Decentralized Blockchains

Prof. Francesco Bergadano

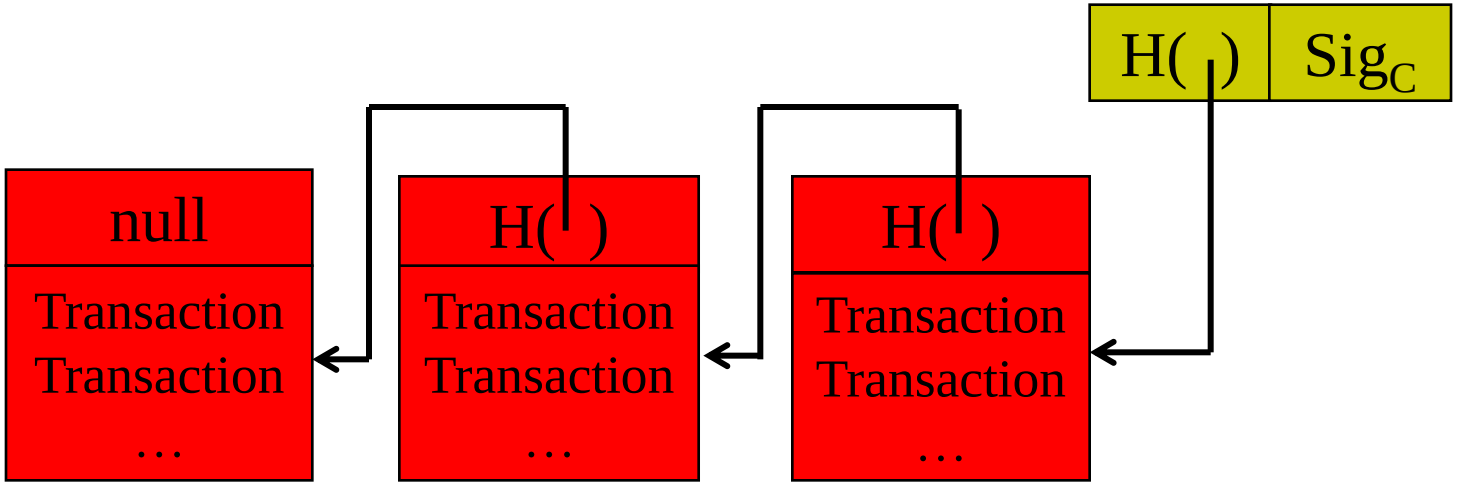
Dipartimento di Informatica

Università di Torino

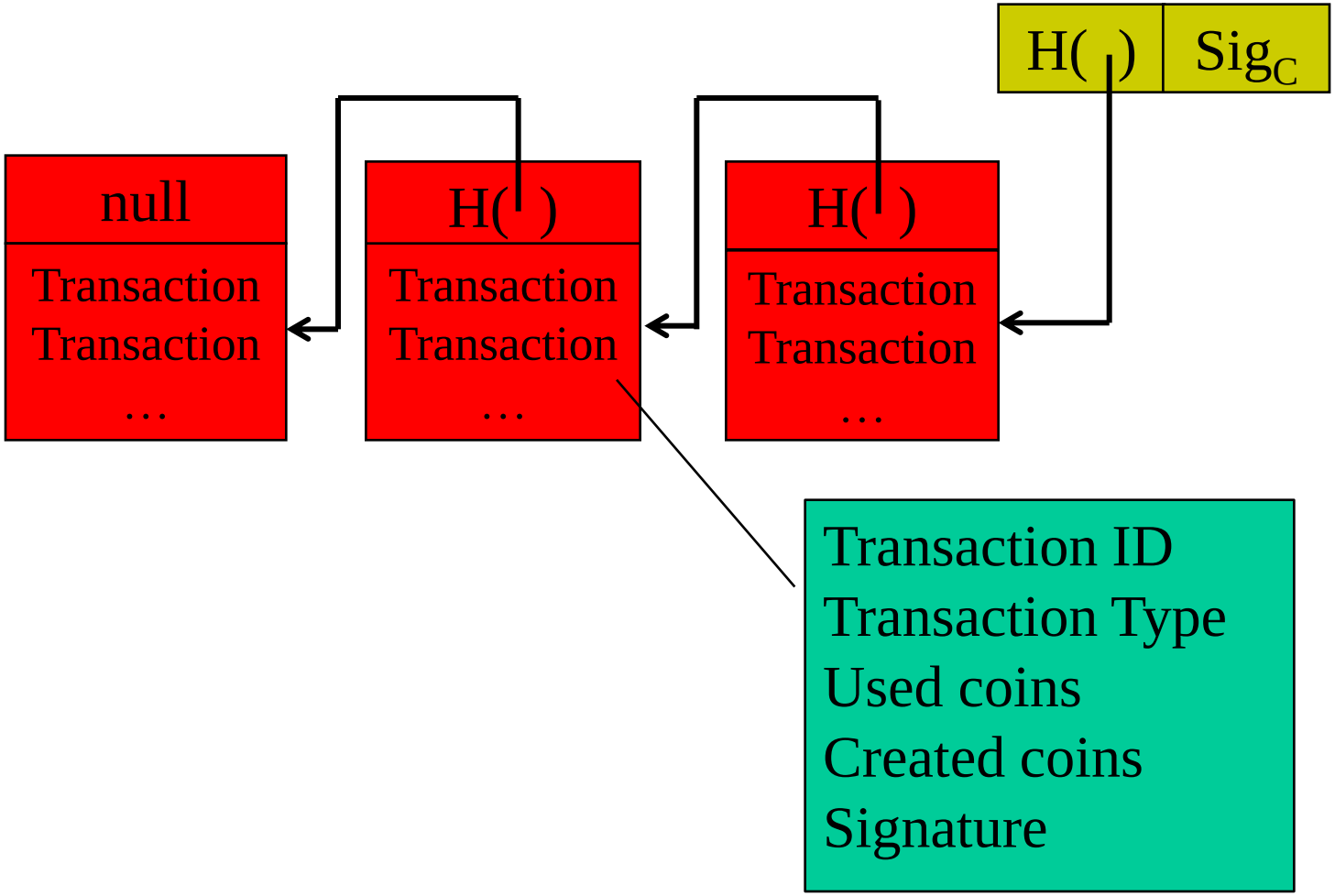
Summary

- Decentralization
- Real-world Bitcoins
- Other Blockchain applications

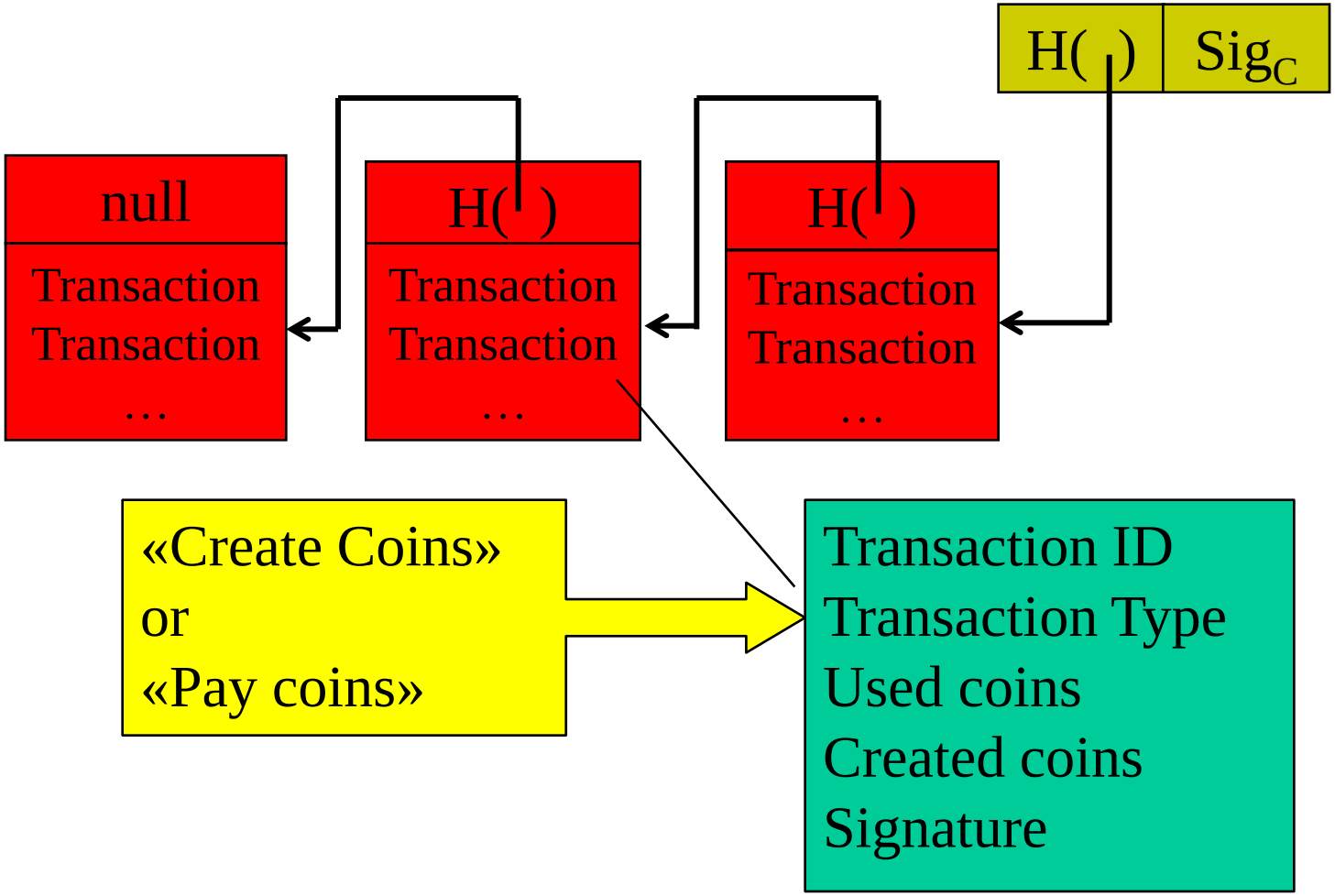
The centralized blockchain



The centralized blockchain



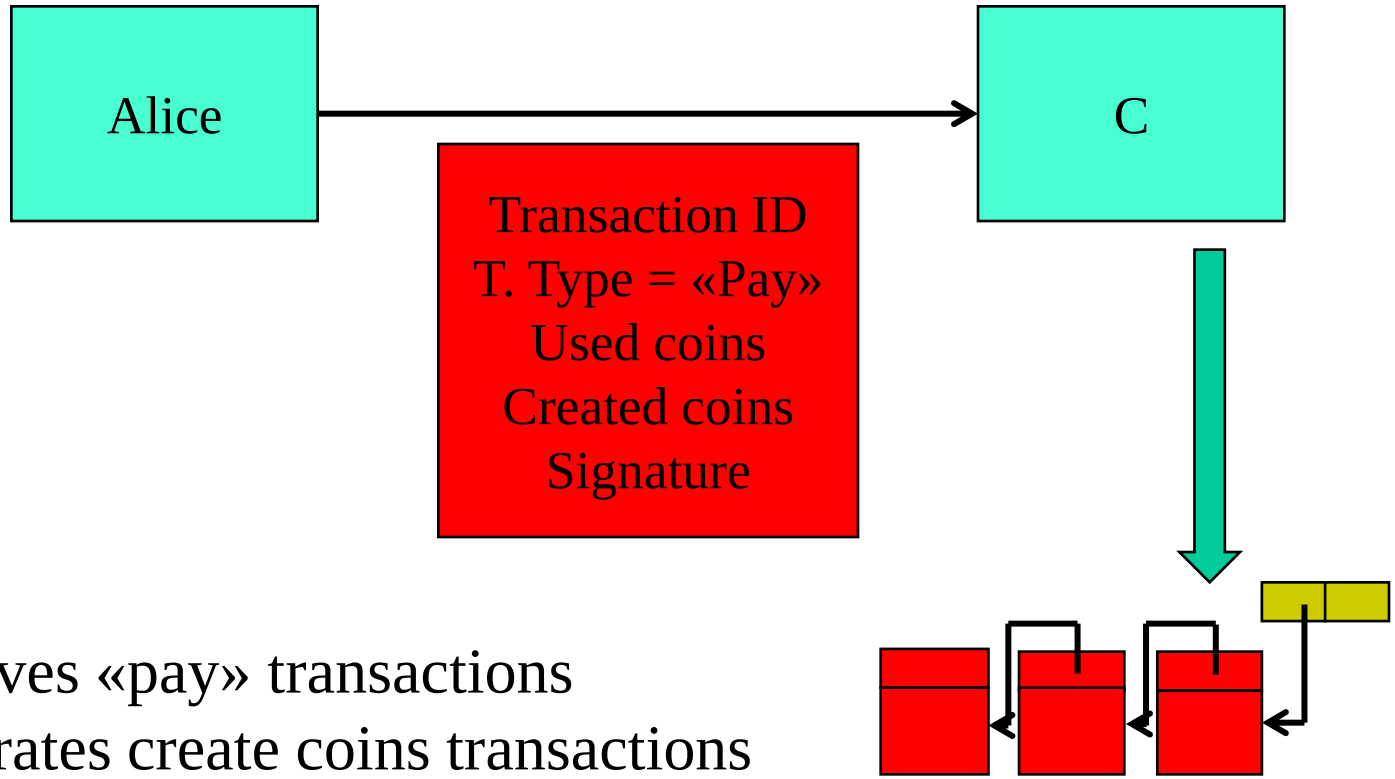
The centralized blockchain



The centralized bitcoin system

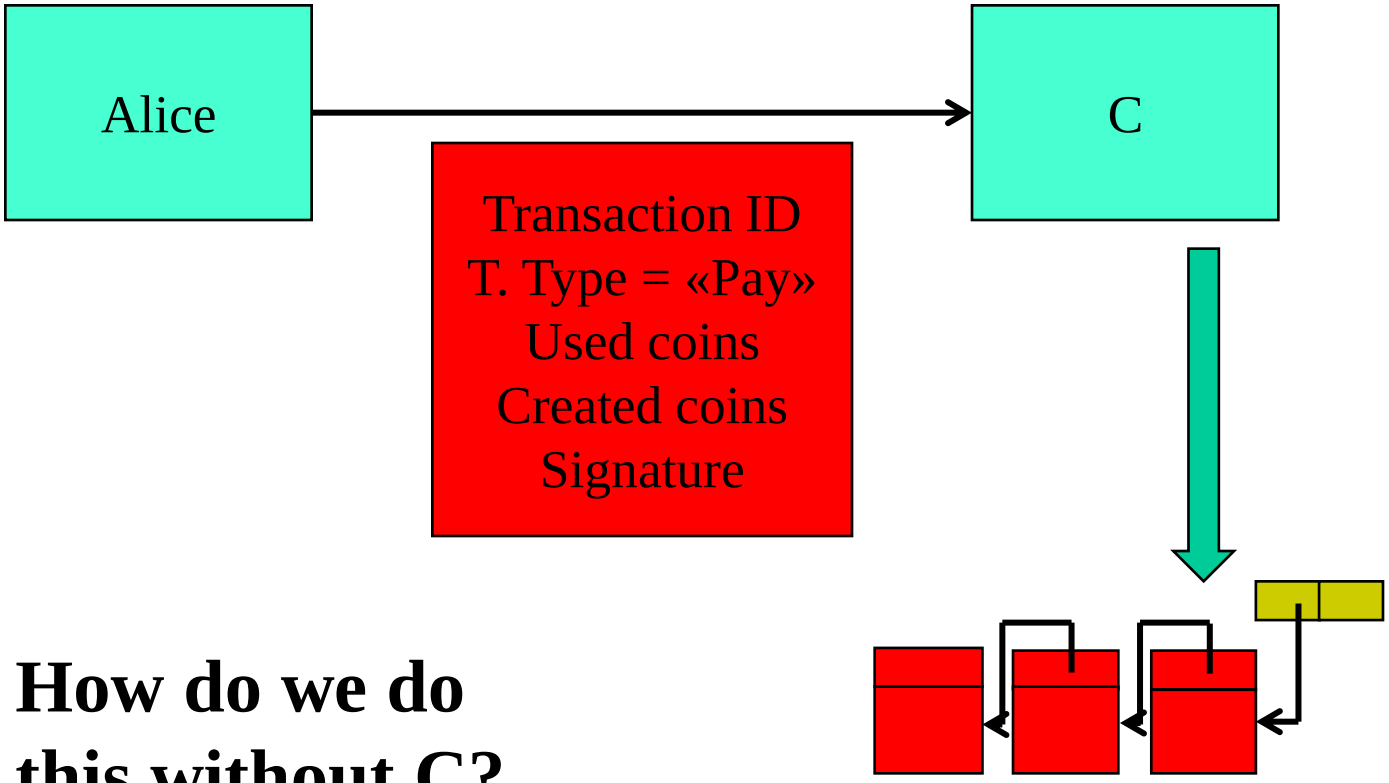
- Coins as correctly signed information
- Only C can create coins
- C manages a tamper-evident blockchain
- Double spending impossible
