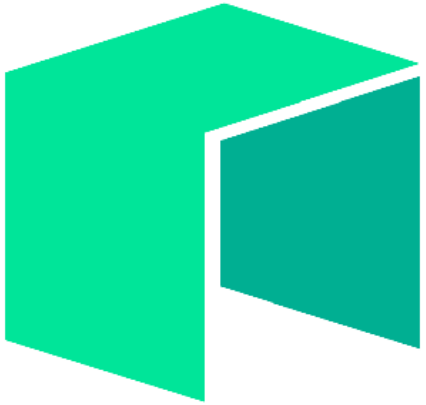
BlockChain - Uvodno predavanje

Stefan Nožinić (stefan@lugons.org)



Motivacija

Zcash

CARDANO

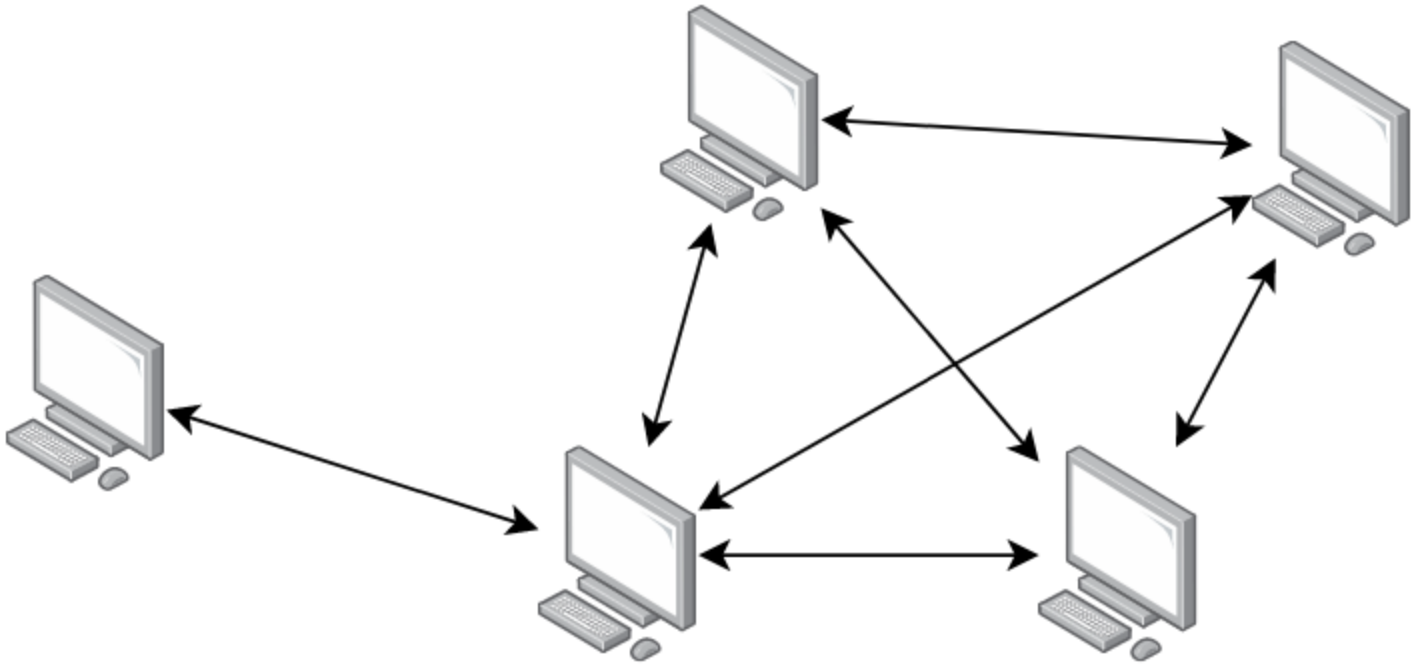
