutta**: bitcoin (kirjoitetaan pienellä kirjaimella eli pienaakkosella eli gemenalla). Tämä on Bitcoin-verkon natiivi valuutta. Bitcoineja tulee olemaan noin 21 miljoonaa kappaletta. Tällä hetkellä pienin määrä bitcoineja on bitcoinin sadasmiljoonasosa eli yksi satoshi.
- **Avoimen lähdekoodin toteutus**: Tämä on alkuperäinen avoimen lähdekoodin projekti, joka toteutettiin C++-kielellä. Nykyään projekti tunnetaan nimellä Bitcoin Core.

Lähde: ”Understanding Bitcoin: Cryptography, Engineering and Economics”

Tiivistefunktiot

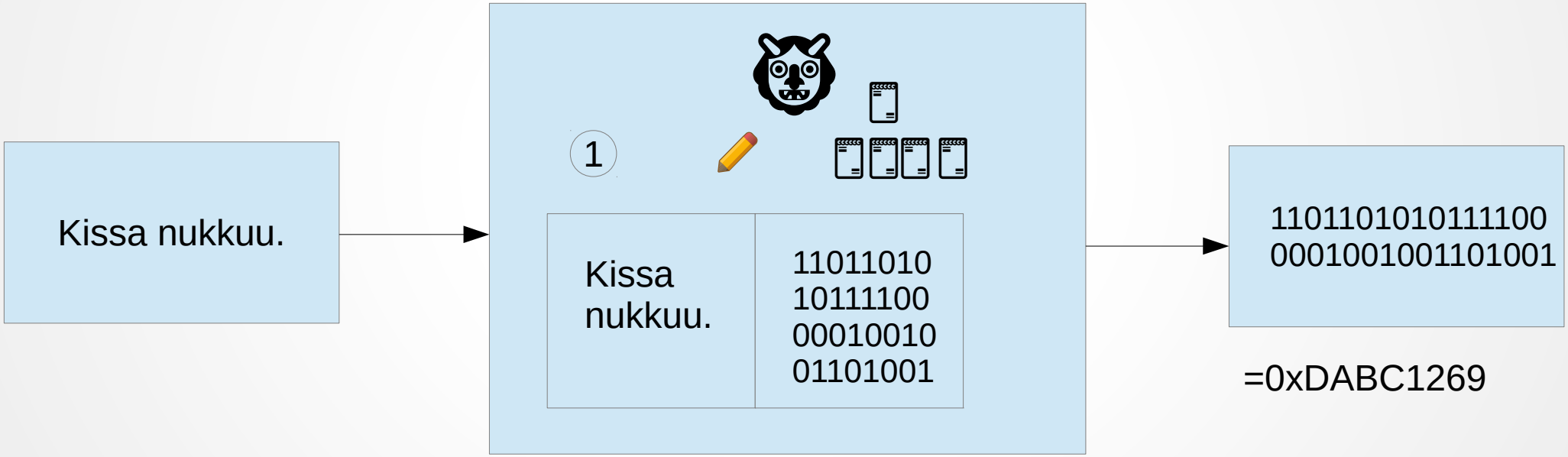
- Yleiset tiivistefunktiot: Mikä tahansa funktio, jolla voi kuvata mielivaltaisen kokoista dataa tietynkokoiseksi dataksi. Näitä tiivistefunktion palauttamia arvoja kutsutaan tiivistearvoiksi, tiivistekoodeiksi tai tiivisteiksi.
- Kryptografiset tiivistefunktiot: Kryptografinen tiivistefunktio on tiivistefunktion erityistapaus, jonka ominaisuudet mahdollistavat sen käytön kryptografiassa. Se on matemaattinen algoritmi, joka kuvaa mielivaltaisen kokoista dataa tietynkokoiseksi bittijonoksi, ja joka on suunniteltu yksisuuntaiseksi funktioksi tarkoittaen sitä, että käänteisfunktion ottaminen on epäkäytännöllistä.

Tiivistefunktiot

- Kuvitellaan laatikko, jossa on olio, kirja, kynä, muistilappuja ja kolikko.
- Kolikon etupuolella lukee ”1” ja kääntöpuolella ”0”.
- Laatikon vasemmassa kyljessä on reikä, josta voi sujauttaa viestin laatikkoon.
- Olio tarkistaa ensin kirjasta, onko sama viesti tullut aiemmin vastaan. Jos ei, olio heittää kolikkoa 32 kertaa ja kirjaa tulokset kirjaan ja muistilapulle. Jos on, olio kopioi kirjasta vanhat tiedot muistilapulle.
- Laatikon oikessa kyljessä on reikä, josta olio sujauttaa muistilapun laatikosta ulos.

