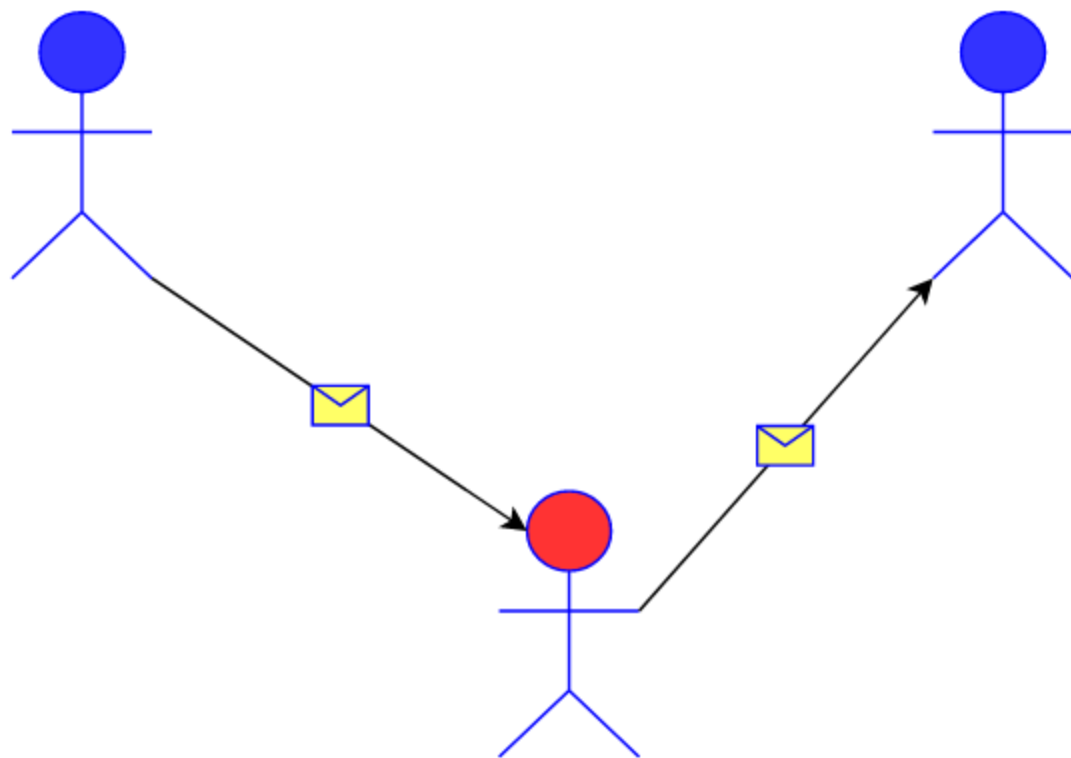


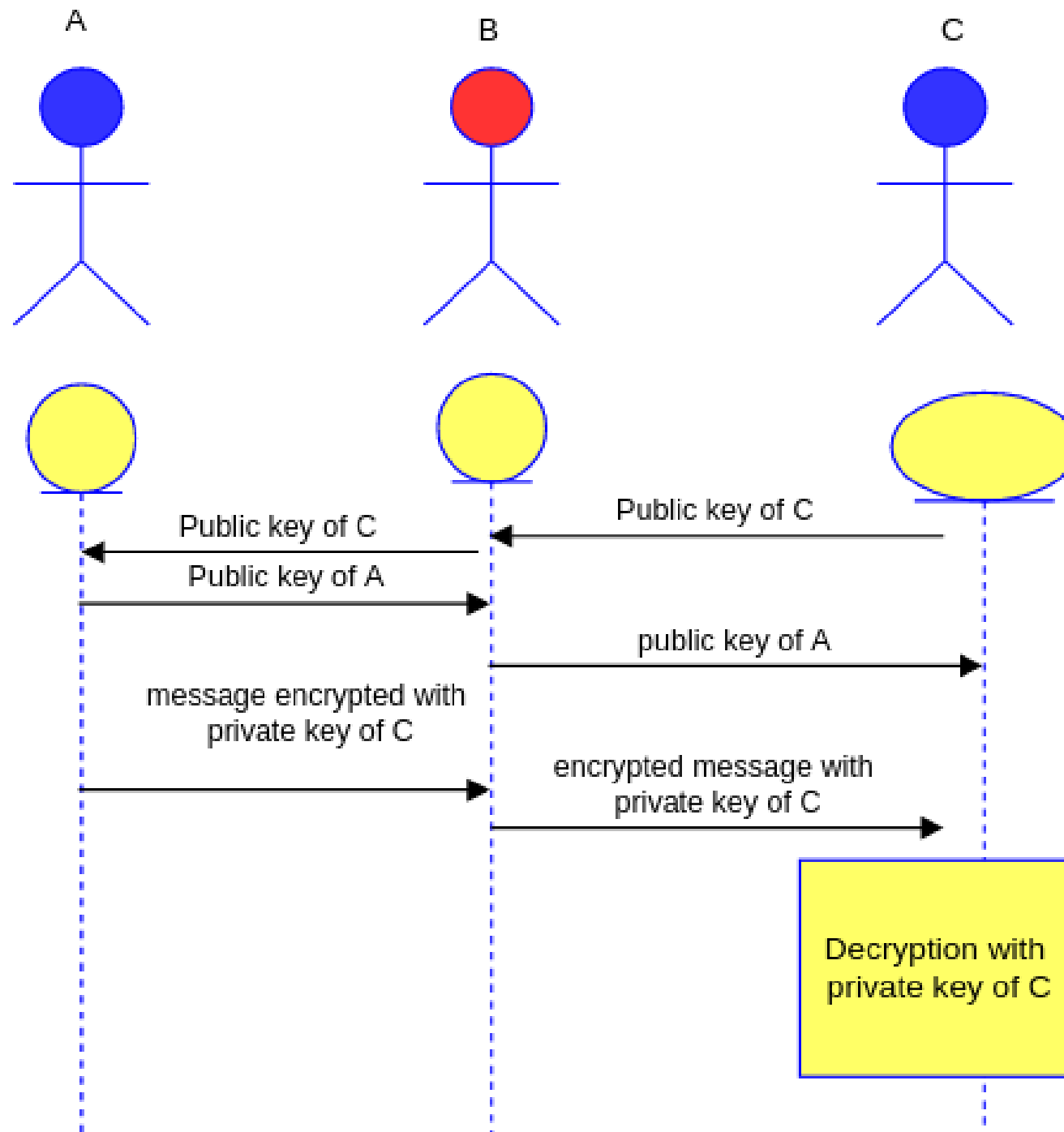
Blockchain - Uvodno predavanje

Stefan Nožinić (stefan@lugons.org)

Osnovni koncepti

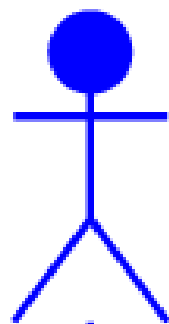
Asimetrična kriptografija



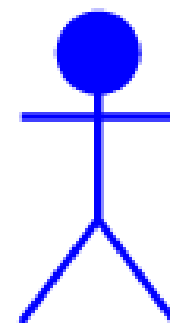


Potpisi i dokaz autentičnosti

A



B



Sends original and
encrypted message



Decrypts message
and checks if the decrypted
message is equal
to original message



