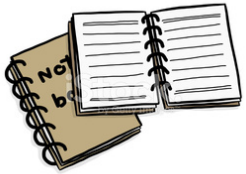
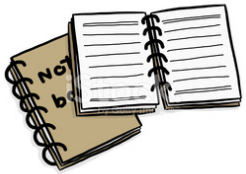
Blockchain as a Platform

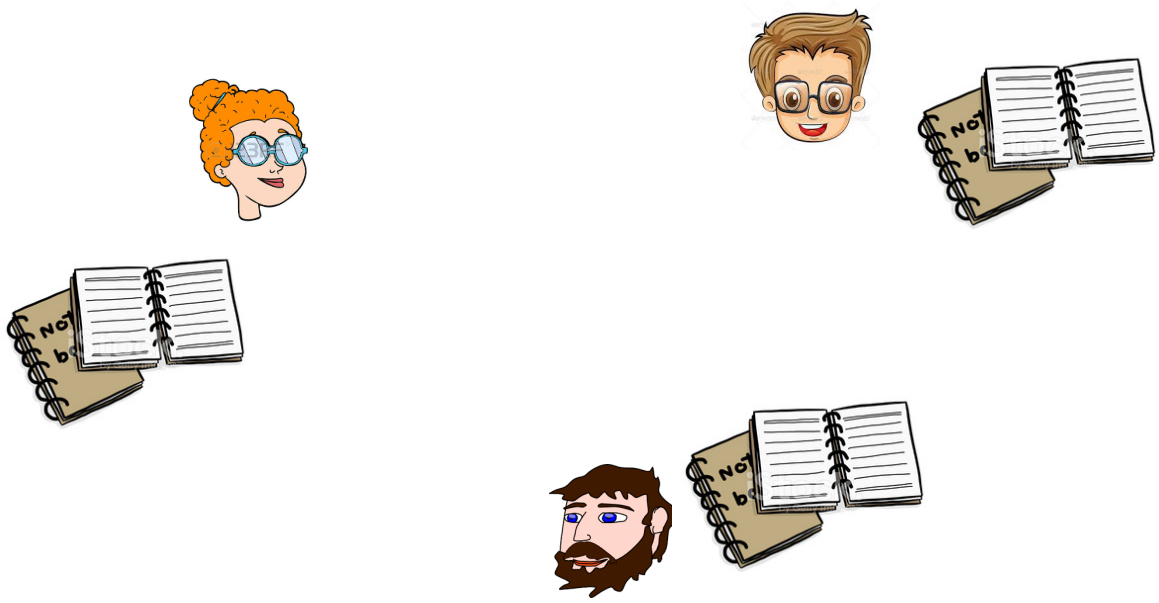
Murat Osmanoglu

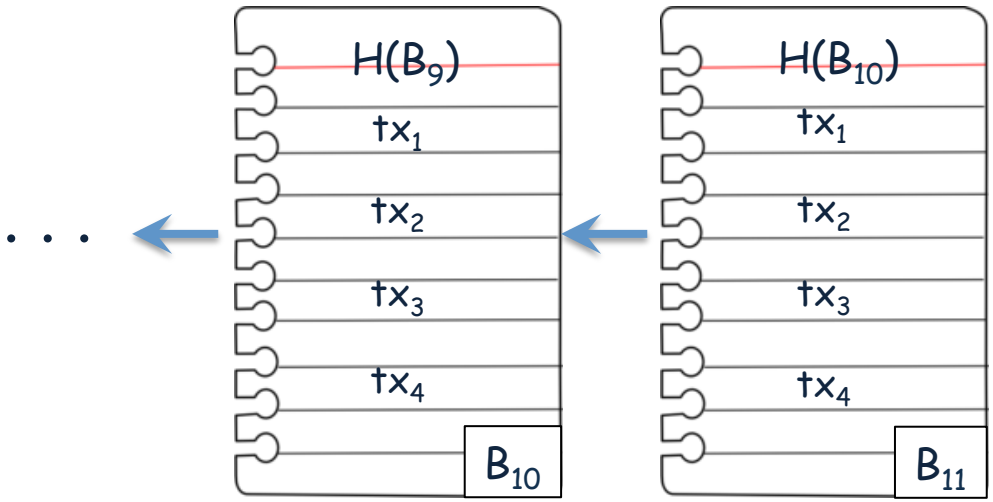
Blockchain



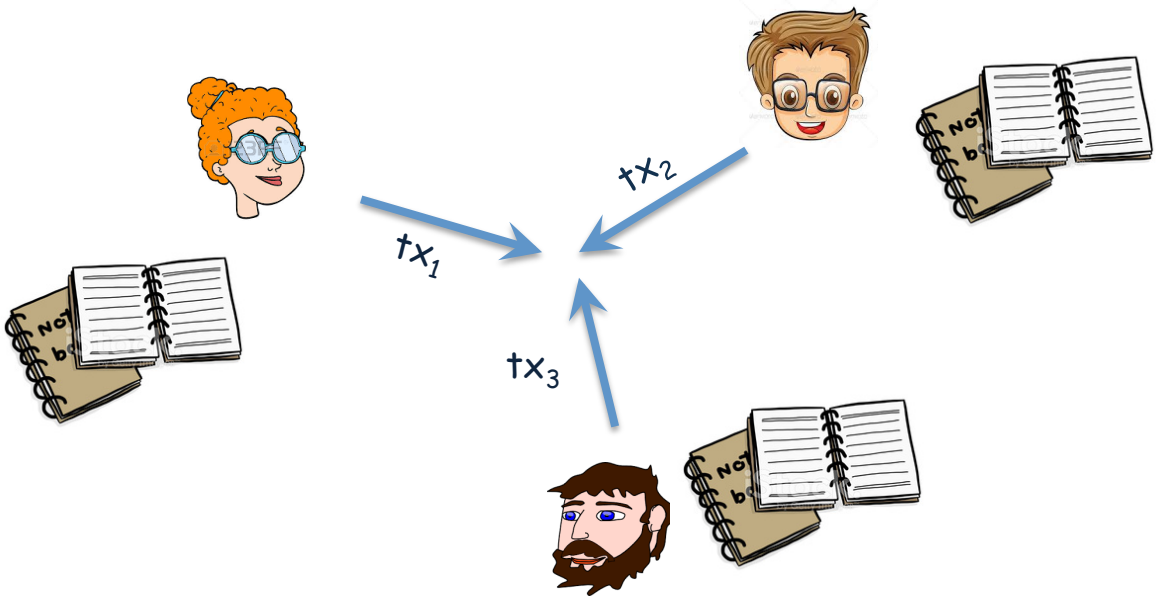


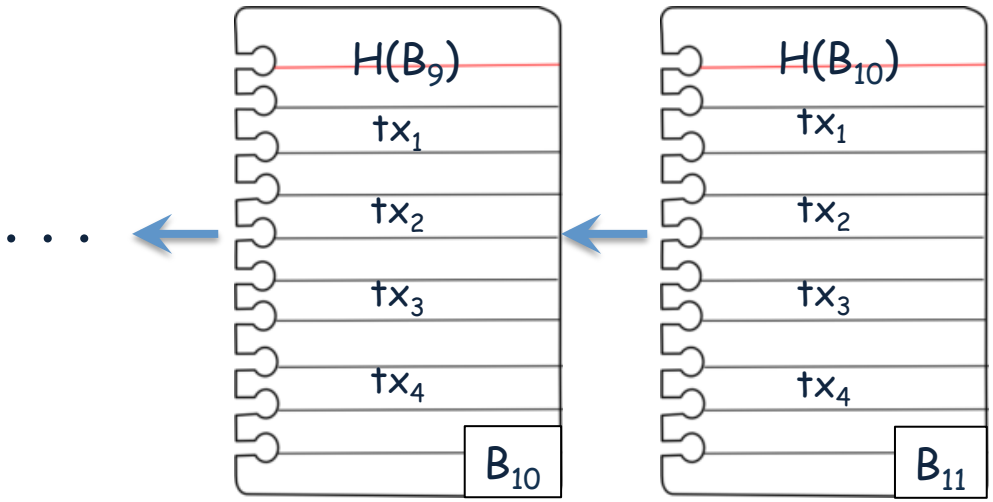
Blockchain



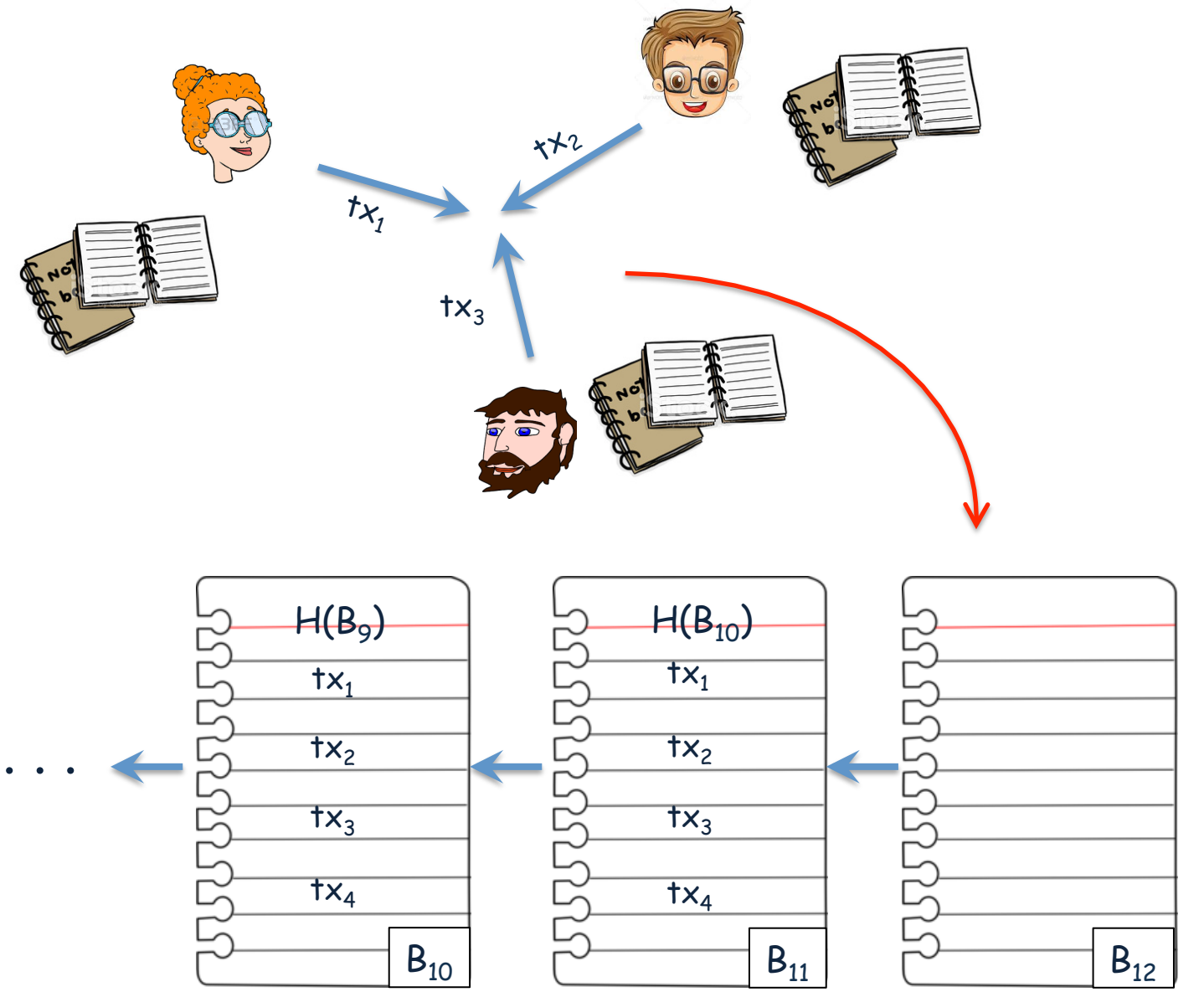


Blockchain

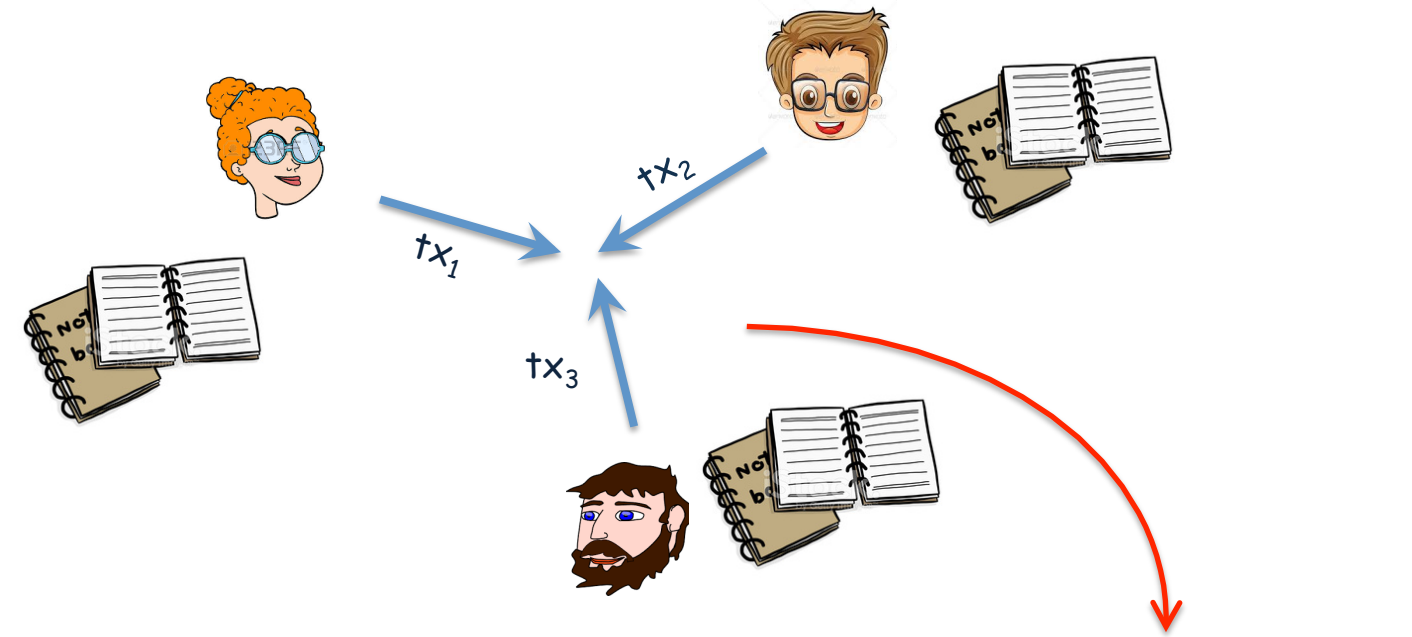


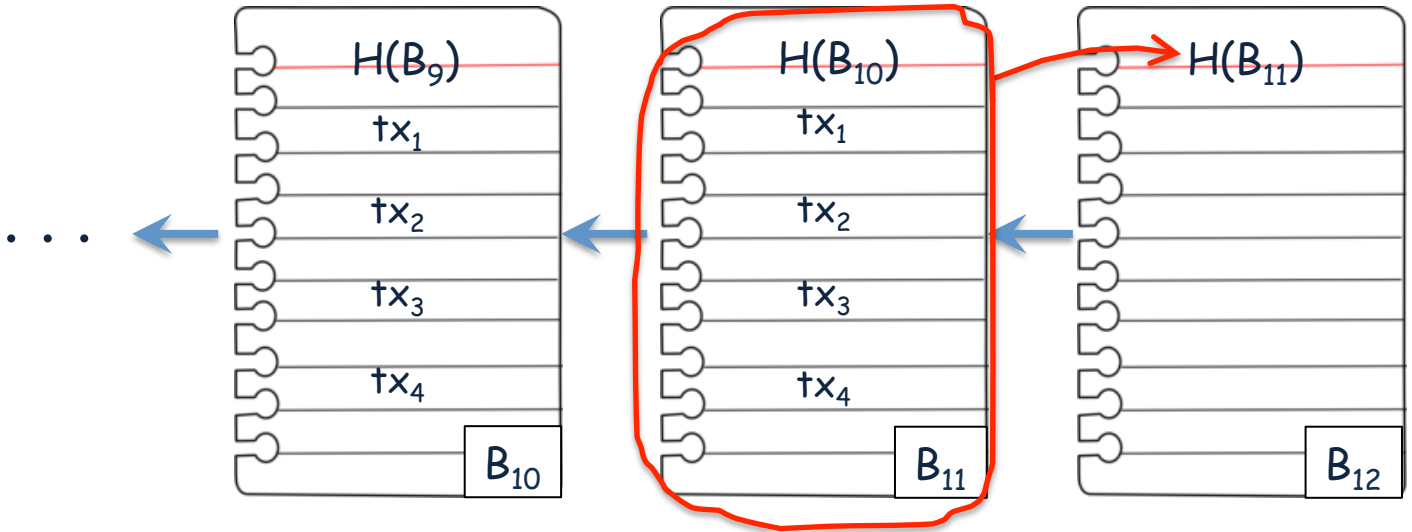


