

Crittografia

lezione del 10 dicembre 2020

ore 9:15

BitCoin



BITCOIN

2008

"Bitcoin": a peer to peer Electronic Cash System

Satoshi Nakamoto

2009

5-N. software

3 gennaio 2009

→ "Blocco Genesi"¹

↳ 50 BTC

12 gennaio 2009

primo trasferimento

→ 10 \$
Hol Finney

2010

primo handover commerciale

INDIRIZZO

utente A

k_A (pub)



si hospone in
indirizzo

k_A (priv)



per firmare le
trasmissioni

ECC

- identificatore di A
- sene per inviare messaggi
ad A
- sene per controllare le
femce di A

WALLET

in rete delle ~~credenziali~~ credenziali che
ottengono le proprie in BTC di un utente
(+ coppia indirizzo / chiave privata associata all'ind.)
+ ~~soft~~ software di gestione

TRANSAZIONE

A $\xrightarrow{\text{BTC}}$ B

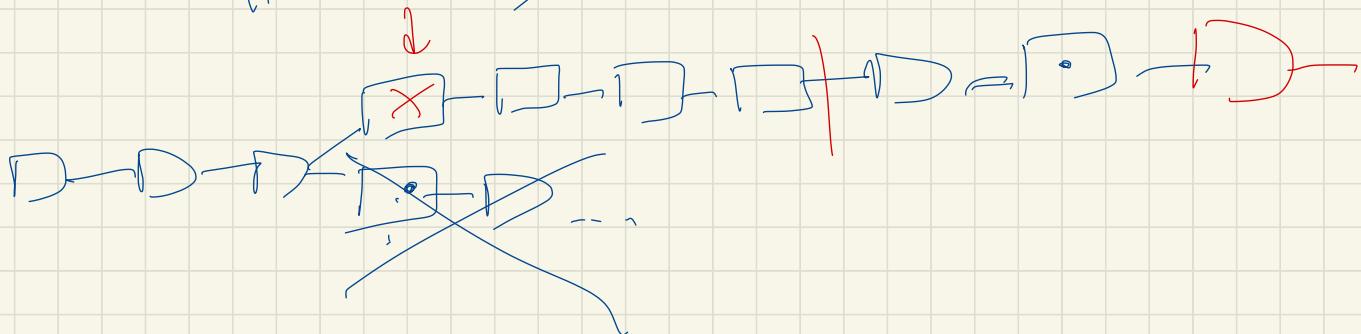
$$m = \text{addr}_A - x - \text{addr}_B$$