Validation result



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

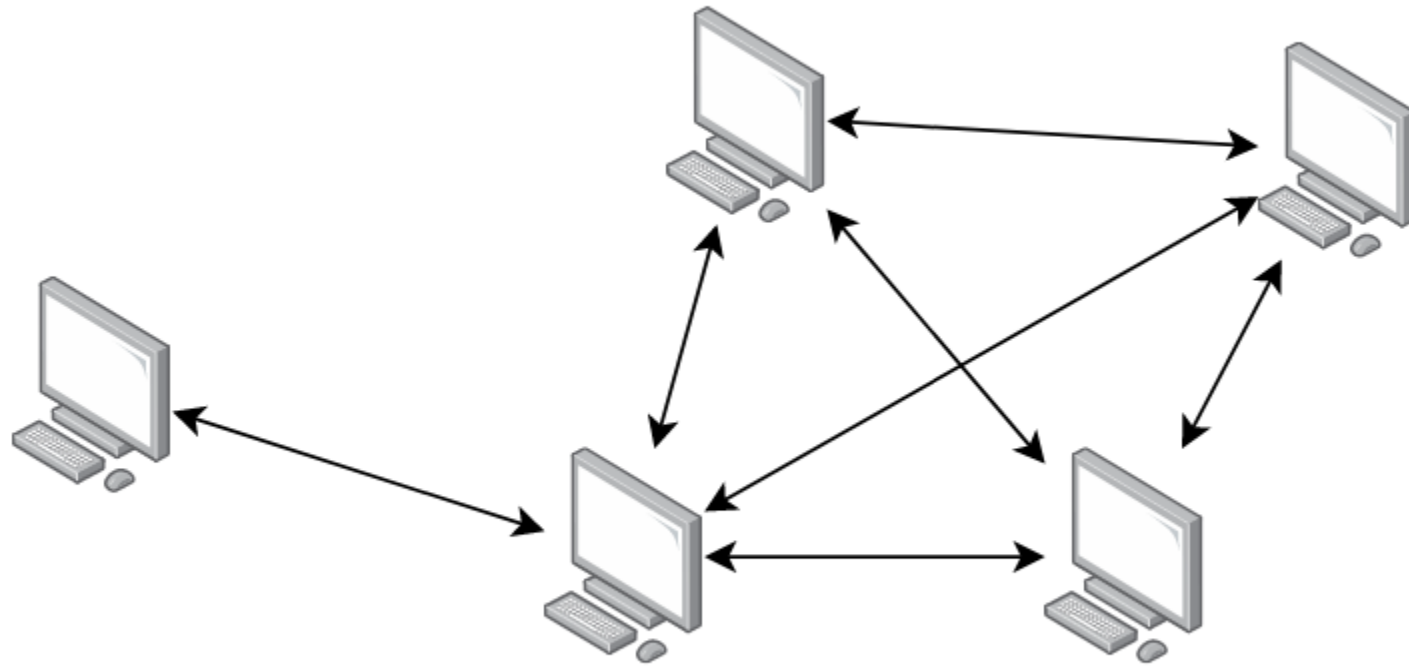
Bilasni ledger

- sadrži listu bilansa stanja

Transakcijski ledger

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

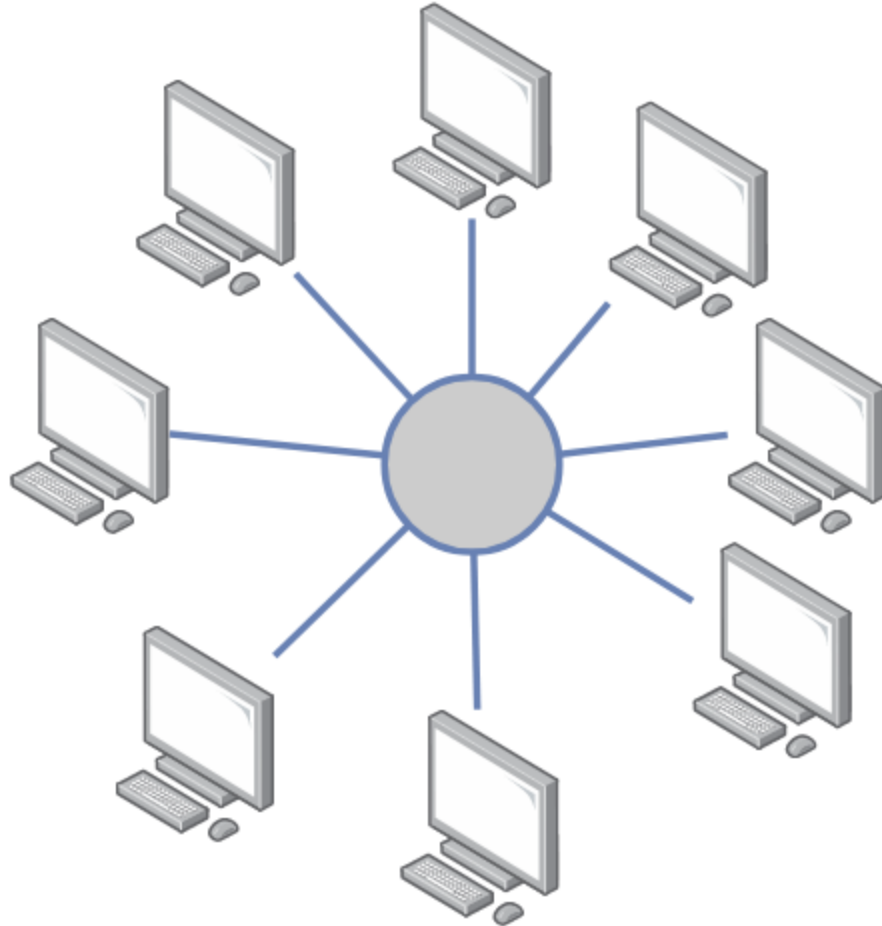
P2P mreža