Blockchain

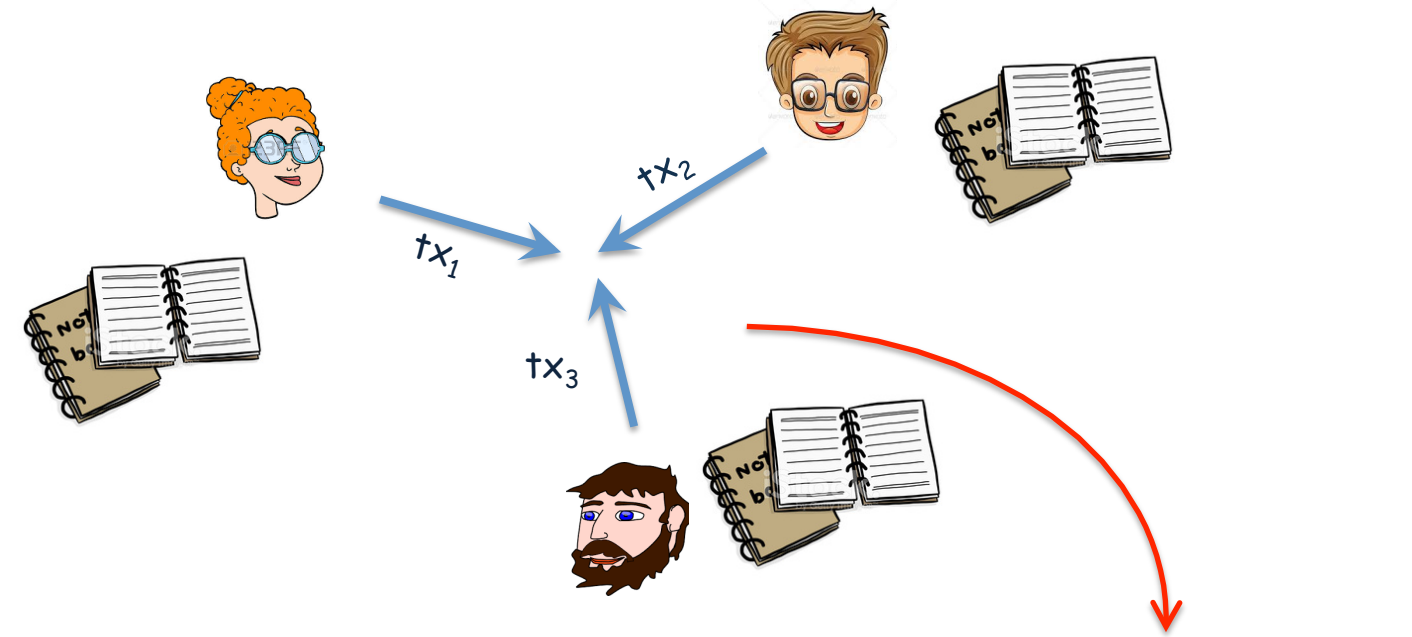


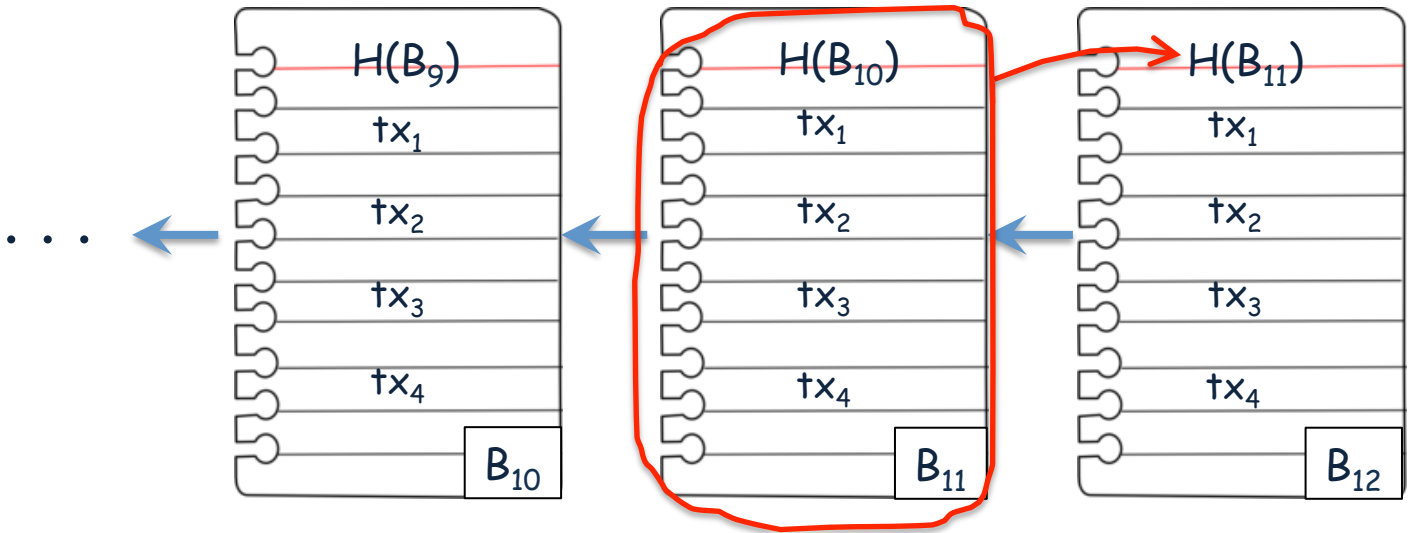
Blockchain


tx1
tx2
tx3

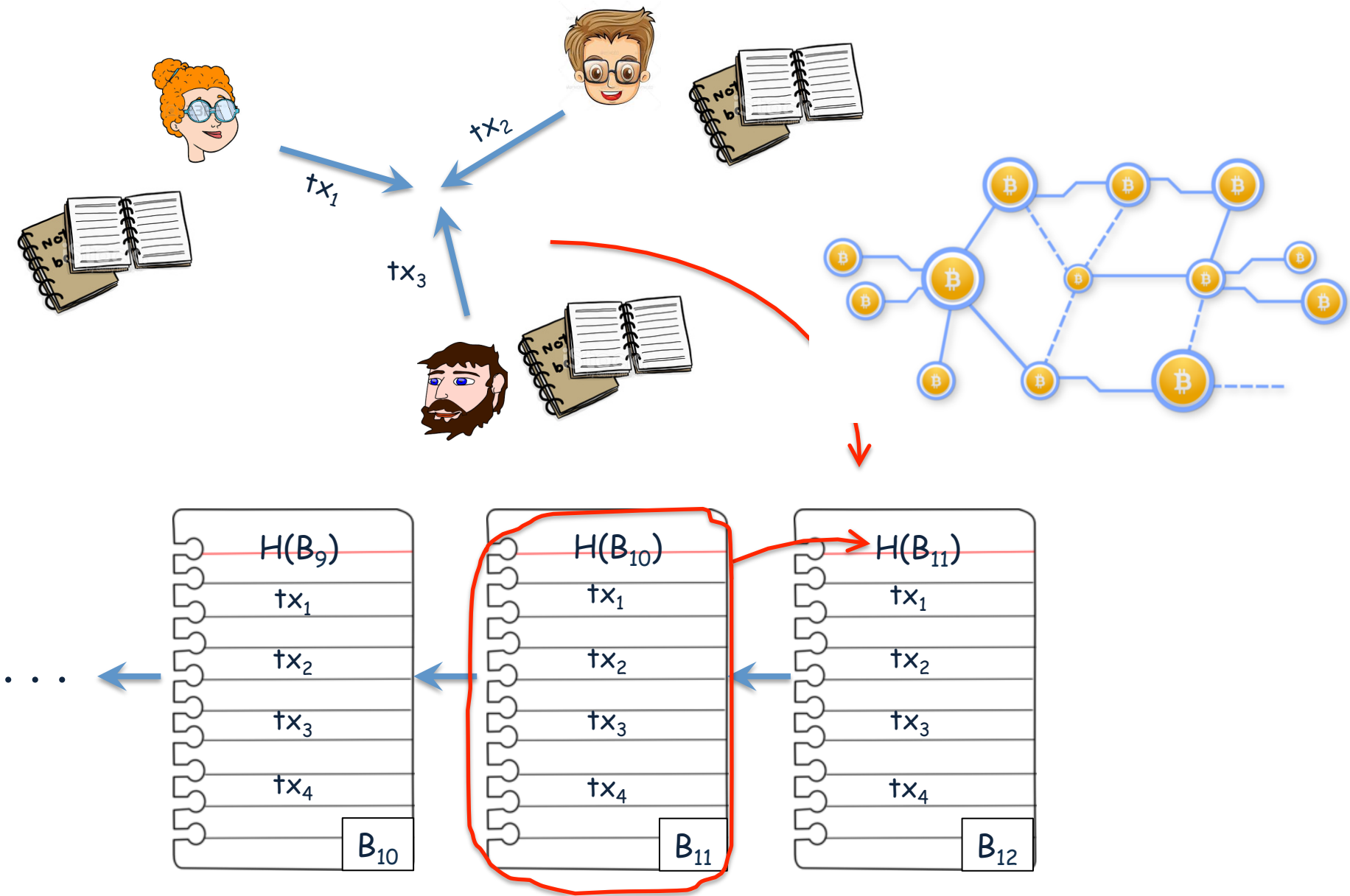

H(B9)
tx1
tx2
tx3
tx4
B10
H(B10)
tx1
tx2
tx3
tx4
B11
H(B11)
B12

Blockchain

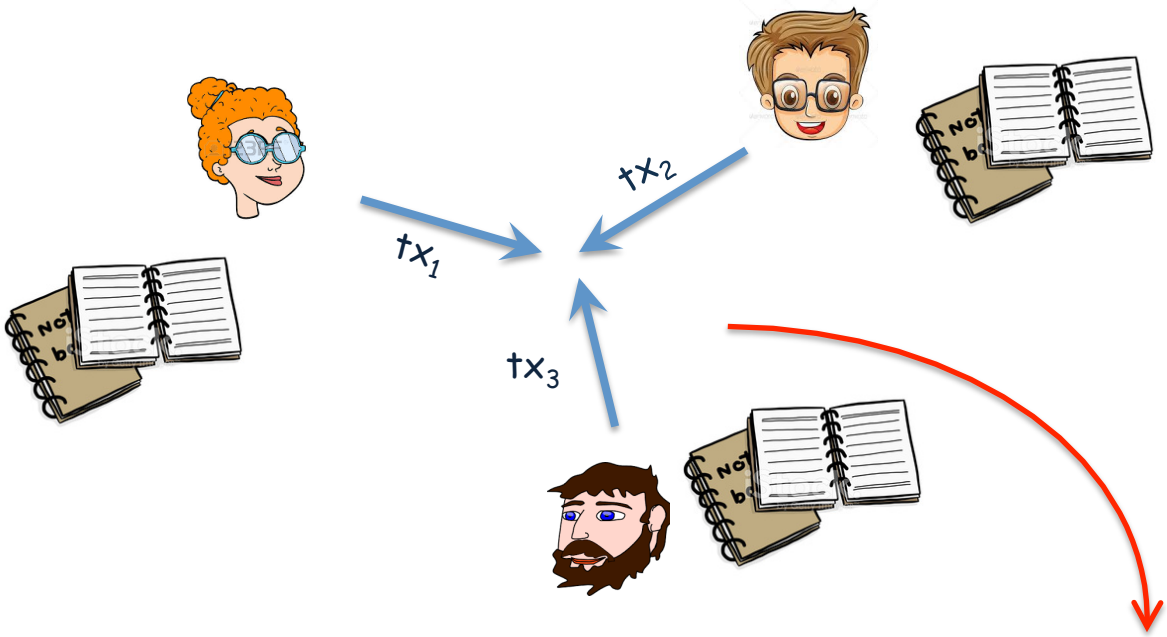

tx_1
tx_2
tx_3


. . .
$H(B_9)$
tx_1
tx_2
tx_3
tx_4
B_{10}
$H(B_{10})$
tx_1
tx_2
tx_3
tx_4
B_{11}
$H(B_{11})$
tx_1
tx_2
tx_3
tx_4
B_{12}