- Users are anonymous (one could create a new ID and pay coins to his new ID)

The centralized blockchain



C receives «pay» transactions
C generates create coins transactions
C checks validity
C accumulates transactions in a new block
C seals the updated blockchain with a signature

Decentralization



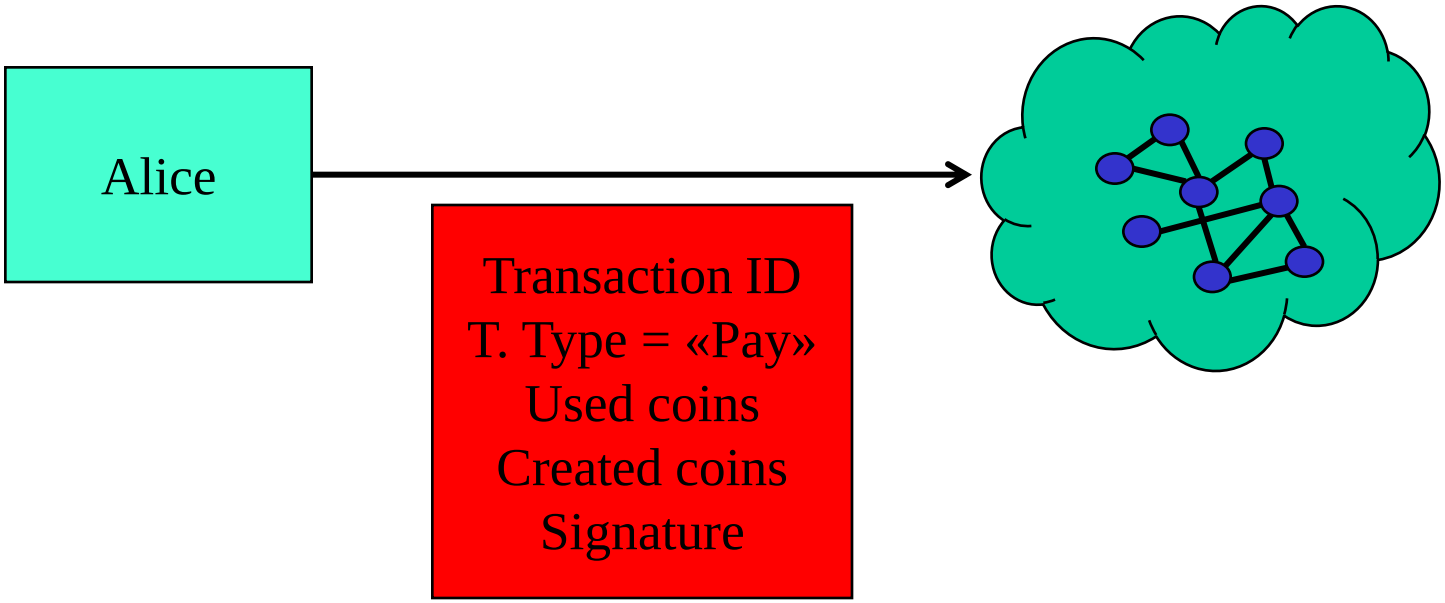
How do we do this without C?

Decentralization

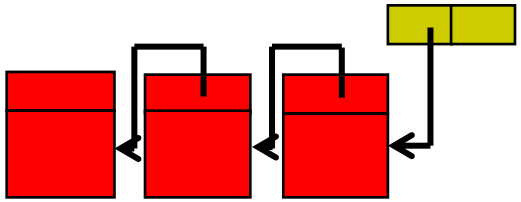
Principles:

1. Substitute C with a peer-to-peer network
2. Nodes in the network will check for validity
3. Signature replaced by “proof of work”
4. Coin creation “embedded” in the operation of adding a block
5. Use of an (economic) incentive