ethereum classic

litecoin

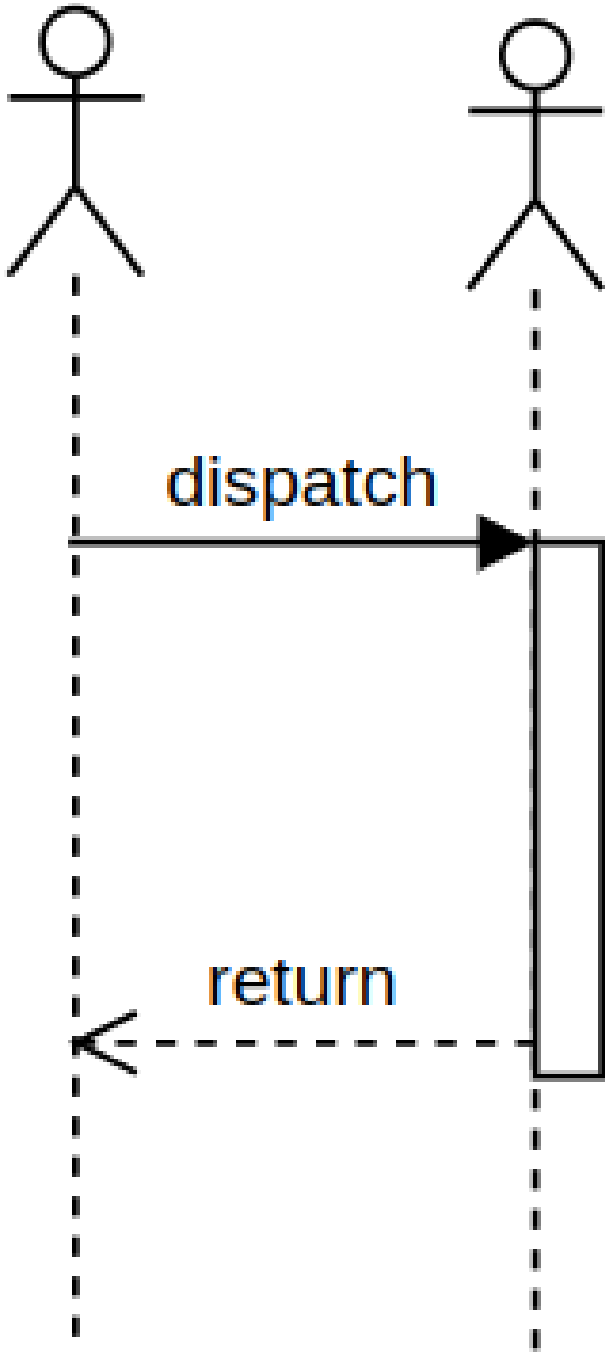
ripple

MONERO

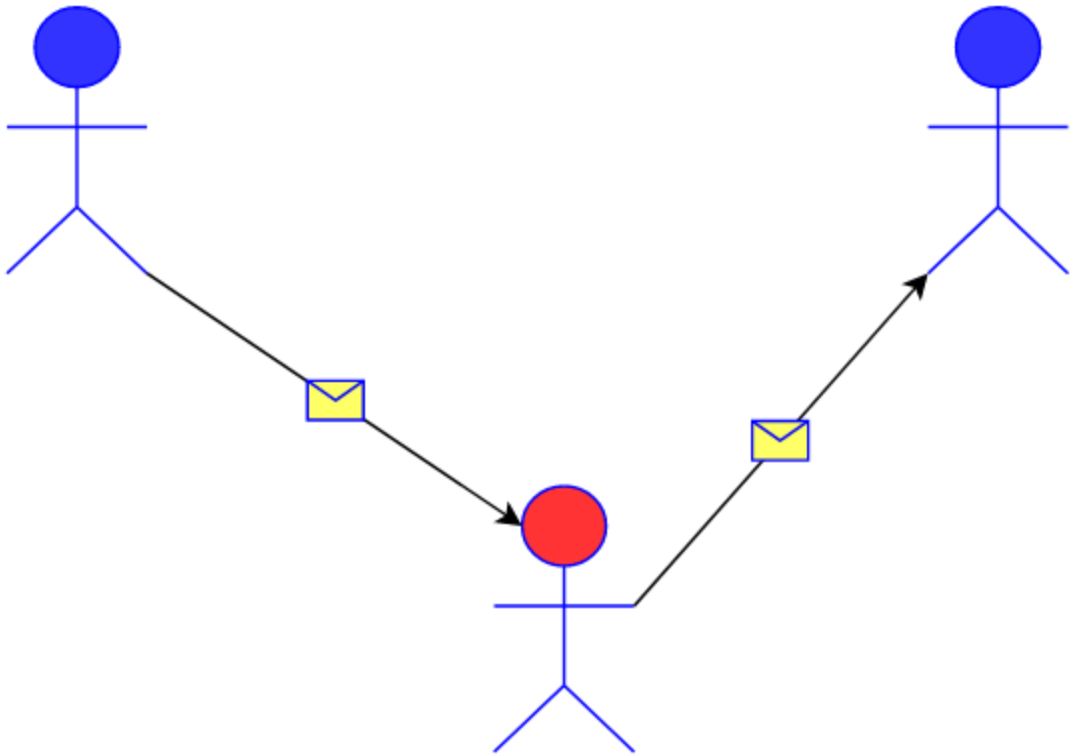
P2P mreža

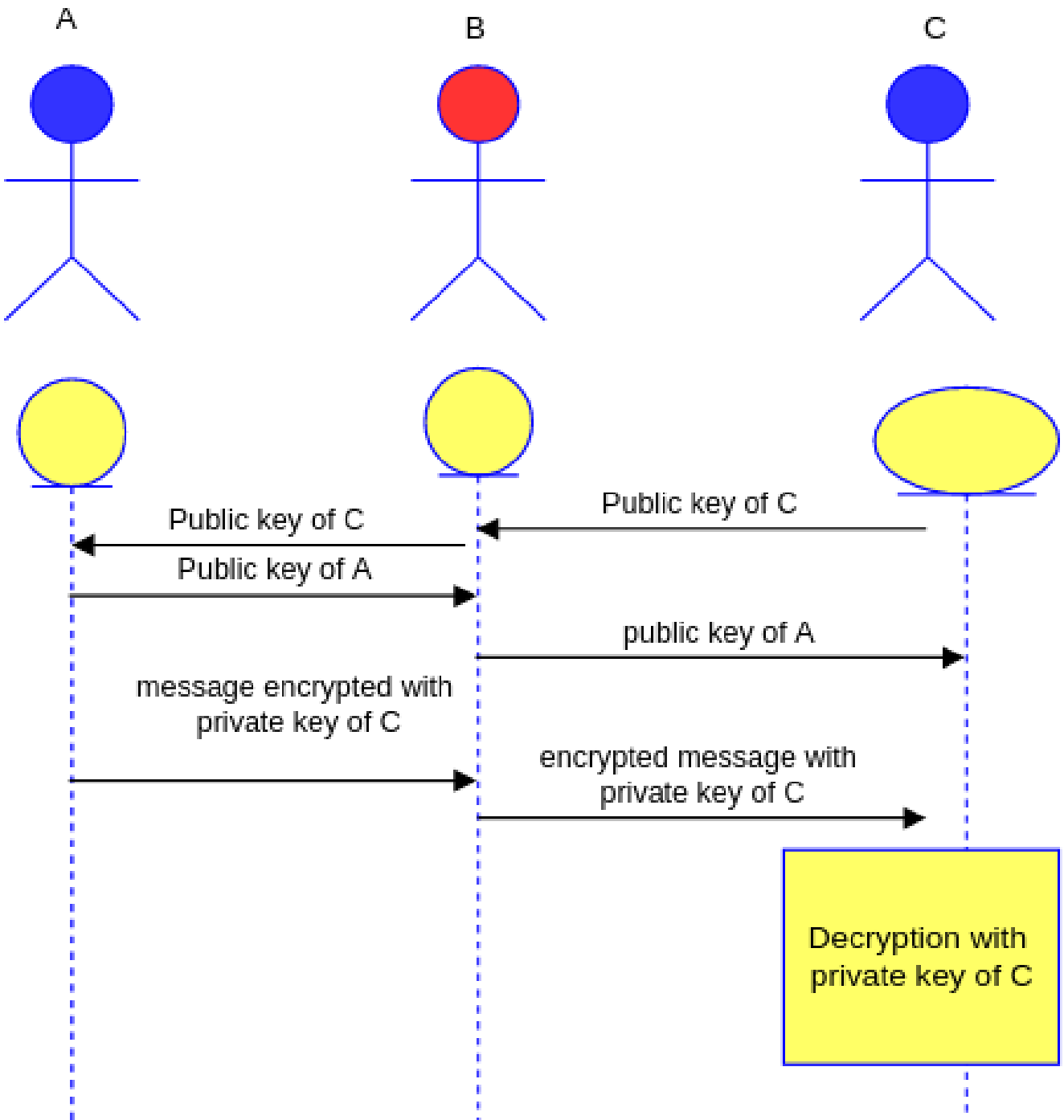


