Krüptoraha alustehnoloogiad

Asse Sauga

Krüptorahanduse Ekspert. Eesti Krüptoraha Liit.

EESTI KRÜPTORAHA LIIT

EESTI KRÜPTORAHA LIIT

Raha muutumine kaubast…

EESTI KRÜPTORAHA LIIT

…müntideks…

EESTI KRÜPTORAHA LIIT

…müntidest paberrahaks…

EESTI KRÜPTORAHA LIIT

…paberrahast bittideks…

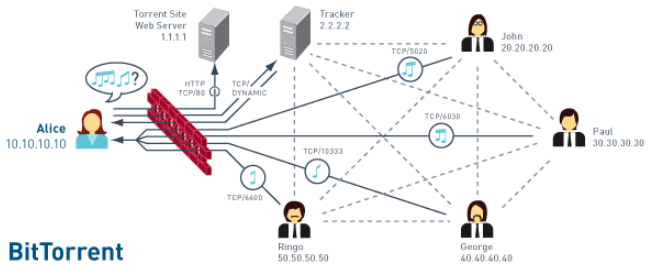
EESTI KRÜPTORAHA LIIT

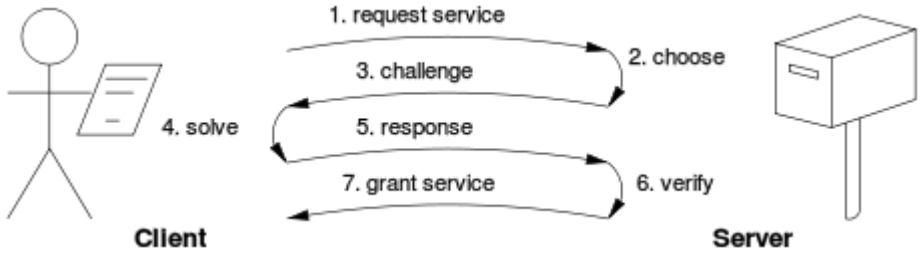
…bittidest kontrollitud bittideks.

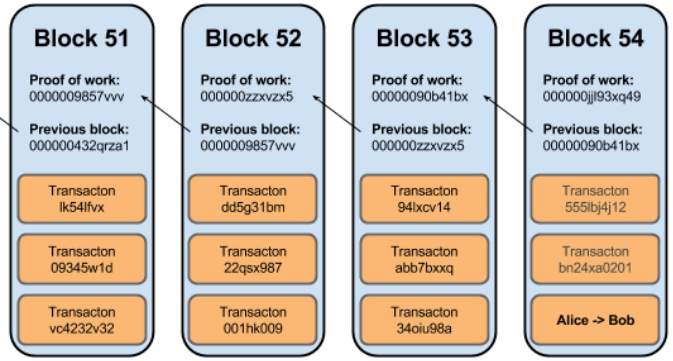
EESTI KRÜPTORAHA LIIT

Kuidas see kõik võimalik on?

