# Kryptovaluuttoista ja lohkoketjuista – osa 3

Jyväskylä 24.4.2018

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

# Digitaalinen allekirjoittaminen

- Asymmetrisen avaimen kryptografiassa käytetään avainpareja, joiden välillä vallitsee matemaattinen yhteys.
- Toista avainta kutsutaan yksityiseksi avaimeksi ja toista julkiseksi avaimeksi.
- Yksityinen avain on suuri satunnaisluku.
- Julkinen avain luodaan yksityisestä avaimesta esimerkiksi ellipisen käyrän matematiikan avulla.
- Yksityinen avain pidetään itsellä salassa, julkinen avain yleensä annetaan muille ihmisille.

# Digitaalinen allekirjoittaminen

- Yksityisellä avaimella kryptattu viesti voidaan dekryptata julkisella avaimella.
- Julkisella avaimella kryptattu viesti voidaan dekryptata yksityisellä avaimella.

# Digitaalinen allekirjoittaminen

- Miten avaimilla voi allekirjoittaa?
- Yleensä kryptataan julkisella avaimella, jolloin viestin vastaanottaja voi dekryptata yksityisellä avaimellaan.
- Digitaalisten allekirjoitusten tapauksessa, kryptataan yksityisellä avaimella, jolloin ”kaikki” voivat dekryptata julkisella avaimella. Viesti ei pysy ”salassa”, mutta tällä tavalla todistetaan, keneltä viesti on peräisin.
- https://8gwifi.org/rsafunctions.jsp

# Digitaalinen allekirjoittaminen

- Alicella on viesti Bobille ”Minä, Alice, maksan 1 bitcoinin Bobille.”
- Alice kryptaa viestin SHA256-tiivisteen yksityisellä avaimellaan.
- Alice lähettää viestin, kryptauksen ja julkisen avaimensa kaikkien nähtäville.
- Jos viestin SHA256-tiiviste ja Alicen julkisella avaimella dekryptattu kryptaus ovat samat, viesti tuli Alicelta.
- Vastaavalla periaatteella Bitcoin-verkon solmut hyväksyvät transaktiot.

# Script-kieli

- Bitcoinissa on oma Script-kieli, jolla voi tehdä yksinkertaisia älysopimuksia. Oikeastaan bitcoin-transaktiot ovat eräänlaisia älysopimuksia.
- Script-kieli on Forth-kielen kaltainen, pinopohjainen, ei Turing-täydellinen kieli, joka käyttää käänteistä puolalaista notaatiota.
- Esimerkkejä käänteisestä puolalaisesta notaatiosta,
  3+4 on 34+
  5*3+4 on 534+*

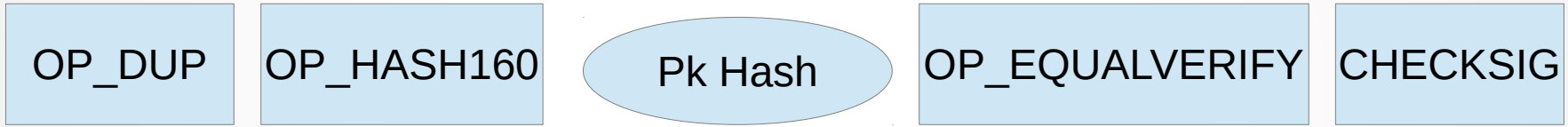
# Script-kieli

- Pinon ideana on LIFO (Last In First Out) eli kirjapinoon lisätään (push) yleensä uusi kirja päällimmäiseksi ja päällimmäinen poimitaan (pop) yleensä ensimmäisenä pois.
- 2+3=5 Bitcoinin Script-kielellä:

  Käänteinen puolalainen notaatio: 23+5=
  OP-koodit: OP_2 OP_3 OP_ADD OP_5 OP_EQUAL

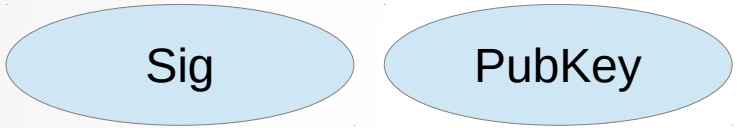
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Ohjeet ja data, jotka Alice antaa transaktion #1 pubkey-skriptissä.