RPC

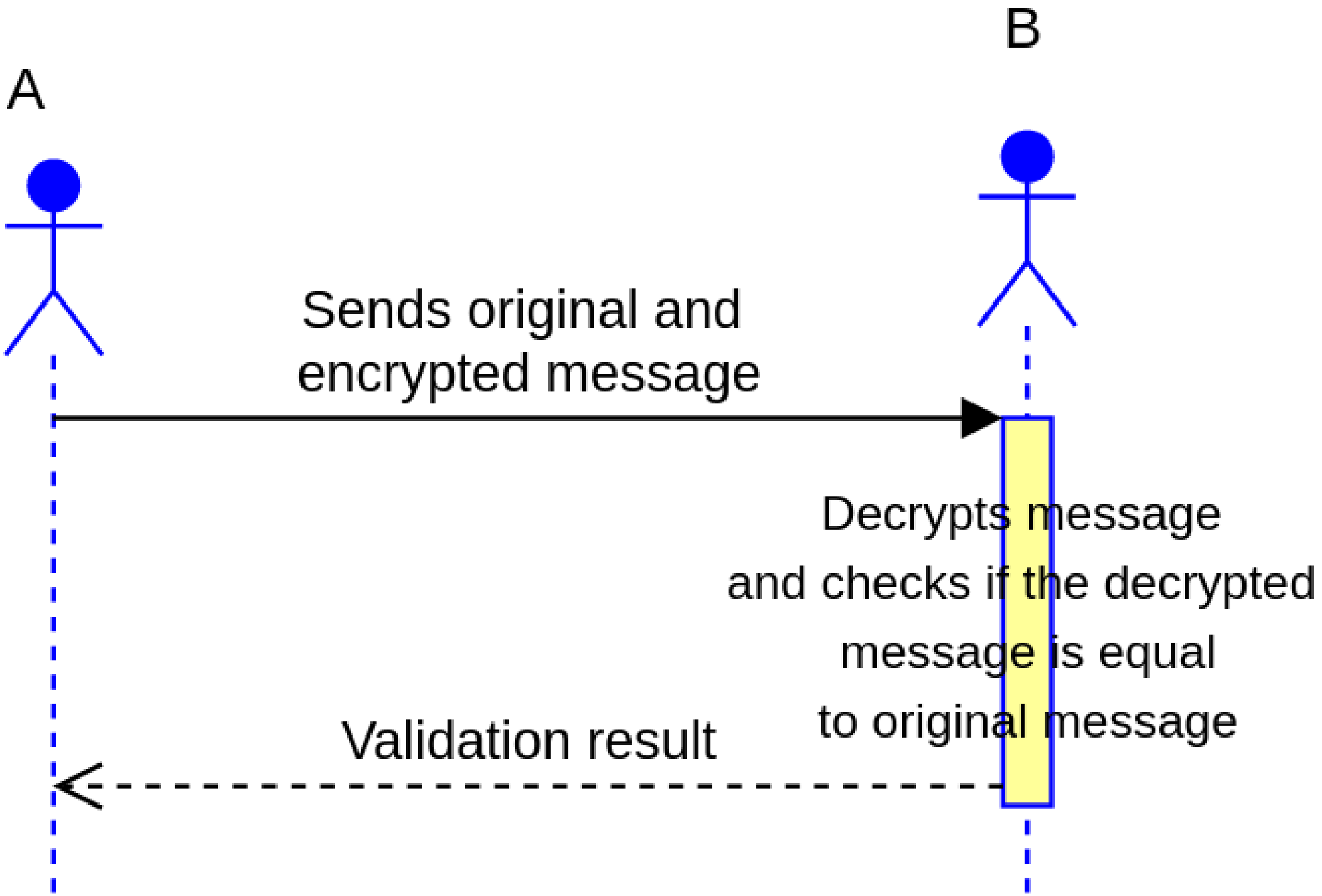


Asimetrična kriptografija

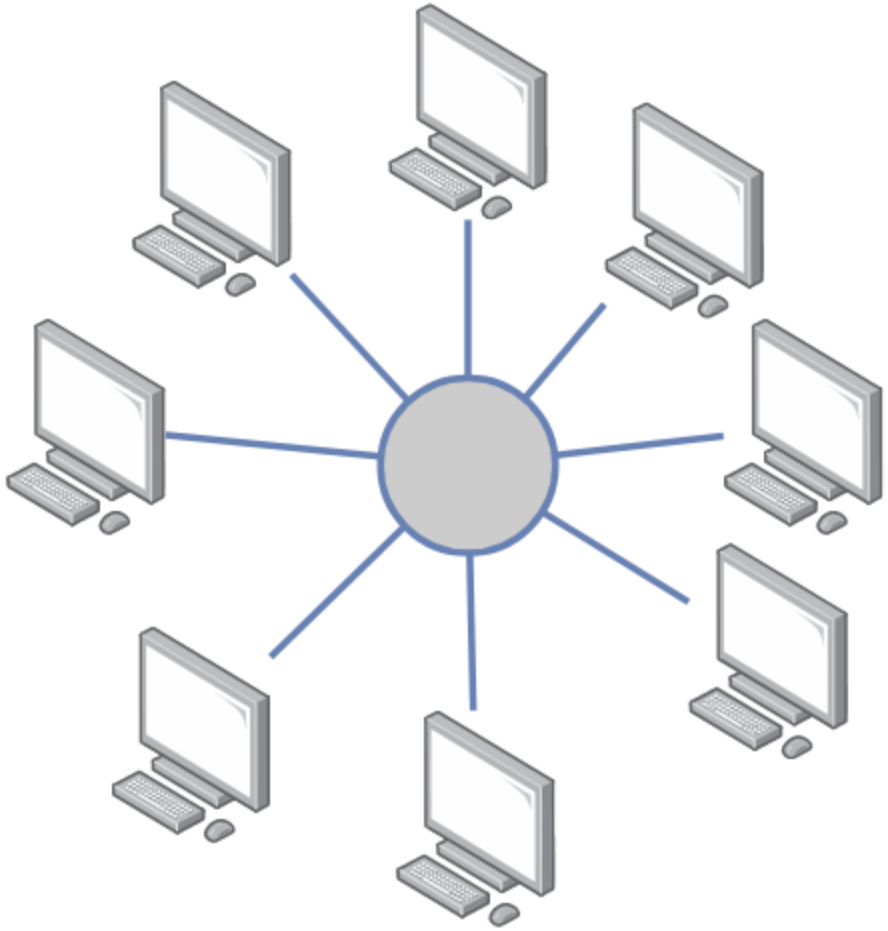



A
B
C
Public key of C
Public key of C
Public key of A