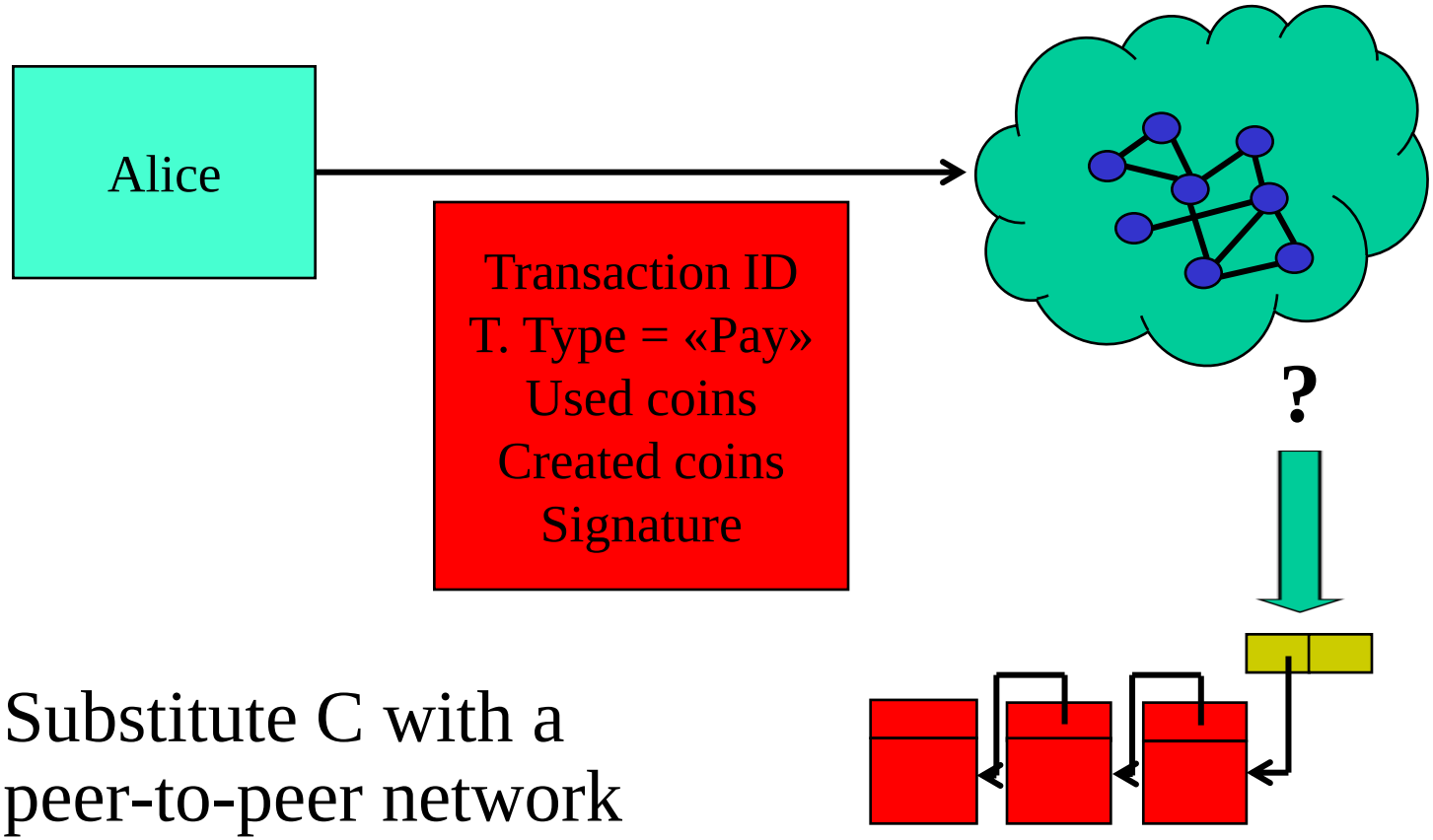
Decentralization



1. Substitute C with a peer-to-peer network
2. Nodes in the network will check for validity

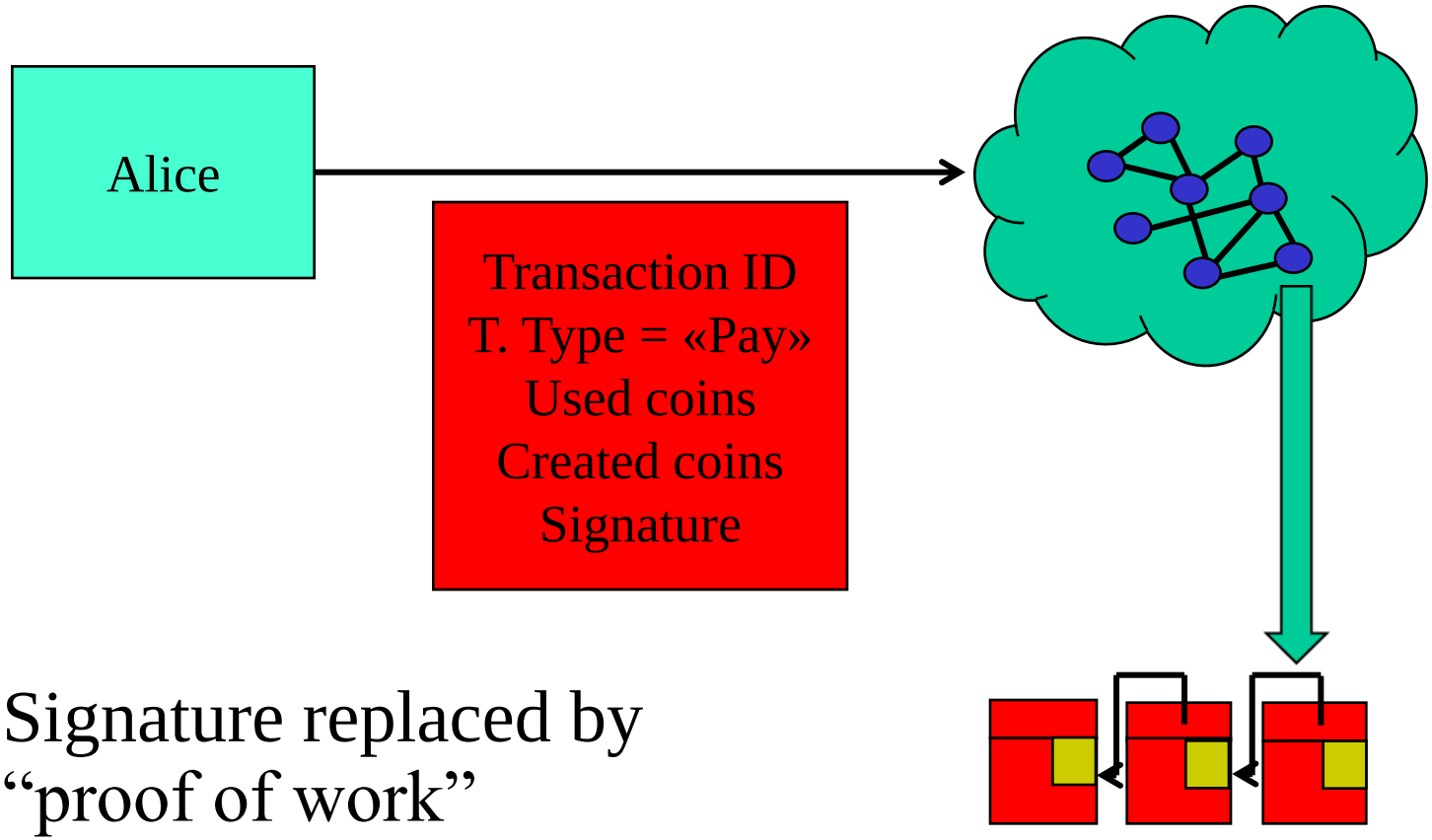


Decentralization



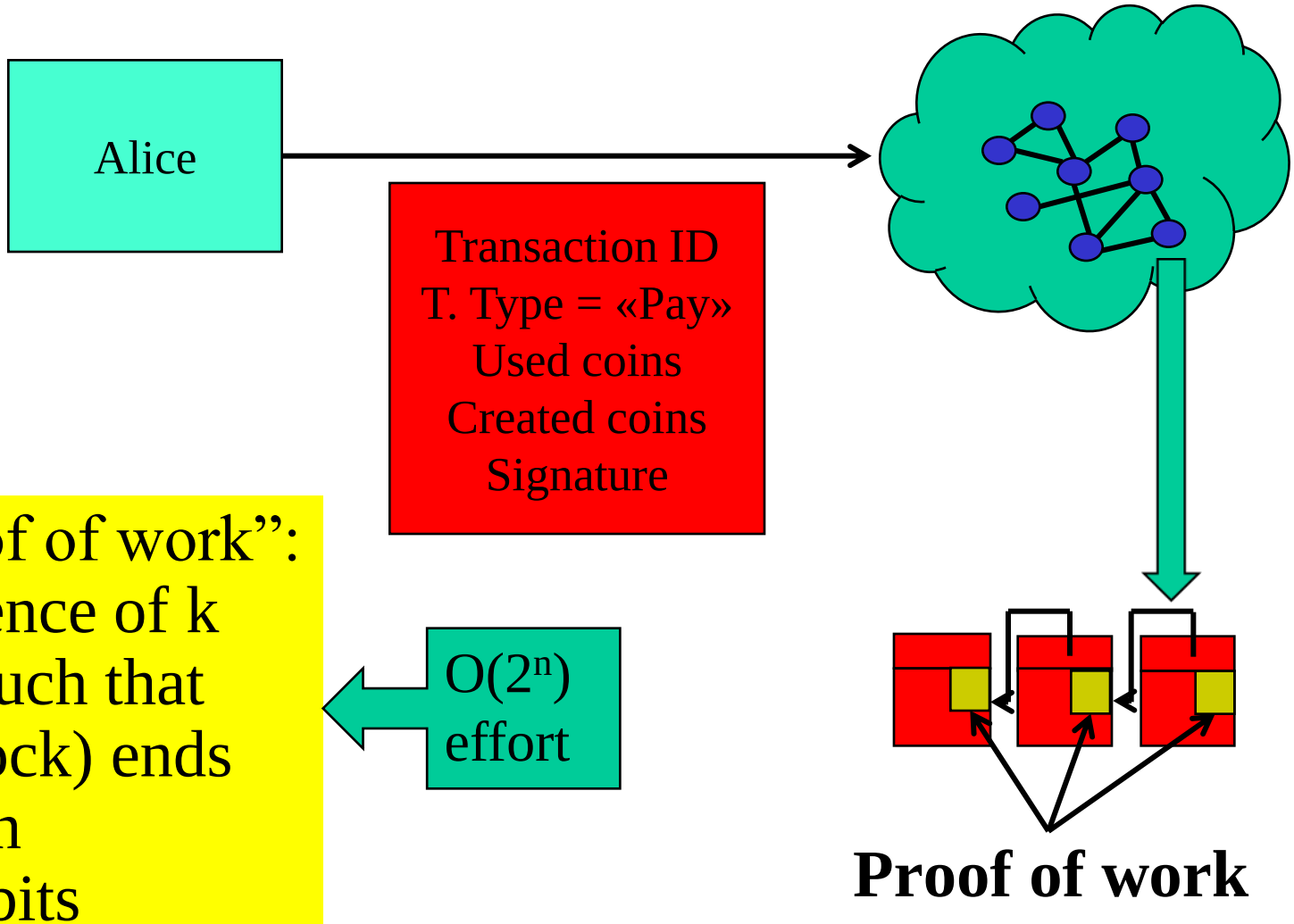
1. Substitute C with a peer-to-peer network
2. Nodes in the network will check for validity