  Lähde: ”Owning Bitcoin: The Illustrated Guide to Security, Privacy, and Possibility”

Tiivistefunktiot



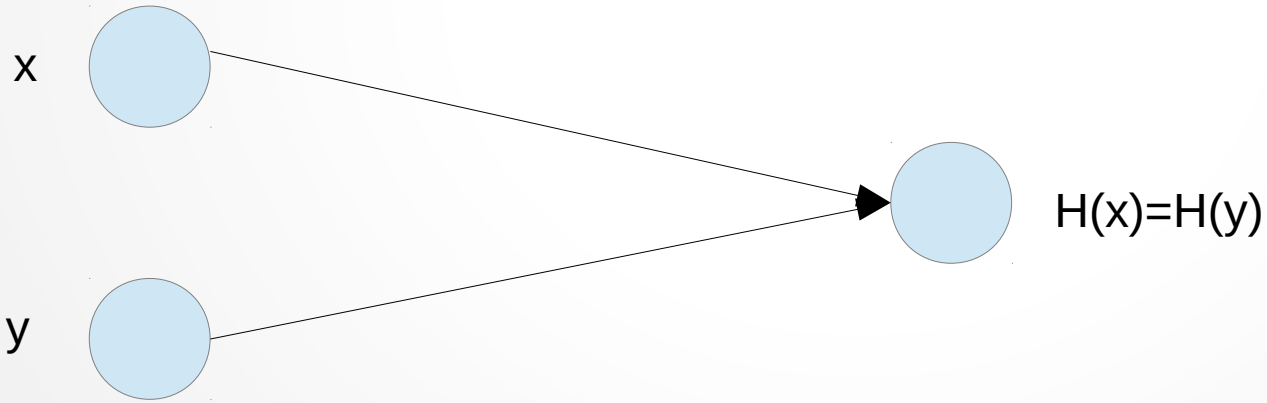
Kryptografisten tiivistefunktioiden tietoturvaominaisuudet

- Ei (löydettäviä) yhteentörmäyksiä
- (myös muita)

  Lähteet: ”Introduction to Crypto and Cryptocurrencies” https://www.coursera.org/learn/cryptocurrency, ”Understanding Bitcoin: Cryptography, Engineering and Economics”

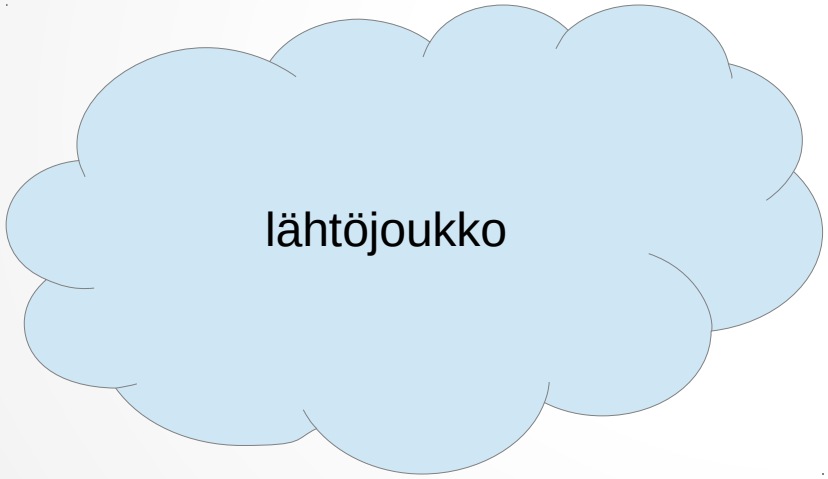
Ei (löydettäviä) yhteentörmäyksiä

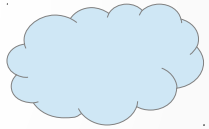
Kukaan ei pysty löytämään x:ää ja y:tä siten, että $x \neq y$ ja $H(x) = H(y)$.



Ei (löydettäviä) yhteentörmäyksiä

- Yhteentörmäyksiä toki on, koska tiivistefunktion lähtöjoukko on paljon suurempi kuin maalijoukko.





maalijoukko

Esimerkki yhteentörmäyksestä

- H(”Kissa nukkuu.”) = 0xDABC1269
- H(”Kissa nukkuu!”) = 0x572AFFF0
- H(”Koira haukkuu!”) = 0xDABC1269

Tiedostojen sormenjälki

- Tiedoston voi tunnistaa sen tiivistefunktion antaman sormenjäljen perusteella.
- MD5(setup.exe) = 0x9b51f5c0f8132886839d806f49f9ff20
- SHA-256(setup.exe) = 0xa490014abc4c937916cd52e58a39a77131e64caa8b8bd7870b8300eb8429085c
- Jos nettisivulla mainitaan, että tiedoston setup.exe SHA-256-tiivisteen tulee olla yllämainittu, mutta omalla koneella suorittamasi SHA-256-tarkistus tiedostolle setup.exe antaa toisenlaisen tiivisteen, on mahdollista, että tiedostoa on peukaloitu! Toinen ikävä mahdollisuus on, että tiedosto on ladattaessa vaurioitunut (esimerkiksi lataaminen on jäänyt kesken).

Avaintenhallinta

- Bitcoinien omistajuus on toteutettu digitaalisten avainten, bitcoin-osoitteiden ja digitaalisten allekirjoitusten avulla.
- Digitaalisia avaimia ei talleteta verkkoon vaan käyttäjän tietokoneelle tiedostoon eli tietokantaan, jota myös lompakoksi kutsutaan.
- Avaintenhallinta on täysin riippumaton Bitcoinin protokollasta ja niitä voidaan luoda ja hallita ilman yhteyttä Internetiin.
- Monissa tilanteissa on jopa suositeltavaa luoda avaimet tietokoneella, joka ei ole koskaan yhteydessä Internetiin.