public key of A
message encrypted with
private key of C
encrypted message with
private key of C
Decryption with
private key of C

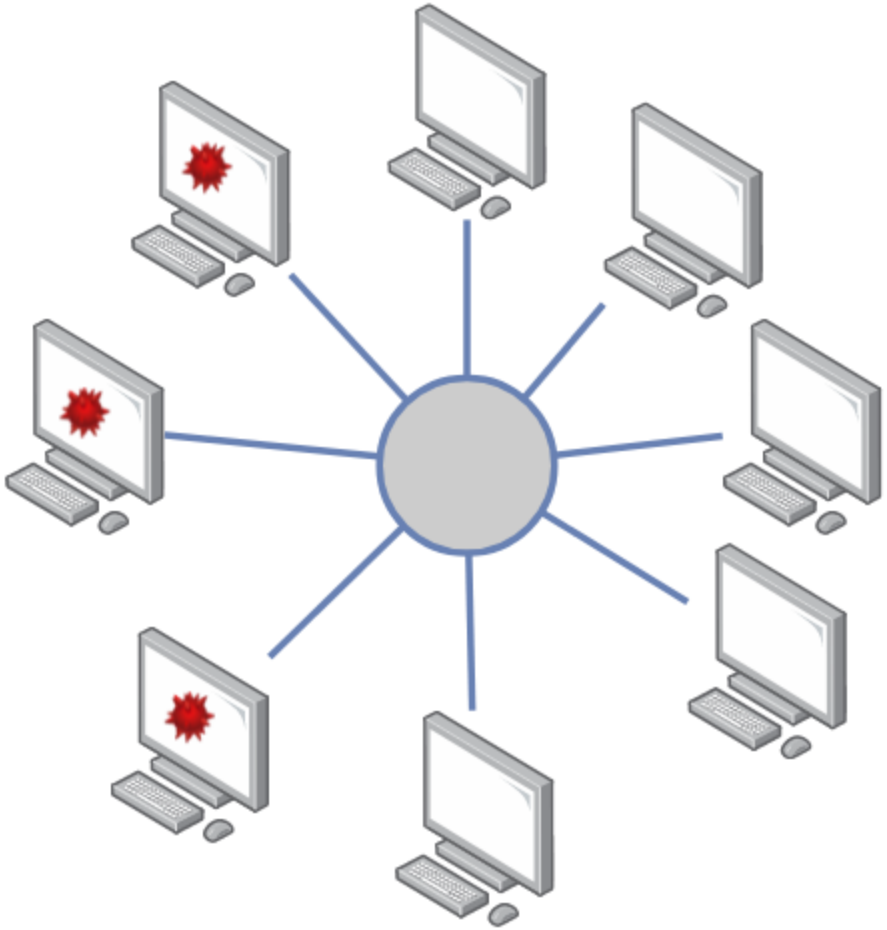
Potpisi i dokaz autentičnosti


A
B
Sends original and
encrypted message
Decrypts message
and checks if the decrypted
message is equal
to original message
Validation result