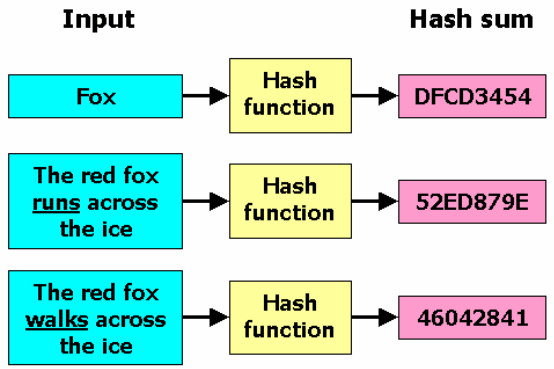
Bitcoini tehnoloogia

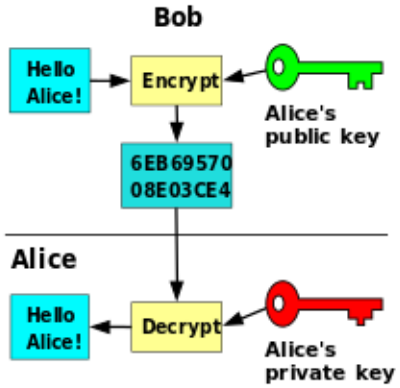






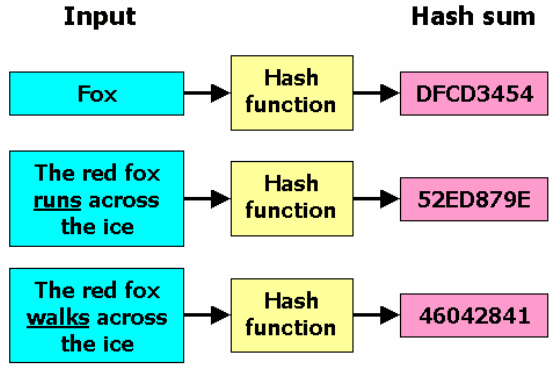
Decentralized





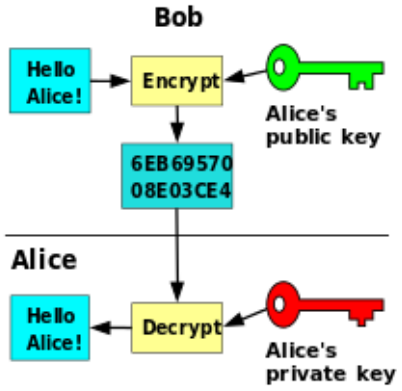
Hash ehk räsi

- Krüptograafiline räsifunktsioon, mida kasutatakse selleks, et kodeerida inimloetav info unikaalseks masinloetavaks infoks („Asse Sauga" räsi võib olla alati näiteks „10B44").
- Igasugune lähteinfo muudatus muudab automaatselt tugevalt ka räsi („Ase Sauga" räsi võib olla hoopis „78D28").
- Bitcoin kasutab SHA-256 räsifunktsiooni – räsi pikkus on 256 bitti ehk 32 baiti. Iga bait = 2 hex numbriga; räsi – 64 hex numbrit.
- SHA256, SHA512, md5 jne.



Võtmepaarid

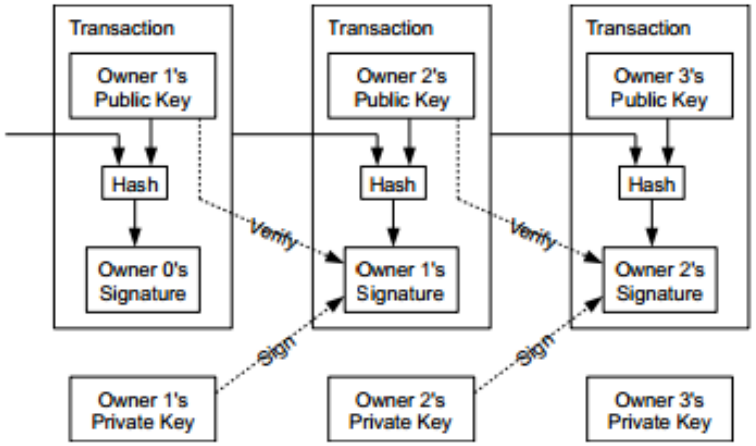
- Bitcoini ülekanded ei ole krüpteeritud – kontoraamat on avalik
- Kasutusel on kaks võtit: privaatvõti (ainult omaniku valduses) ja kõigile avalik võti.
- Ülekande saatja krüpteerib sõnumi saaja avaliku võtmega (aadress)
- Saaja dekrüpteerib sõnumi oma privaatvõtmega
- Võtmete vahel on asümmeetriline suhe – privaatvõtmest saab genereerida avaliku võtme kuid vastupidi mitte.
- Sama meetodit teistpidi kasutatakse sõnumite allkirjastamisel – sõnum allkirjastatakse saatja privaatvõtmega ning avaliku võtmega saab sõnumi kergesti verifitseerida.
- Allkirjastamisel kasutatakse ECDSA (Elliptic Curve Digital Signature Algorithm)