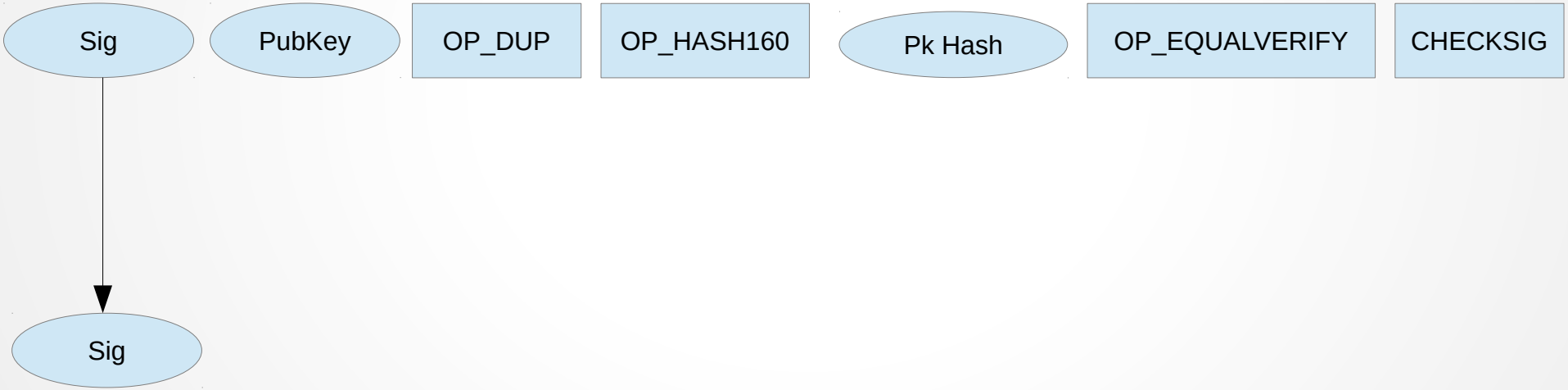
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Data, jonka Bob antaa transaktion #2 allekirjoitus-skriptissä.



# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Bobin allekirjoitusskriptin allekirjoitus lisätään (push) tyhjään pinoon (stack). Koska se on pelkkää dataa, mitään ei tehdä sille.

