

PoW \rightarrow PoX

\hookrightarrow PoS

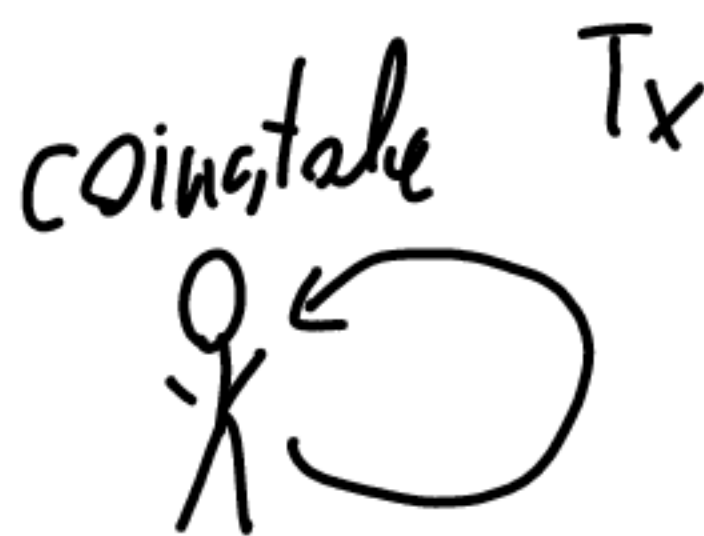
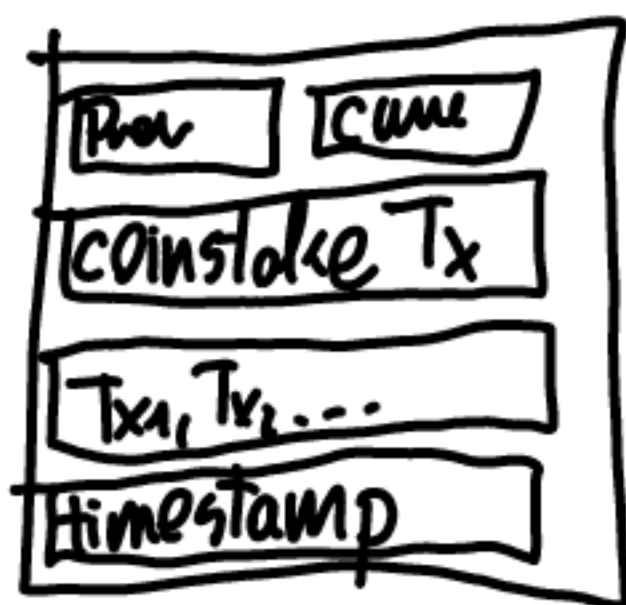
\hookrightarrow Hybrid \rightarrow PoA

PoS - "PPcoin: Peer-to-Peer Cryptocurrency with Proof-of-Stake"
Sunny King, Scott Nadal. 2012

idea: exchange computational difficulty with value in stake

in PoW: $Pn[L=i] = \frac{w_i}{\sum_{j \in J} w_j}$, $(h(\text{block}))_2 < D(z)$ where z is network specific.

In PoS:



$\text{coinage} = \text{coinstake.value} \cdot \text{coinstake.time}$

PoS miner:

```
block ← BuildBlock()
while  $(h(\text{block}))_2 > D(\text{coinage})$ :
    block.timestamp ← now()
broadcast(block)
```

problems? nodes go idle after publishing a block.

PoA:
problems with PoW:

- centralization problem
- 51% malicious:
- stops the network - PoW-Dos
- double spending - lost in trust

Pos:

- network going idle

greedy:

- PoW-Dos \rightarrow higher fees
- ds \rightarrow gaining

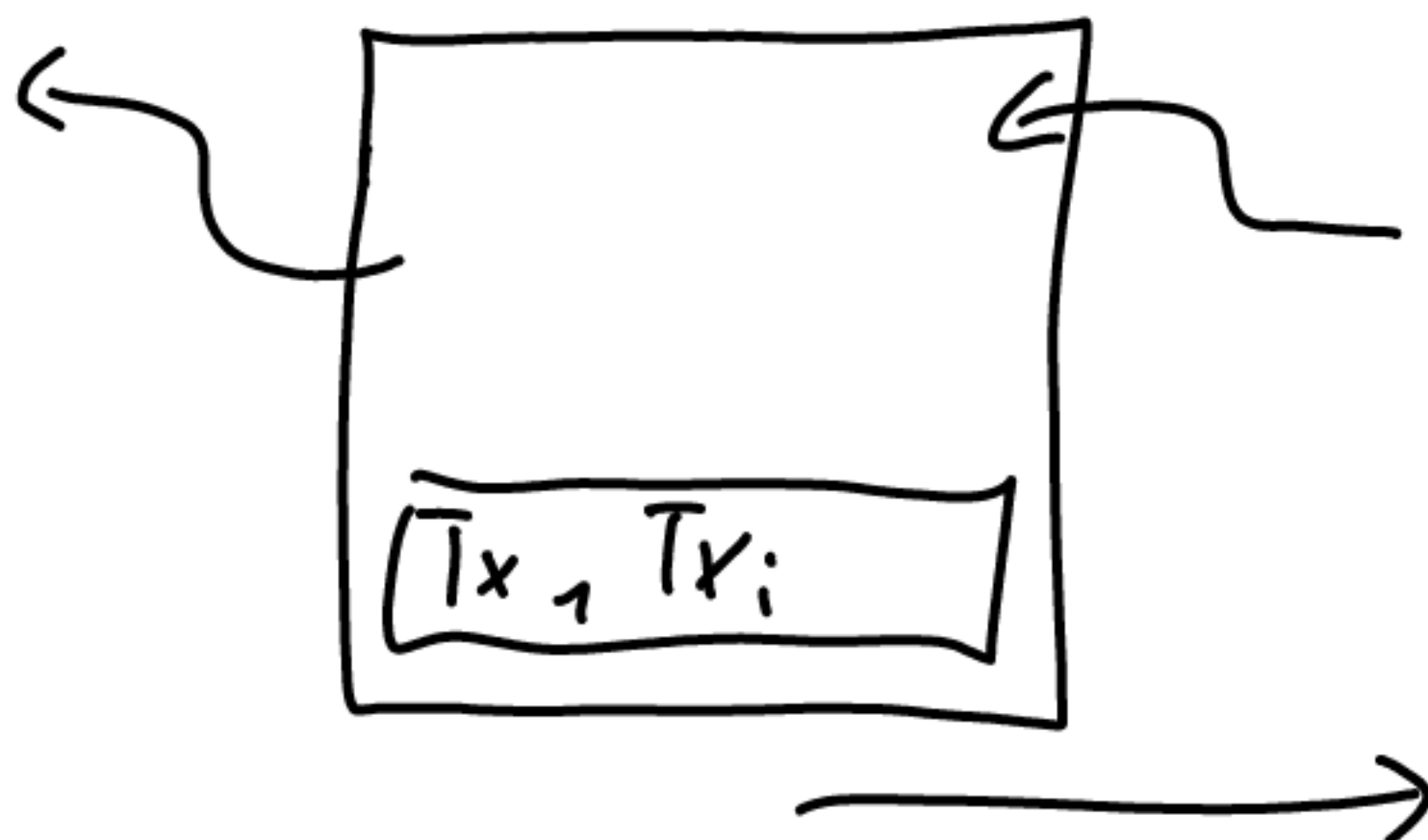
nodes leaving the
network has power \uparrow

Protocol:

Follow-the-satoshi (FTS)


$$FTS: \{0,1\}^n \rightarrow SI$$

$$FTS \sim U$$



$$\text{Pow}(\boxed{\text{BHeader}}) < D(z)$$

BHeader



$\text{FTS}(\text{BHeader} || "1")$
 $\text{FTS}(\text{BHeader} || "2")$
 \vdots
 $\text{FTS}(\text{BHeader} || "N")$

\downarrow
 $\{S_1, S_2, \dots, S_N\}$

if $S_i \in \{S_1, S_2, \dots, S_{N-1}\}$:
 $(\text{BHeader}, 6) \rightarrow$

if $S_i == S_N$