Decentralization



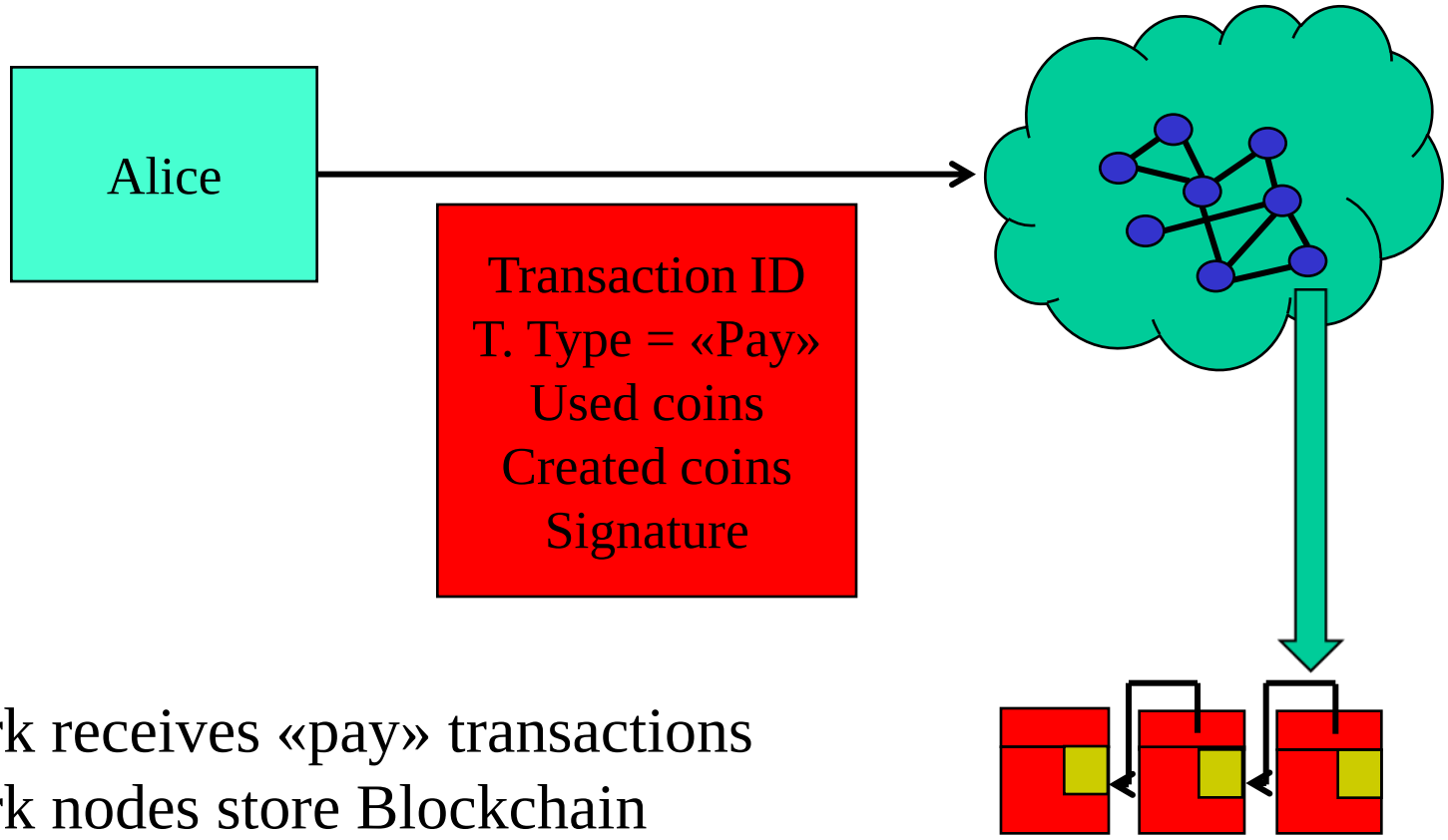
3. Signature replaced by "proof of work"

Decentralization



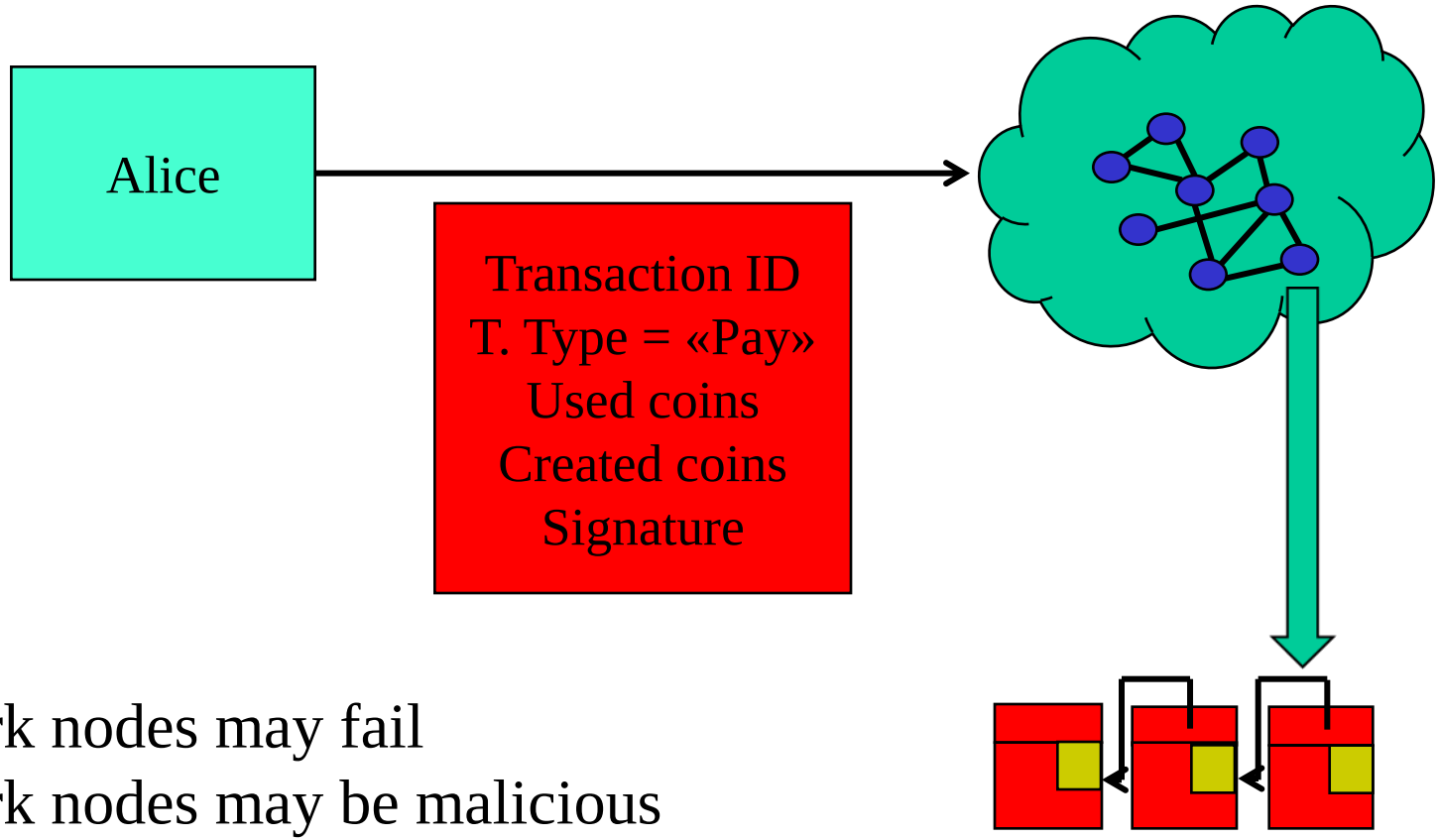
"proof of work": sequence of k bits such that H(block) ends with n zero bits

Decentralization



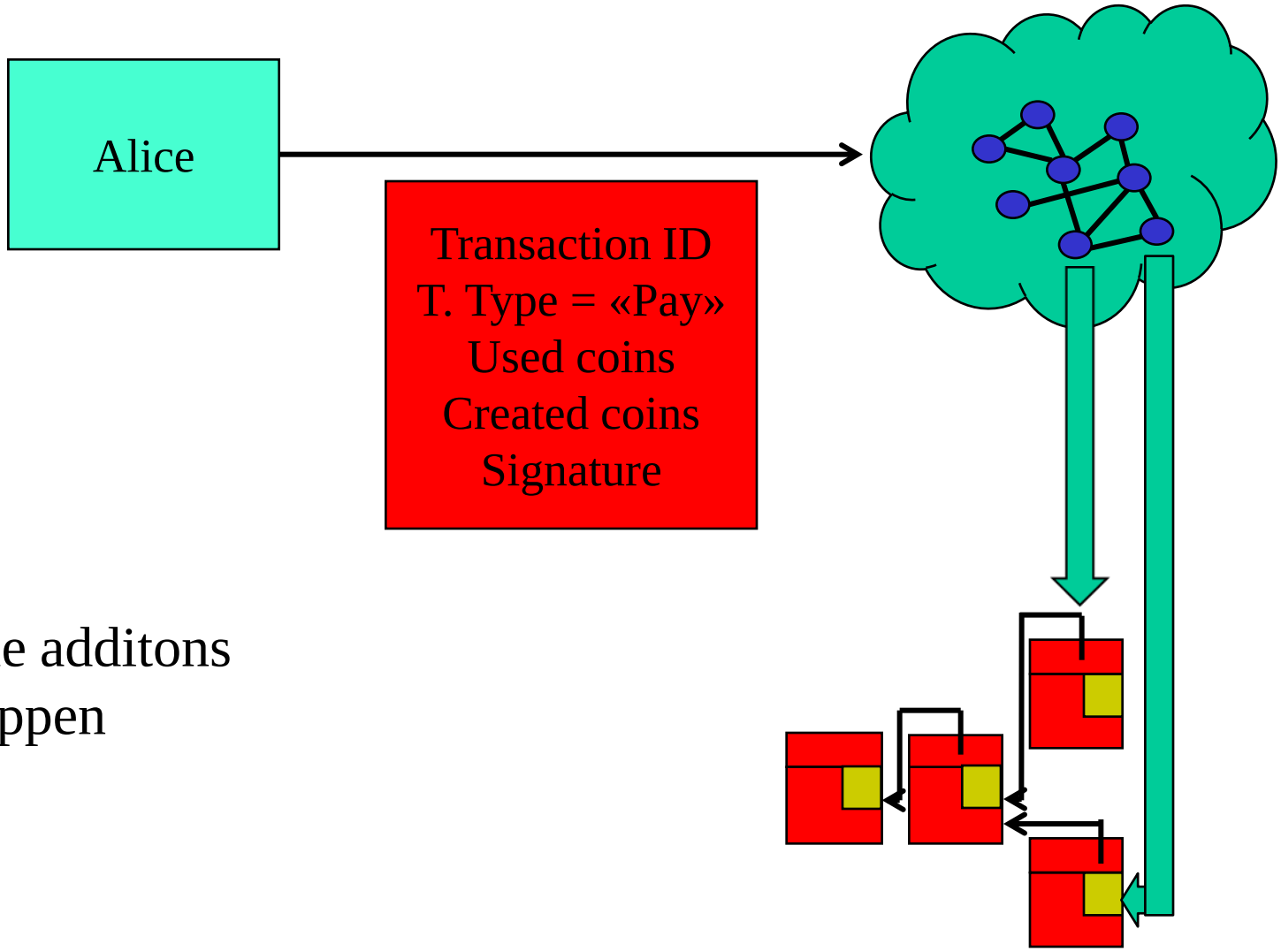
Network receives «pay» transactions
Network nodes store Blockchain
One node adds a block (and creates coins)
New node includes «proof of work»
Blockchain is «sealed» by chain of proofs of work

… but



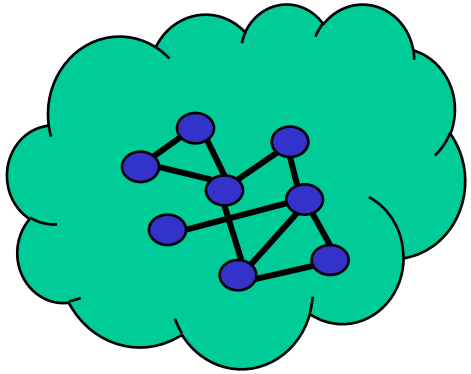
Network nodes may fail
Network nodes may be malicious
Messages between nodes may be lost
Network latency

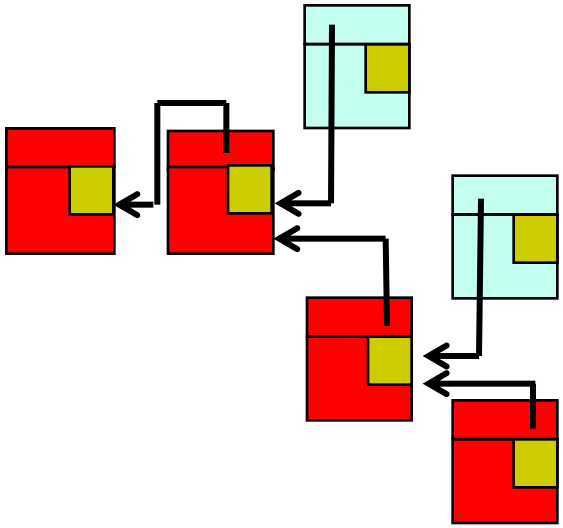
… hence



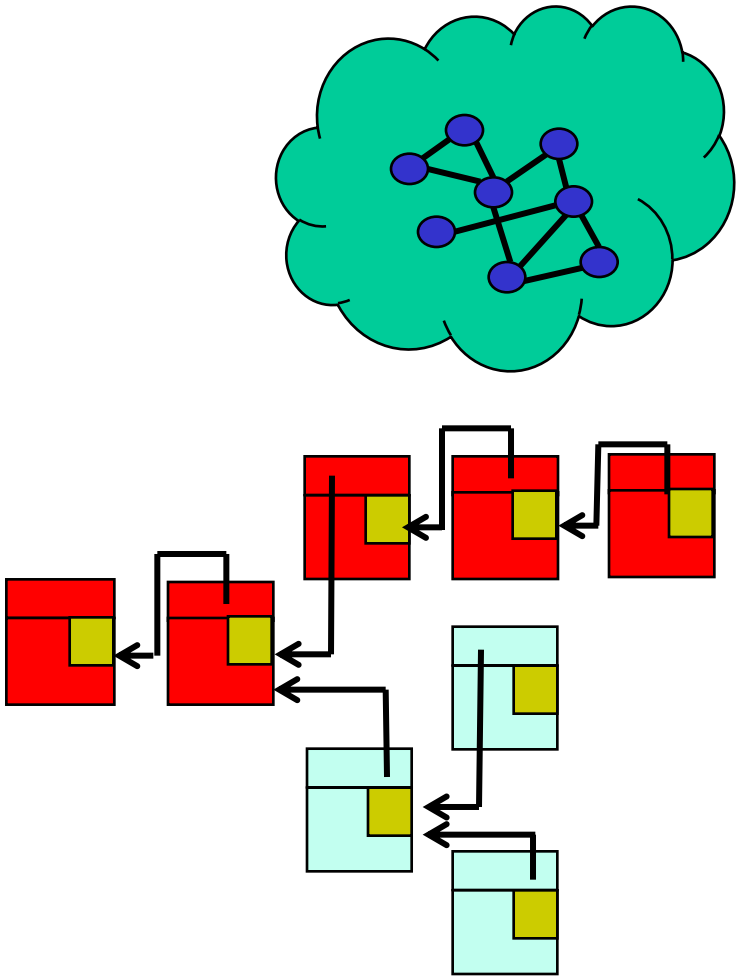
Multiple additons
may happen

How the Blockchain grows

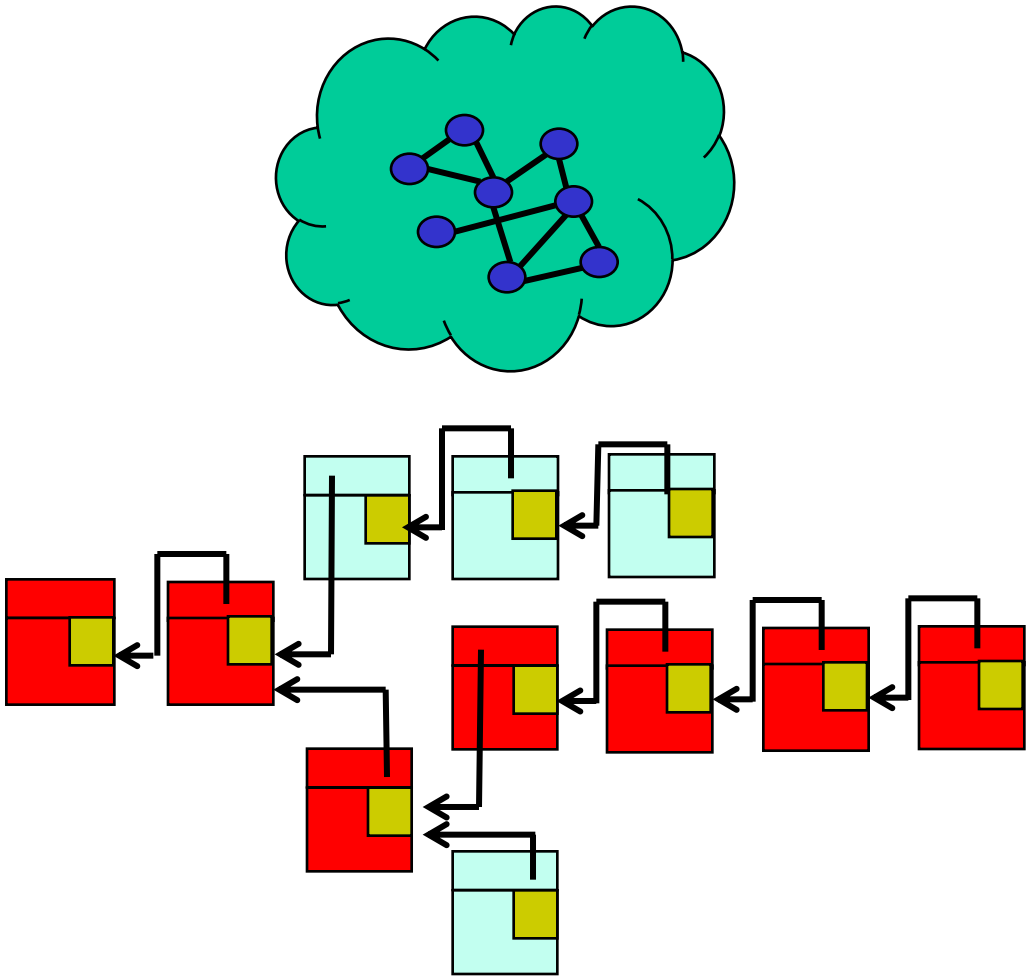




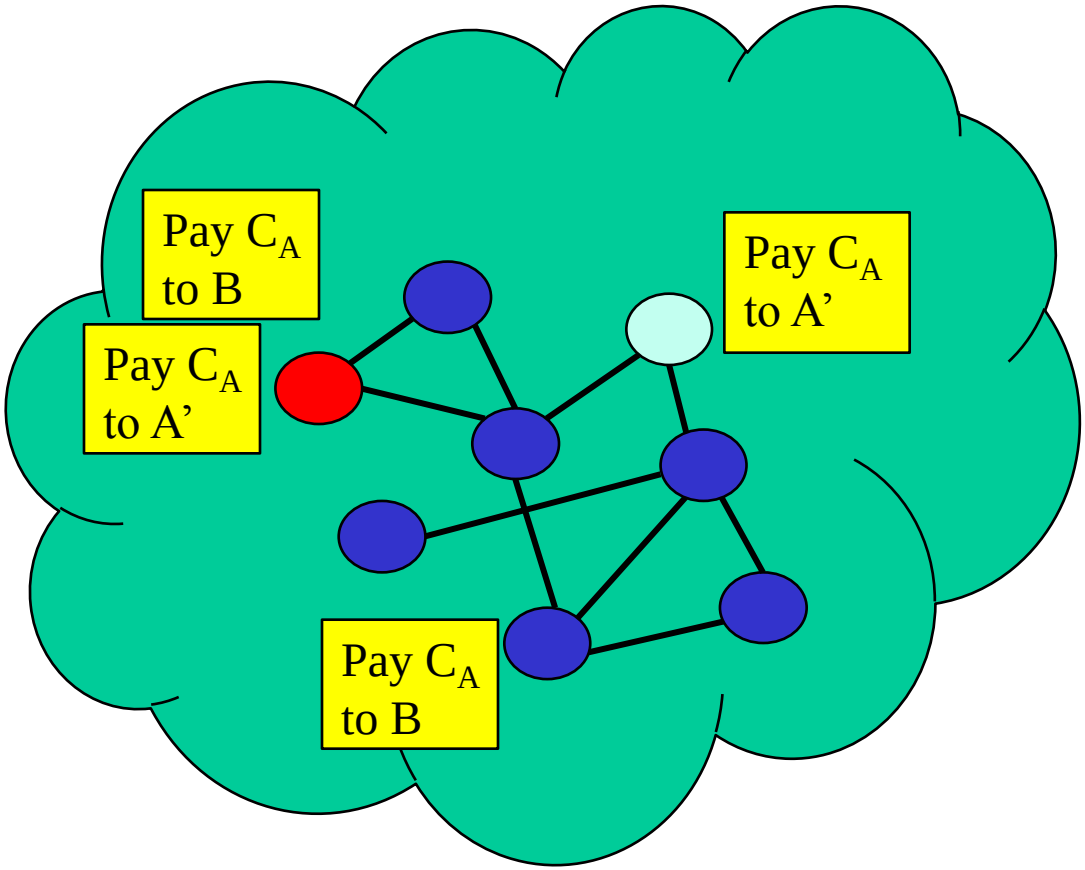
How the Blockchain grows



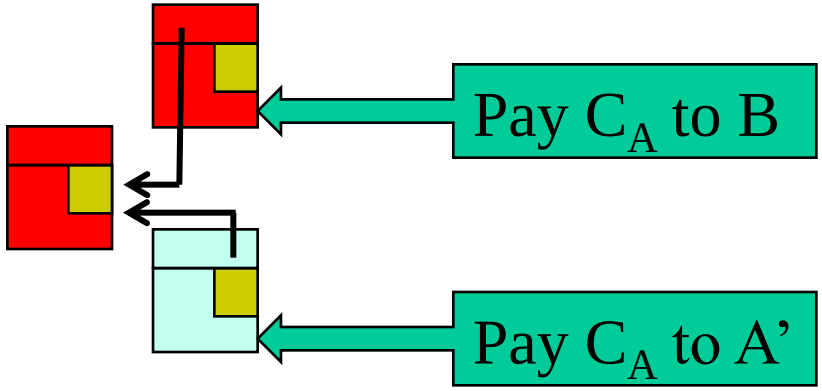
How the Blockchain grows



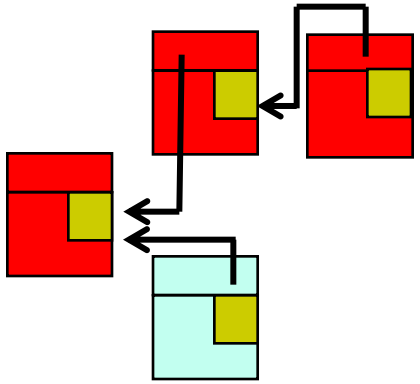
How to avoid double spending



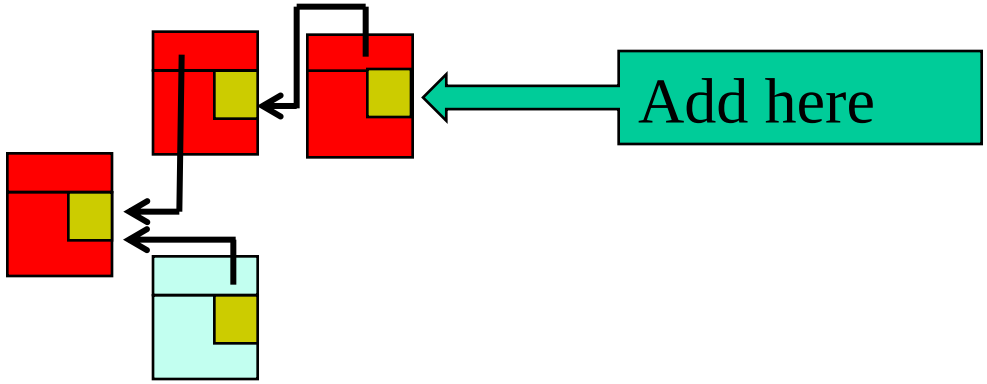
How to avoid double spending



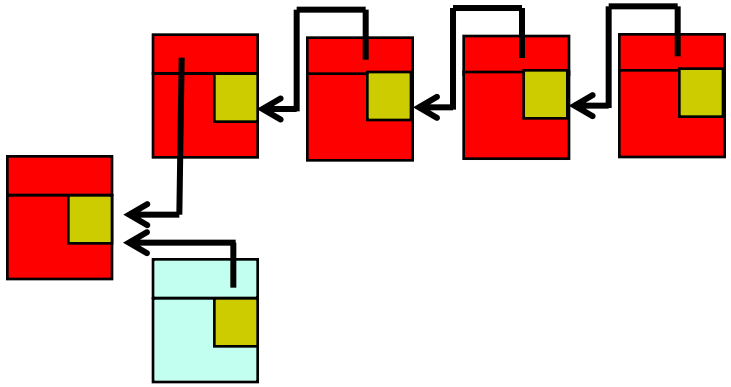
How to avoid double spending



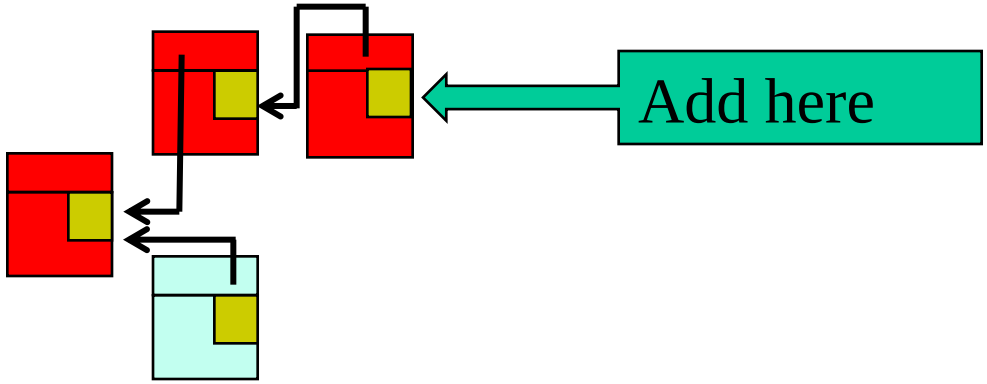
How to avoid double spending



How to avoid double spending

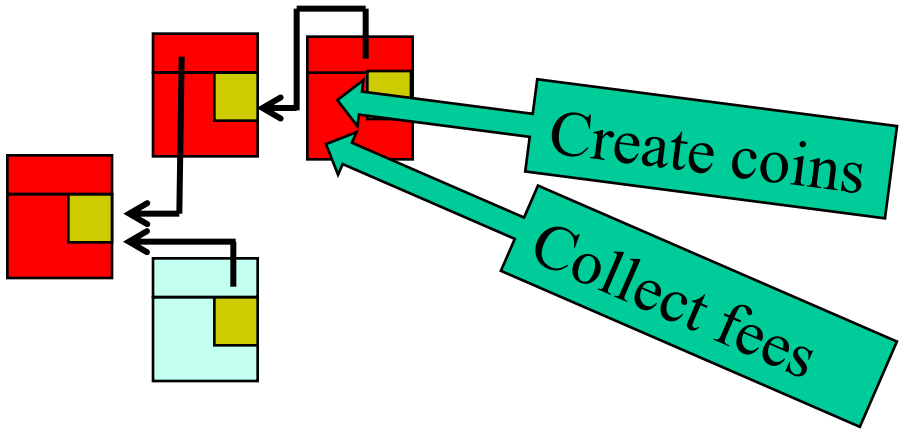


Why add here?



Because this chain more likely to live on
And this chain more likely to live on if valid
And … we prefer our node to be in a lively chain
because my node addition in a lively chain brings a reward

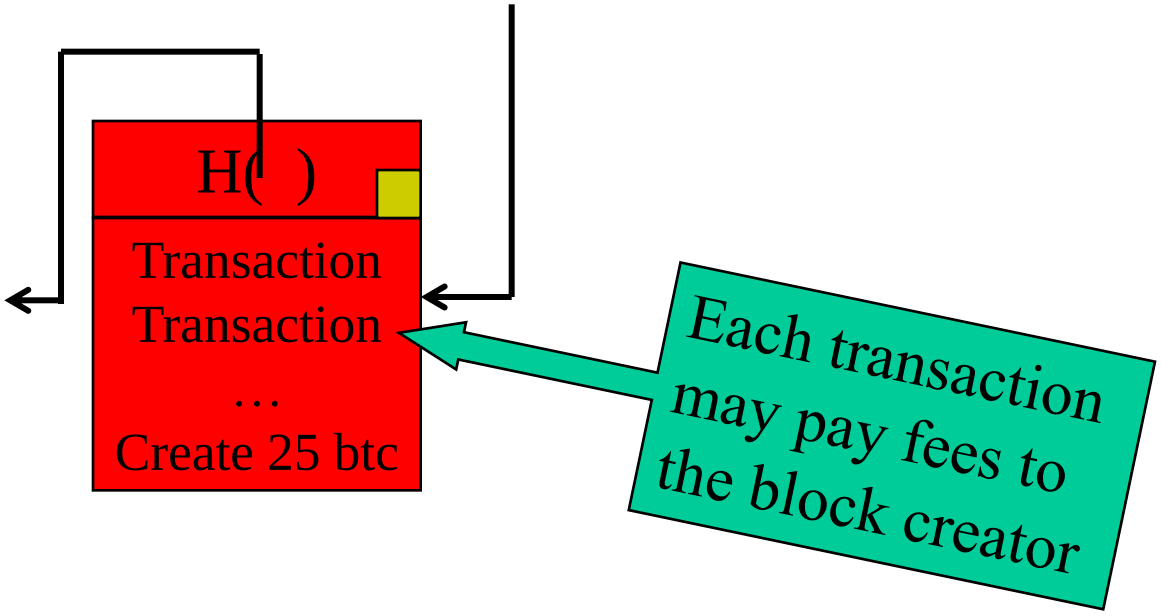
Reward or “incentive”



The reward is

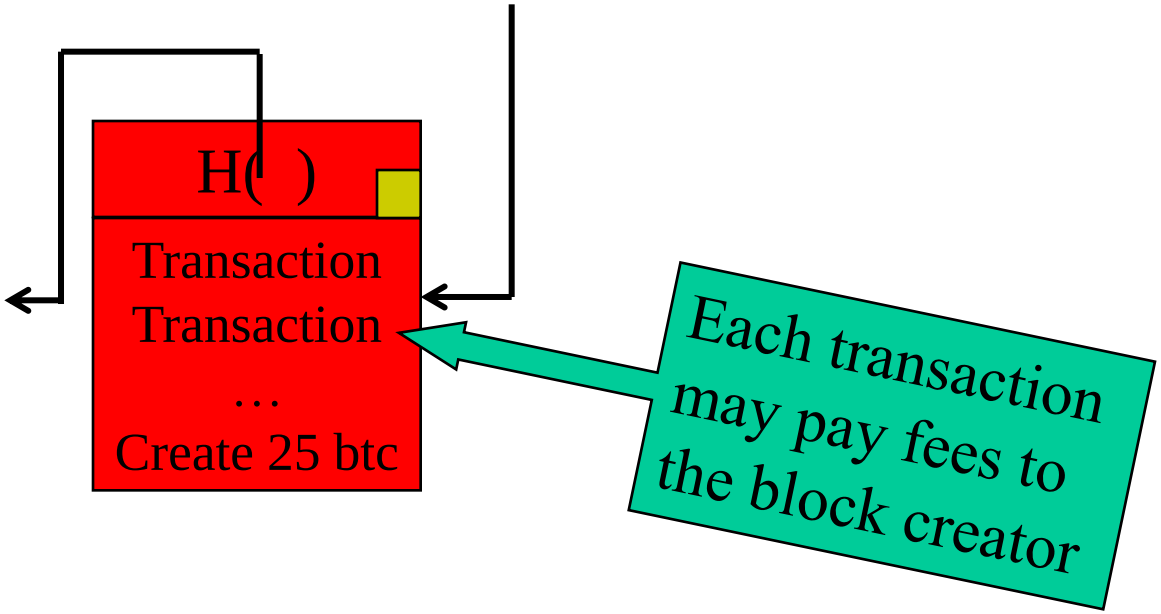
- the embedded ability of including a «create coins» transaction in the newly created block
- the embedded ability of collecting transaction fees

Bitcoin creation



Initially, 50 bitcoins where awarded to the block creator
This is halved every 4 years
Ends in year 2040

Bitcoin creation



Proof of work difficulty tailored so as to
make average time between blocks to be 10 minutes

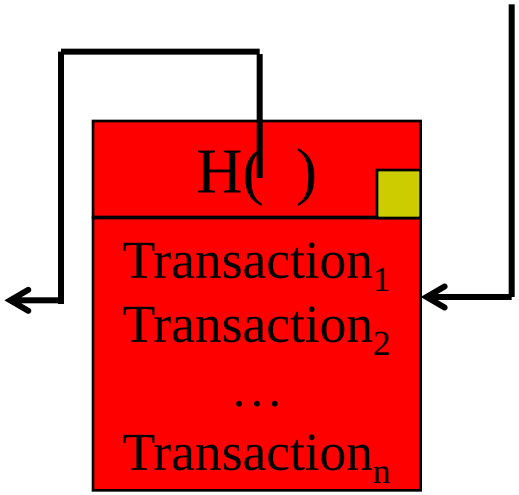
Number of blocks in a year = 6 per hour * 24 hours * 365 = 52.560