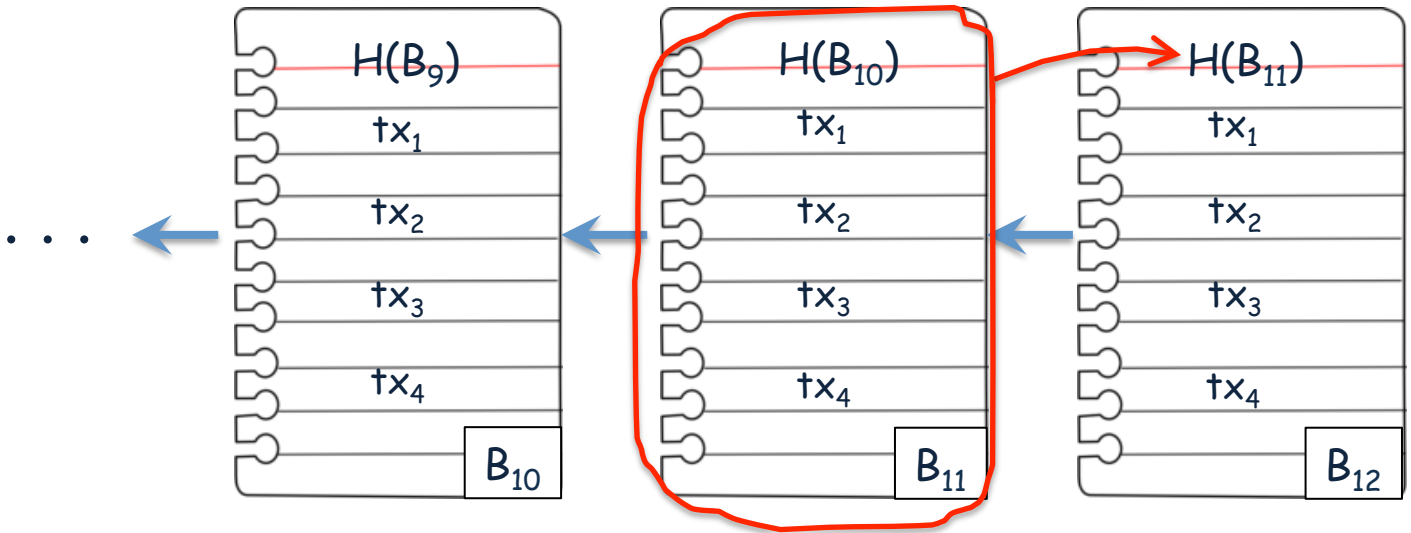
Blockchain


tx_1
tx_2
tx_3
$H(B_9)$
tx_1
tx_2
tx_3
tx_4
B_{10}
$H(B_{10})$
tx_1
tx_2
tx_3
tx_4
B_{11}
$H(B_{11})$
tx_1
tx_2
tx_3
tx_4
B_{12}
. . .

Blockchain



- Pseudonymous
- Democratic desicions through consensus protocols in a wild enviroment
- Immutable history of transactions
- Distibuted (not suffering signle point of failure)
- Uncensorable
- Transparent



Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one

Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :

Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)

Bitcoin Transaction

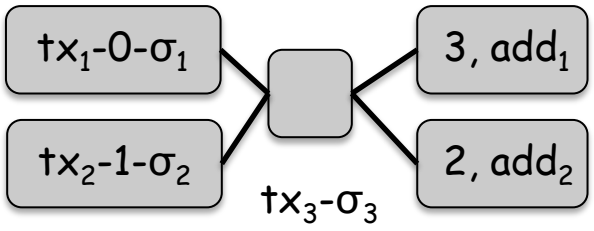
- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)

Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid

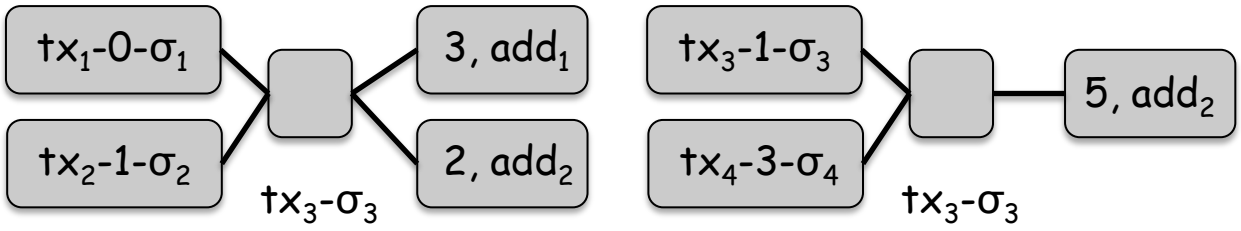
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



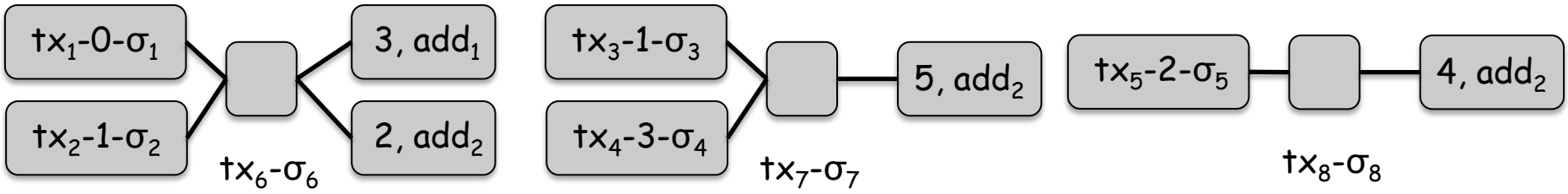
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



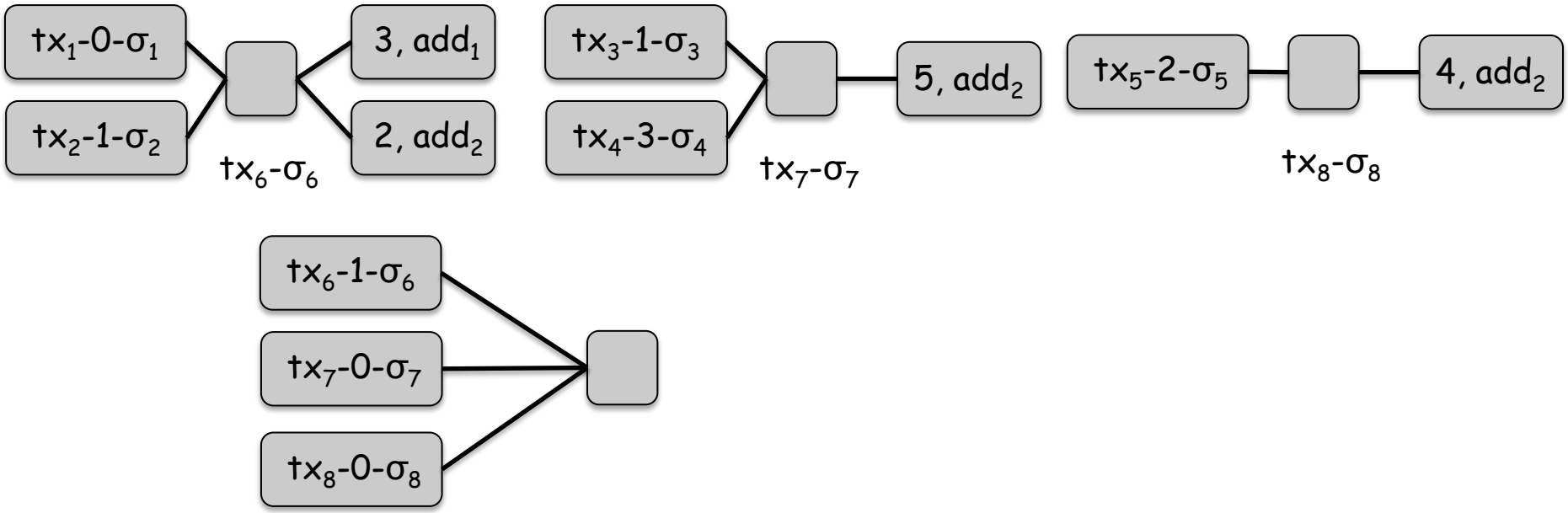
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



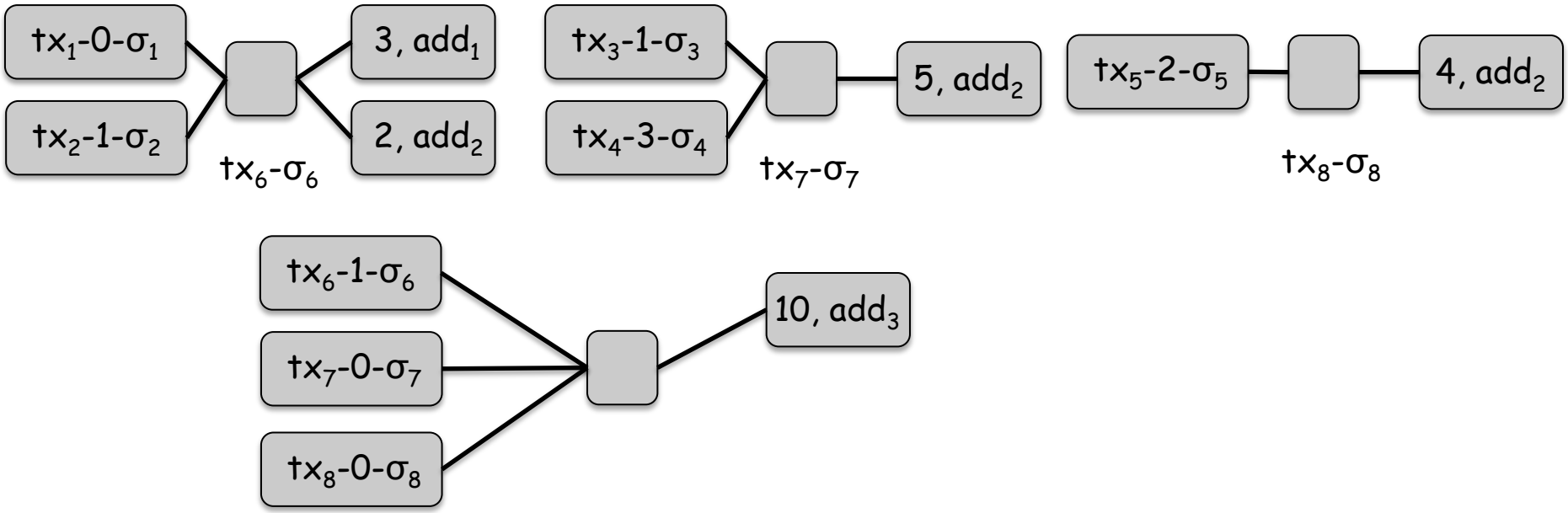
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



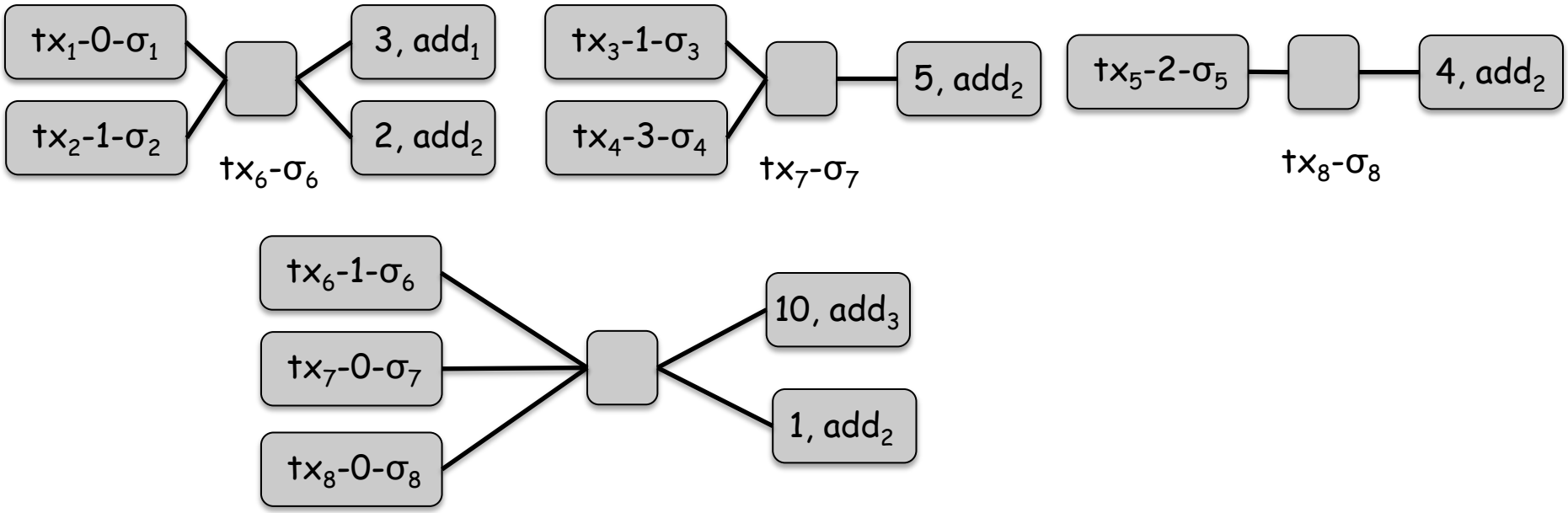
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