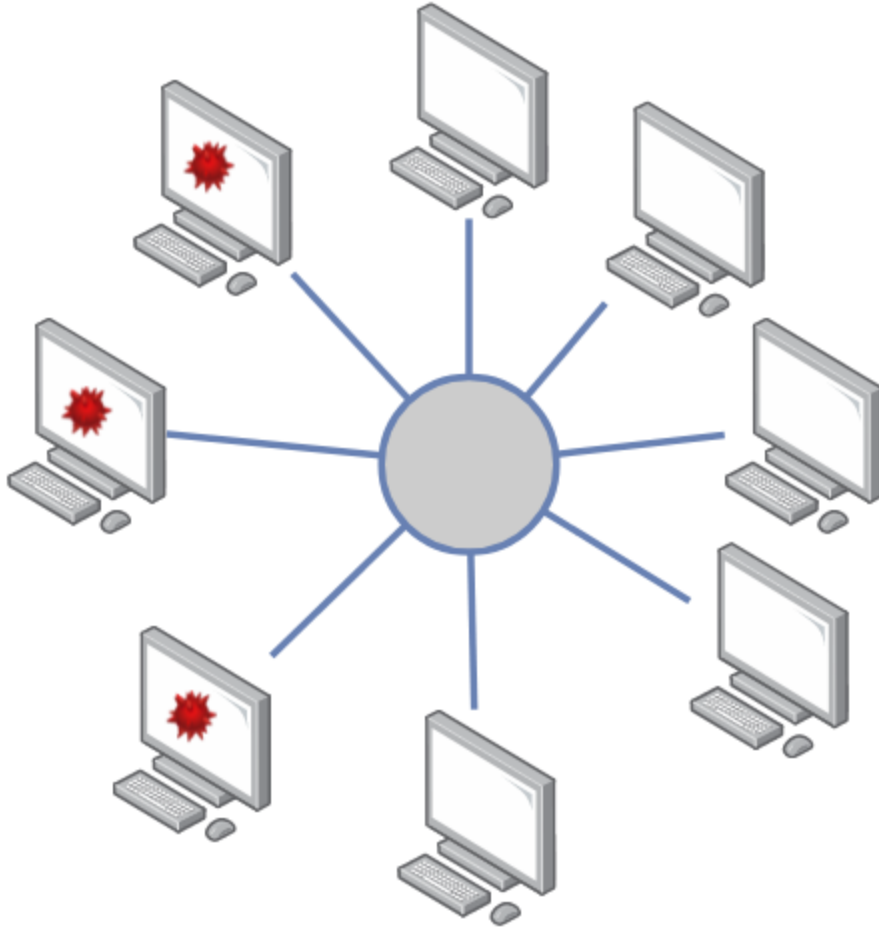
Double spending

Pošaljalac	Primalac	Vrednost	Kusur
A	B	\$100	\$400
A	B	\$600	\$1000

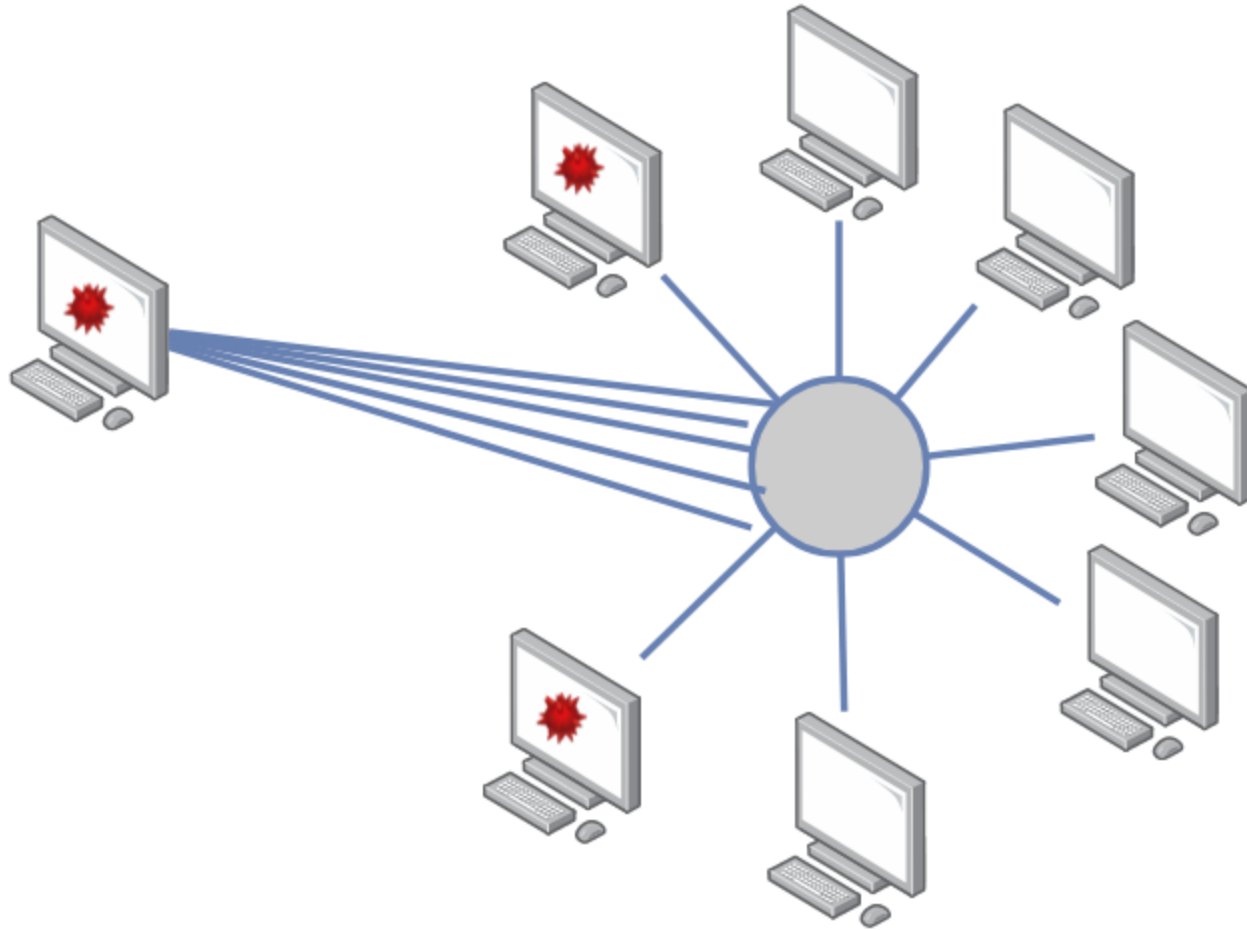
Konsensus



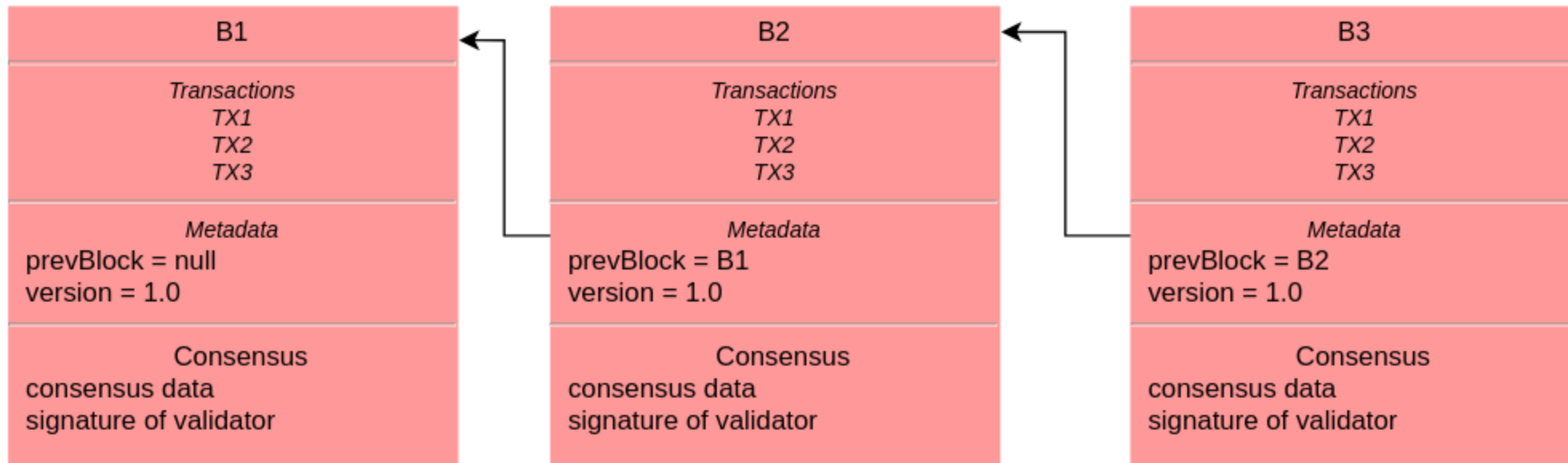
Byzantine Fault Tolerance



Sybill attack



Blokov



Konsenzus u prisustvu malicioznih procesa

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

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

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

Consensus layer
creates block of
last N transactions

Proof of work Proof of stake Proof of delegated stake Proof of authority

Pitanja?