

BLOCKCHAIN WHITEBOARD LECTURES BY MICHAEL CLAUDIUS 22. MARCH 2018

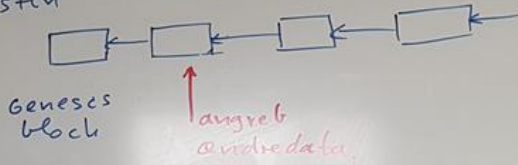
(BB) BLOCKCHAIN (Wiki, Original artikel)
Block chain lagtet liste af blocks.
← ← ←
tidligere.

Block : Hash (tidligere blok), tidsstempel, transaktions data)
P2P network Alle nodes lige
Distribueret, decentralt, redundant 100%

Eksempler Bitcoin > 300 GB, 70% miners i kina
Ethereum billig elektricitet
Jura, Shipping

Public vs private BB
100% kontrol.

Listen

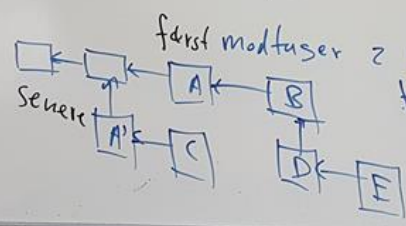


Blockchain
 IPsec VPN
 (OpenVPN)

Skal ændre alle senere blokke. **UMULIGT**
 Pga 10 min tid til at generere block

Hard fork Alle nodes med gammelt SW ændres til nyt
 ELDER ——— " ——— nyt ——— " ——— Samme

Temporary fork



først modtager 2 blokke verificeret af forskellige miners.

Proof of work

Nonce: stort-prime.

.. Hash $\boxed{0000 | \dots H \dots}$
Block $\begin{cases} \rightarrow \text{Minner} \\ \rightarrow \text{Minner} \\ \rightarrow M_3 \end{cases}$ Skal finde antallet
foranstillet

Transaktioner (T)

Merkle tree $\begin{cases} \downarrow \\ \downarrow \end{cases}$ Block $\begin{cases} \downarrow \\ \downarrow \end{cases}$ (500 T
i Bitcoin block)

Owner 1 $\xrightarrow{T_1}$ Owner 2

$$K_1^- = (H(T_1, K_2^+))$$

↑ signatur.

Timestamp

$$\text{timestamp}(t) \rightarrow H(t, \text{Block}_1)$$

Block

57% fiendtløse miners

$$H(H(t_1, \text{Block}_1), \text{timestamp } t_2, \text{Block}_2)$$

Blockchain
IPSec VPN
(open VPN)

$75 \cdot 10^{10} = 75 \text{ TWh}$
om året
0.23% af
hele verden
DU $2.7 \cdot 10^{10} \text{ kWh}$