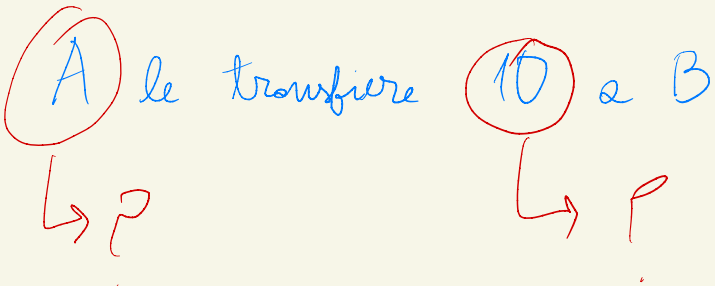
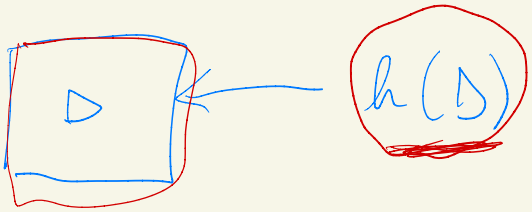
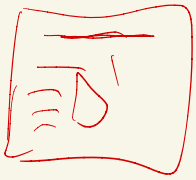
BITCOIN

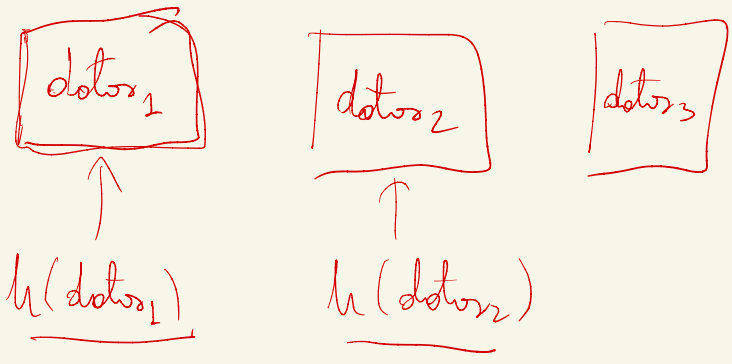