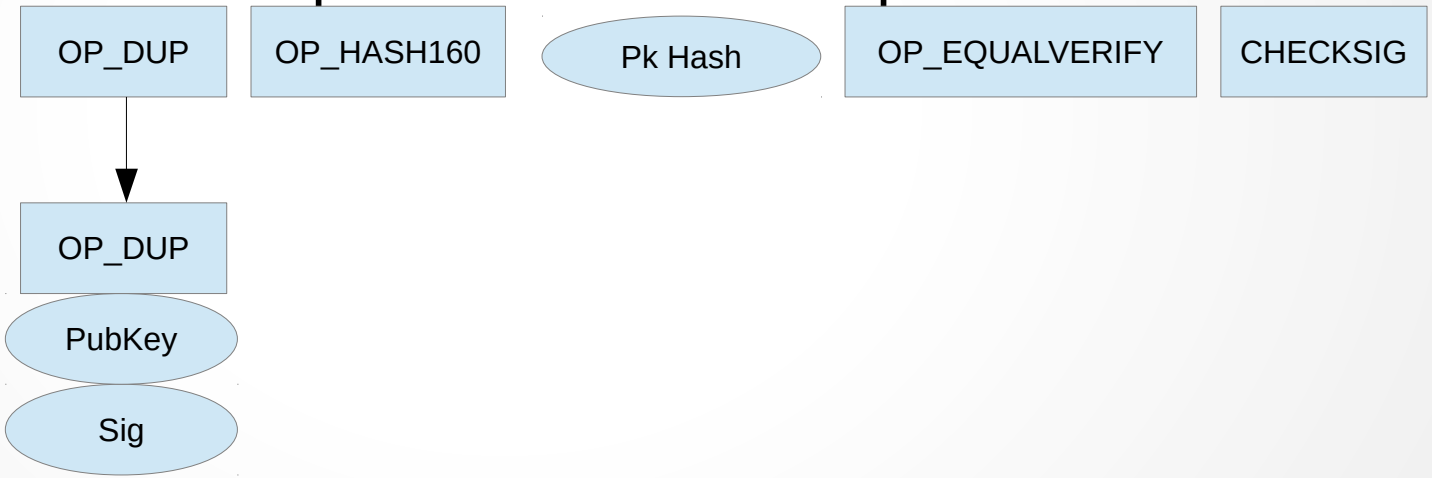


# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Julkinen avain lisätään allekirjoituksen päälle.

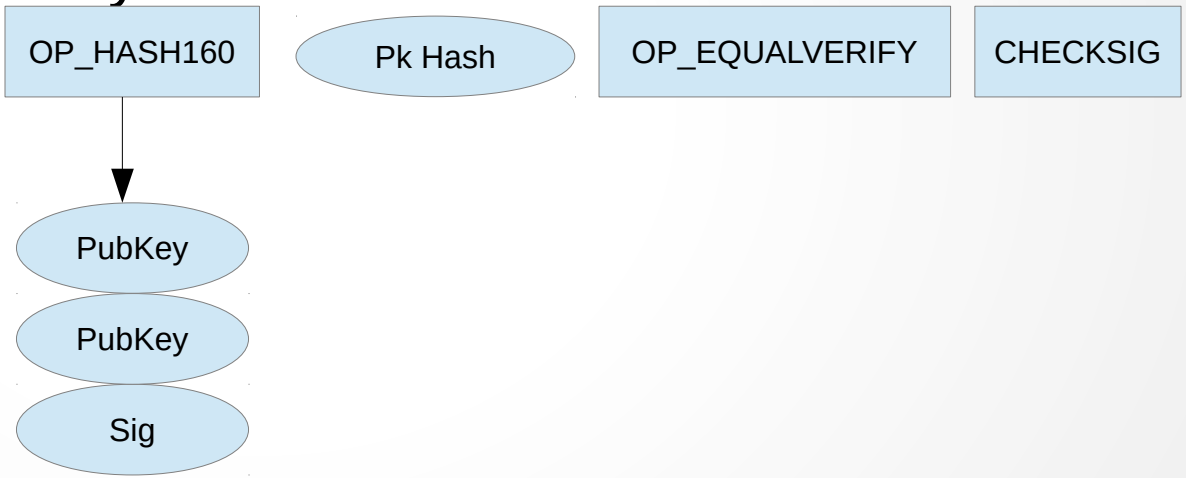
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Alicen pubkey-skriptin OP_DUP-operaatio suoritetaan. OP_DUP lisää pinoon kopion datasta, joka on tällä hetkellä pinon päällä eli tässä tapauksessa tekee kopion Bobin julkisesta avaimesta.