Konsenzus



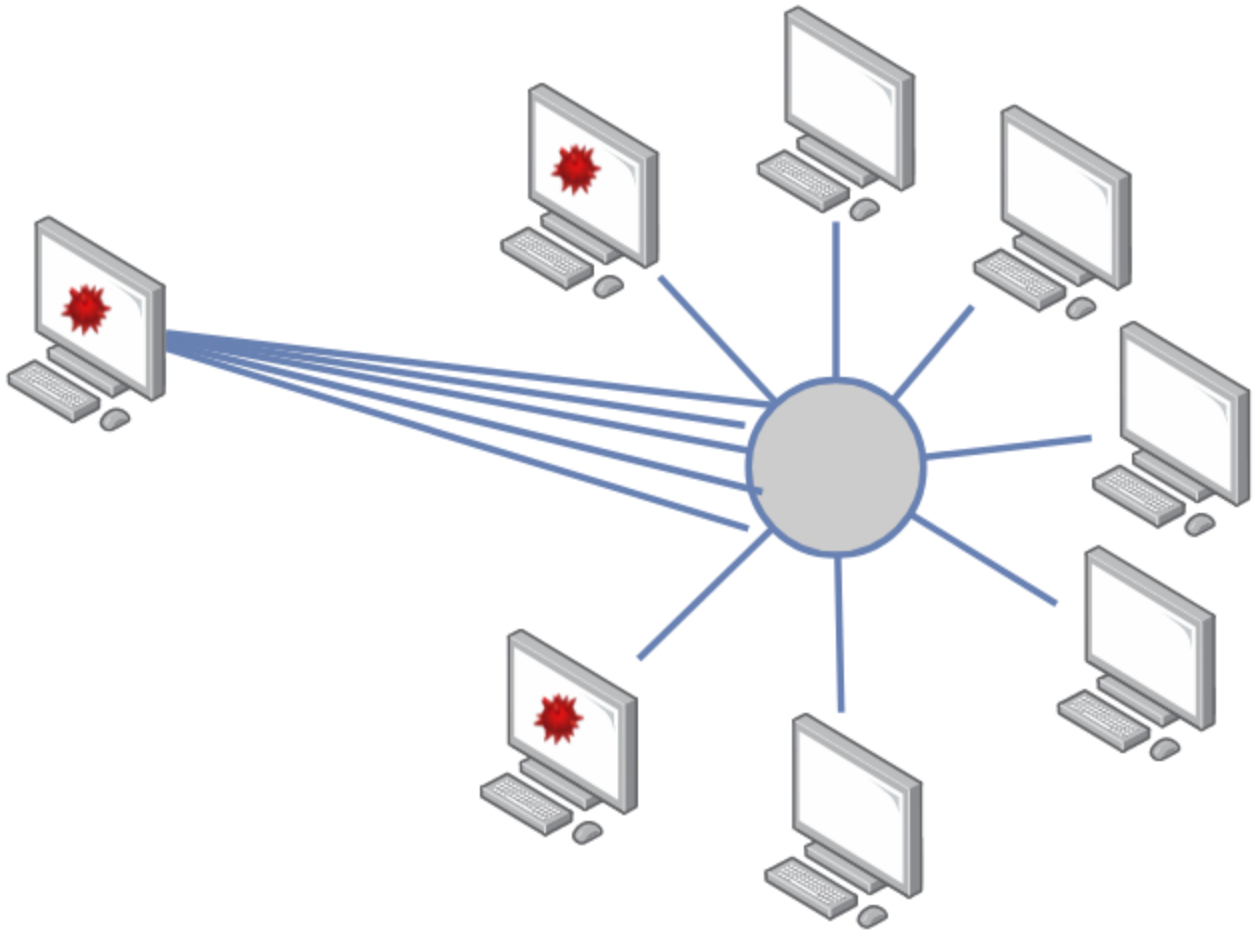
Byzantine Fault Tolerance



Double spending

Pošaljilac	Primalac	Vrednost	Kusur
A	B	$100	$400
A	B	$600	$1000

Sybill attack



HashCash

Proof of work

Append-only log

Vreme	Autor	Podaci
15616	A	....
28615	B	....
30160	C	....