Total btc = (4*50+4*25+4*12.5+…)*52.560= about 21 million

Total bitcoins in 2040

number of years	reward	number of blocks	number of created coins	year
4,00	50,00	52.560,00	10.512.000,00	2008
4,00	25,00	52.560,00	5.256.000,00	2012
4,00	12,50	52.560,00	2.628.000,00	2016
4,00	6,25	52.560,00	1.314.000,00	2020
4,00	3,13	52.560,00	657.000,00	2024
4,00	1,56	52.560,00	328.500,00	2028
4,00	0,78	52.560,00	164.250,00	2032
4,00	0,39	52.560,00	82.125,00	2036
4,00	0,20	52.560,00	41.062,50	2040
			20.982.937,50	

Space reduction

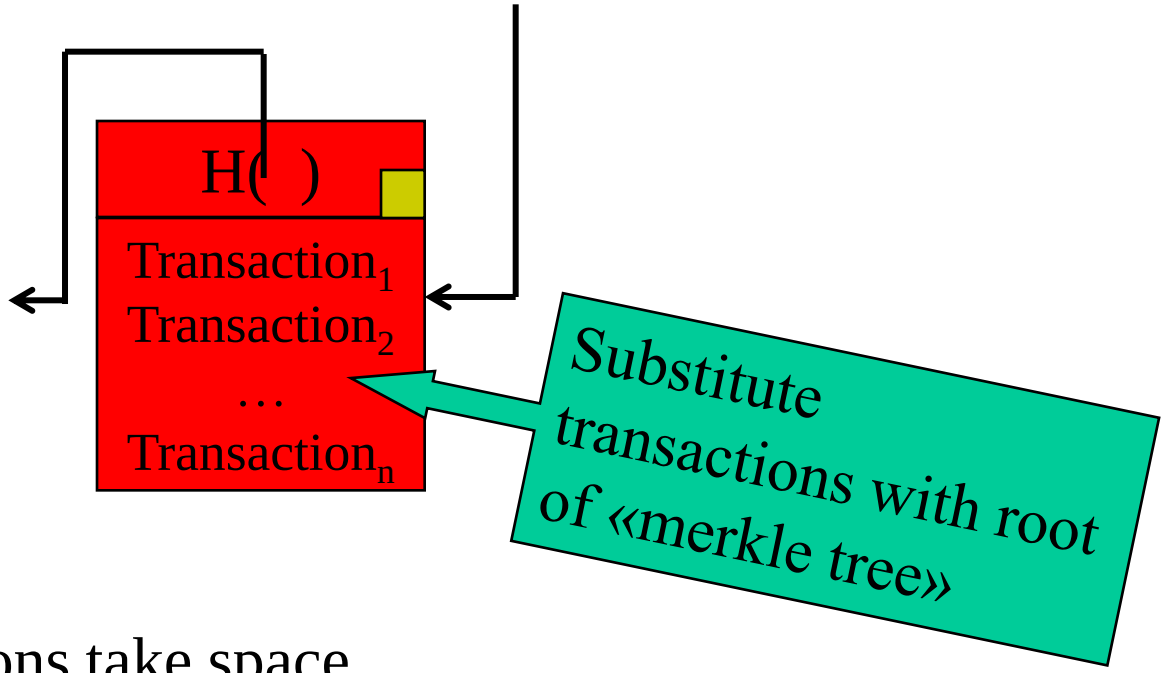


Transactions take space

Blockchain needs to be stored by all active nodes

⇒ we need to reduce space

Space reduction

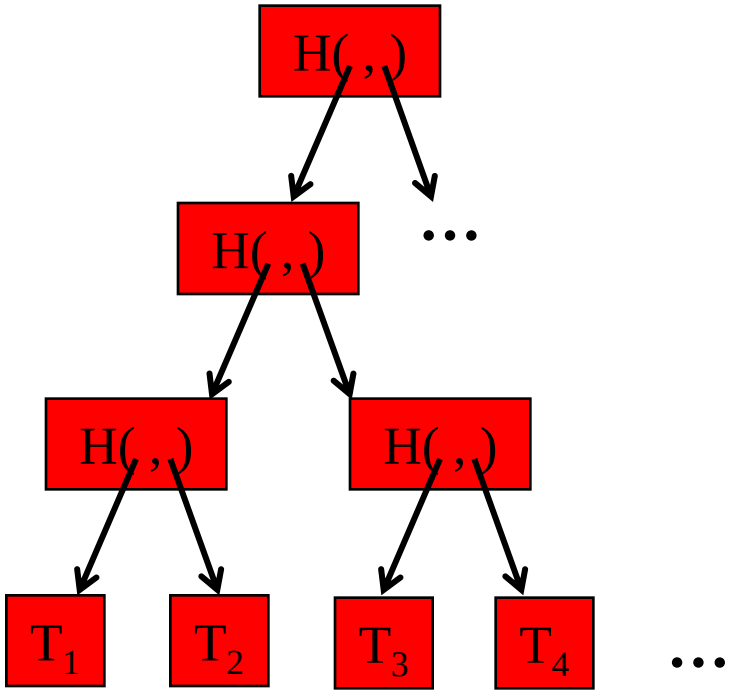


Transactions take space

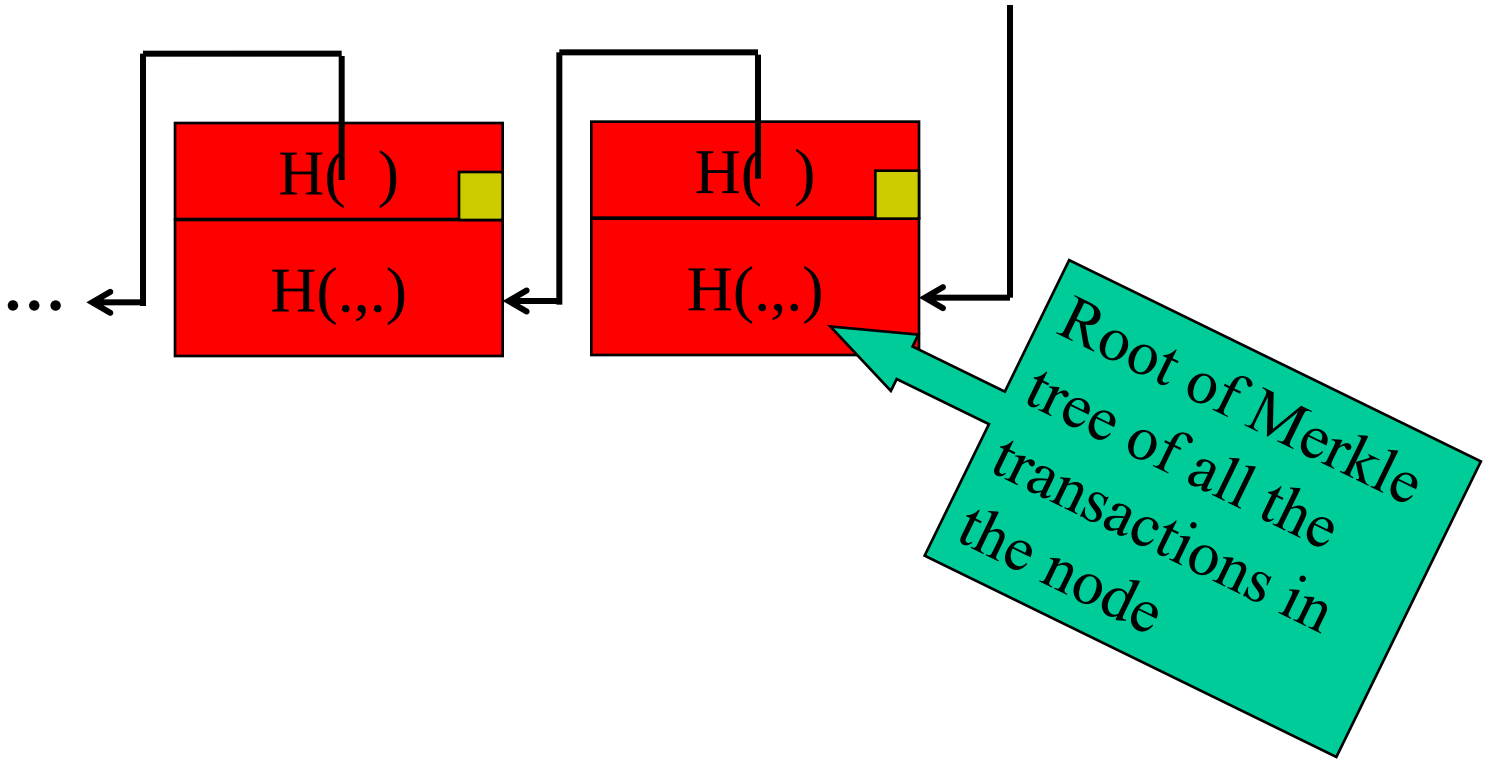
Blockchain needs to be stored by all active nodes