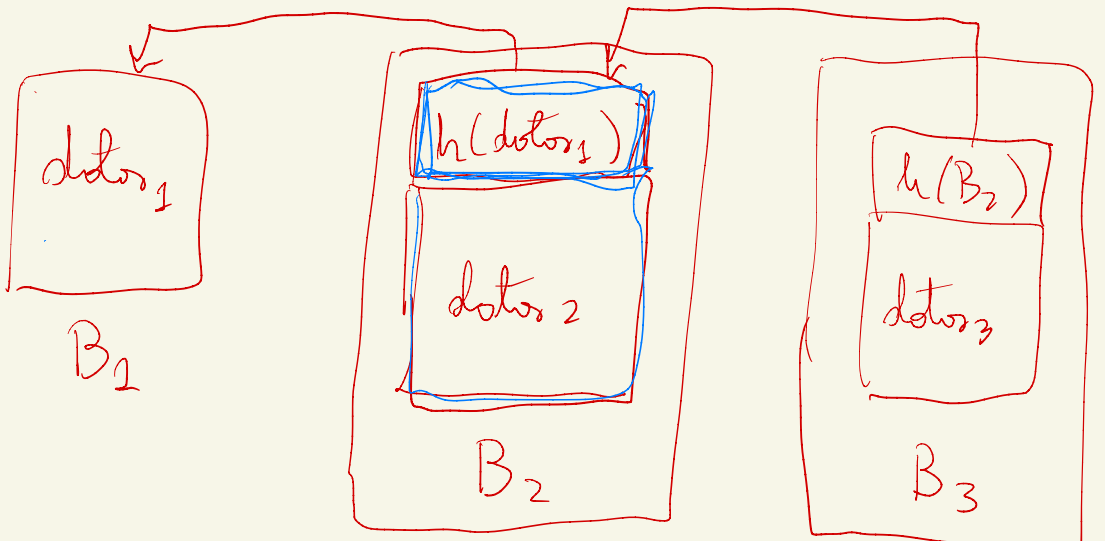
BLOCKCHAIN



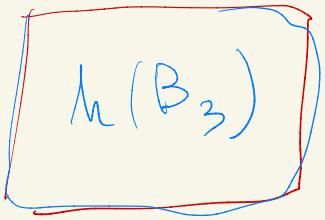


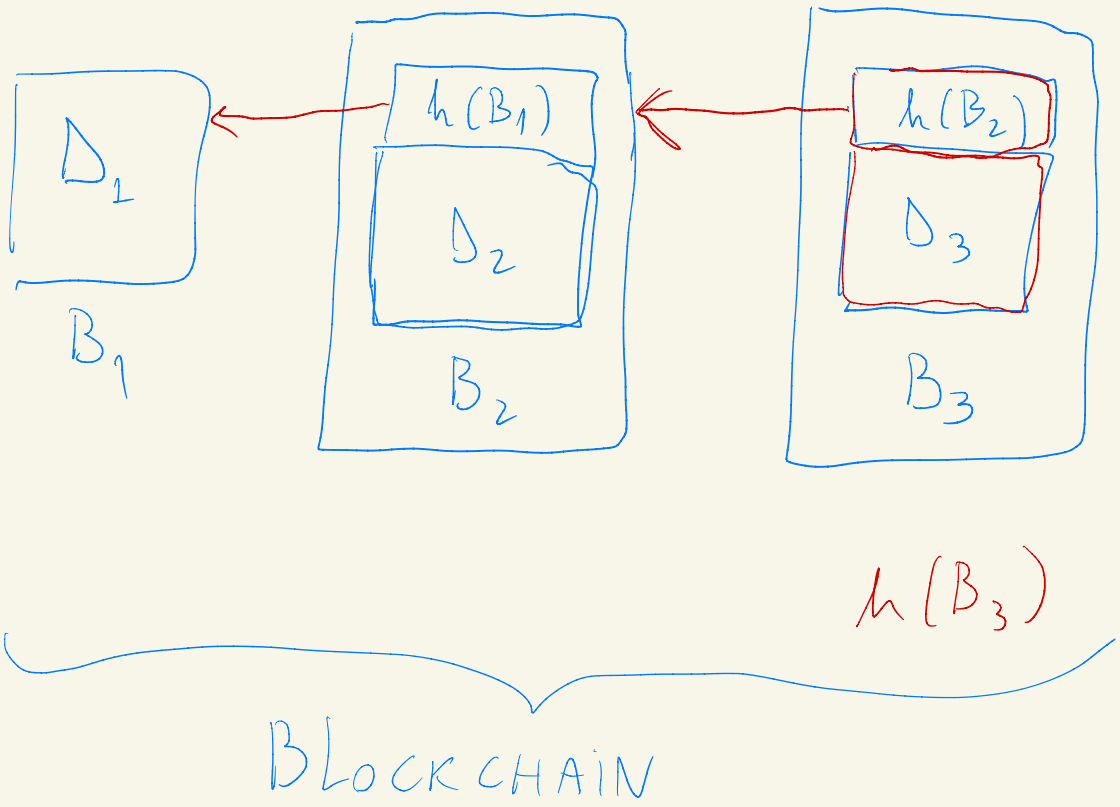
$h(D') \neq h(D)$

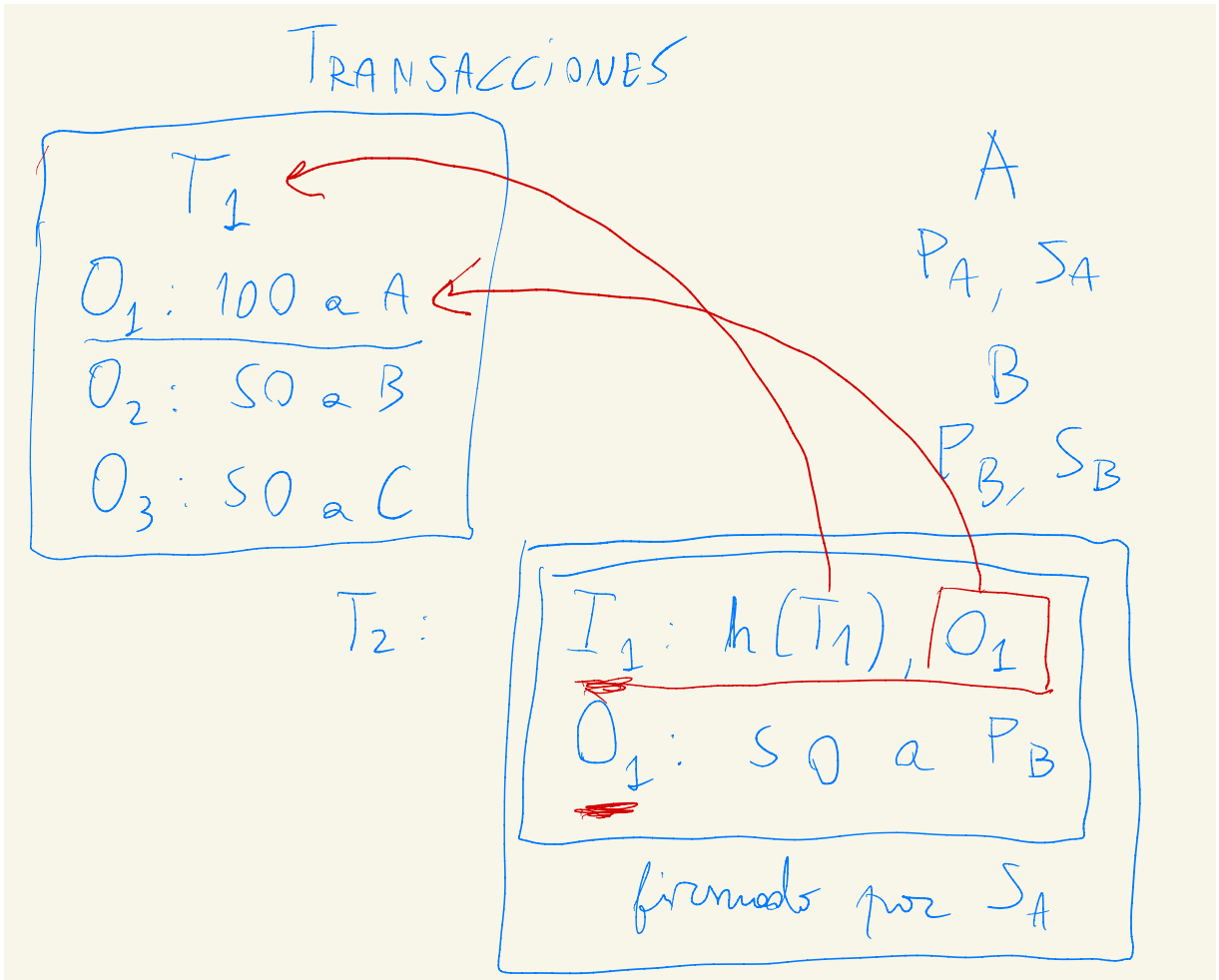




$h(B_2') \neq h(B_2)$




D1
h(B1)
D2
h(B2)
D3
B1
B2
B3
h(B3)
BLOCKCHAIN


TRANSACCIONES
T_1
O_1: 100 a A
O_2: 50 a B
O_3: 50 a C
A
P_A, S_A
B
P_B, S_B
T_2:
I_1: h(T_1), O_1
O_1: 50 a P_B
firmado por S_A