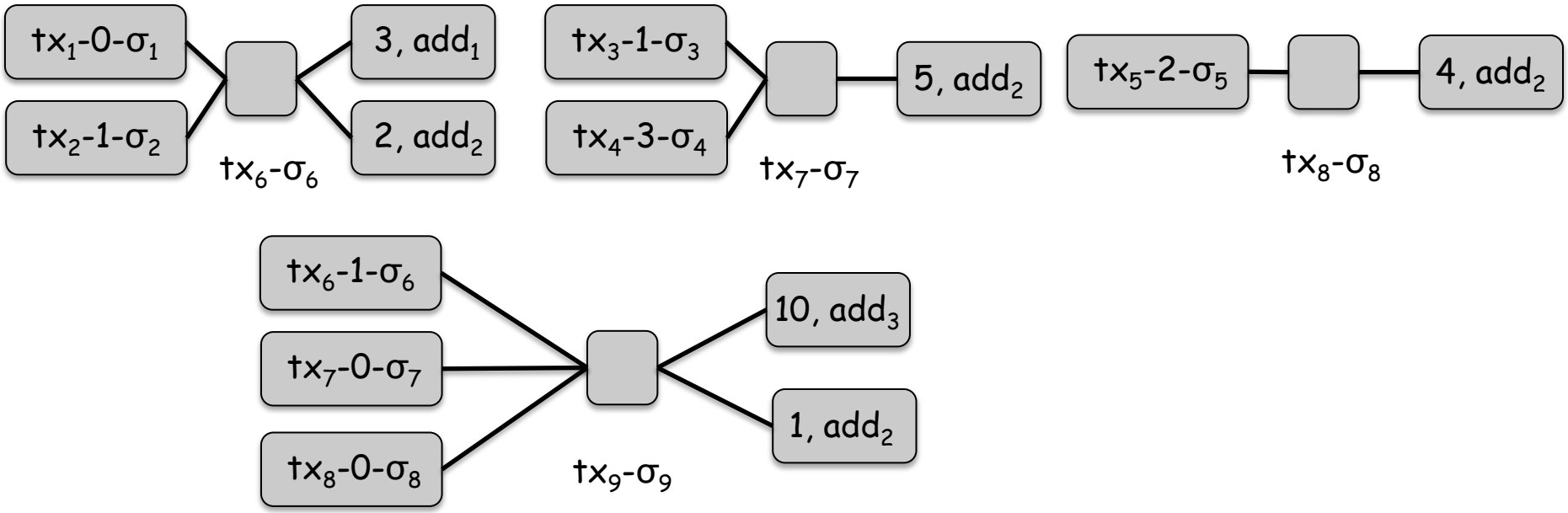
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



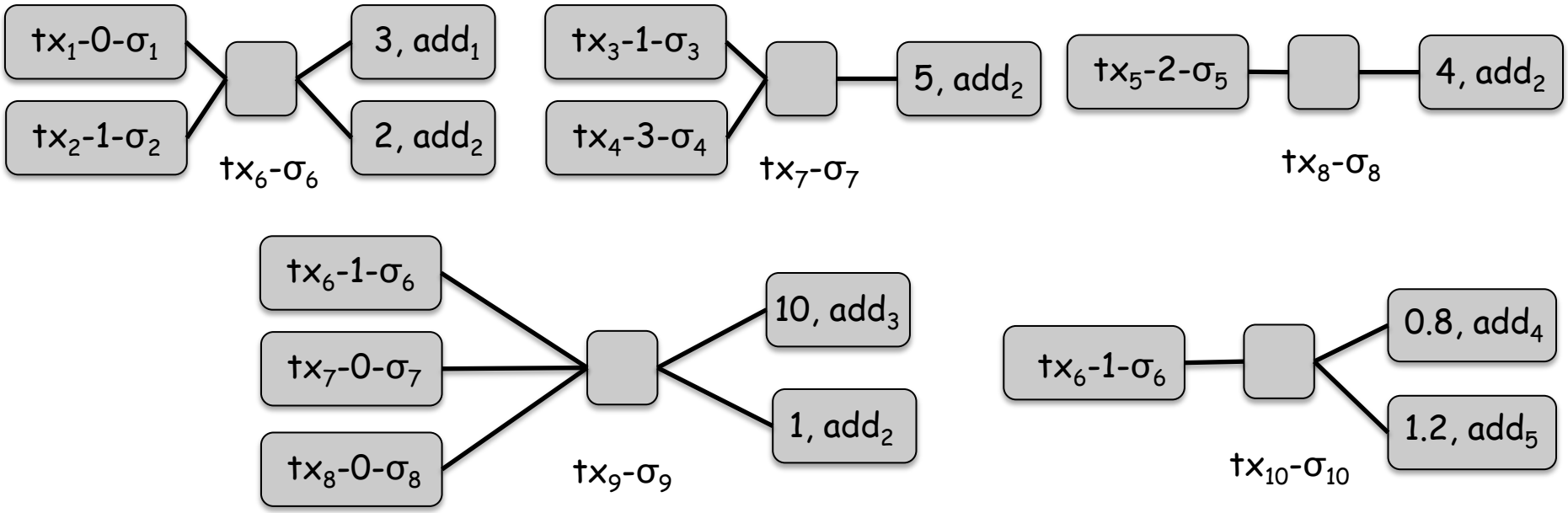
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



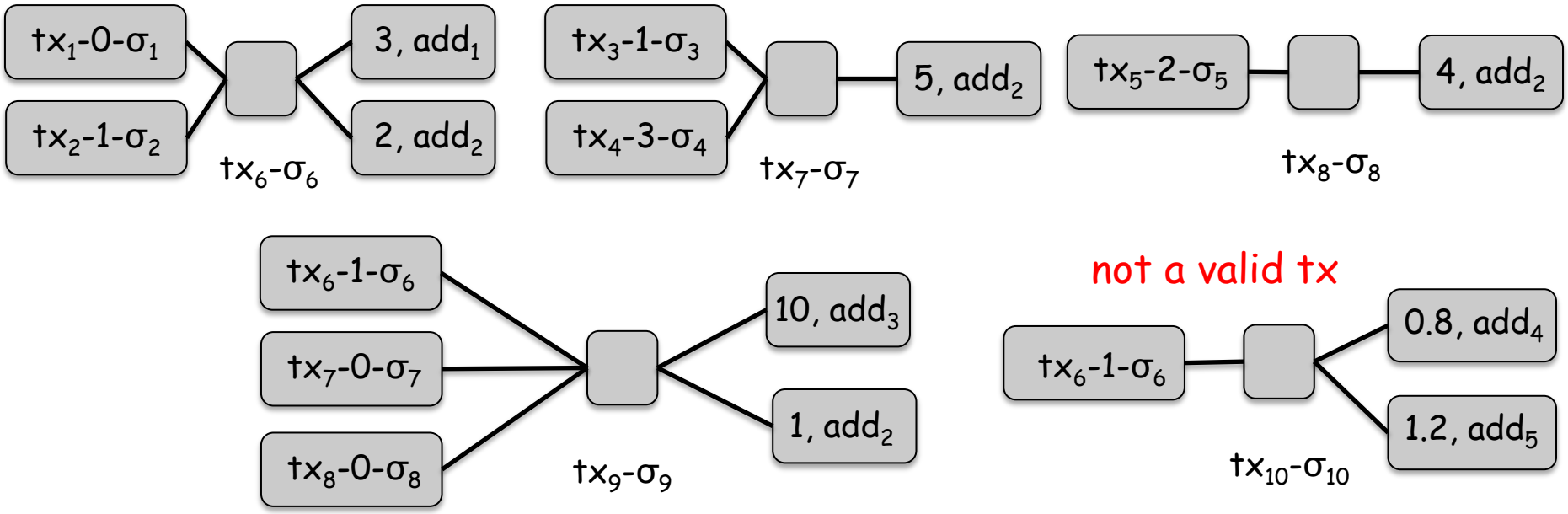
Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



Bitcoin Transaction

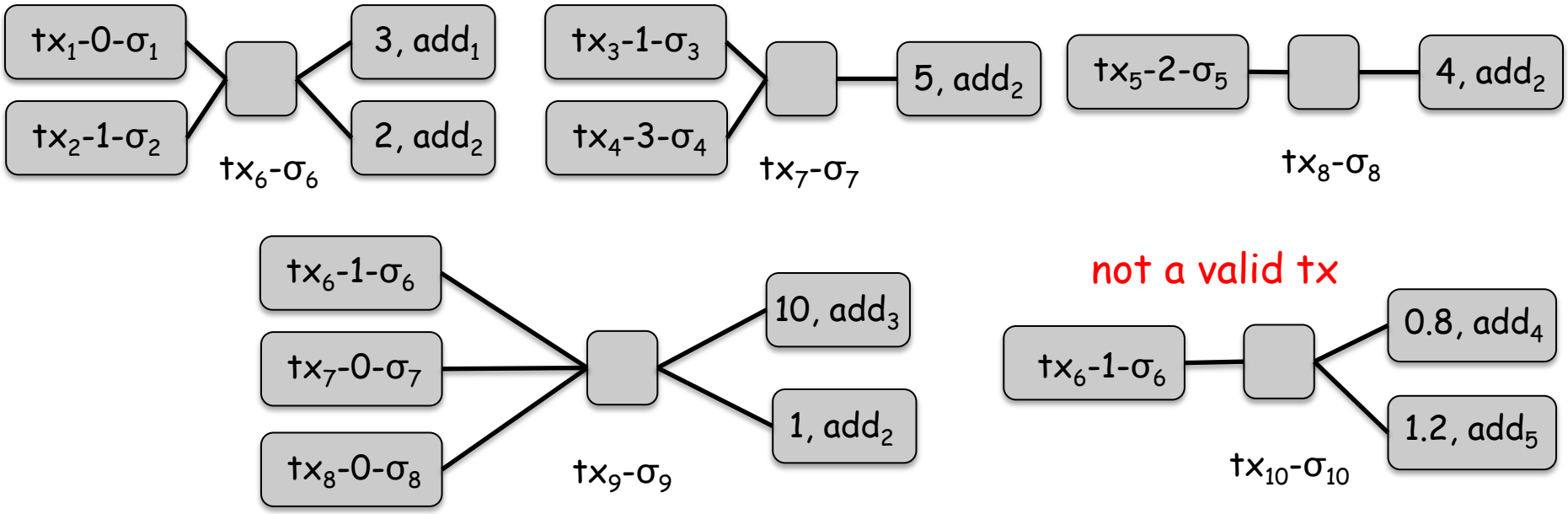
- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent [illegible] der from previous transactions (pr[illegible])
  - output : instruc[illegible]ue, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid

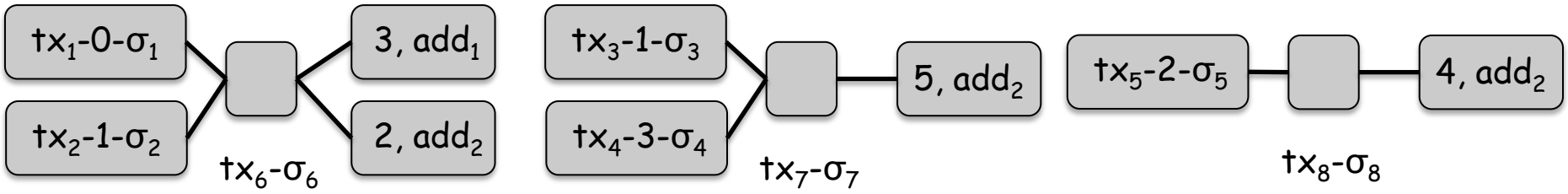
- UXTO – based transaction model (unspent transaction output)

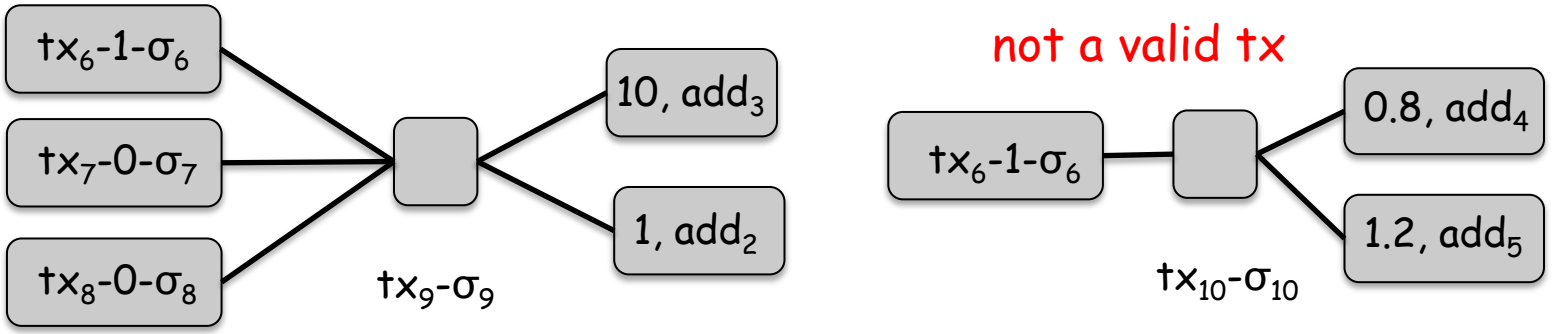


Bitcoin Transaction

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent ...der from previous transactions (pr...)
  - output : instruc...ue, scriptpublickey)
- if the transaction o...re is valid, the transaction considered as valid

- UXTO – based transaction model (unspent transaction output)
- Account-based transaction model





Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state

Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure

Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure
- anyone can create his own state transition function

Ethereum

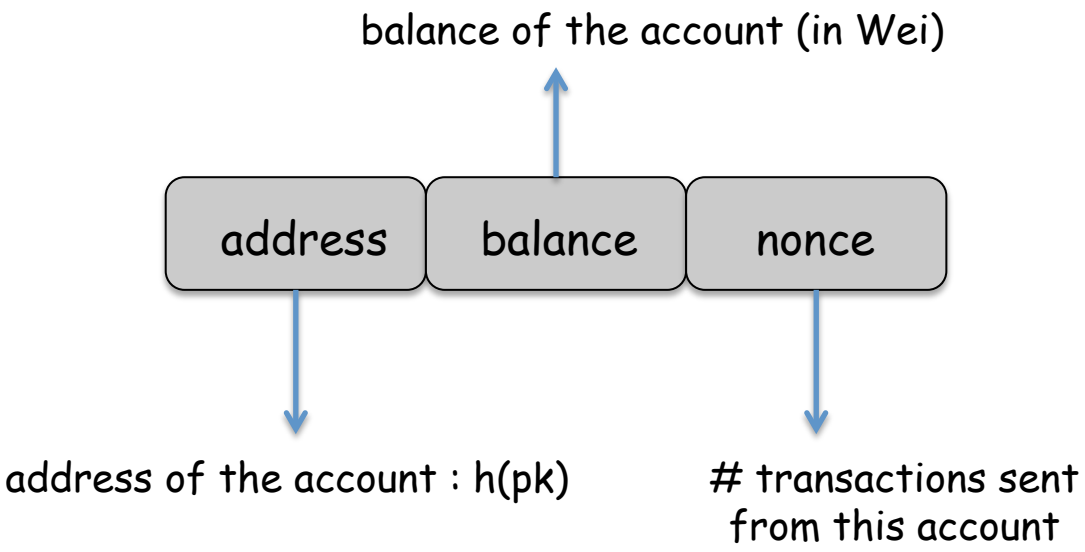
- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure
- anyone can create his own state transition function
- global state : accounts
  - they interact with each other through transactions

Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure
- anyone can create his own state transition function
- global state : accounts
  - they interact with each other through transactions

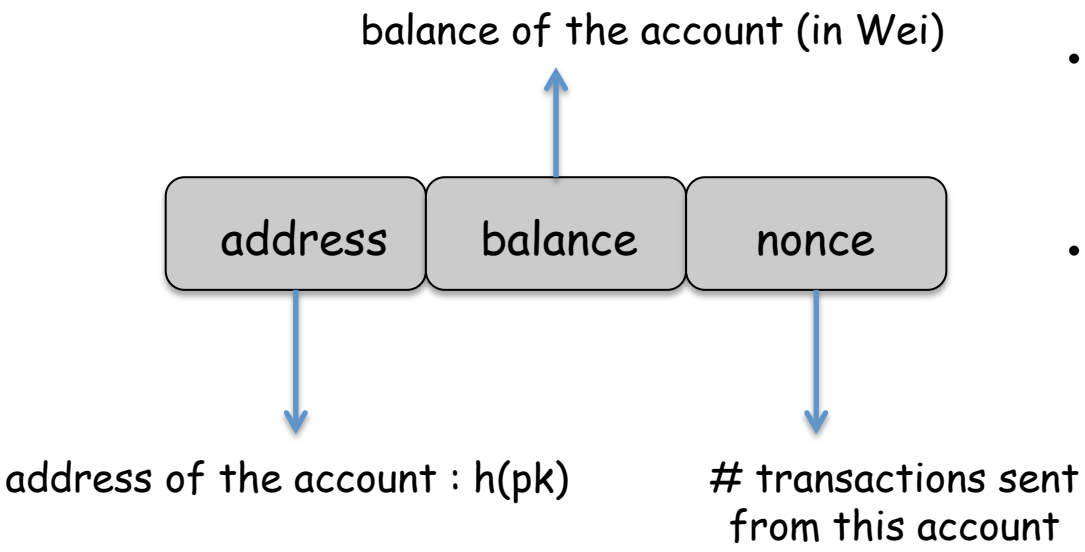
Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure
- anyone can create his own state transition function
- global state : accounts
  - they interact with each other through transactions



Ethereum

- transaction-based deterministic replicated state machine
  - a virtual machine that applies changes to global state
- a global decentralized computing infrastructure
- anyone can create his own state transition function
- global state : accounts
  - they interact with each other through transactions



- Wei : the smallest denomination used in Ethereum network
- 1 ether = 10^{18} Wei

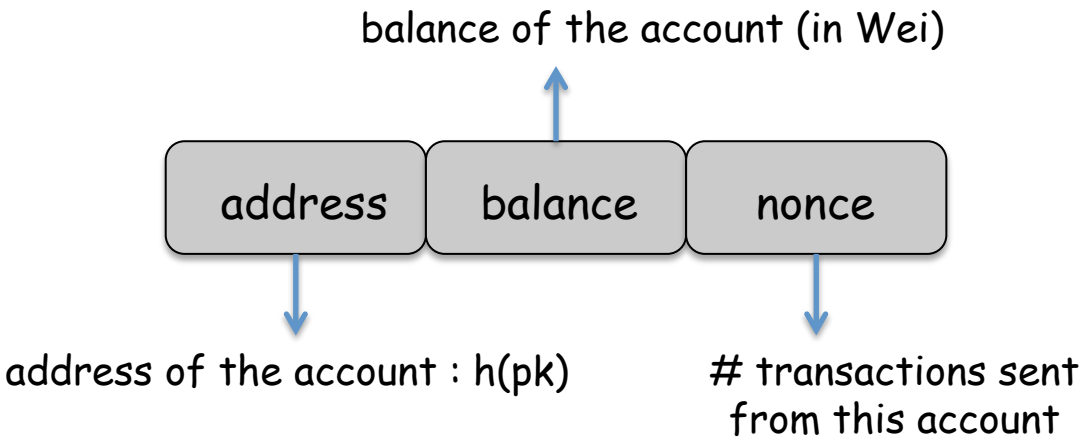
Ethereum

- personel accounts

- contract accounts

Ethereum

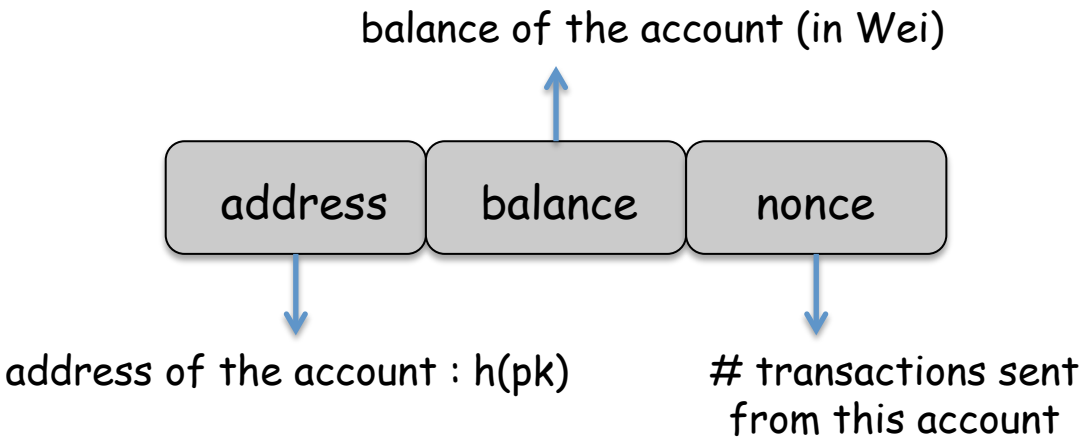
- personel accounts



- contract accounts

Ethereum

- personel accounts



- contract accounts

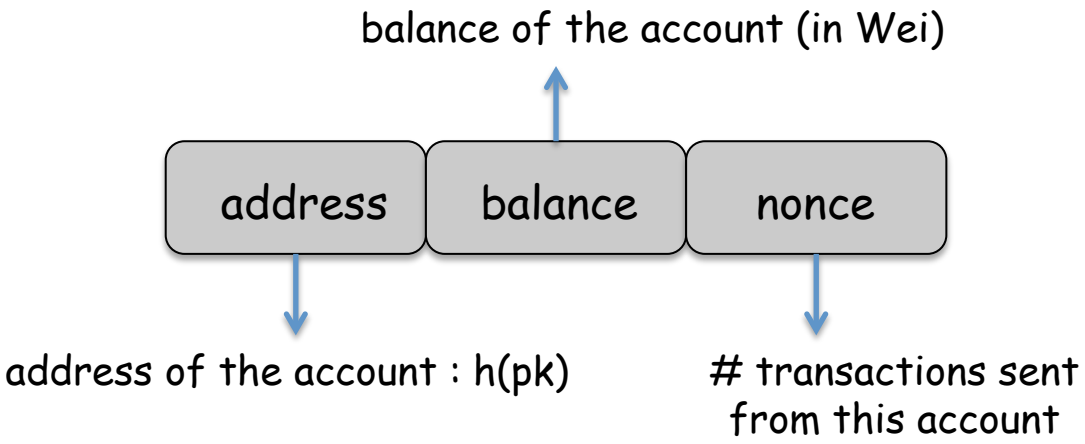
smart contract : a piece of codes that autonomously execute the terms of a contract

they are trigged by addressing a transaction to them

they are executed independently and authonomously in a prescribed manner on every node in the network