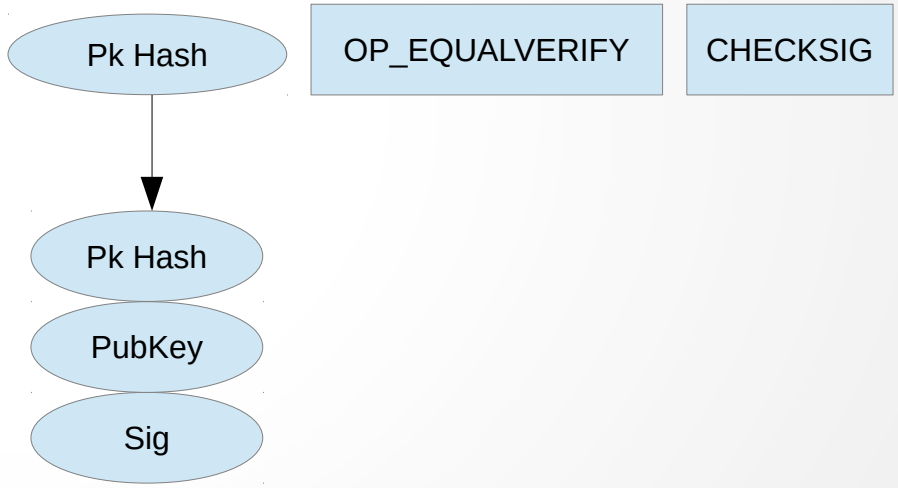
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- OP_HASH160-operaatio tiivistää syötteen kahdesti: ensin SHA-256:llä, sitten vielä RIPEMD-160:lla. Pinossa ylimpänä ollut Bobin julkinen avain on nyt tiivistemuodossa.



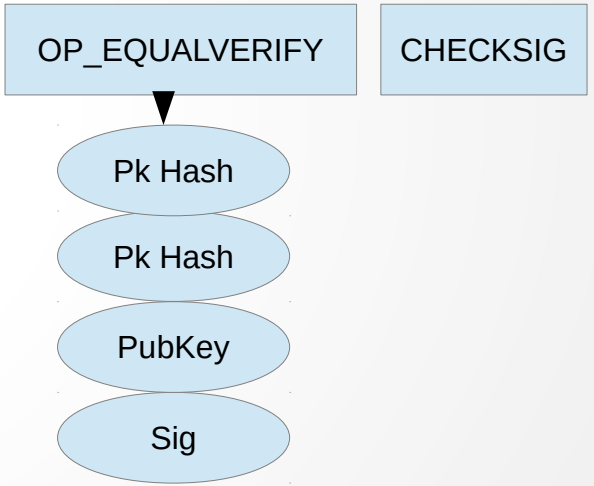
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Nyt Alicen pubkey-skripti lisää pinoon pubkey-tiivisteen, jonka Bob antoi. Tämän jälkeen pinossa pitäisi olla kaksi kappaletta Bobin pubkey-tiivisteitä ylimpänä.



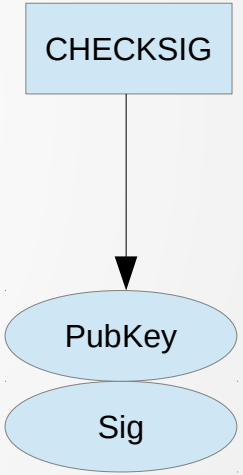
# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Nyt Alicen pubkey-skripti suorittaa OP_EQUALVERIFY-opraation, joka on sama kuin OP_EQUAL-operaatio ja OP_VERIFY-operaatio suoritettuina peräkkäin.
- OP_EQUAL vertaa pinon kahta ylimmäistä arvoa. Se poimii tutkitut arvot pois pinosta ja korvaa ne vertailun tuloksella 0 (epätotta) tai 1 (totta).
- OP_VERIFY tutkii pinon ylimmäisen arvon. Jos arvo on epätotta, suoritus loppuu ja transaktion validointi epäonnistuu. Muutoin poimitaan tosi-arvo pinosta.



# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Lopuksi Alicen pubkey-skripti suorittaa OP_CHECKSIG-operaation, joka tutkii Bobin allekirjoituksen ja Bobin julkisen avaimen. Jos tämän vertailun arvo on totta, lisätään kyseinen totuusarvo pinoon.



# Maksa julkisen avaimen tiivisteelle (P2PKH) -transaktio

- Jos arvo Epätotta ei ole pinossa pubkey-skriptin suorittamisen jälkeen, transaktio on kelvollinen.

TRUE