EESTI KRÜPTORAHA LIIT

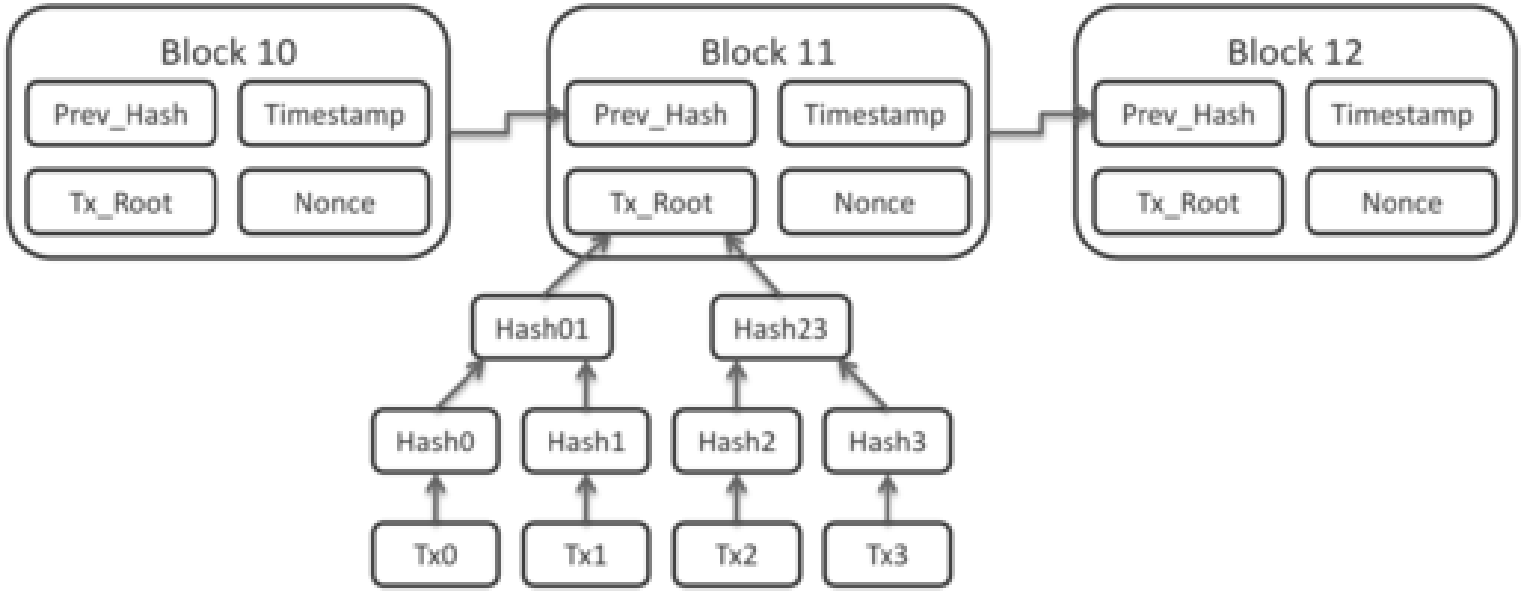
Krüptograafia ülekannetes

- BTC ülekanded sisaldavad omanikuinfot.
- Bitcoinide omanikud on identifitseeritavad krüptograafiliste võtmepaaride kaudu.
- Avaliku võtme kaudu saab genereerida aadressi, mida teab kogu võrk.
- Privaatvõti on Bitcoinide omanik ja sellega allkirjastatakse kõik ülekanded.
- Kõik ülekanded säilitatakse blokkides. Blokid on omavahel seotud blokiahelasse, säilitamaks terviklikkuse ning ajalise järjestuse.