T_1

O_1: 100 a A

O_2: 50 a B

T_2

I_1: $h(T_1)$, O_1

O_1: 50 a P_B

O_2: 50 a P_A

firmar con S_A

T_3

I_1: $h(T_1)$, O_2

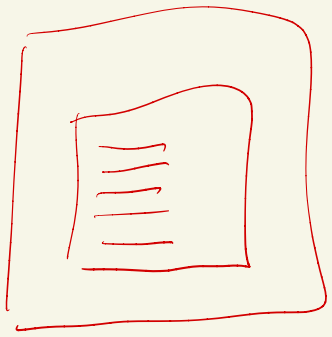
I_2: $h(T_2)$, O_1

O_1: 80 a P_C

O_2: 20 a P_B

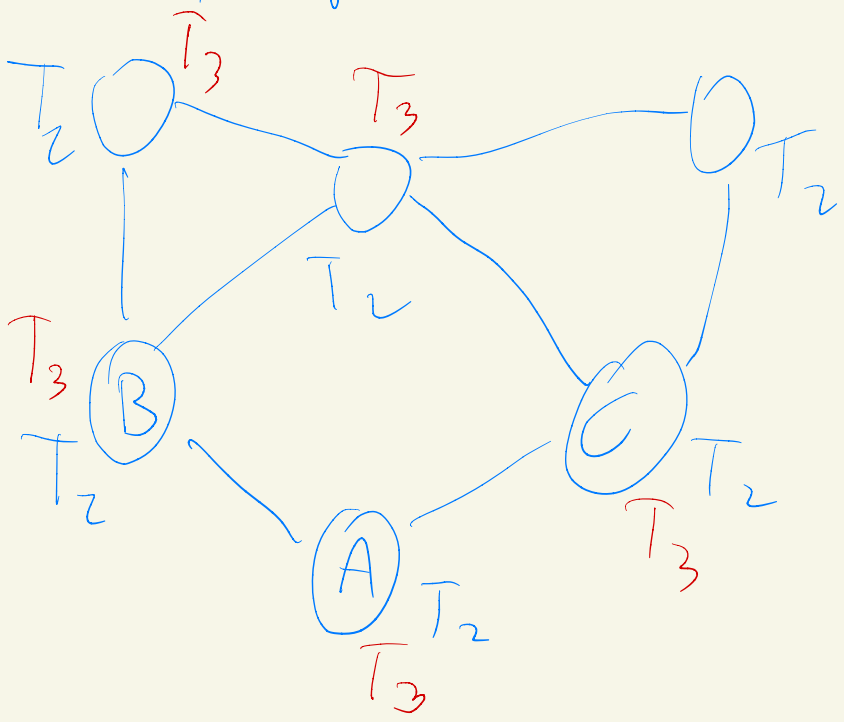
firma$_1$ S_B

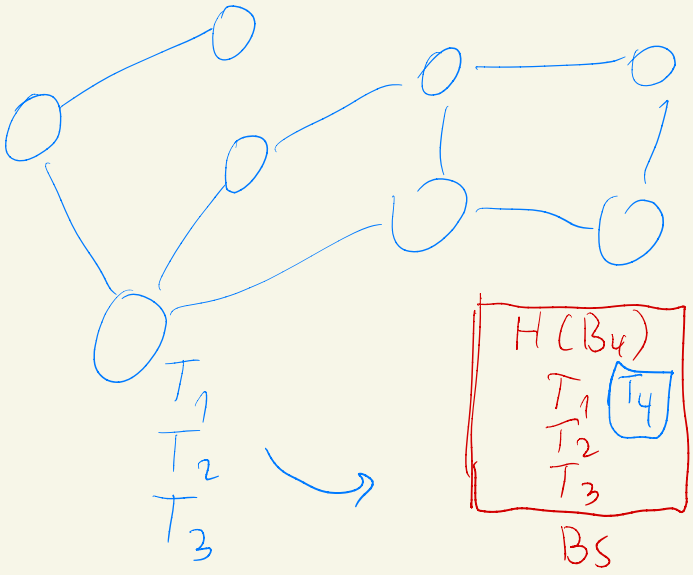
firma$_2$ S_B



Bloque

- Todos almacenen todos los bloques
- Si quiero hacer una transacción, decir a todos los vecinos
- Si alguien recibe una transacción, informar a sus vecinos




T1
T2
T3
H(B4)
T1
T4
T2
T3
BS


B1
B2
B3
B4
BS