  Lähde: ”Mastering Bitcoin: Programming the Open Blockchain”

Yksityinen avain

- Yksityinen avain (private key) on yleensä 256-bittinen luku eli se koostuu 256 binäärinumerosta. Bitcoin-maailmassa yksityinen avain on satunnainen kokonaisluku välillä [1, n-1], missä n = FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140.
- Yksityisen avaimen luonti on siis pohjimmiltaan luvun valitsemista väliltä $[1, 2^{256}]$.
- Validien yksityisten avainten alueeseen vaikuttaa Bitcoinin käyttämä ECDSA secp256k1 -standardi.

  Lähde: https://en.bitcoin.it/wiki/Private_key

Yksityinen avain

- Yksityisellä avaimella voi käyttää bitcoineja eli lähettää niitä eteenpäin.
- Yksityinen avain on vähän niin kuin pankkitilin salainen PIN-koodi. Sitä ei saa koskaan paljastaa kenellekään, koska se riittää rahojen varastamiseen.
- Yksityisiä avaimia ei yleensä säilytetä tietokoneella salaamattomassa muodossa.
- Yleensä bitcoin-lompakko huolehtii automaattisesti yksityisistä avaimista.
- Epäilysten pitäisi nousta, jos joku pyytää vaikkapa sähköpostitse suorittamaan komennon ”bitcoin-cli dumpprivkey 1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy” ja lähettämään ohjelman antaman tulosteen ”KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ”.

Kuinka luodaan Bitcoin-osoite? (1/)

Luodaan yksityinen avain heittämällä kolikkoa 256 kertaa. Saadaan binääriluku:

0001100011100001010010100111101101101010001100000111111101000010011010101001010011111000000100010100011100000001111001111100100011100111011101001110011111111001101001000111111000010110000100000001101011101101100101001101000100000011000110010000101110010100.

Tämä on heksadesimaalina:
0x18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725.

Kuinka luodaan Bitcoin-osoite? (2/)

Julkinen avain (K) lasketaan yksityisestä avaimesta (k) elliptisen käyrän kertomisella: K = k * G, missä G on generaattoripiste, joka on määritelty secp256k1-standardissa, ja on kaikille Bitcoin-avaimille sama. Julkiseksi avaimeksi saadaan K = (x, y), missä

x = 0x50863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B2352,
ja y = 0x2CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6.

Liitetään nämä koordinaatit peräkkäin ja laitetaan etuliitteeksi heksa 0x04, jolloin saadaan

K =

0x0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6.

Kuinka luodaan Bitcoin-osoite? (3/)

Otetaan SHA-256-tiiviste julkisesta avaimesta:
SHA256(K) = SHA256(0x0450...A6) =
0x600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408.

Kuinka luodaan Bitcoin-osoite? (4/)

Otetaan RIPEMD-160-tiiviste edellisestä SHA-256-tiivisteestä:
RIPEMD160(0x60...08) =
0x0109667760069 53D5567439E5E39F86A0D273BEE.

Kuinka luodaan Bitcoin-osoite? (5/)

Lisätään edellisen RIPEMD-160-tiivisteen eteen versioetuliite (0x00, kun käytämme Bitcoinin pääverkkoa): 0x00010966776006953D5567439E5E39F86A0D273BEE.

Kuinka luodaan Bitcoin-osoite? (6/)

Otetaan SHA-256-tiiviste edellisestä laajennetusta RIPEMD-160-tuloksesta:
SHA256(0x00010966776006953D5567439E5E39F86A0D273BEE) =
0x445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094.

Kuinka luodaan Bitcoin-osoite? (7/)

Otetaan SHA-256-tiiviste edellisestä SHA-256-tiivisteestä:
SHA256(0x445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094) = 0xD61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30.

Kuinka luodaan Bitcoin-osoite? (8/)

Otetaan edellisestä SHA-256-tiivisteestä 4 ensimmäistä tavua eli 8 ensimmäistä heksadesimaalia: 0xD61967F6.

(1 tavu = 8 bittiä: esim. 1111 1111 = FF = 2 heksaa.
4 tavua = 32 bittiä: esim. 11111111 11111111 11111111 11111111 = FF FF FF FF = 8 heksaa.)

Kuinka luodaan Bitcoin-osoite? (9/)

Lisätään edellisessä kohdassa saadut neljä tarkistussummatavua (0xD61967F6) kohdassa 5 saadun laajennetun RIPEMD-160-tiivisteen (0x00010966776006953D5567439E5E39F86A0D273BEE) loppuun: 0x00010966776006953D5567439E5E39F86A0D273BEED61967F6.

Kuinka luodaan Bitcoin-osoite? (10/10)

Enkoodataan vielä edellisen kohdan tulos Base58-muotoon:
Base58(0x00010966776006953D5567439E5E39F86A0D273B
EED61967F6) = 16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM.