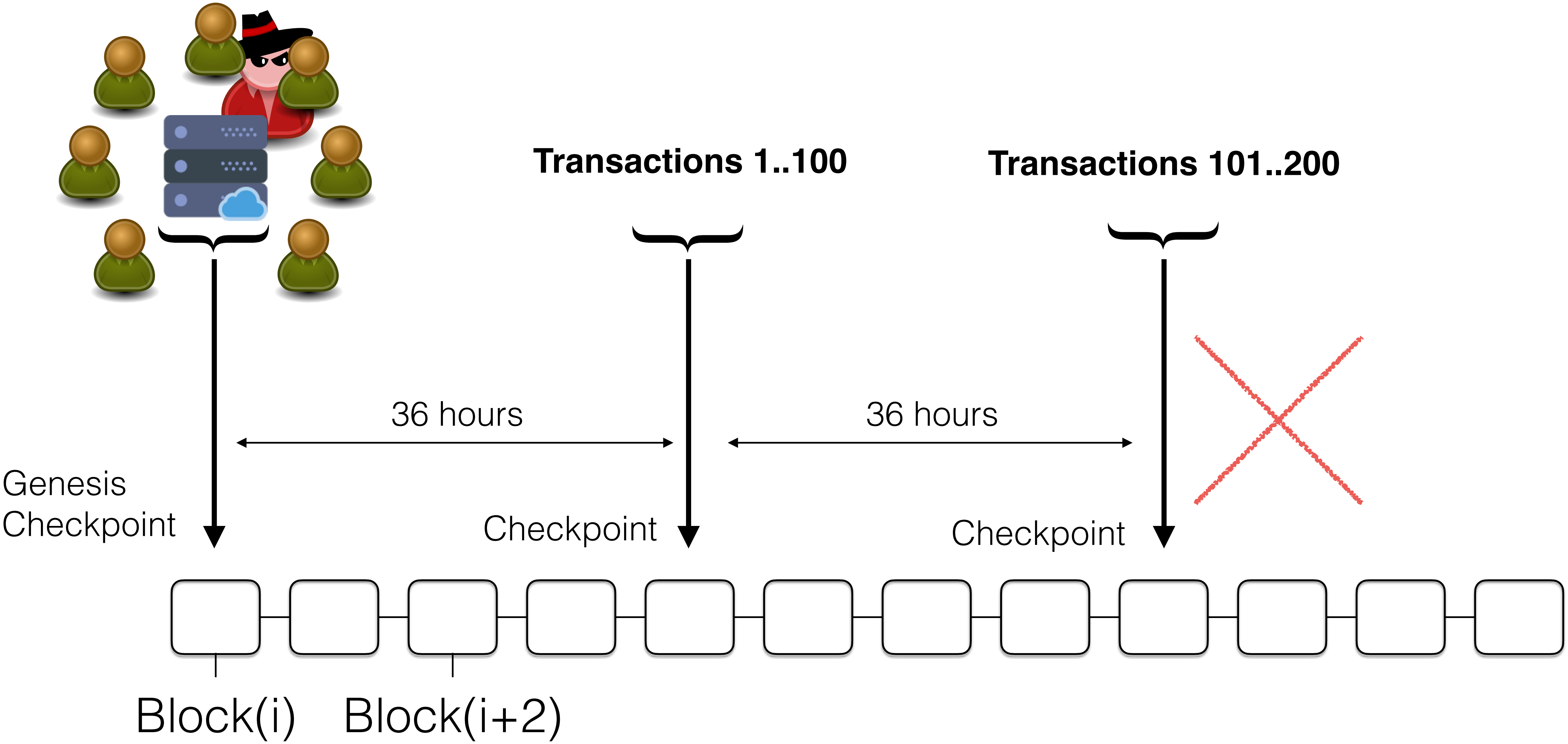
Commit-Chains
NOCUST Security

NOCUST operator disappears
… just after checkpoint



Transactions 1..100

Transactions 101..200

36 hours

36 hours

Genesis
Checkpoint

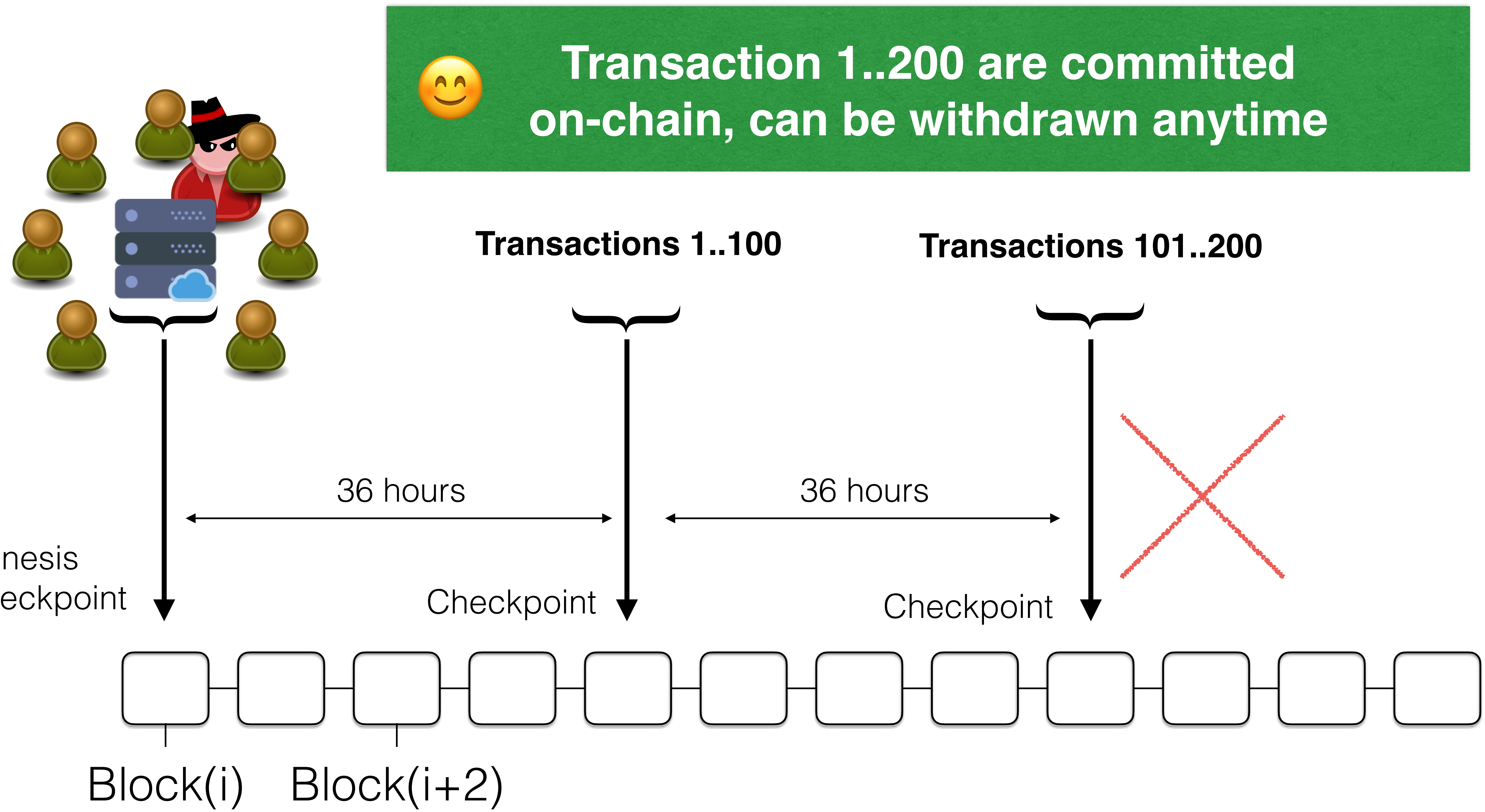
Checkpoint

Checkpoint

Block(i)

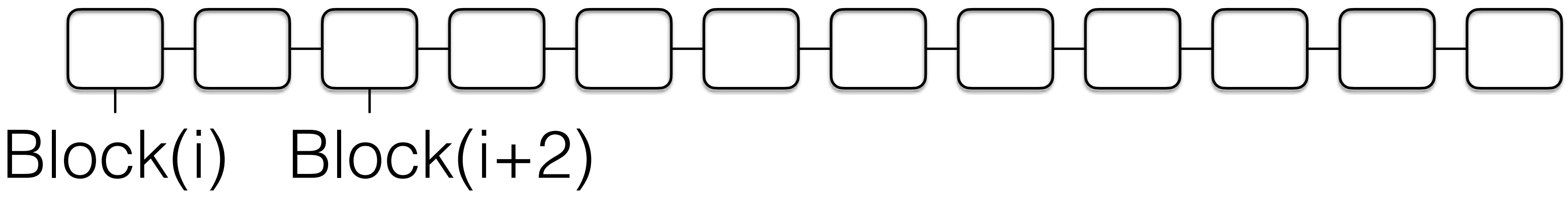
Block(i+2)

NOCUST operator disappears
… just after checkpoint

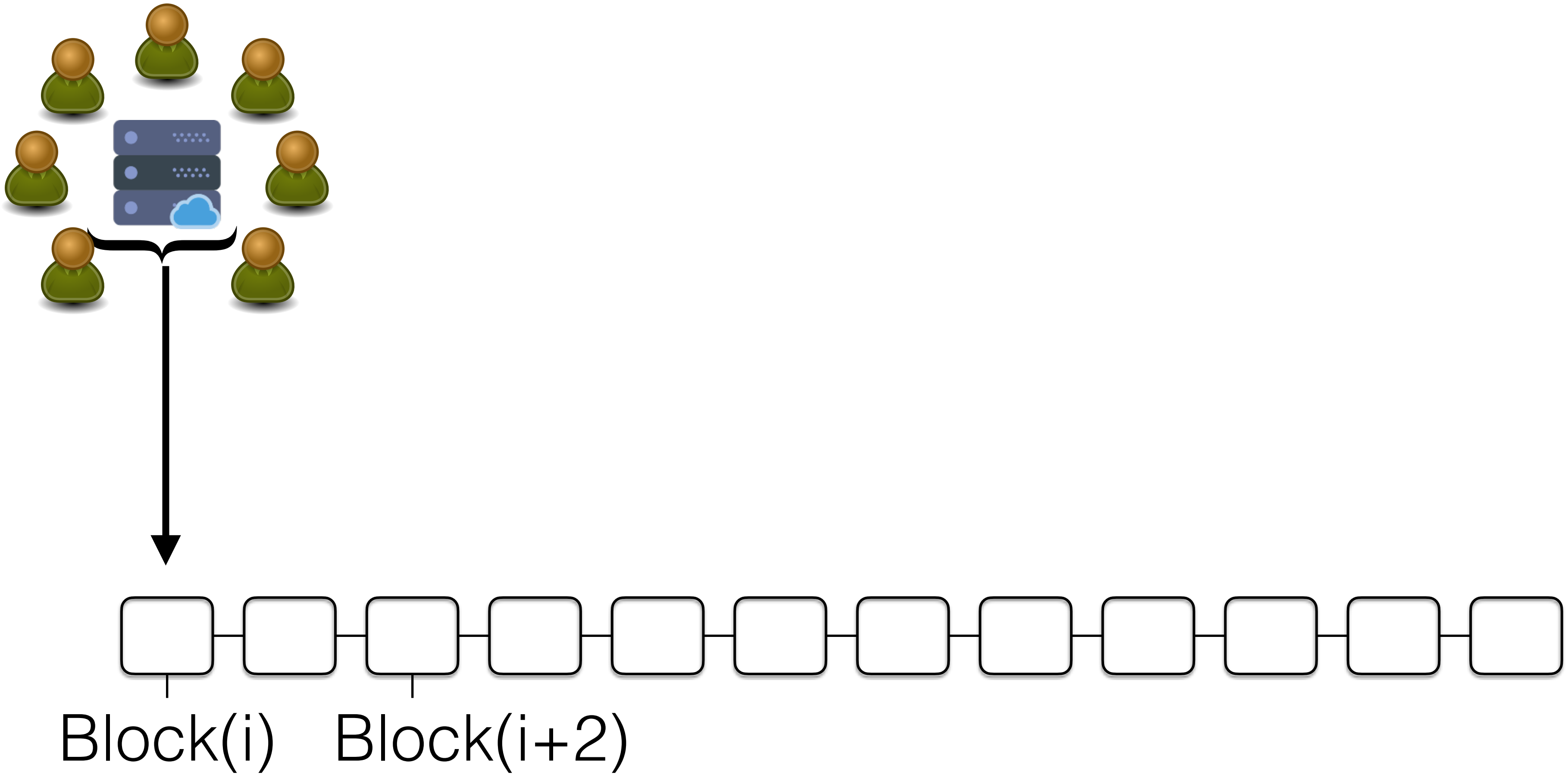


😊 Transaction 1..200 are committed on-chain, can be withdrawn anytime

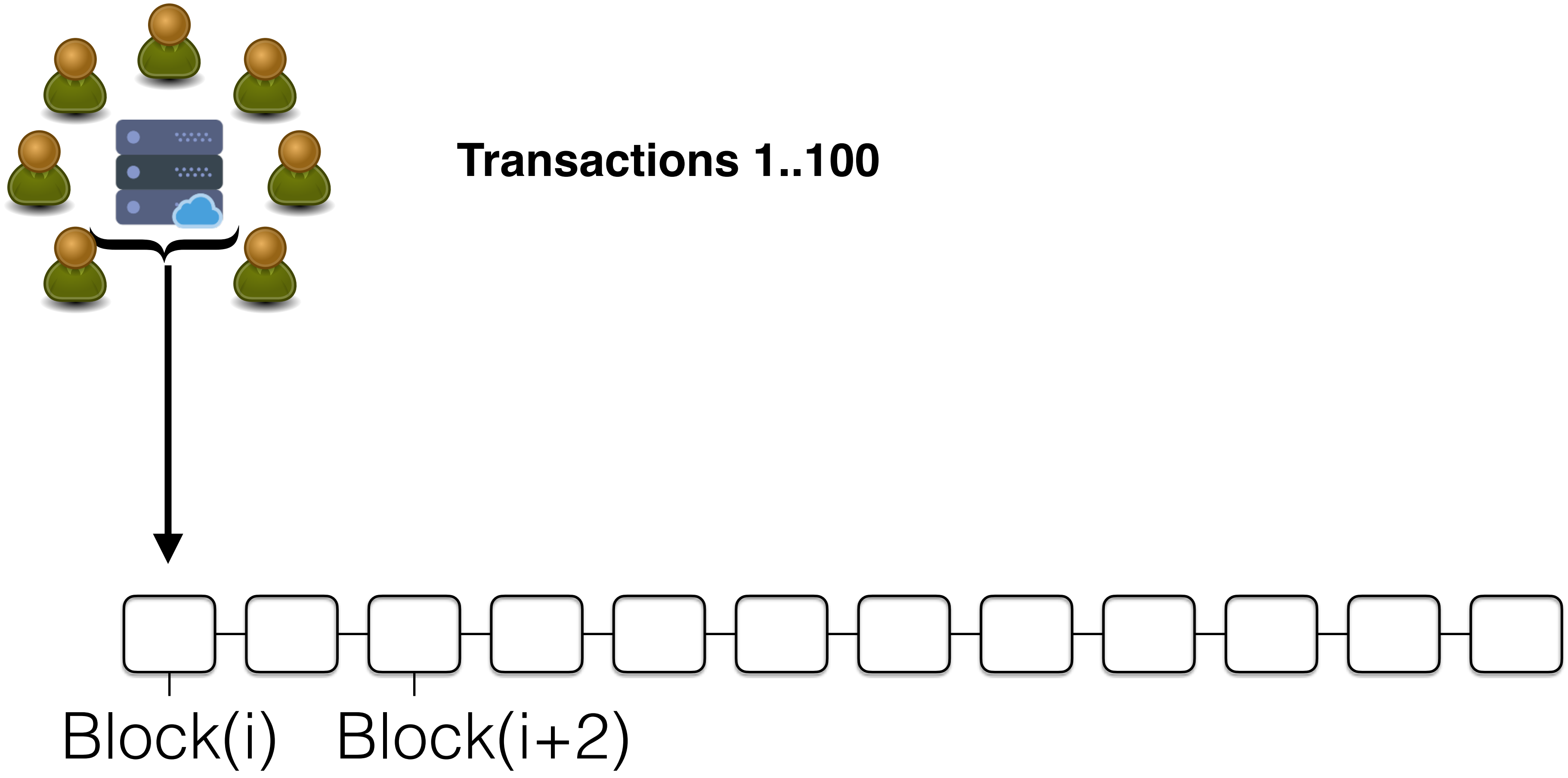
NOCUST server disappears
… after a few transactions



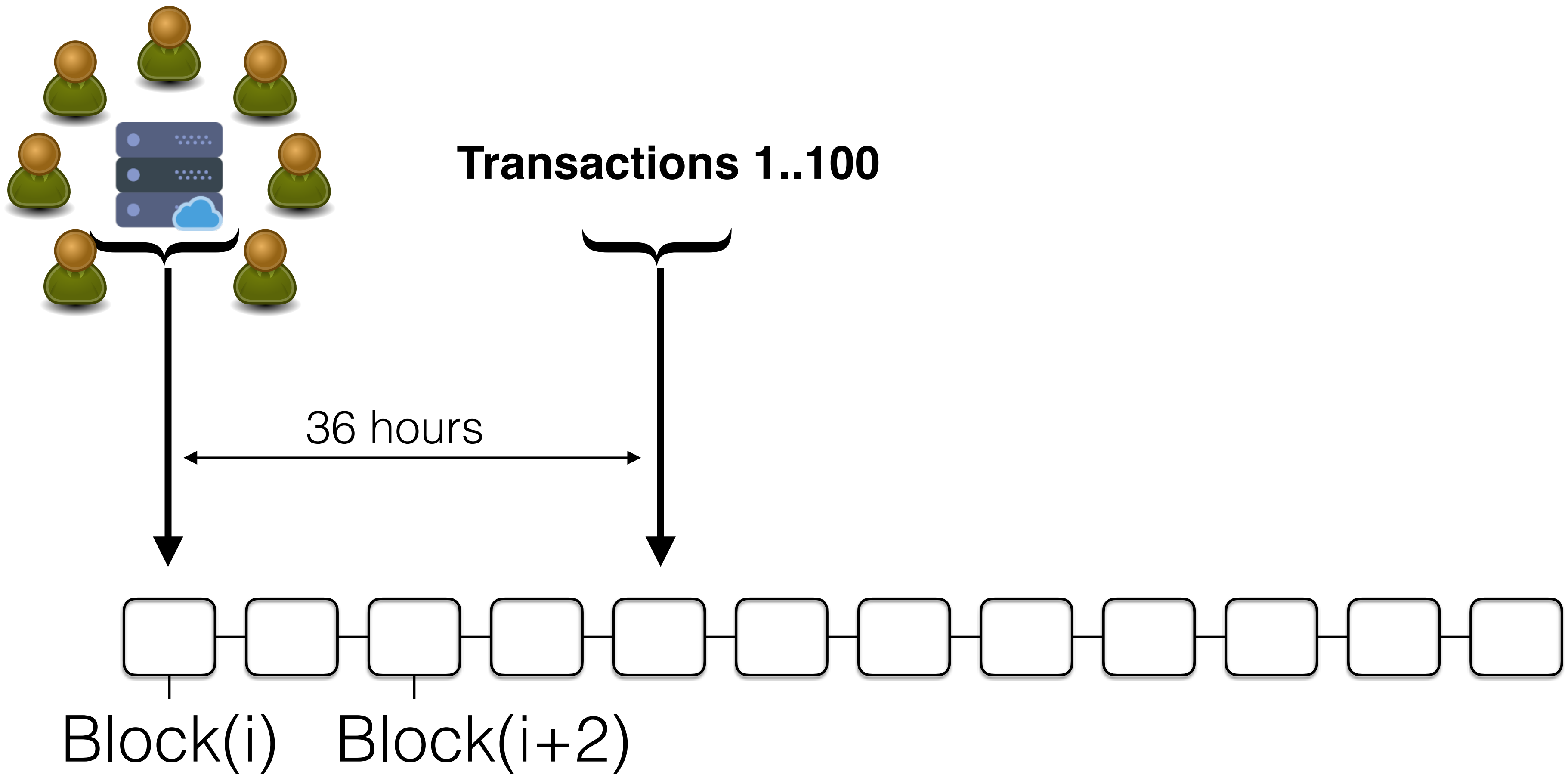
NOCUST server disappears
… after a few transactions



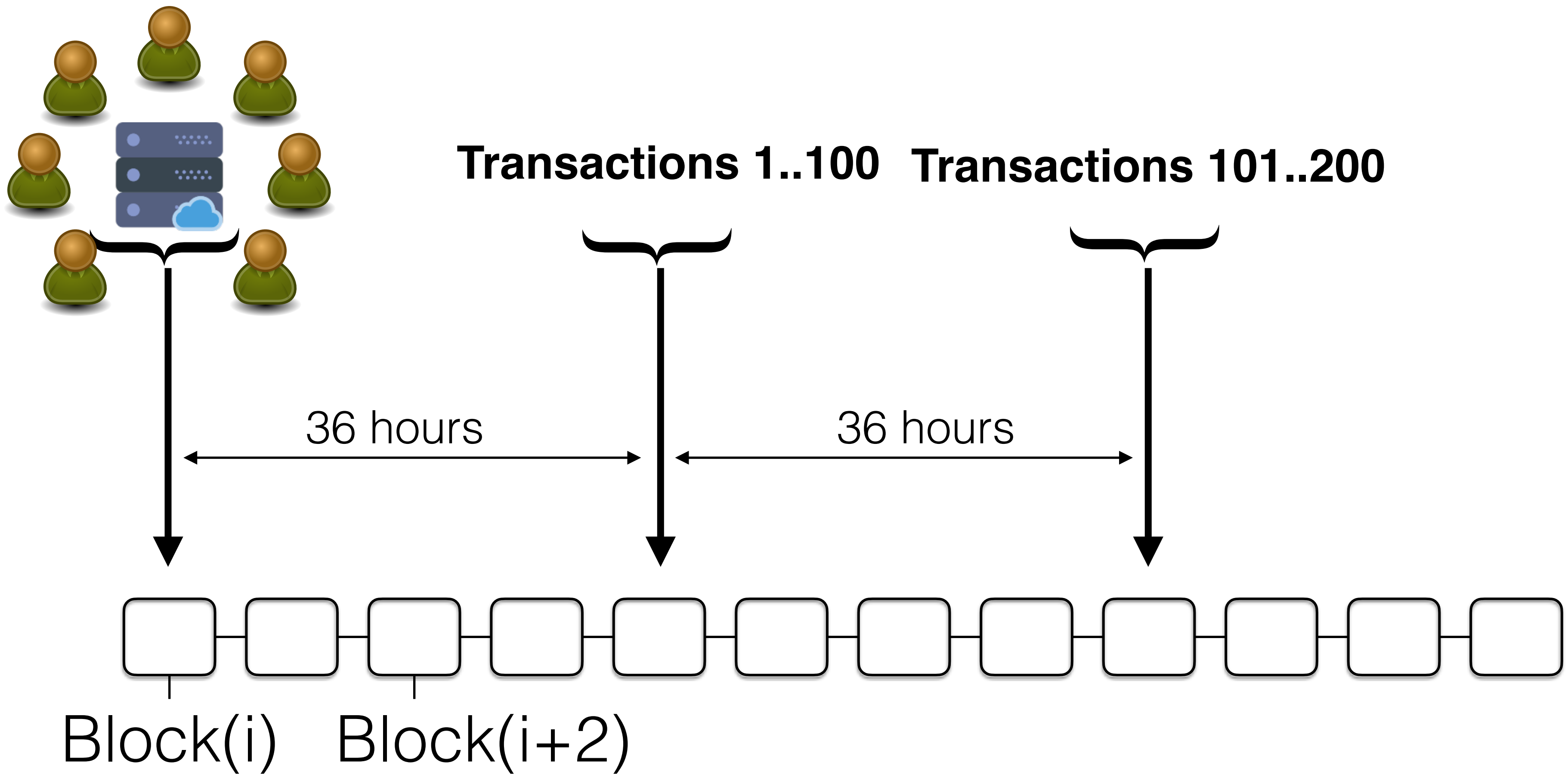
NOCUST server disappears
… after a few transactions



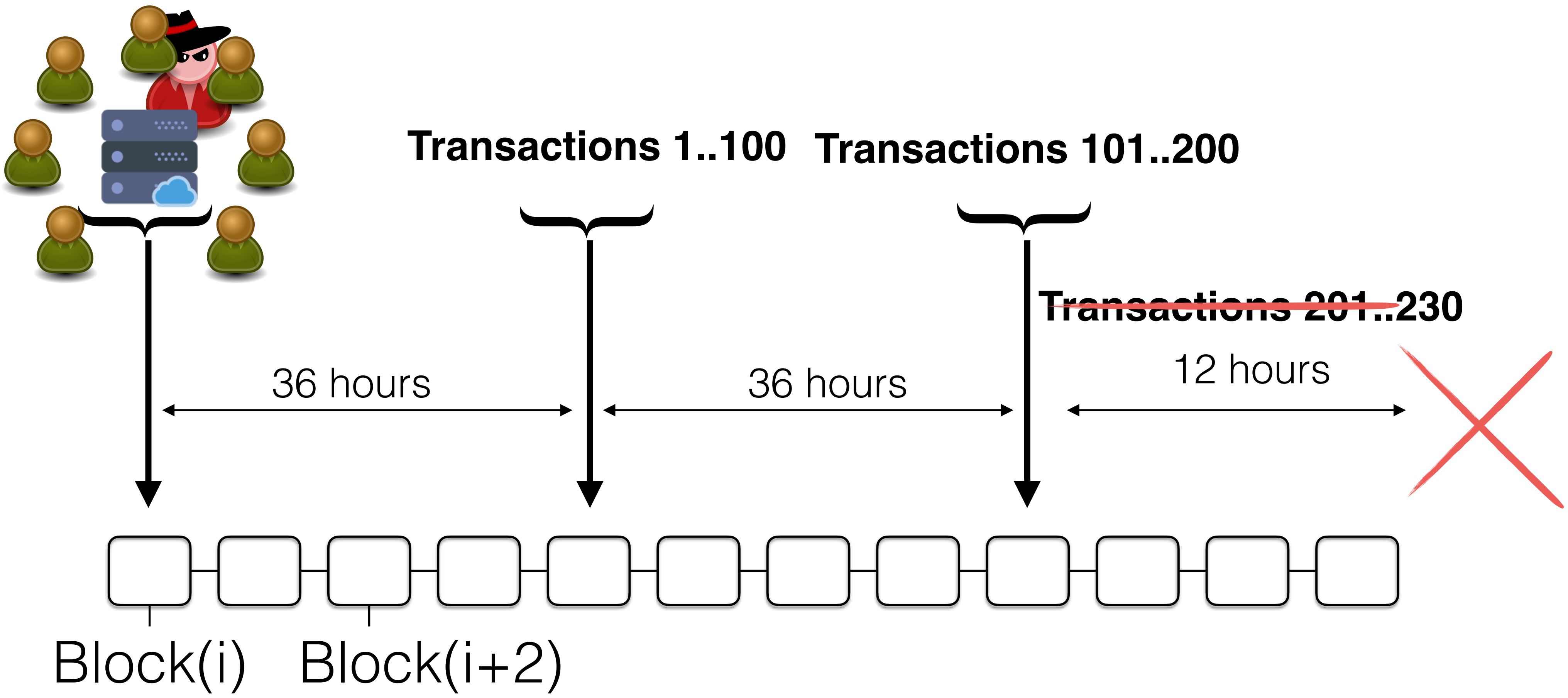
NOCUST server disappears
… after a few transactions



NOCUST server disappears
… after a few transactions



NOCUST server disappears
… after a few transactions



Transactions 1..100

Transactions 101..200

~~Transactions 201..~~230

36 hours

36 hours

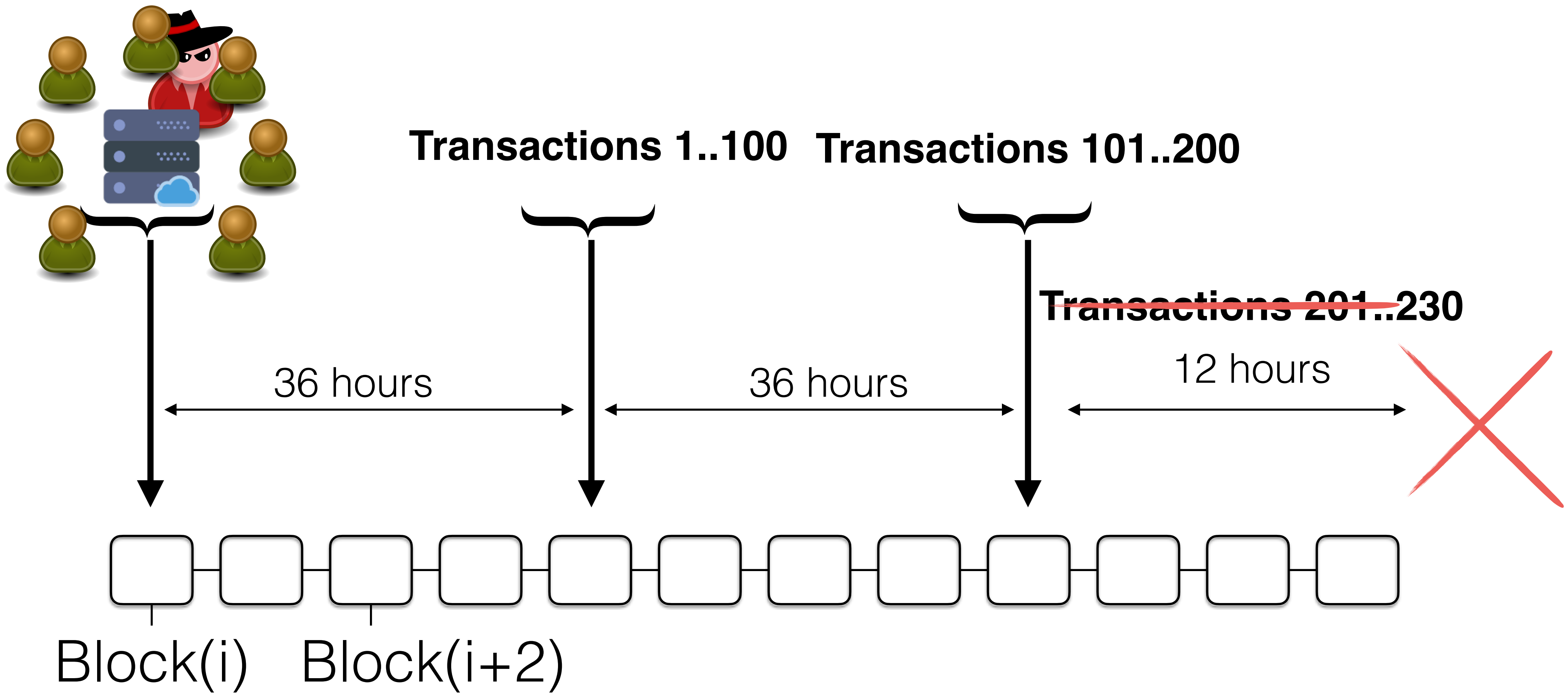
12 hours

Block(i)

Block(i+2)

NOCUST server disappears
… after a few transactions

😊 Transaction 1..200
are safe



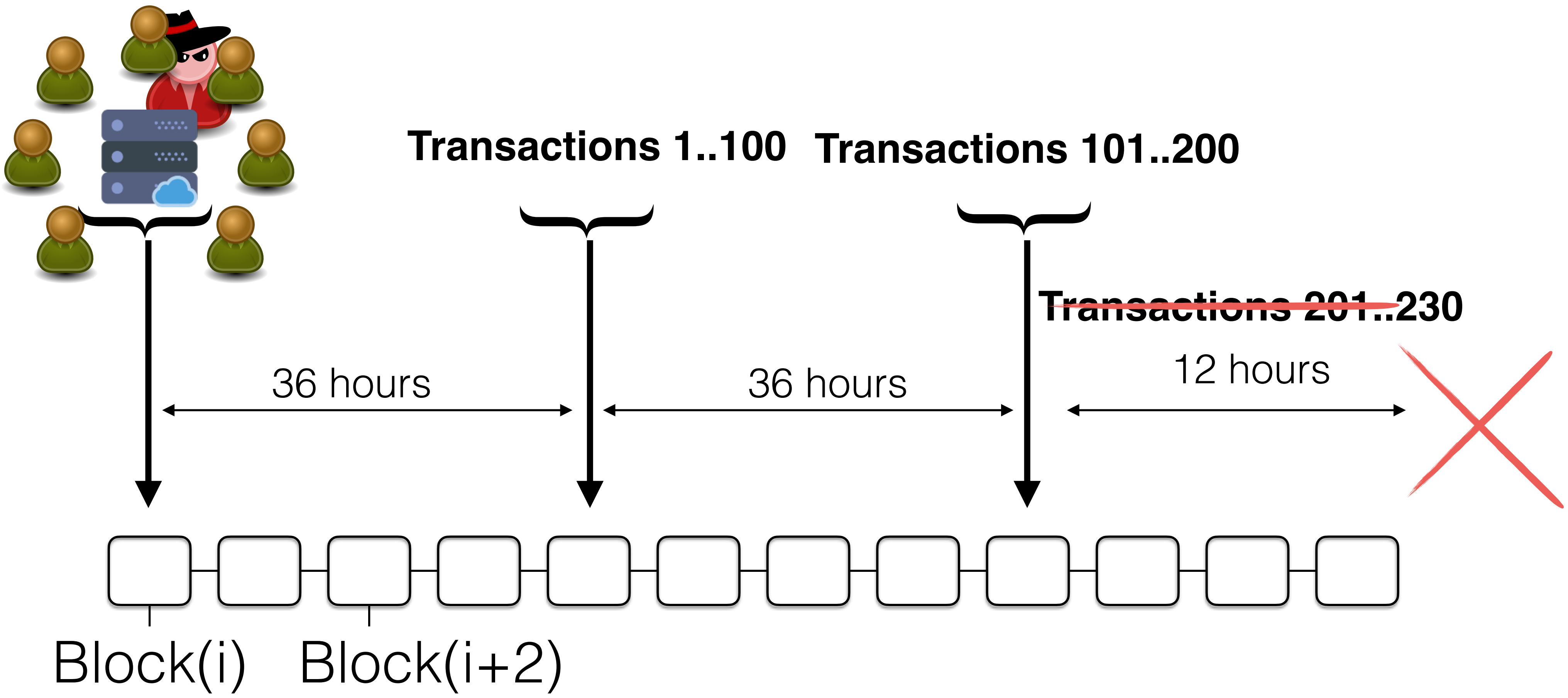
Transactions 1..100 Transactions 101..200

~~Transactions 201..230~~

NOCUST server disappears
… after a few transactions

😊 **Transaction 1..200 are safe**

😫 **Transaction 201..230 are not committed on chain!**

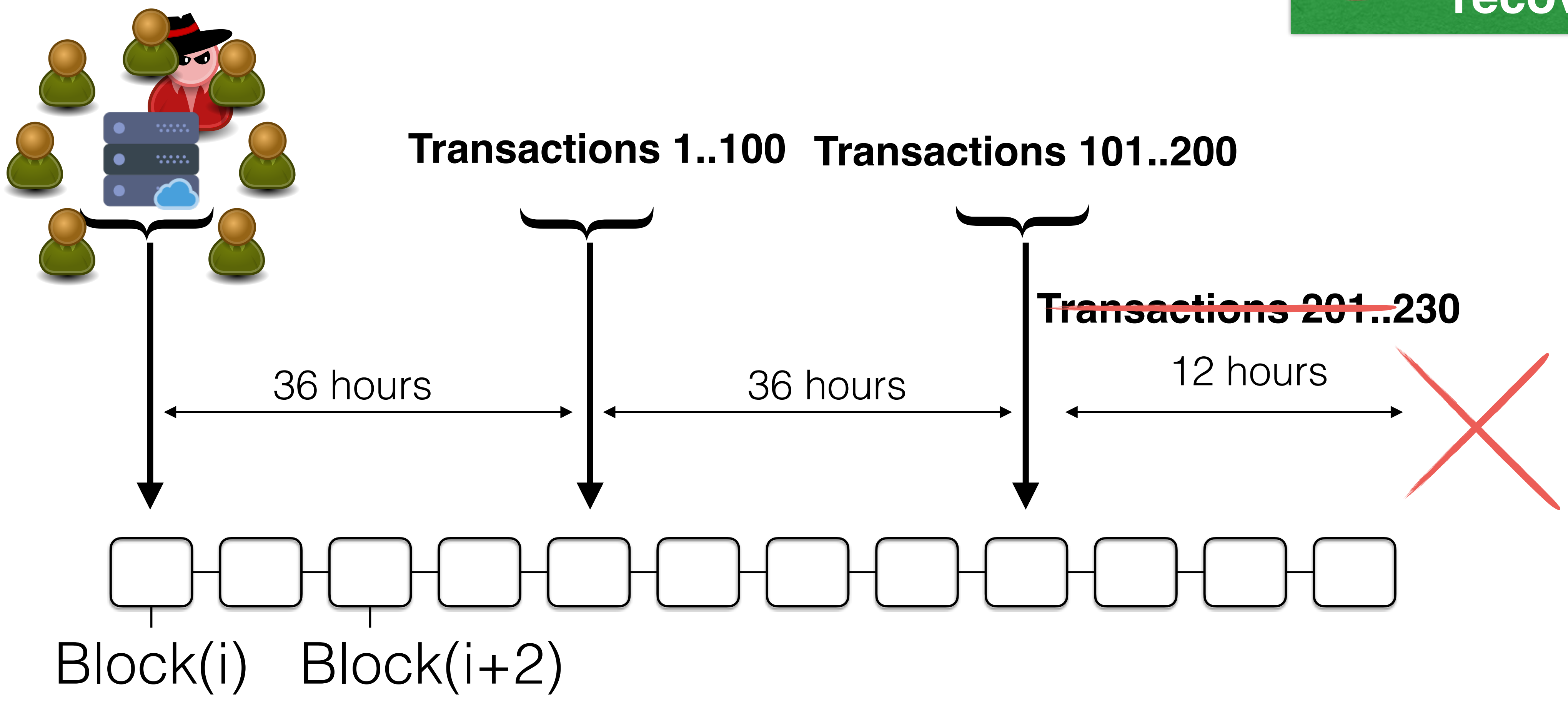


NOCUST server disappears … after a few transactions

😊 Transaction 1..200 are safe

😫 Transaction 201..230 are not committed on chain!

💰 Insurance Pool recovers tx 😊



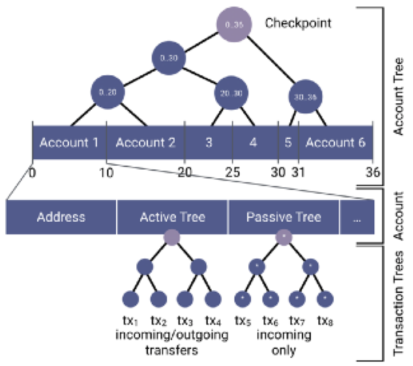
Users to attempt double-spending

Bob = 50 ETH

50 Ether

Alice

Bob’



Users to attempt double-spending

50 ETH

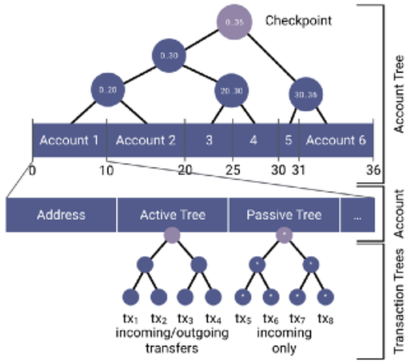
Alice

Bob = 50 ETH

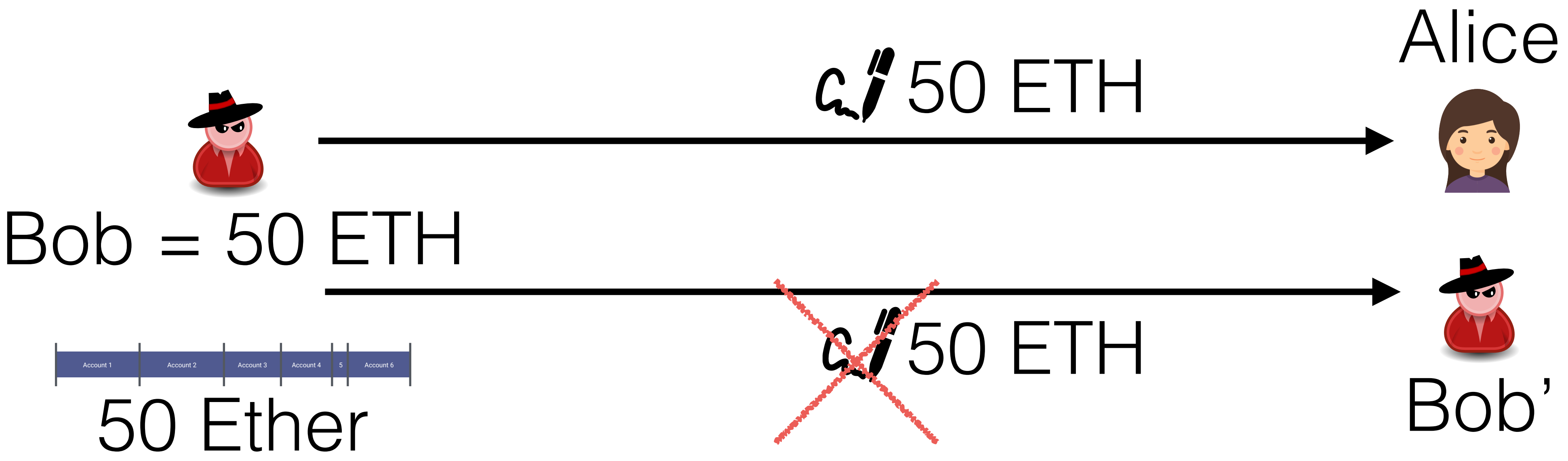
Account 1
Account 2
Account 3
Account 4
5
Account 6

50 Ether

Bob’



Users to attempt double-spending



Alice

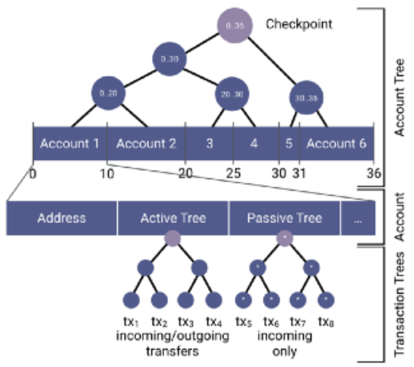
50 ETH

Bob = 50 ETH

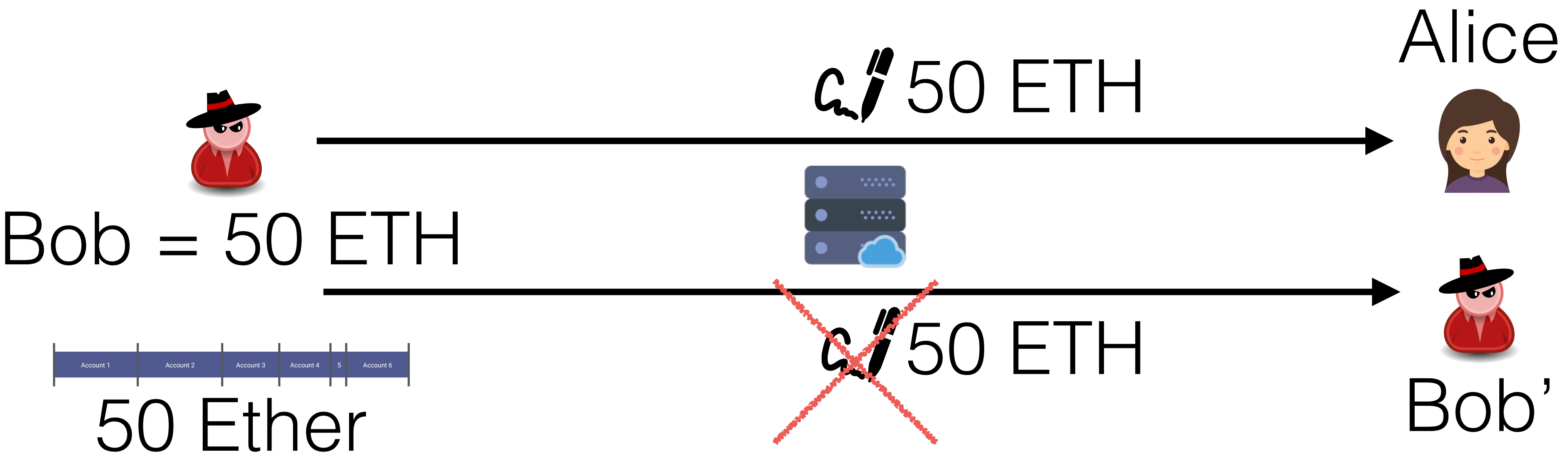
50 ETH

Bob’

50 Ether



Users to attempt double-spending



50 ETH

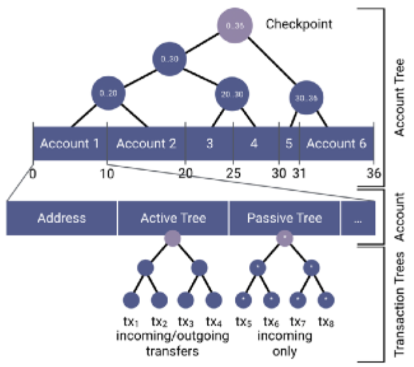
Alice

Bob = 50 ETH

50 ETH

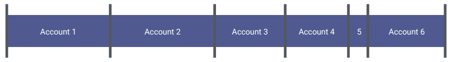
Bob’

50 Ether

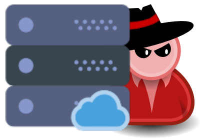


NOCUST server colludes with client to attempt double-spending

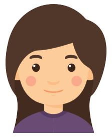
Bob = 50 ETH



50 Ether

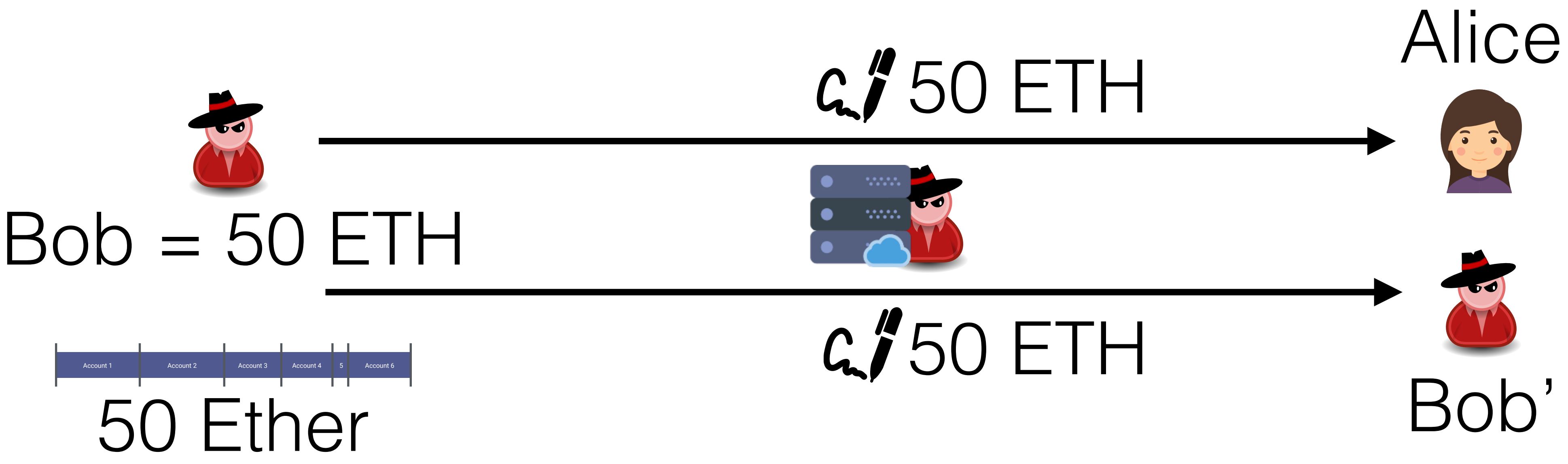


Alice



Bob’

NOCUST server colludes with client to attempt double-spending



Alice

50 ETH

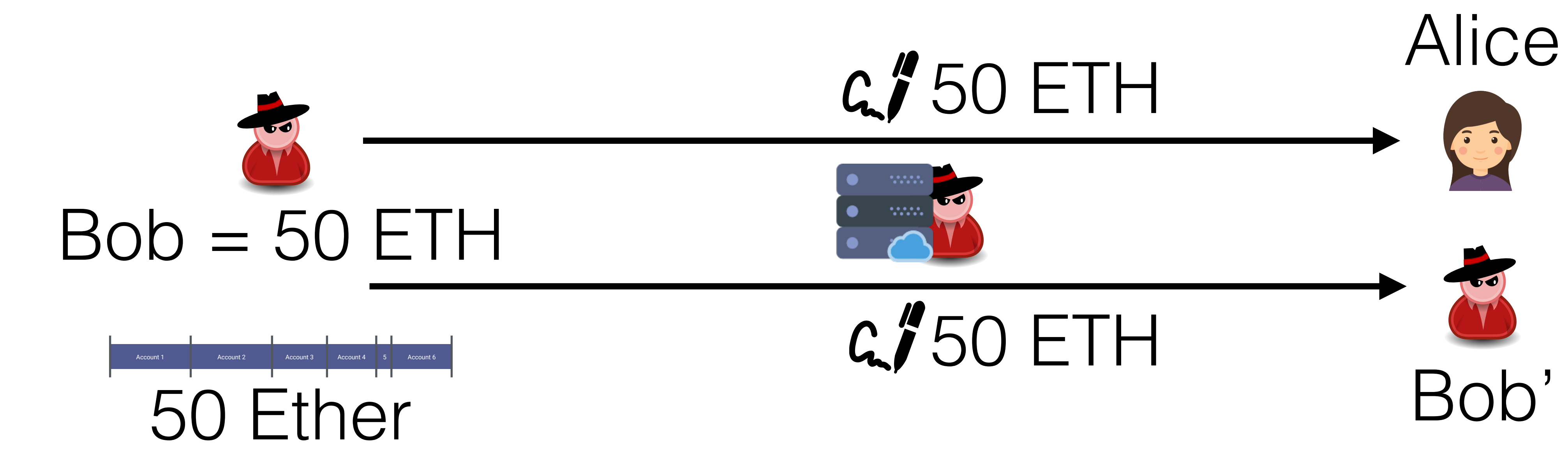
Bob = 50 ETH

50 ETH

Bob’

50 Ether

NOCUST server colludes with client to attempt double-spending



Alice

50 ETH

Bob = 50 ETH

50 ETH

Bob’

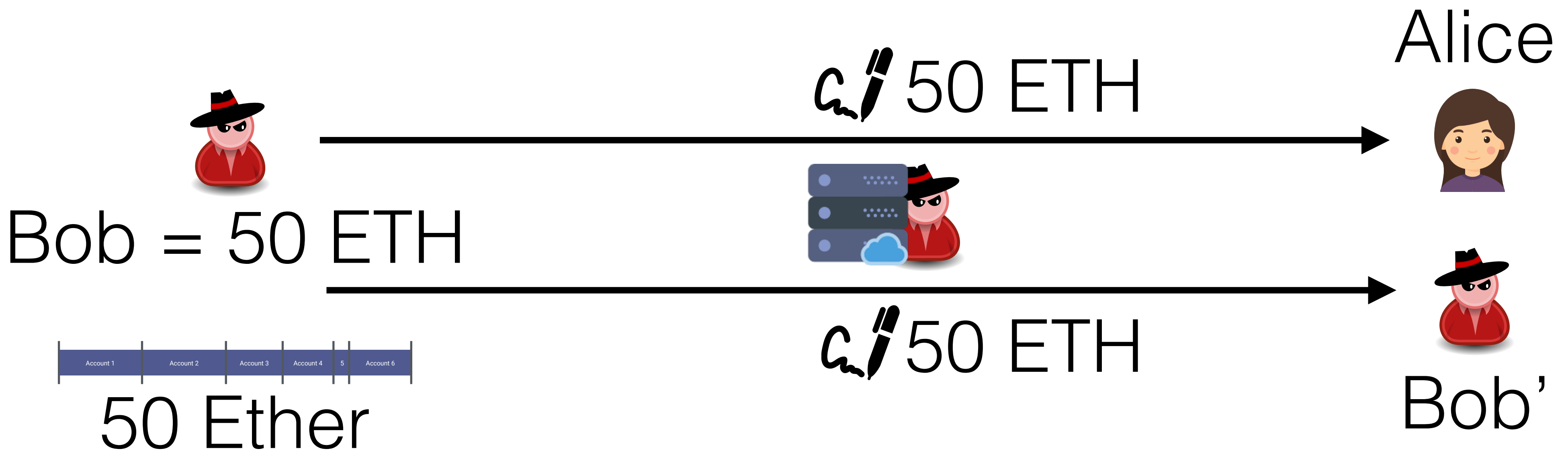
50 Ether

Attempt to create coins

50 Ether != 100 Ether

Operator is challenged !

NOCUST server colludes with client to attempt double-spending



Alice

50 ETH

Bob = 50 ETH

50 ETH

Bob’

50 Ether

Attempt to create coins

50 Ether != 100 Ether

Operator is challenged !

Attempt to steal coins

50 Ether of Alice are lost

Operator is challenged !