Transakcija

Sadrži:

- adresu pošiljaoca
- adresu primaoca
- vreme
- identifikator prethodne transakcije
- dodatne metapodatke u zavisnosti od konkretne implementacije
- podatke (npr, vrednost, kod, ...)
- potpis privatnim ključem pošiljaoca

Ledger

- Transakcijski ledger
- bilansni ledger

Bilansni ledger

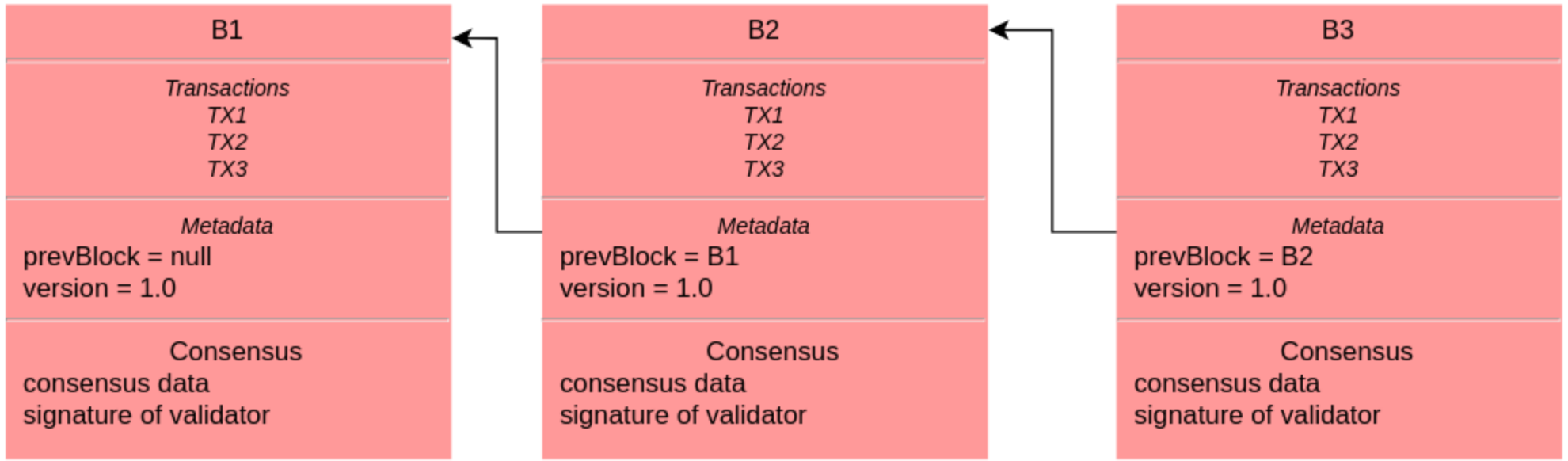
Nalog	Stanje
A	$300
B	$400
C	$1000

Nalog	Stanje
A	$0
B	$400
C	$1300

Transakcijski ledger

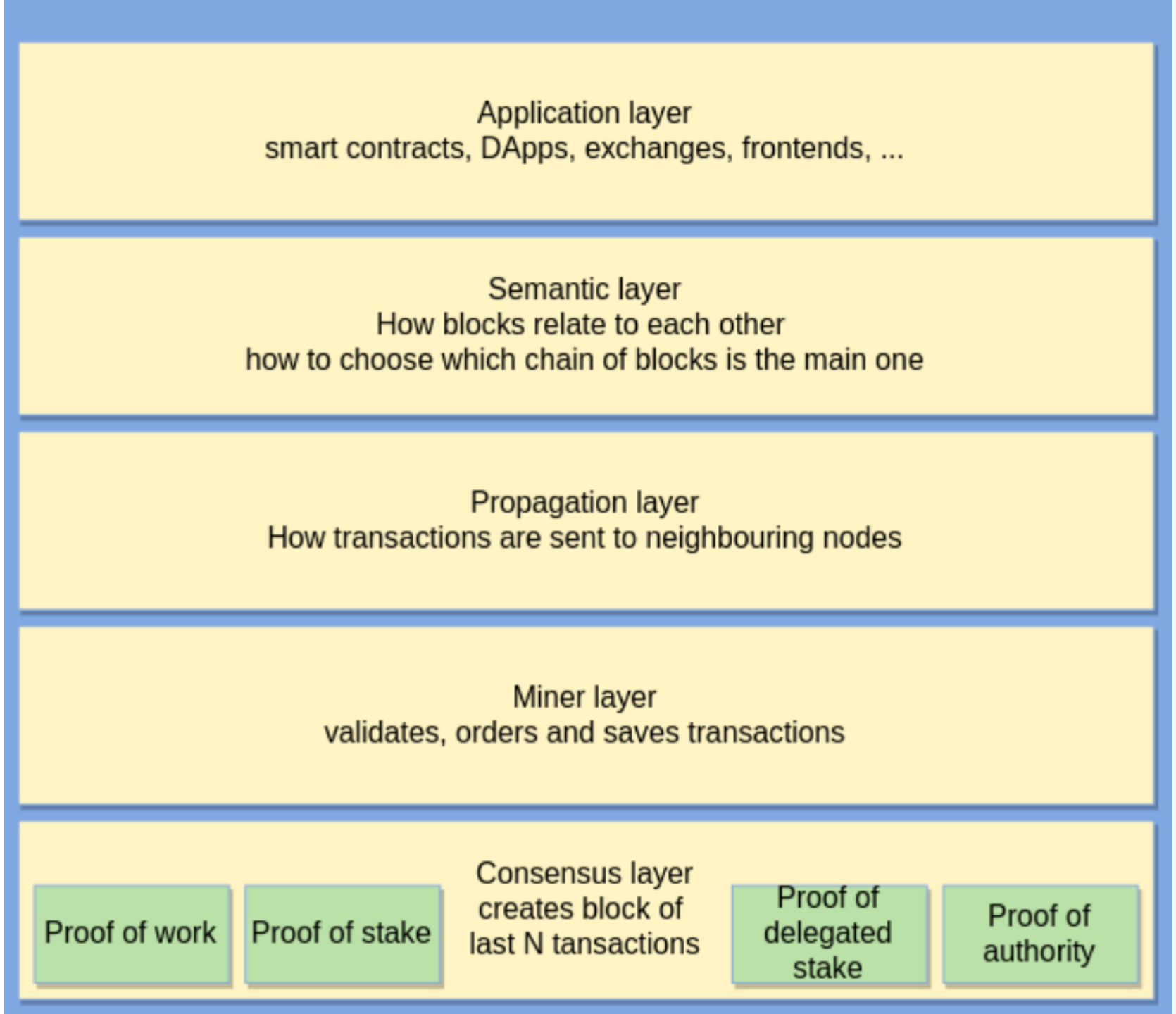
Pošaljilac	Primalac	Vrednost	Kusur
A	B	$100	$400
B	C	$100	$1000
C	A	$100	$0

Blokovi


B1
Transactions
TX1
TX2
TX3
Metadata
prevBlock = null
version = 1.0
Consensus
consensus data
signature of validator
B2
Transactions
TX1
TX2
TX3
Metadata
prevBlock = B1
version = 1.0
Consensus
consensus data
signature of validator
B3
Transactions
TX1
TX2
TX3
Metadata
prevBlock = B2
version = 1.0
Consensus
consensus data
signature of validator

Coinbase

- zašto bi neko validirao blokove ako može da se osloni na druge čvorove da rade težak posao?


Application layer
smart contracts, DApps, exchanges, frontends, ...
Semantic layer
How blocks relate to each other
how to choose which chain of blocks is the main one
Propagation layer
How transactions are sent to neighbouring nodes
Miner layer
validates, orders and saves transactions
Proof of work
Proof of stake
Consensus layer
creates block of
last N tansactions
Proof of
delegated
stake
Proof of
authority

Čvorovi u mreži

- full nodes - stores whole blockchain, transactions, and is able to validate all transactions
- pruning nodes - prune some transactions after validation (block created) and aging
- lightweight nodes - store blockchain headers only
- miners - create new blocks and perform proof of work / stake / …
- mining pool operators - full node that uses other miners and redistributes reward
- wallets - creates key pairs, store its transactions, view its transactions, send transactions and receive transactions to itself
- mempool - keeps track of unconfirmed but validated transactions

Konsenzus u prisustvu malicioznih procesa

- Proof of work
- Proof of stake
- Proof of authority
- Proof of burn
- ...

Bitcoin

bitCoin analiza

Pitanja?