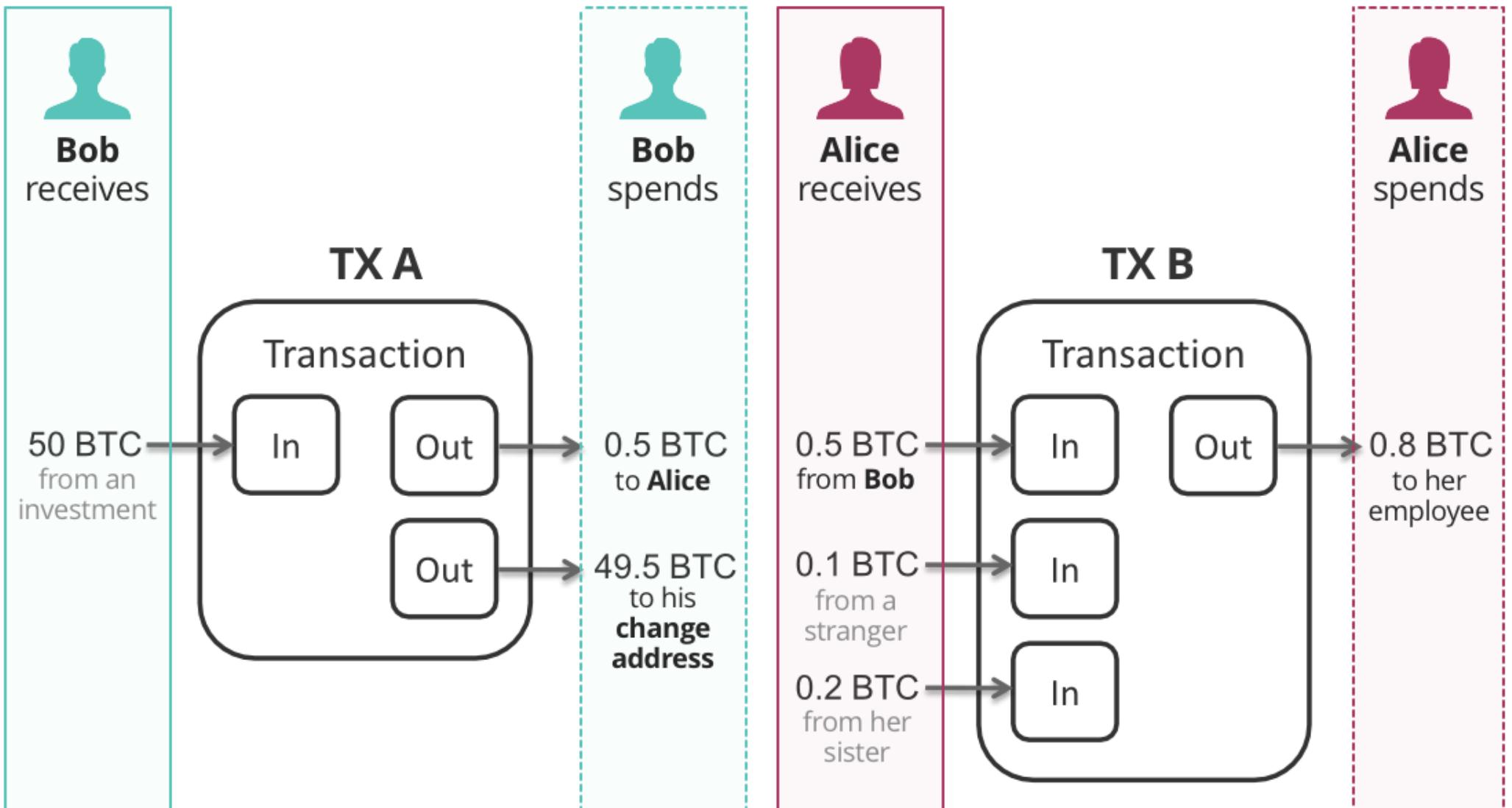
$$h = \text{SHA-256}(m)$$

FIRMA $f = \text{Sig}(h, k_A(\text{priv}))$

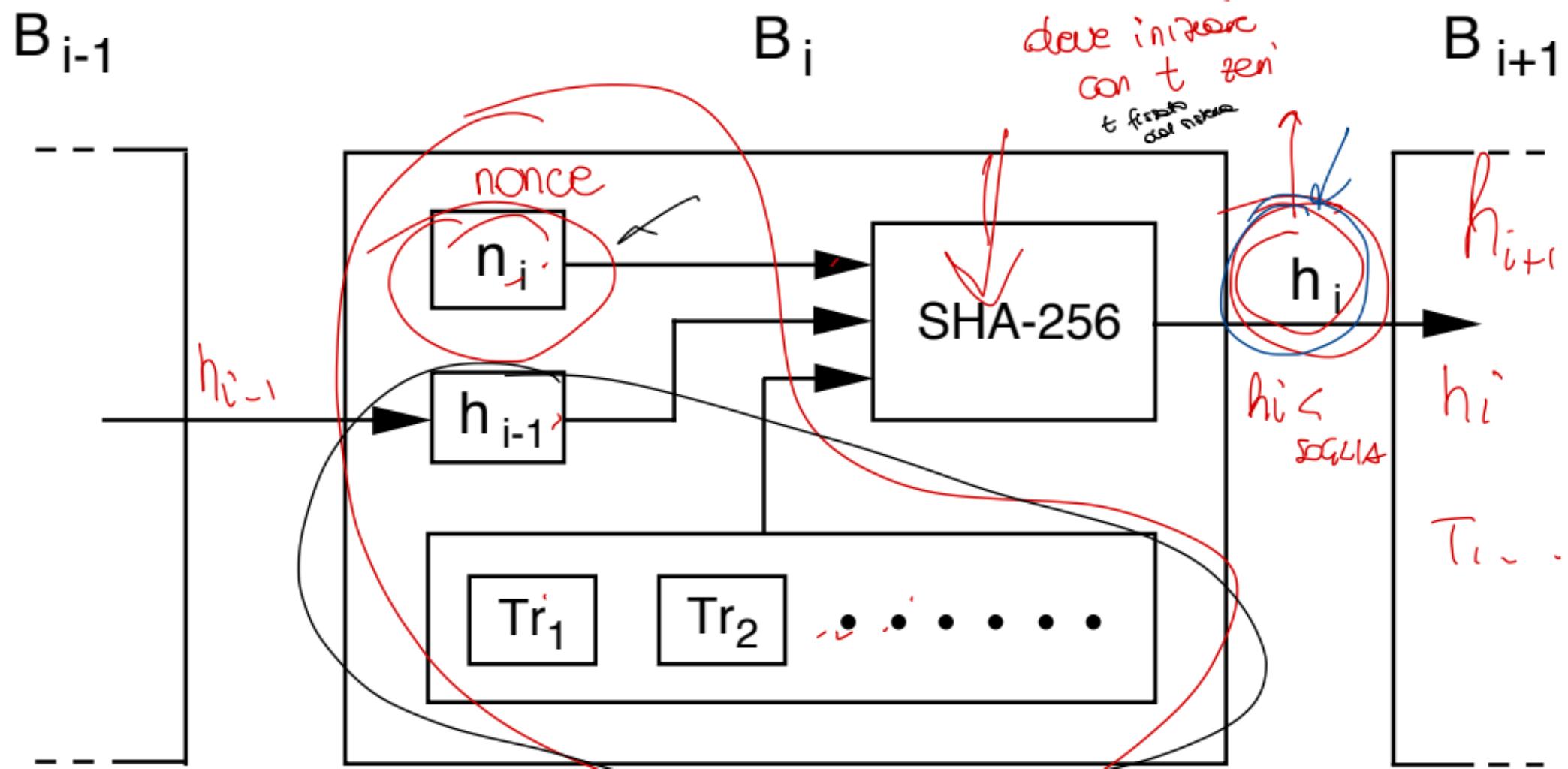
BROADCAST

A di finire $\langle m, f \rangle$ sulla rete



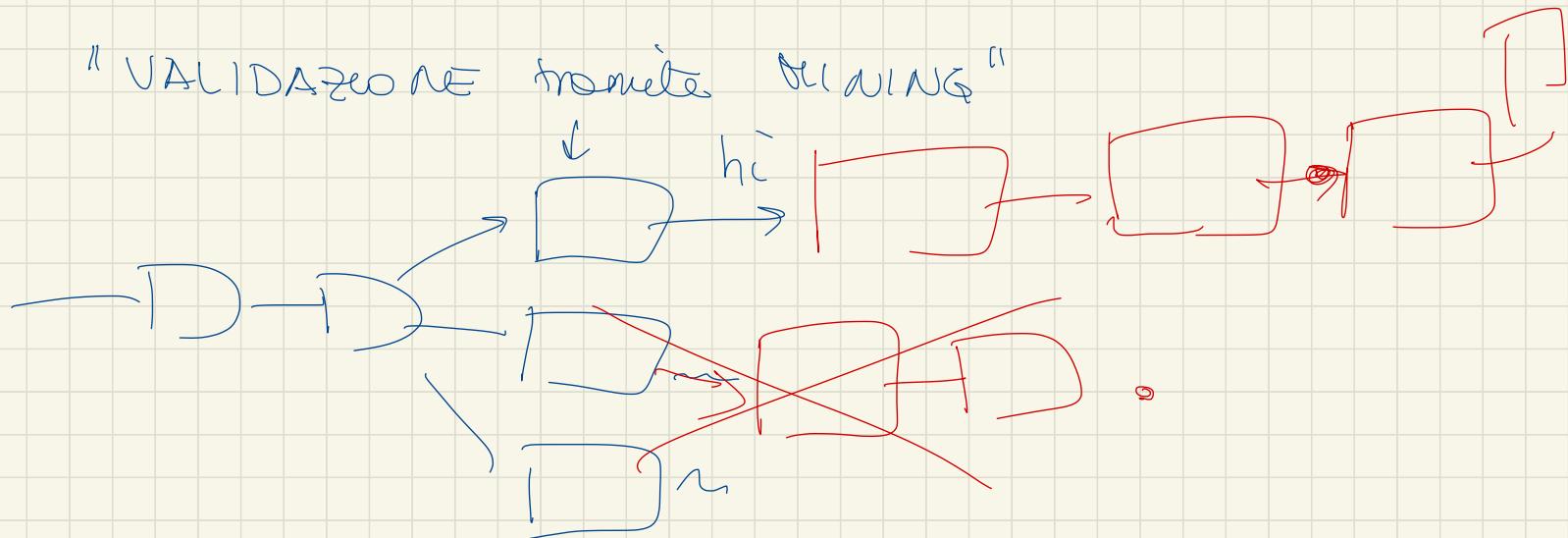


$$\sum \text{Input} \geq \sum \text{Output}$$



MINER : nodi che validano le transazioni
e aggiornano i blocchi. I blocchi sono chiamati

"VALIDATORI NEI tramite MINING"



- il nodo che ha il voto, lo diffonde per broadcast ai altri nodi
- i nodi che controllano, convalidano le transazioni delle creare
transazioni, esprimono il loro consenso per creare "nuovi blocchi" e "aggiornare" la