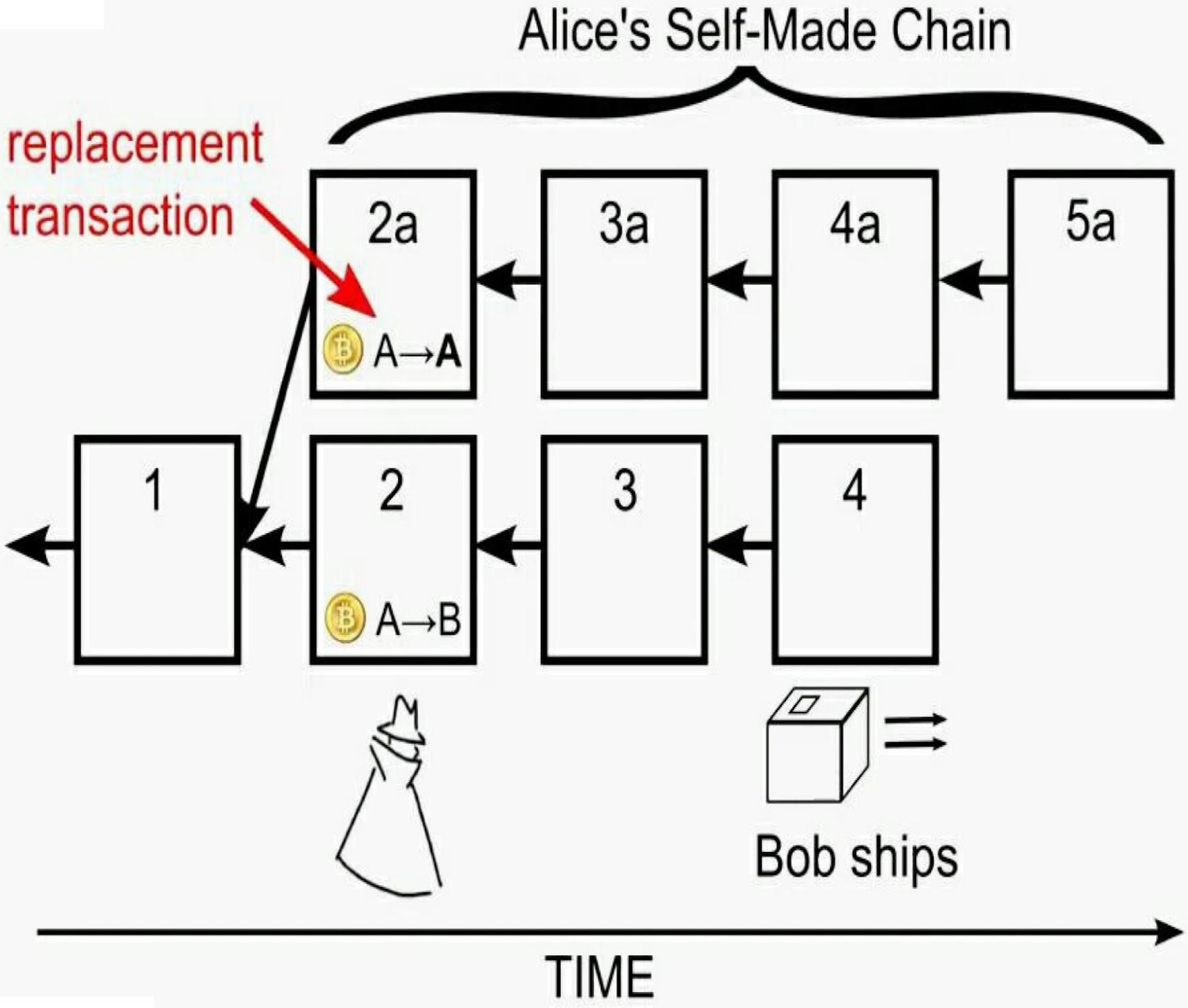
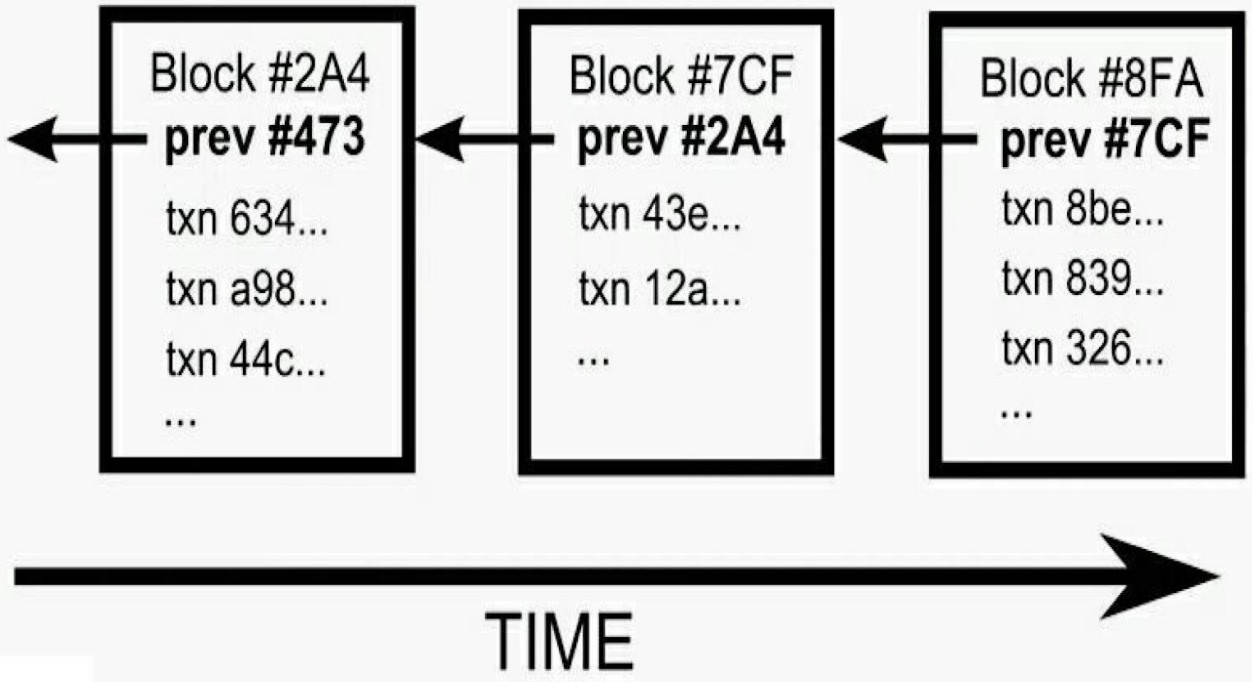
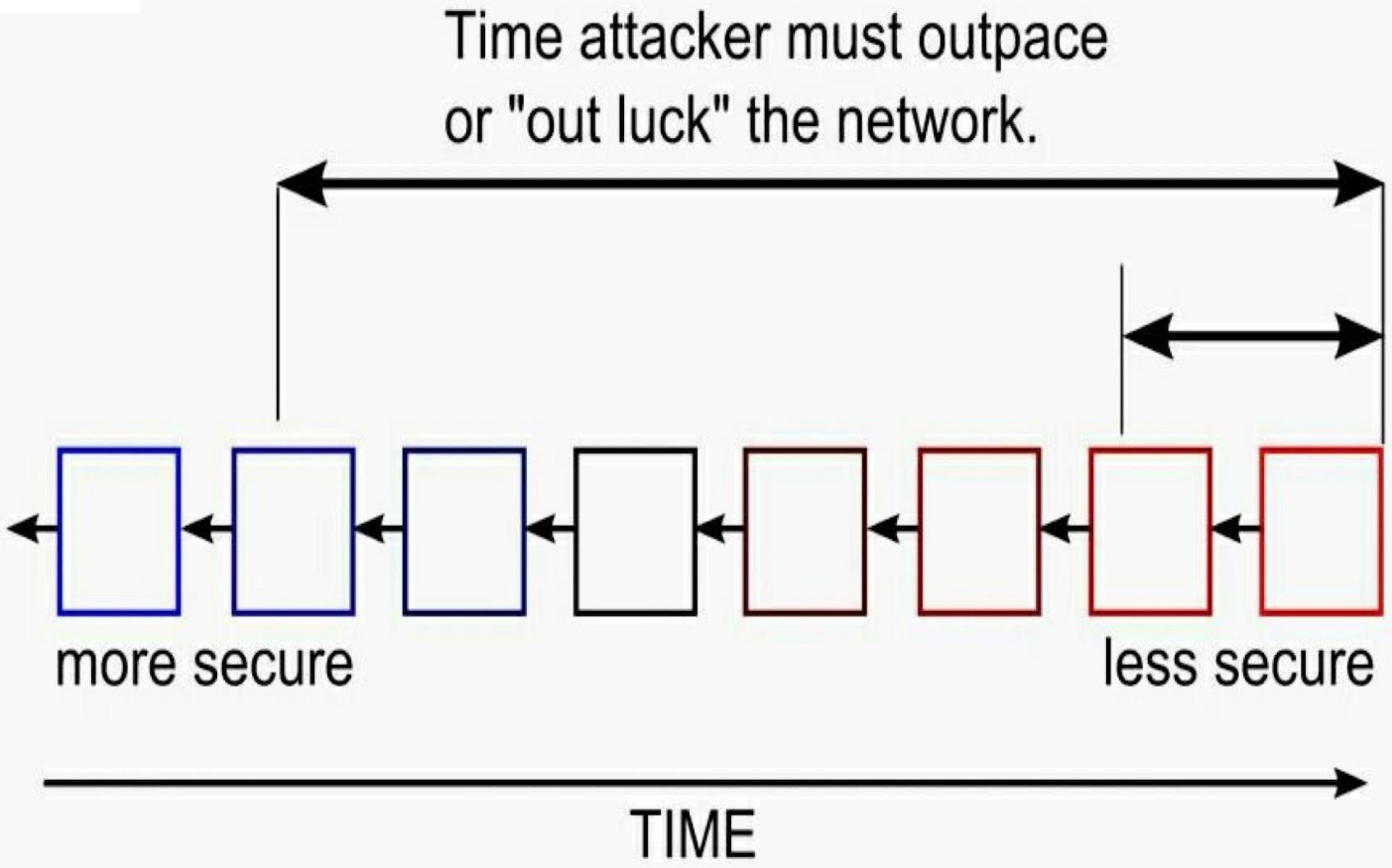
Особенности технологии Block Chain

Докладчик: курсант Бражников Д.А.

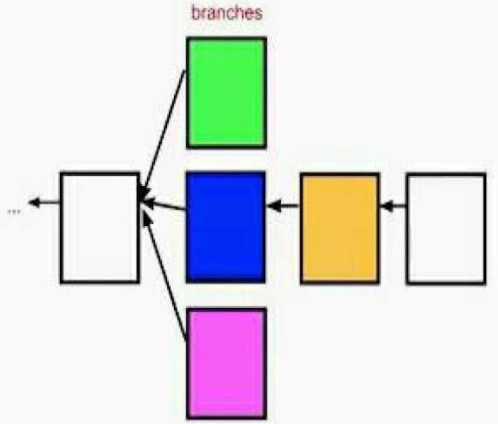

Alice's Self-Made Chain
replacement
transaction
2a
3a
4a
5a
A→A
1
2
3
4
A→B
Bob ships
TIME

Ordering Solution: The Block Chain

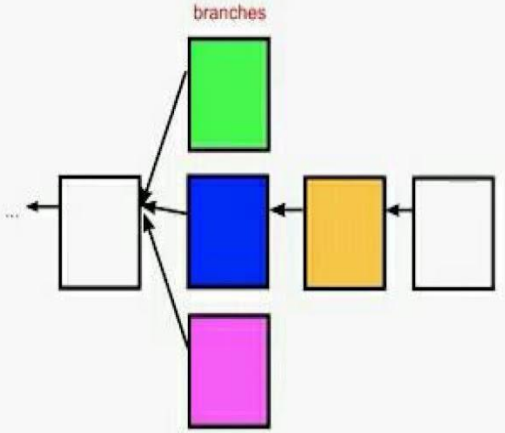



Time attacker must outpace
or "out luck" the network.
more secure
less secure
TIME

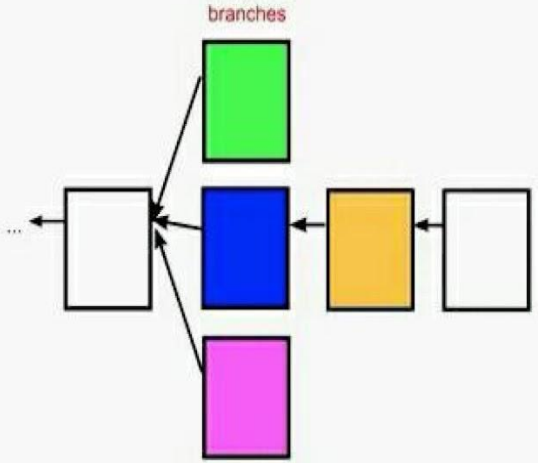
Travis's
Block Chain



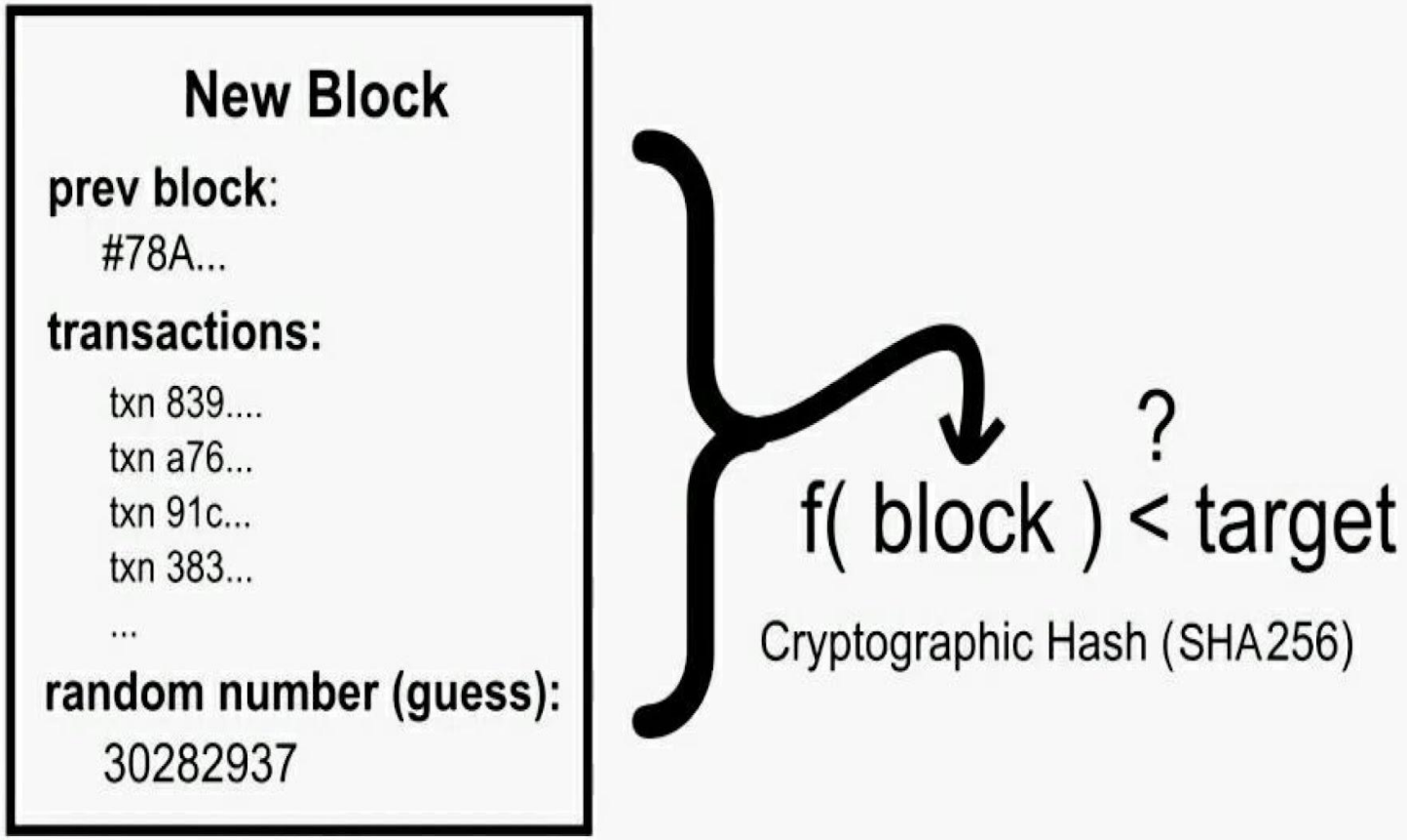
Your
Block Chain



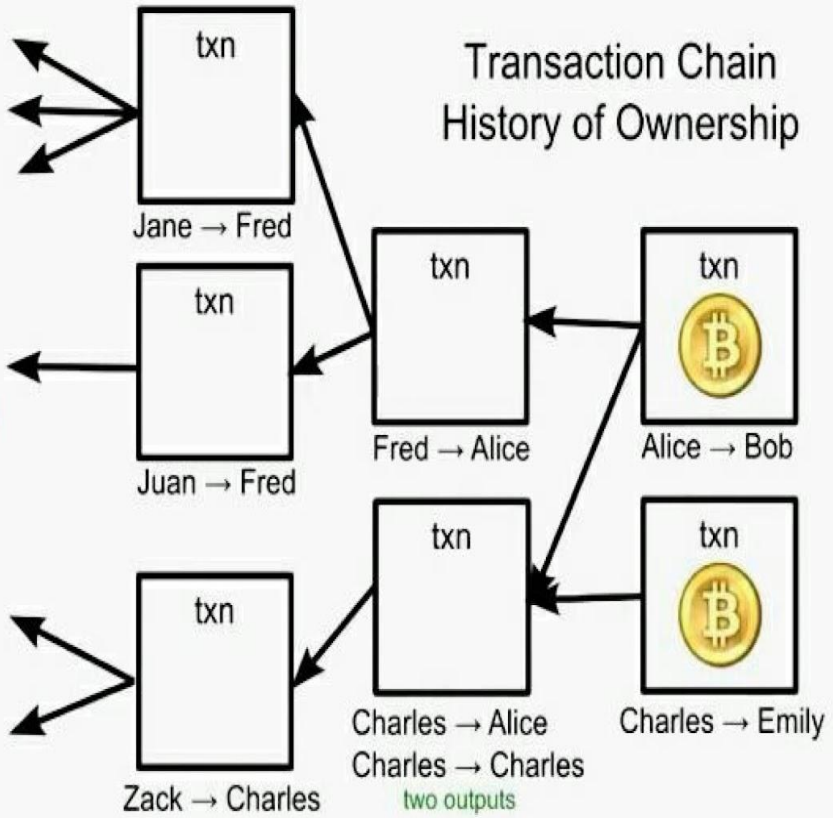
Carol's
Block Chain



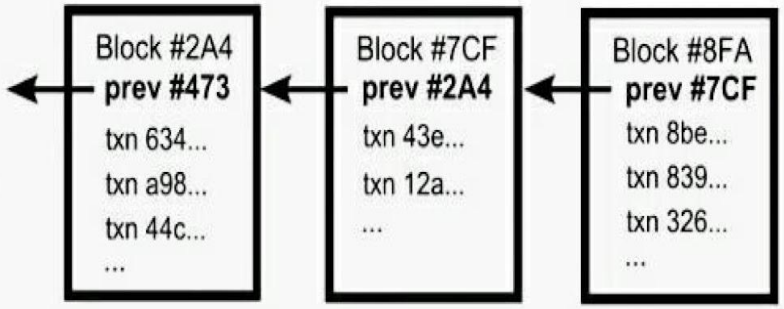
Block Puzzle



Transaction Chain:
History of Ownership

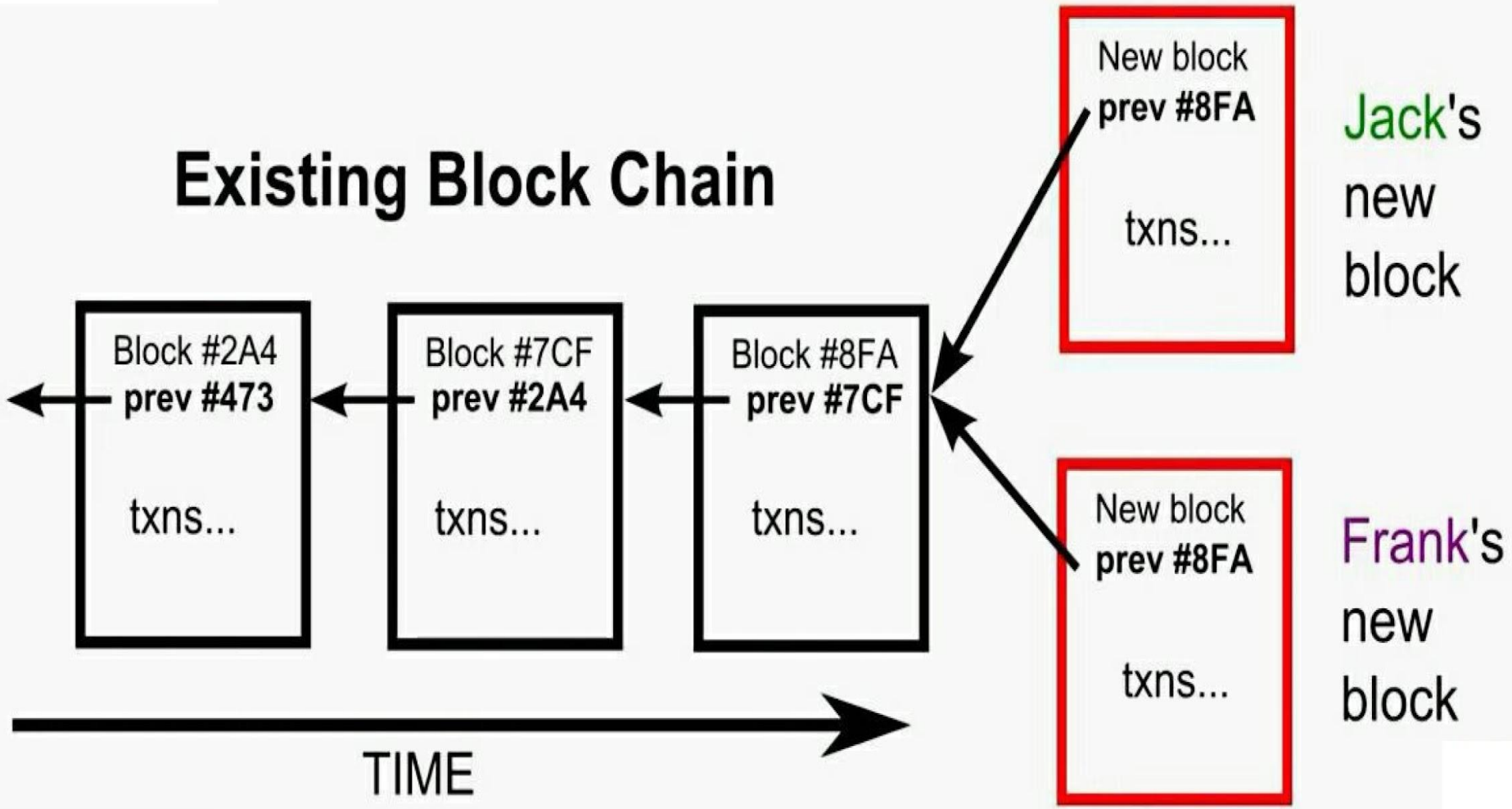


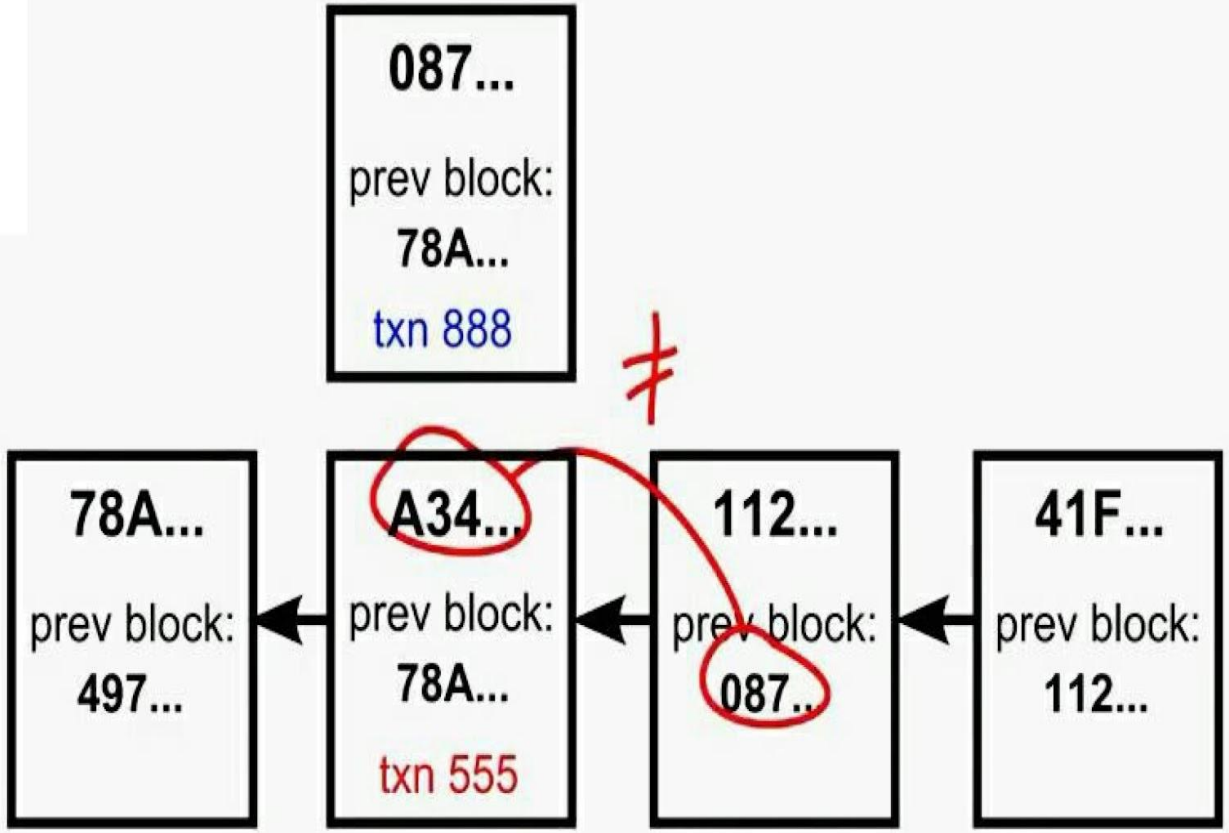
Block Chain:
Transaction Ordering



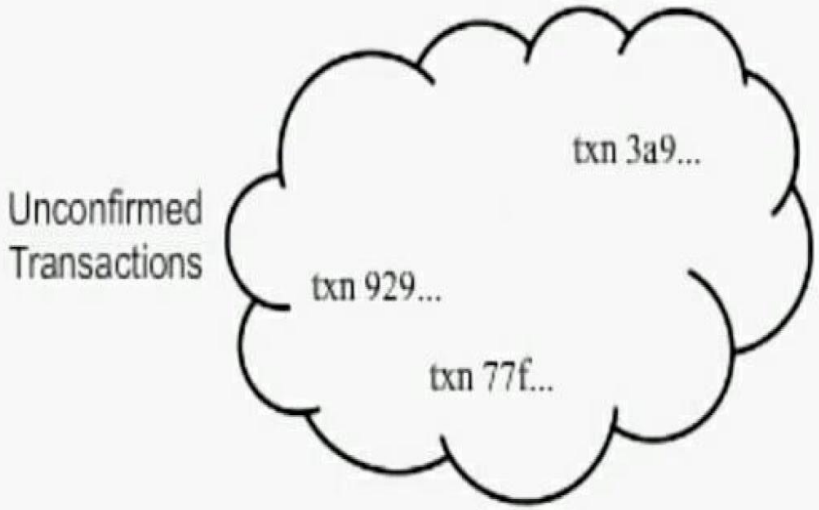
Bitcoin Transaction Security

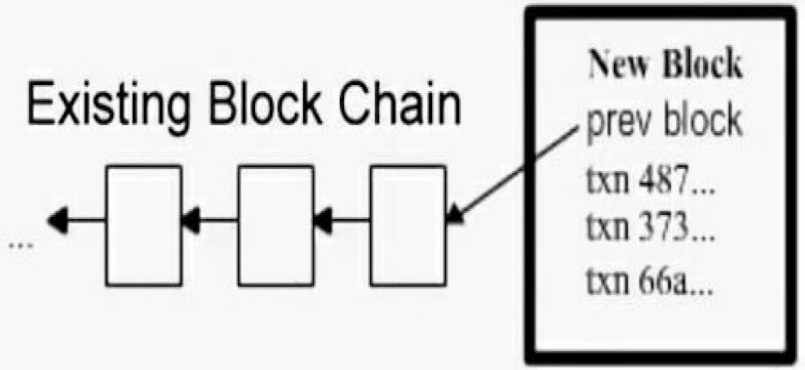
1. Digital Signatures
2. Referenced Transactions


potential next blocks
Existing Block Chain
Block #2A4
prev #473
txns...
Block #7CF
prev #2A4
txns...
Block #8FA
prev #7CF
txns...
New block
prev #8FA
txns...
Jack's new block
New block
prev #8FA
txns...
Frank's new block
TIME

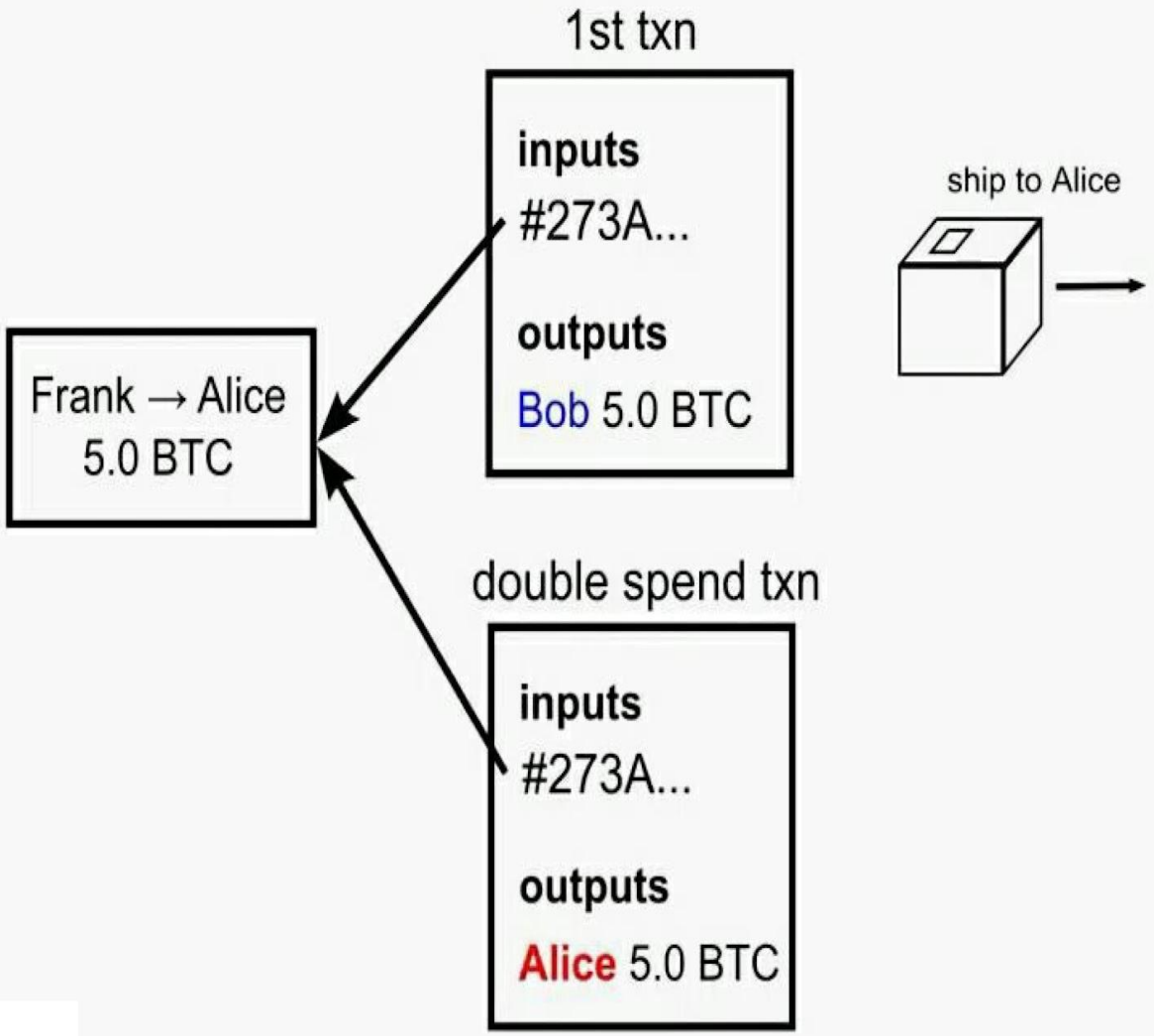

087...
prev block:
78A...
txn 888
≠
78A...
prev block:
497...
A34...
prev block:
78A...
txn 555
112...
prev block:
087...
41F...
prev block:
112...

Block Creation

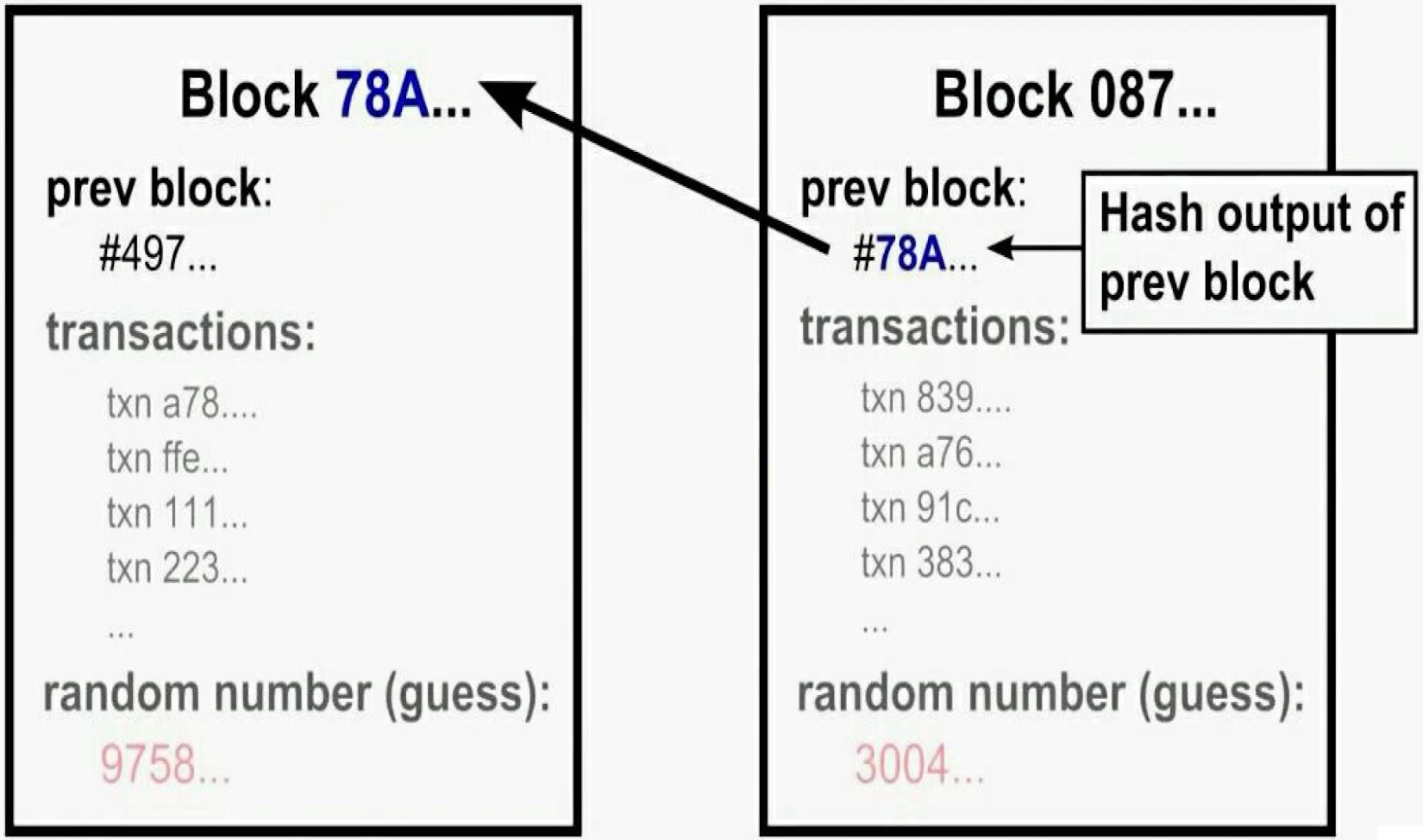


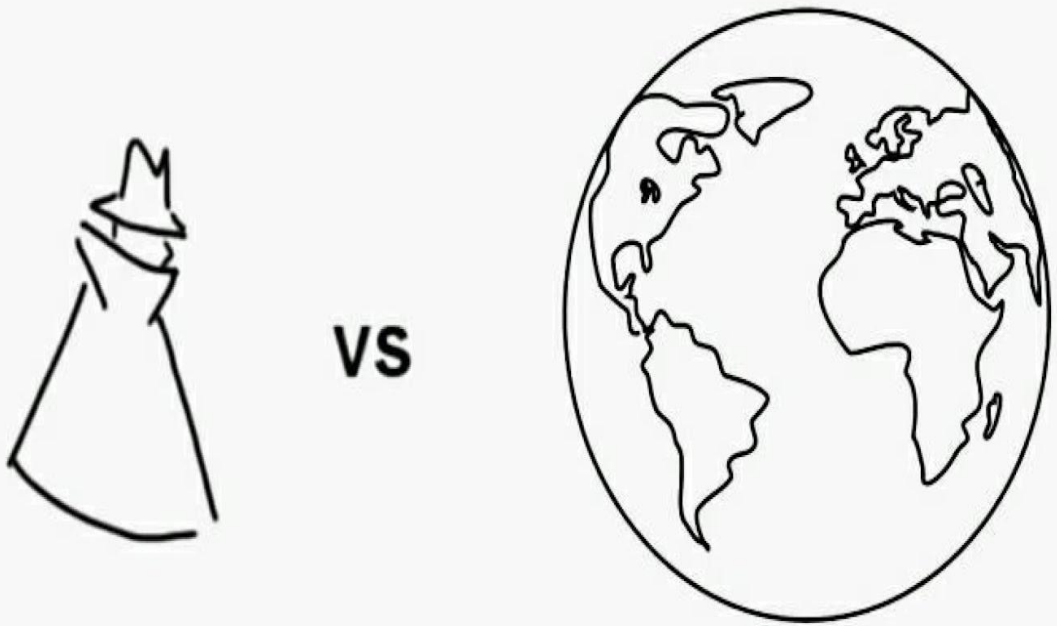


Double Spending Fraud

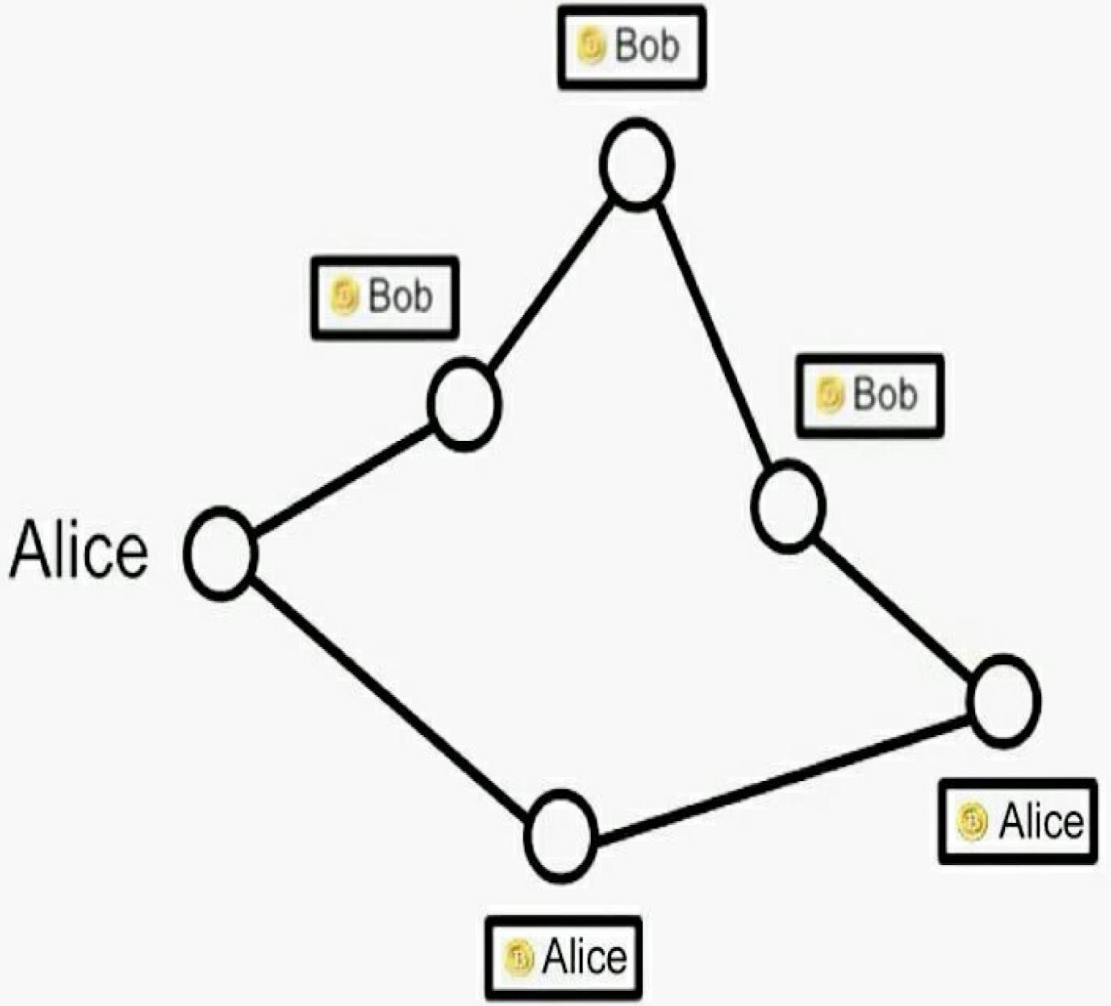


Hash outputs = Block IDs

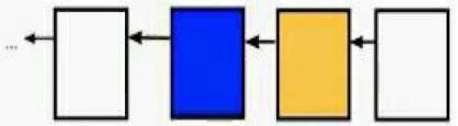



VS

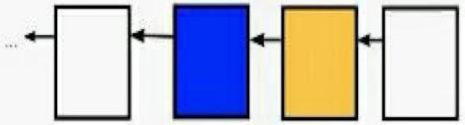
Double Spending Fraud



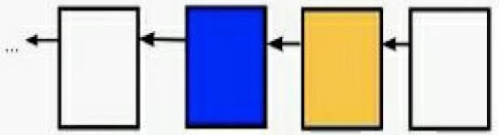
Travis's
Block Chain



Your
Block Chain



Carol's
Block Chain



Спасибо за внимание!