Ethereum

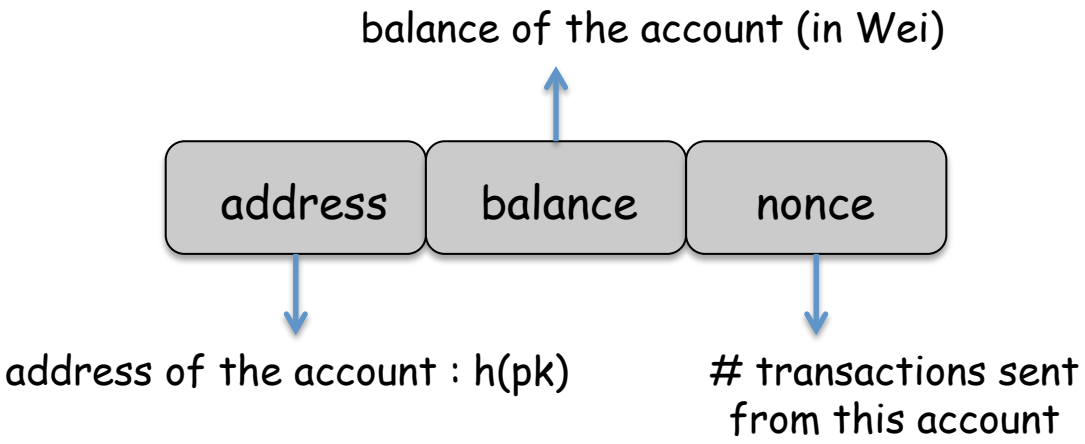
- personel accounts



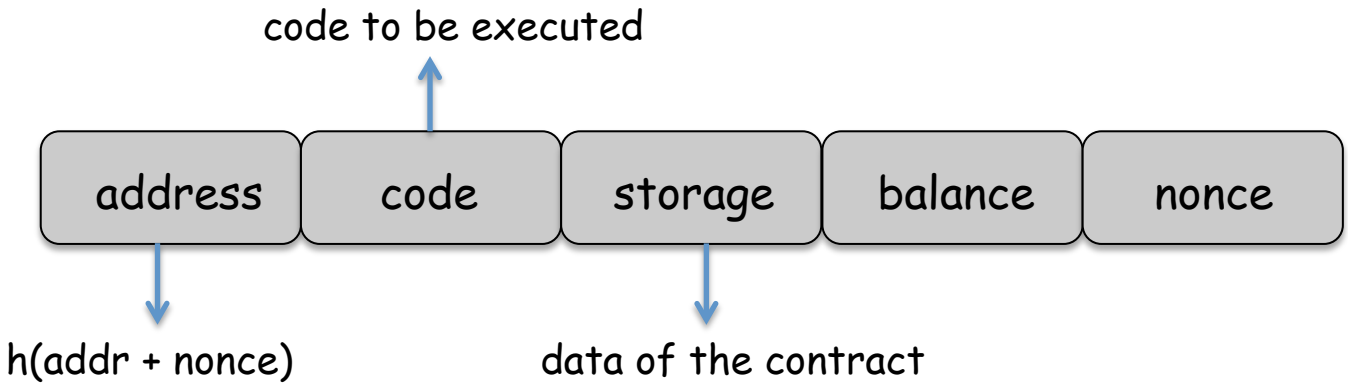
- contract accounts

Ethereum

- personel accounts

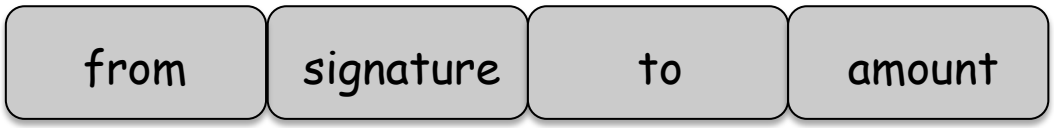


- contract accounts



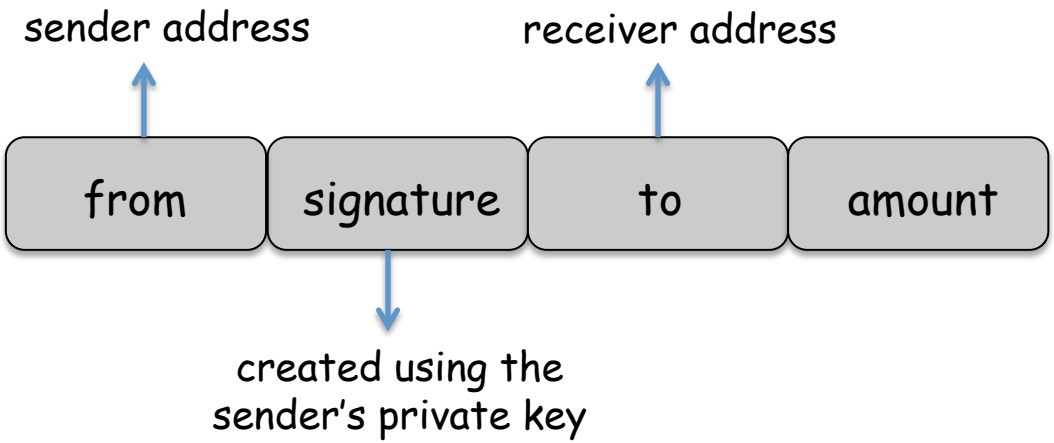
Ethereum

- transactions



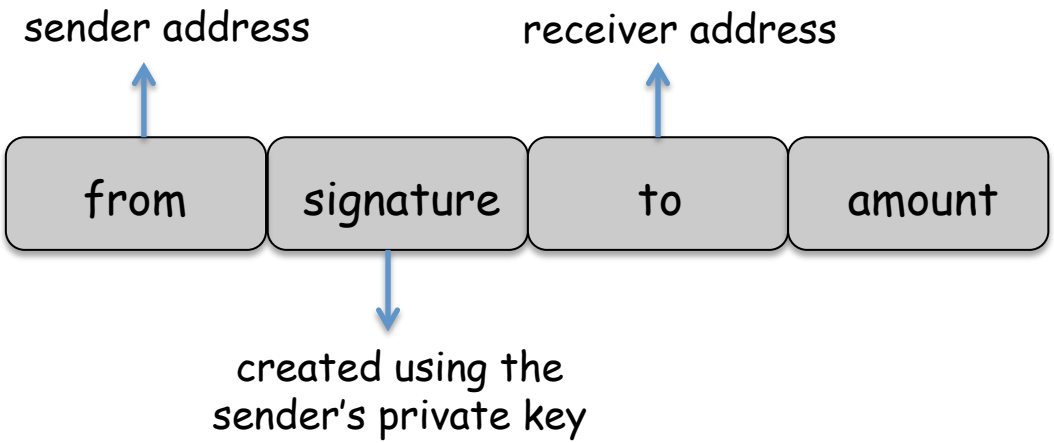
Ethereum

- transactions

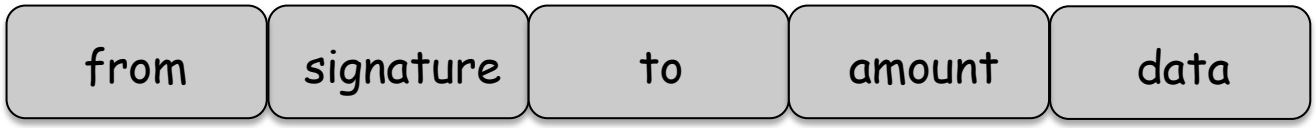


Ethereum

- transactions

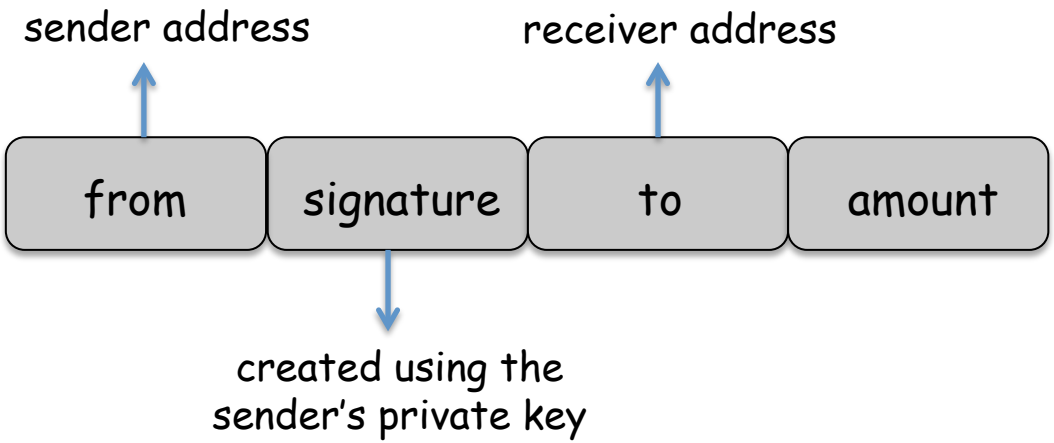


- contract creation

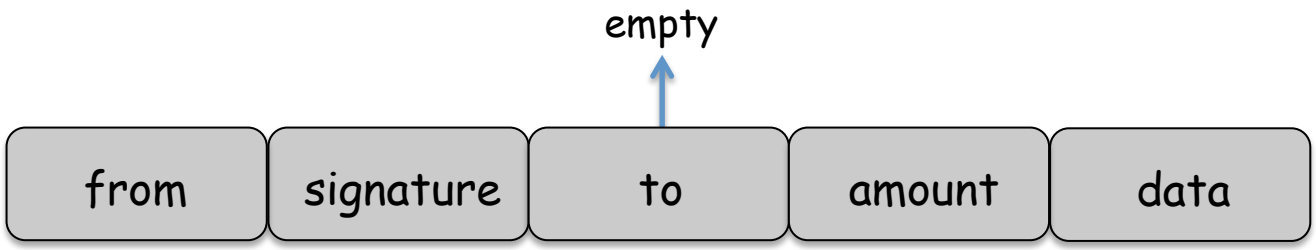


Ethereum

- transactions

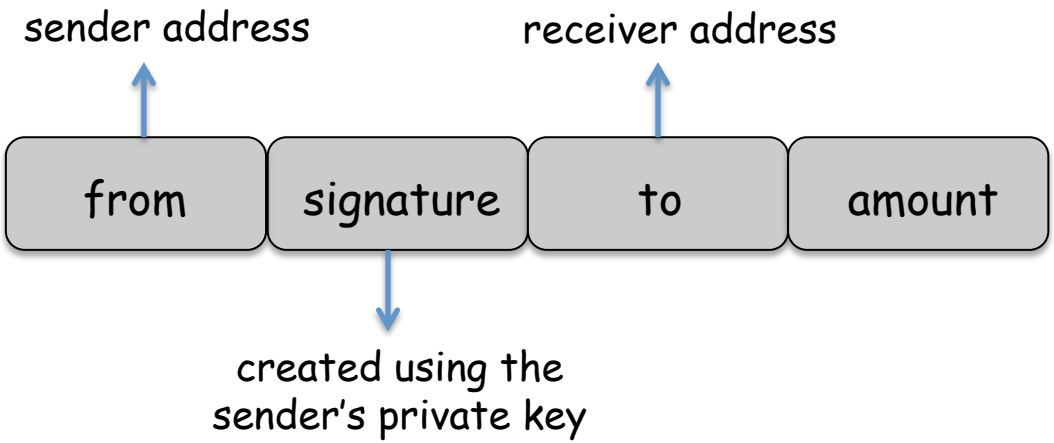


- contract creation

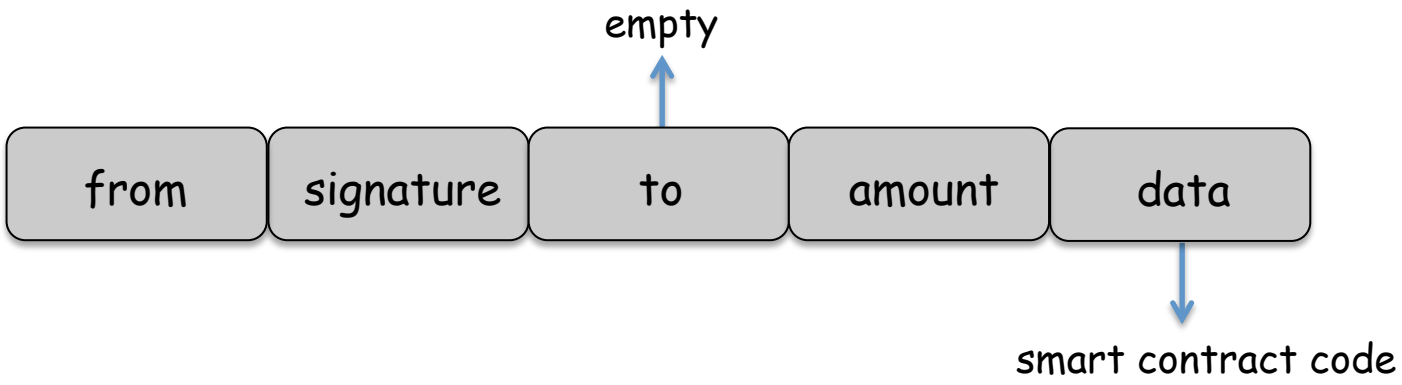


Ethereum

- transactions

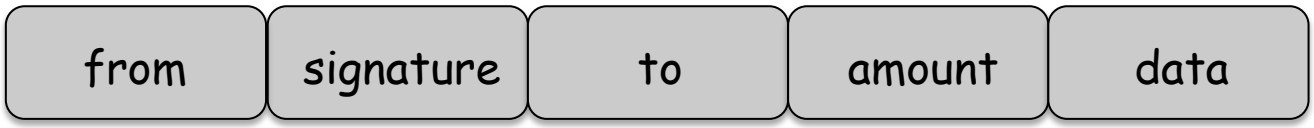


- contract creation



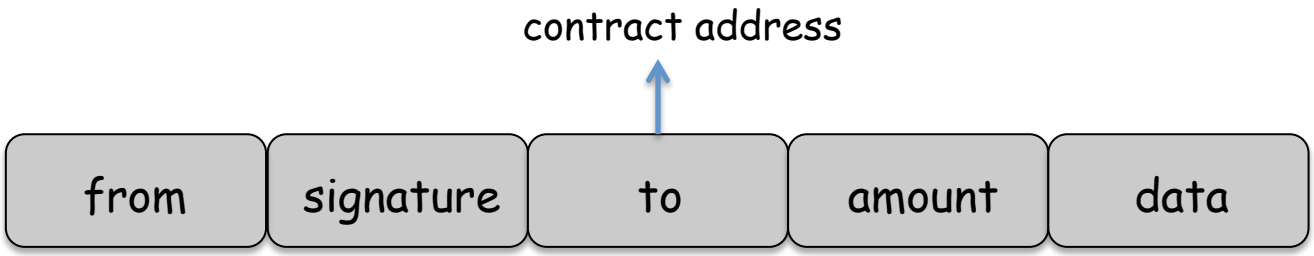
Ethereum

- contract interaction



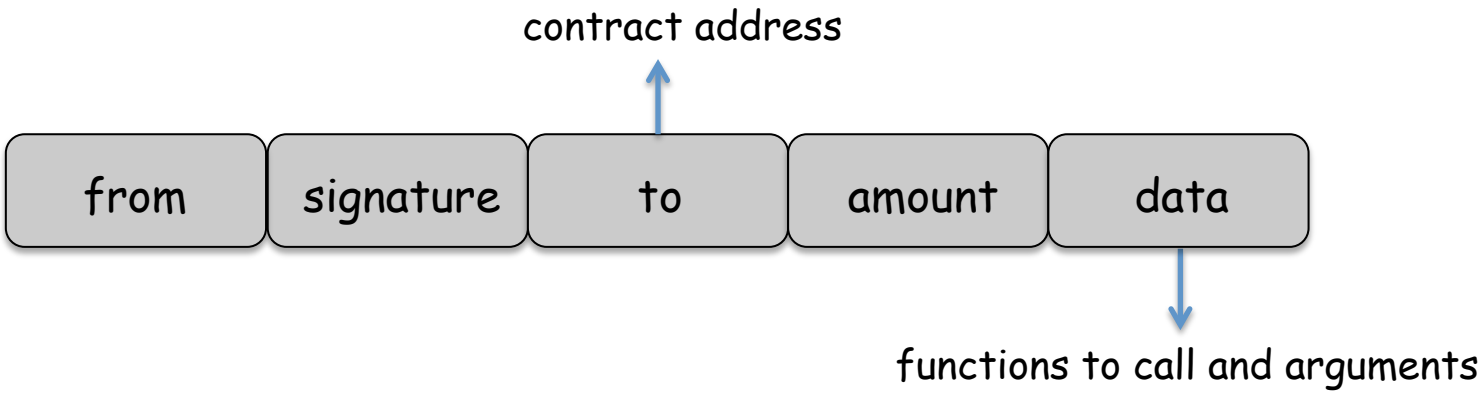
Ethereum

- contract interaction



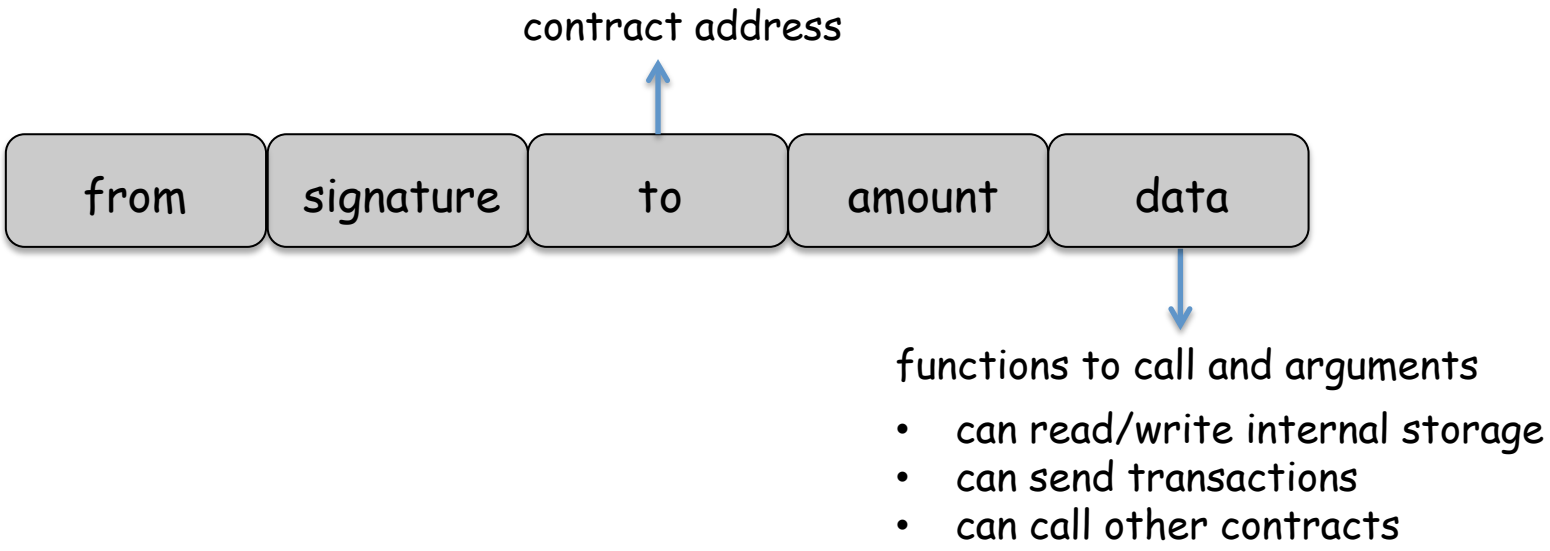
Ethereum

- contract interaction



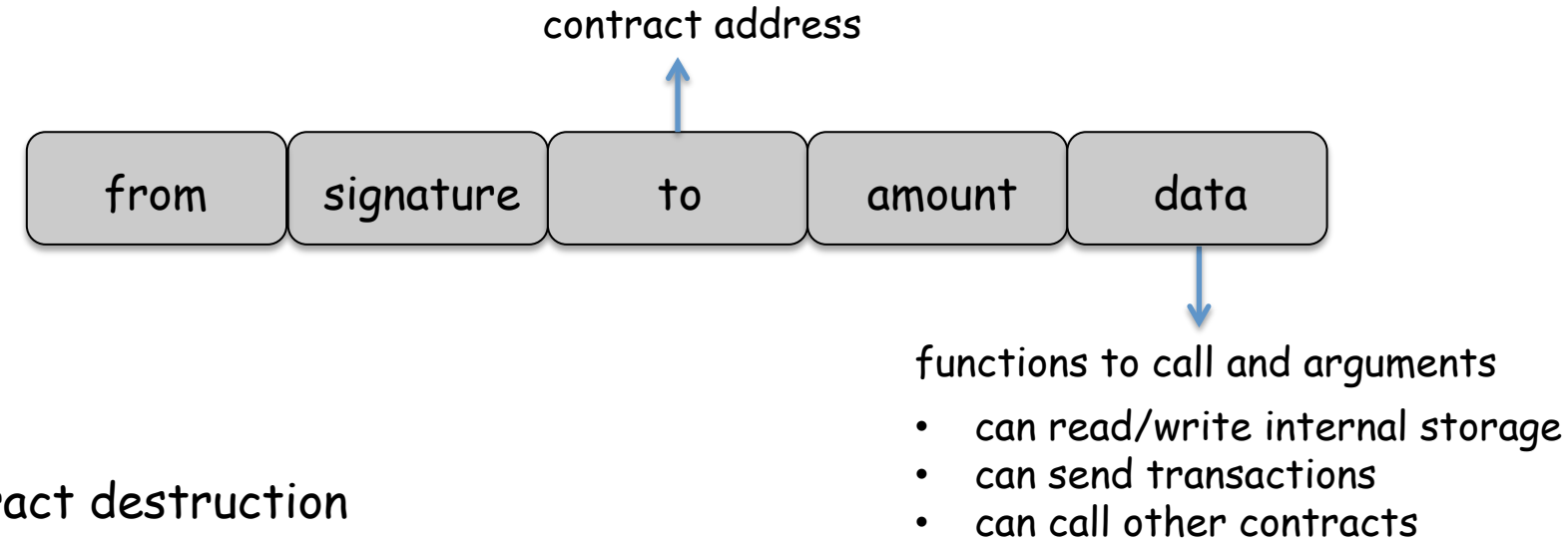
Ethereum

- contract interaction

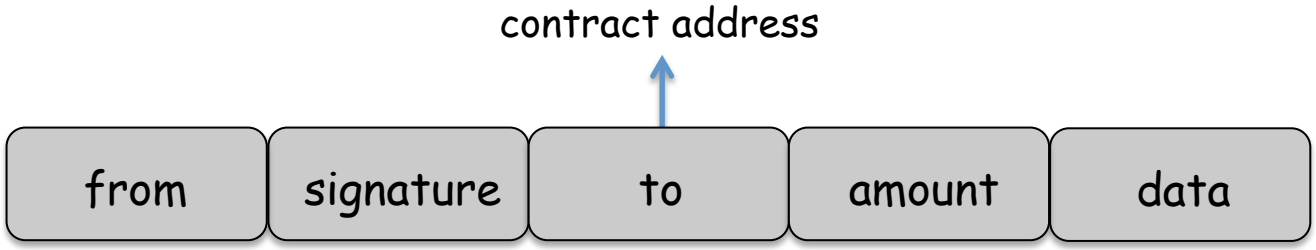


Ethereum

- contract interaction

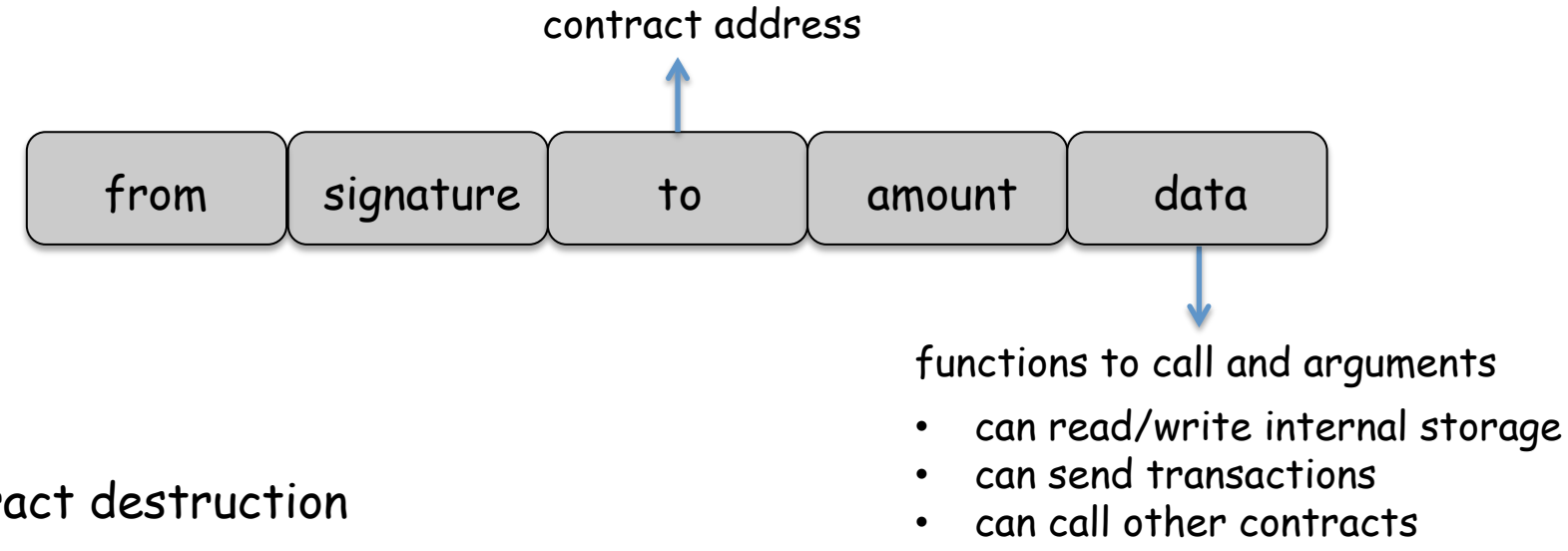


- contract destruction

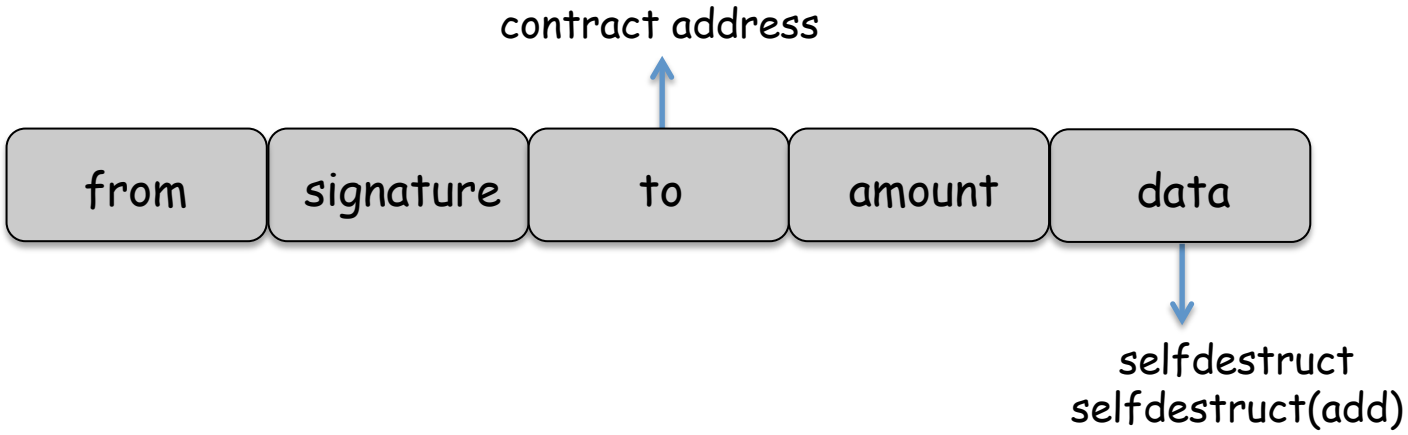


Ethereum

- contract interaction

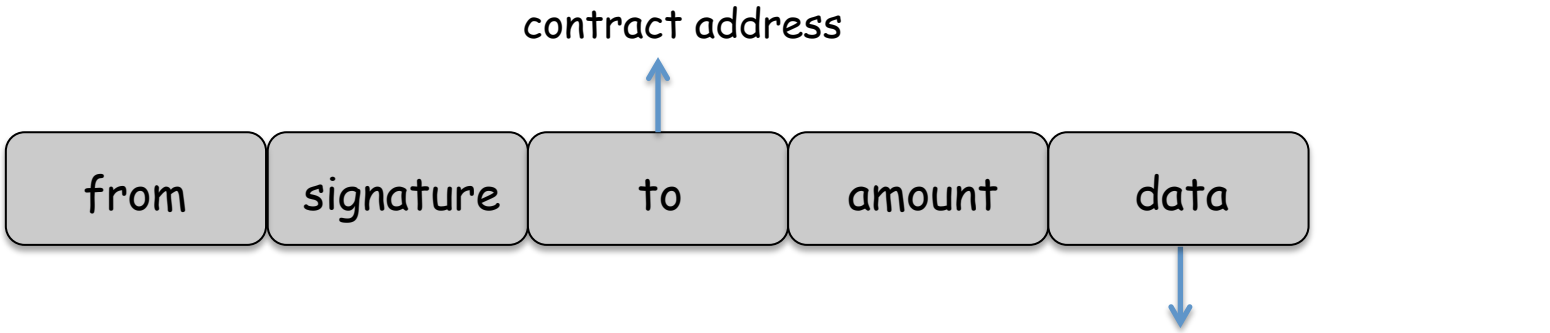


- contract destruction

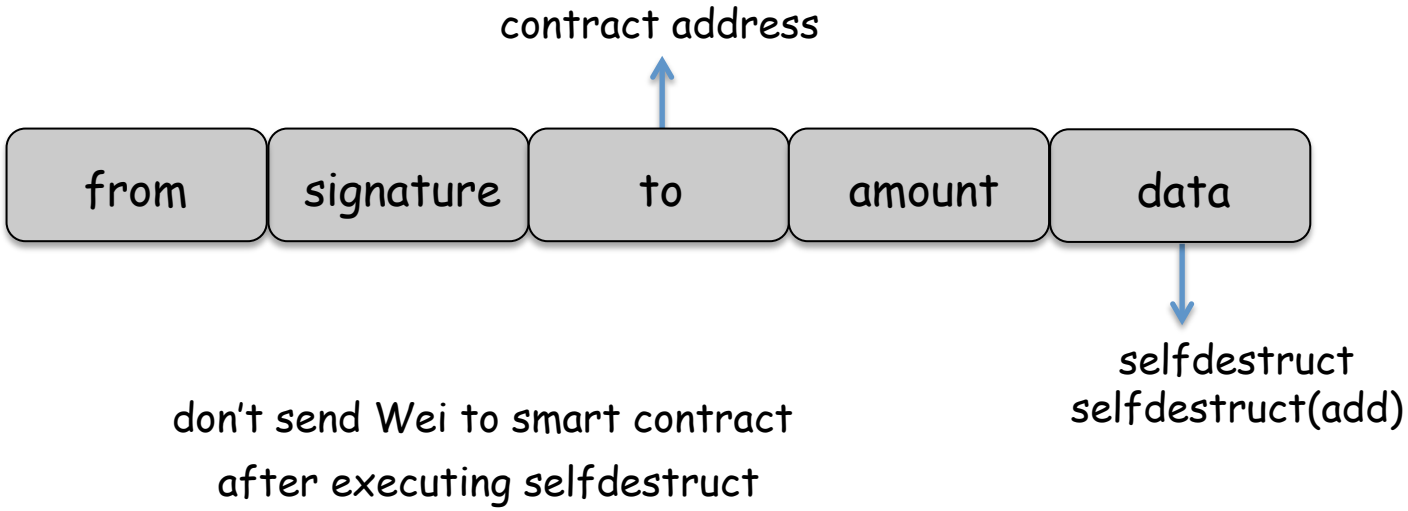


Ethereum

- contract interaction



- contract destruction



Ethereum

- blocks contains a list of transactions and most recent state

Ethereum

- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions

Ethereum

- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions
  - miners collect transactions they receive and reflect them to global state by embedding them into a new block

Ethereum

- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions
  - miners collect transactions they receive and reflect them to global state by embedding them into a new block
- block creation time is about 12-15 seconds

Ethereum

- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions
  - miners collect transactions they receive and reflect them to global state by embedding them into a new block
- block creation time is about 12-15 seconds
- uses proof-of-work for consensus with a different hash function (planned to change with proof-of-stake)

Ethereum

- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions
  - miners collect transactions they receive and reflect them to global state by embedding them into a new block
- block creation time is about 12-15 seconds
- uses proof-of-work for consensus with a different hash function (planned to change with proof-of-stake)
- reward 2ETH + fees

Ethereum

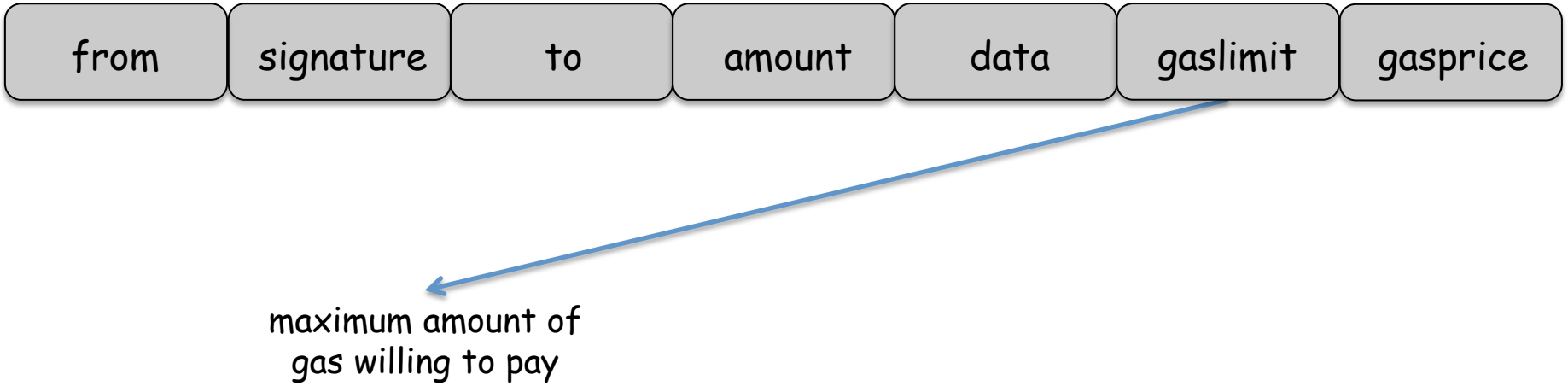
- blocks contains a list of transactions and most recent state
  - users request state transitions by broadcasting transactions
  - miners collect transactions they receive and reflect them to global state by embedding them into a new block
- block creation time is about 12-15 seconds
- uses proof-of-work for consensus with a different hash function (planned to change with proof-of-stake)
- reward 2ETH + fees
  - every computation step has a fee paid in gas
  - gas is a unit used to measure computations