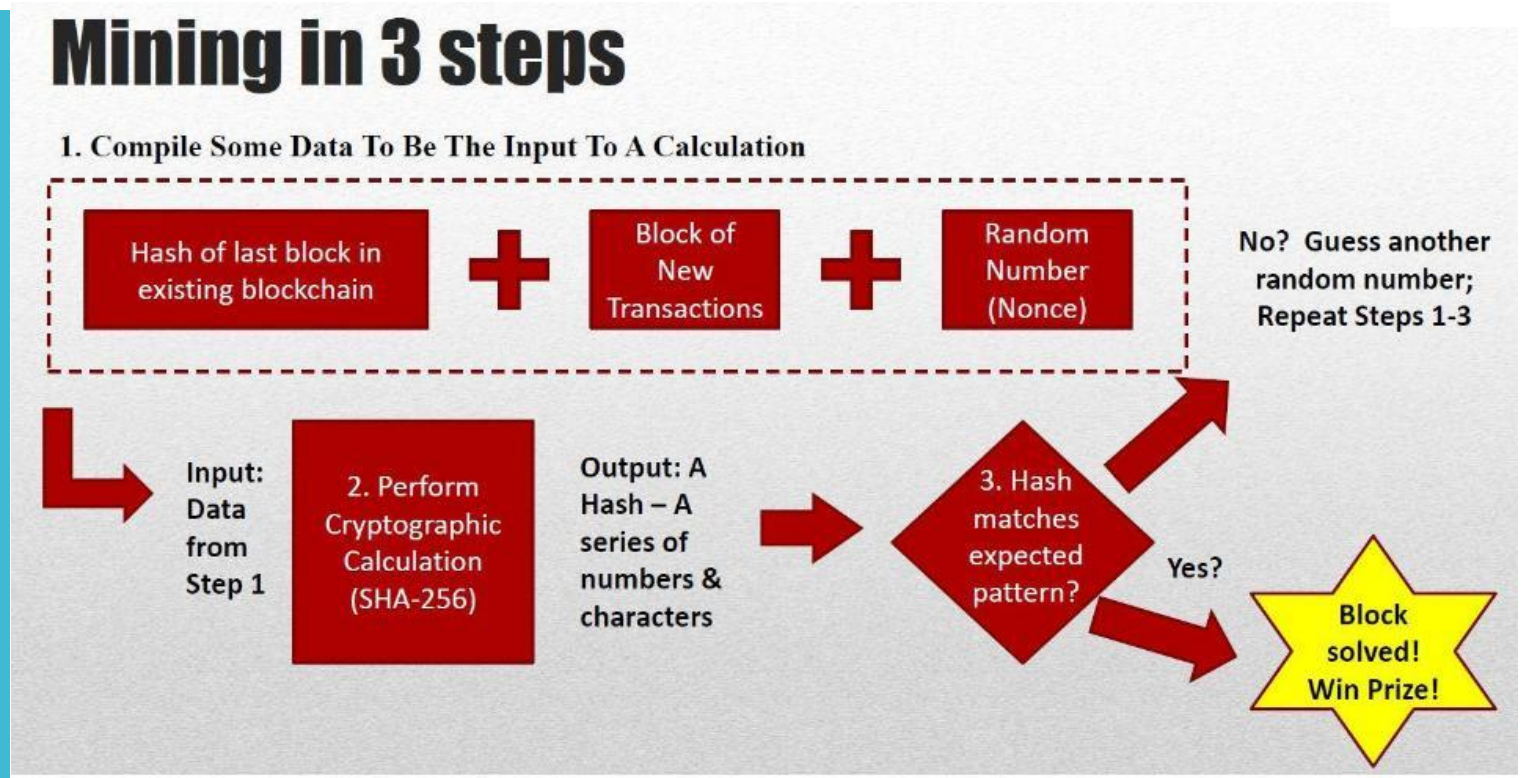
EESTI KRÜPTORAHA LIIT

Blokiahel



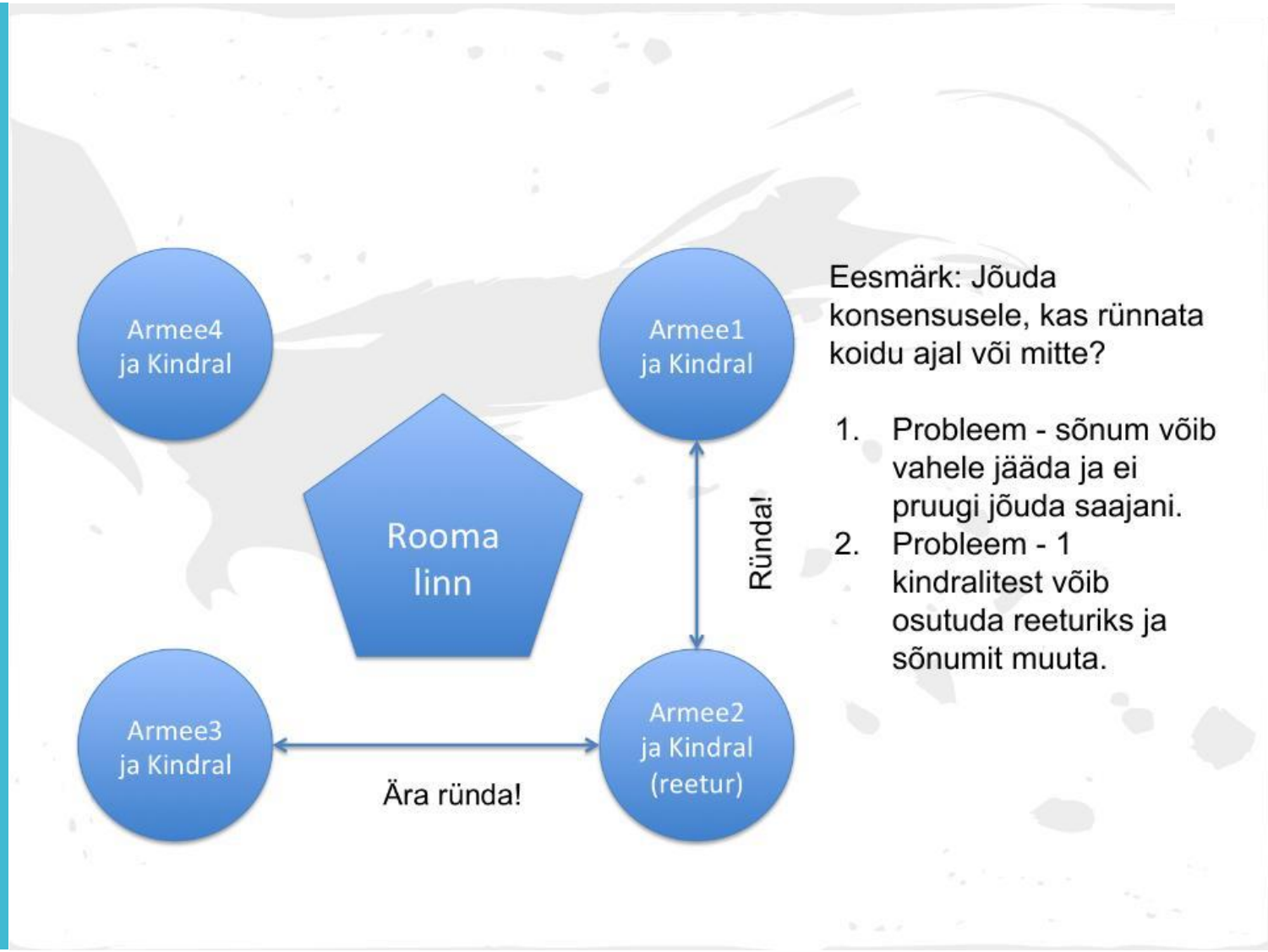
EESTI KRÜPTORAHA LIIT

Kaevandamine



1. Liidetakse kokku eelmise bloki räsi, ülekanded ning suvaline number (nonce)
2. Arvutatakse andmetest uus räsi
3. Võrreldakse tulemust mustriga

Bütsantsi kindralite probleem



Eesmärk: Jõuda konsensusele, kas rünnata koidu ajal või mitte?

1. Probleem - sõnum võib vahele jääda ja ei pruugi jõuda saajani.
2. Probleem - 1 kindralitest võib osutuda reeturiks ja sõnumit muuta.

EESTI KRÜPTORAHA LIIT

Tulemused?

- Bitcoin on ikka veel elus
- Seninägemata nähtus - raha kui sõnumi tüüp
- Bitcoin on palju, palju rohkem kui pelgalt raha

EESTI KRÜPTORAHA LIIT

Aitähh!

Asse Sauga
Juhatuse liige
Eesti Krüptoraha Liit
Asse.sauga@gmail.com
5035347