⇨ we need to reduce space

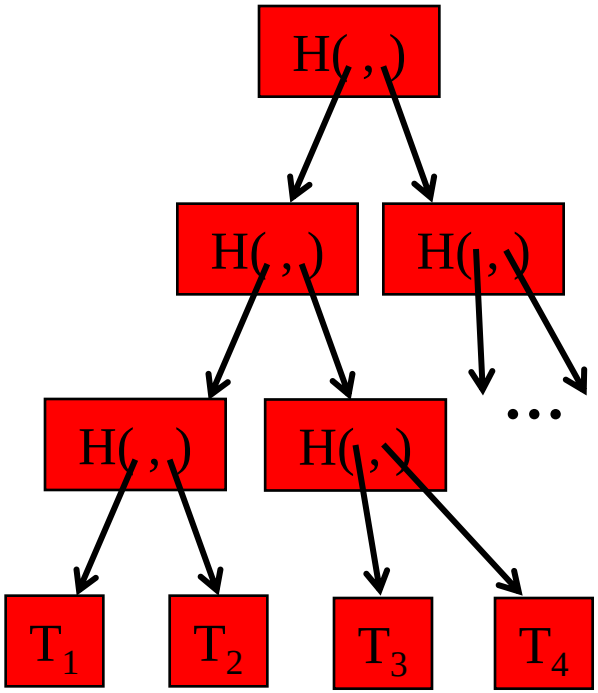
Merkle tree

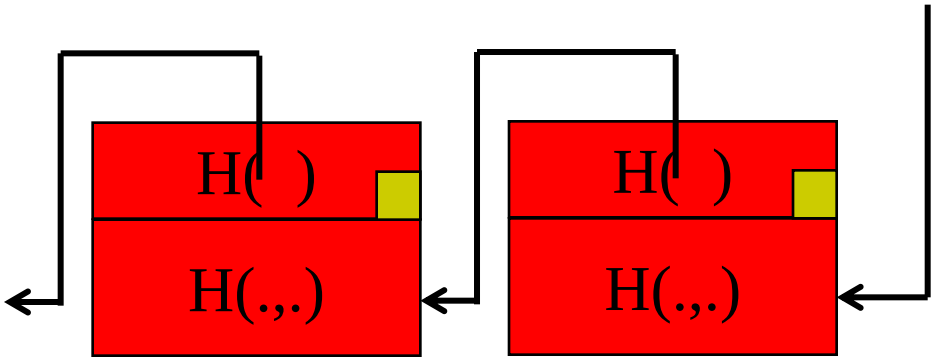


Optimized Blockchain

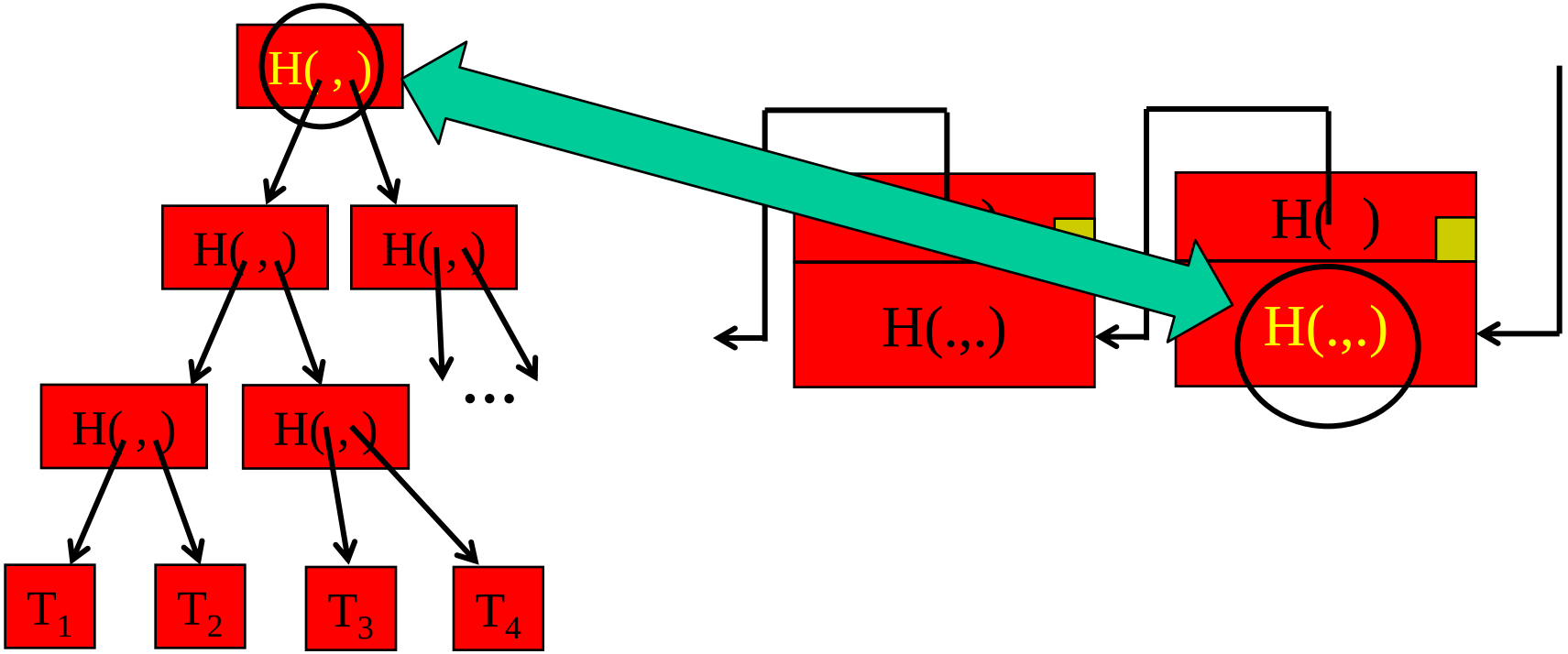


Proof of membership

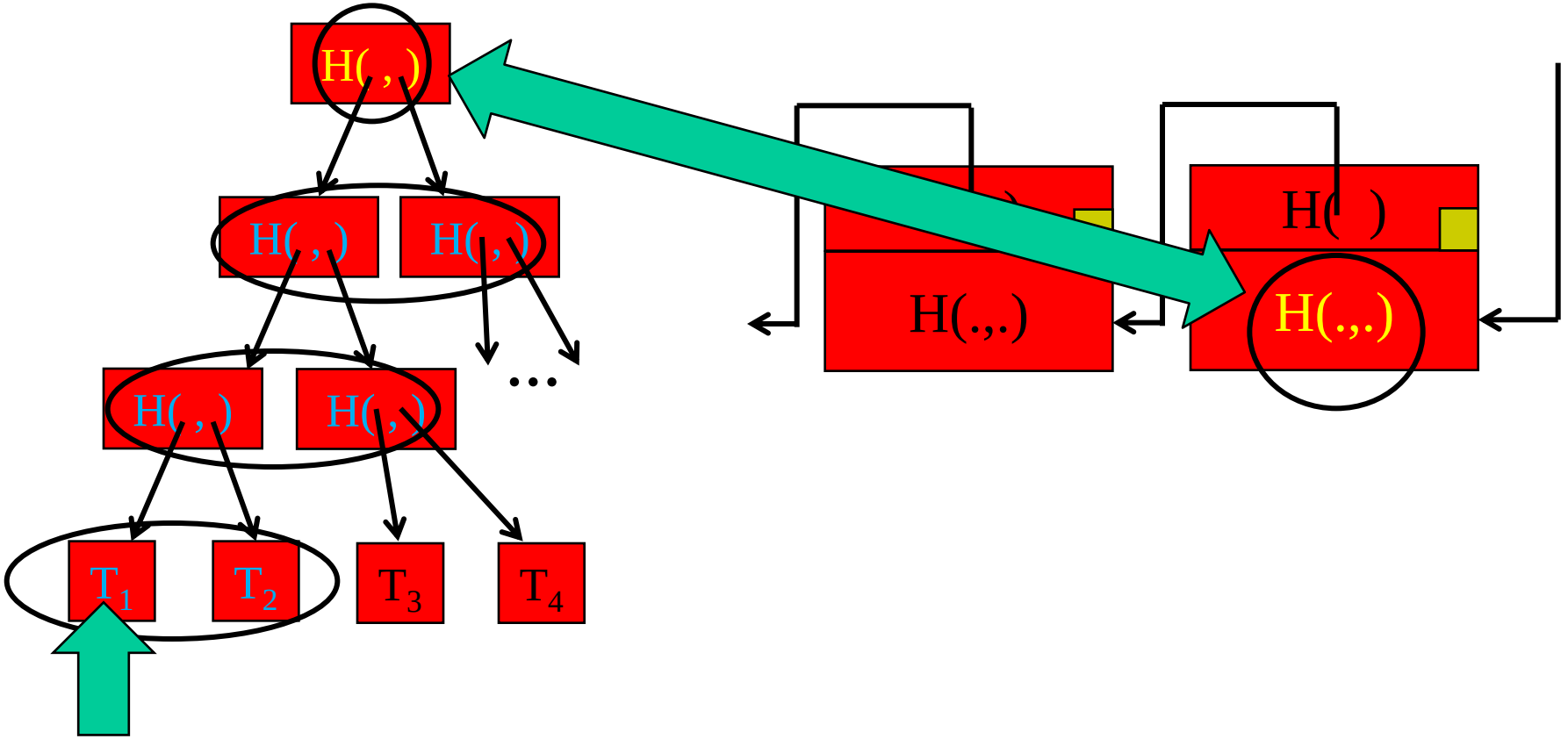




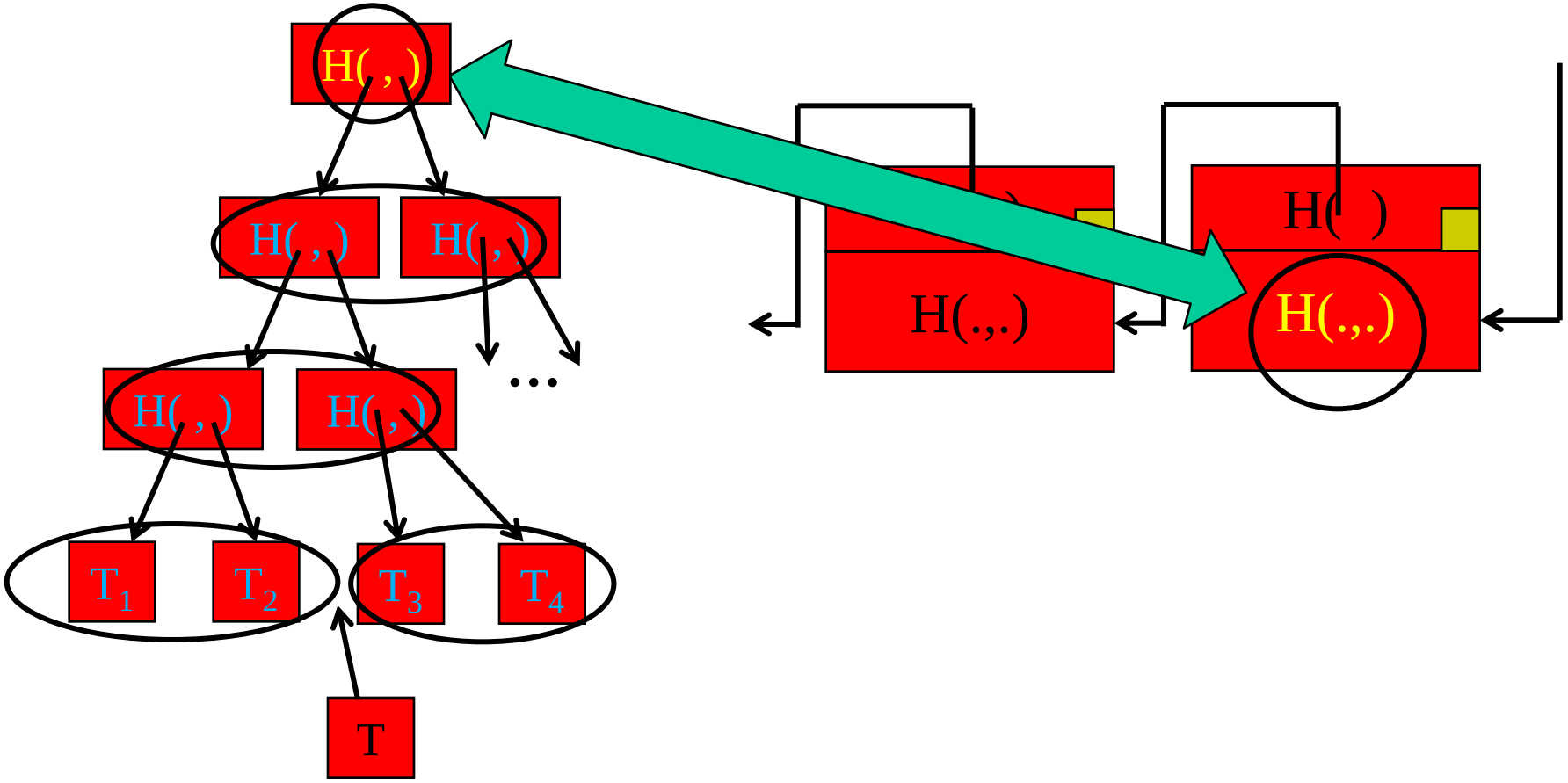
Proof of membership



Proof of membership



Proof of non membership



Conclusions

- Bitcoins as signed information
- Network consensus for validity
- Proof of work for “sealing” blocks