Ethereum

- transactions

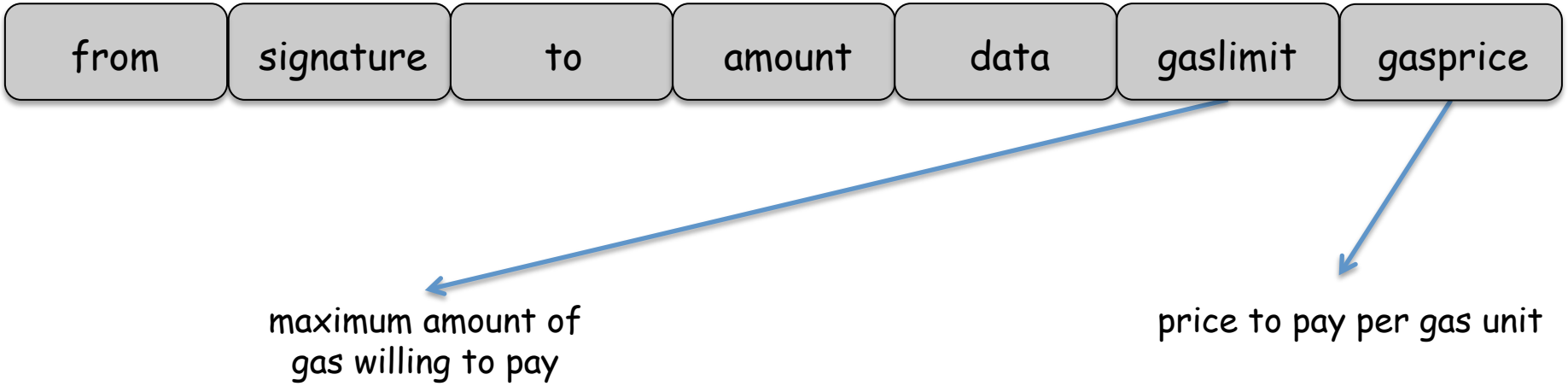
Ethereum

- transactions



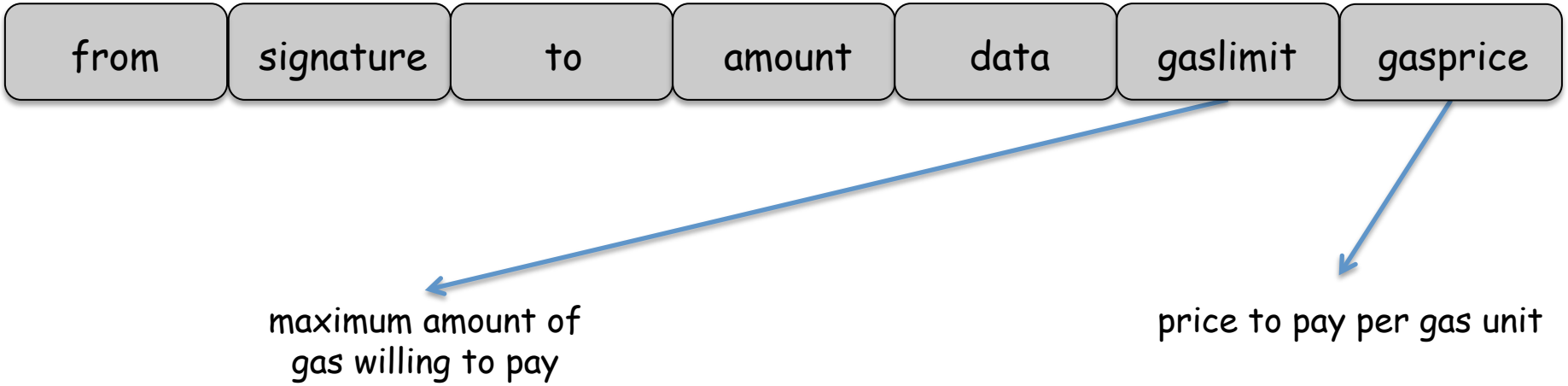
Ethereum

- transactions



Ethereum

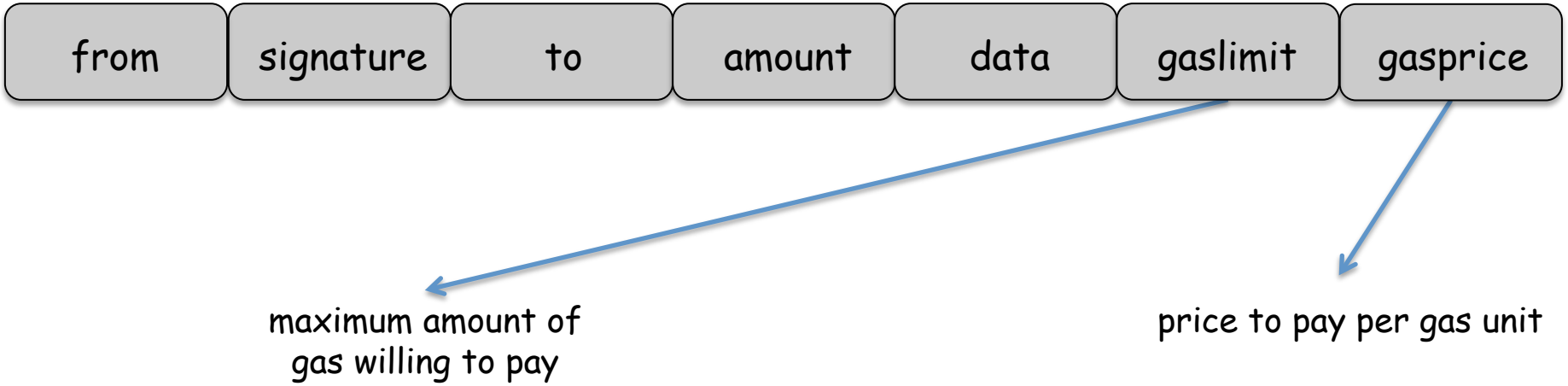
- transactions



- all unused gas is refunded at the end of transaction

Ethereum

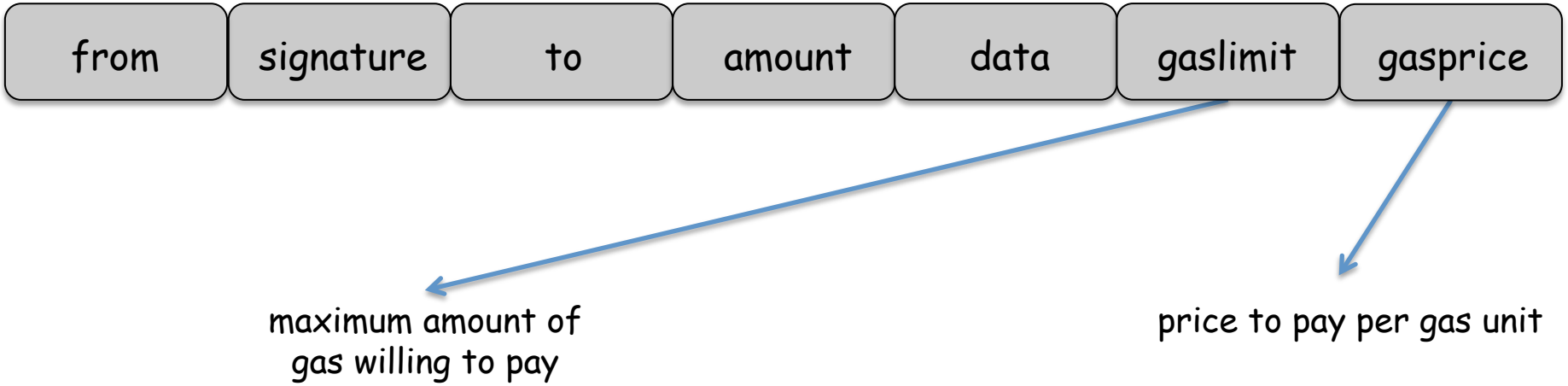
- transactions



- all unused gas is refunded at the end of transaction
- Blocks have gas limit

Ethereum

- transactions



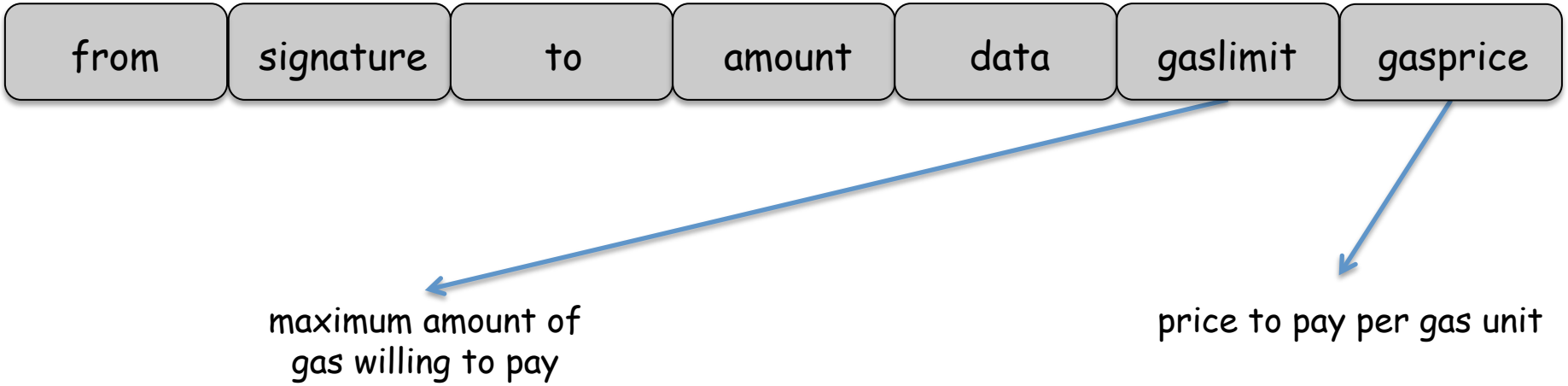
- specifies how quickly a transaction will be confirmed

- all unused gas is refunded at the end of transaction

- Blocks have gas limit

Ethereum

- transactions

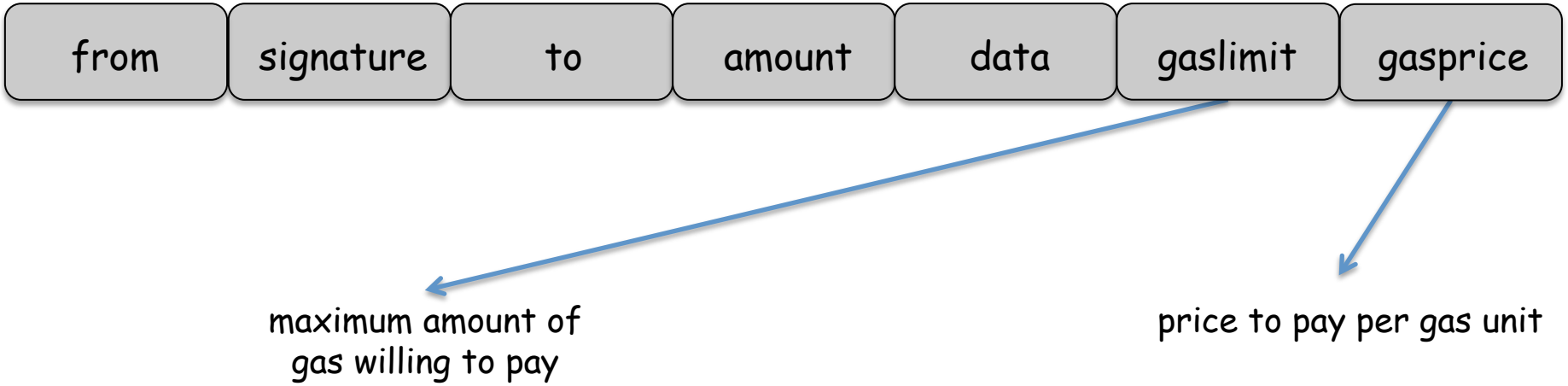


- all unused gas is refunded at the end of transaction
- Blocks have gas limit

- specifies how quickly a transaction will be confirmed
- gas limit x gas price = transaction fee

Ethereum

- transactions



- all unused gas is refunded at the end of transaction
- Blocks have gas limit

- specifies how quickly a transaction will be confirmed
- gas limit x gas price = transaction fee
- 50000 x 20 Gwei = 0.001 ETH (max)

Ethereum

- transactions

- if the signature is valid and the receiver has enough Wei in his balance to pay the required gas, than the transaction considered as valid transaction

Account - based	UXTO - based
conceptually simple	higher privacy
transactions smaller in size	simpler parallelization of transactions
executing transactions in parallel relatively hard	

Ethereum

Account - based	UXTO - based
conceptually simple	higher privacy
transactions smaller in size	simpler parallelization of transactions
executing transactions in parallel relatively hard	

Ethereum

Account - based	UXTO - based
conceptually simple	higher privacy
transactions smaller in size	simpler parallelization of transactions
executing transactions in parallel relatively hard	

- assume you broadcast two different transactions within 10 seconds

  in distributed system, there is no guarantee that they collect your first transaction first and the second one second

Ethereum

Account - based	UXTO - based
conceptually simple	higher privacy
transactions smaller in size	simpler parallelization of transactions
executing transactions in parallel relatively hard	

- assume you broadcast two different transactions within 10 seconds

  in distributed system, there is no guarantee that they collect your first transaction first and the second one second

- assume someone sends some ether to a receiver by signing the transaction (replay attack)

  receiver can copy the signed transaction and keep broadcasting it till the sender loses all his money

Ethereum

Account - based	UXTO - based
conceptually simple	higher privacy
transactions smaller in size	simpler parallelization of transactions
executing transactions in parallel relatively hard	

- assume you broadcast two different transactions within 10 seconds

  in distributed … collect your first transacti…

- assume someone … ing the transaction (replay attack)

  receiver can copy the signed transaction and keep broadcasting it till the sender loses all his money

- add the sender's nonce value to each transaction to avoid such cases