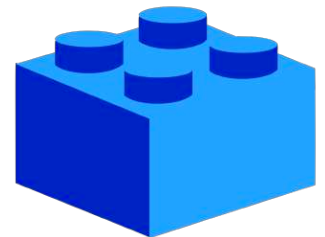


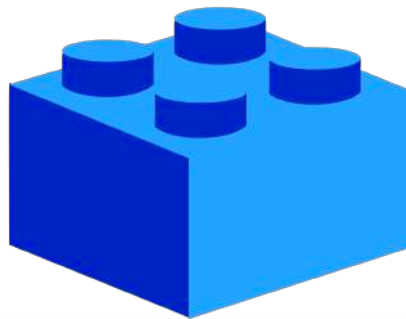
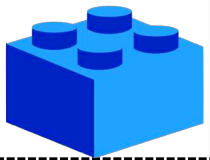
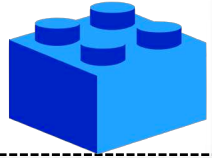
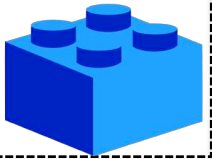


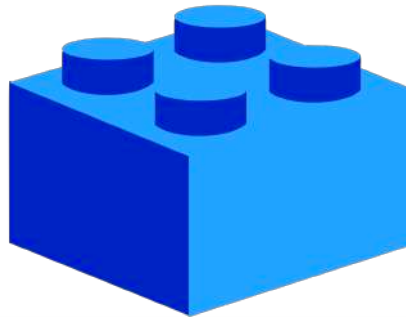
Using Property-Based Testing in Blockchain applications

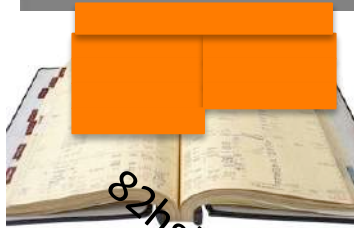
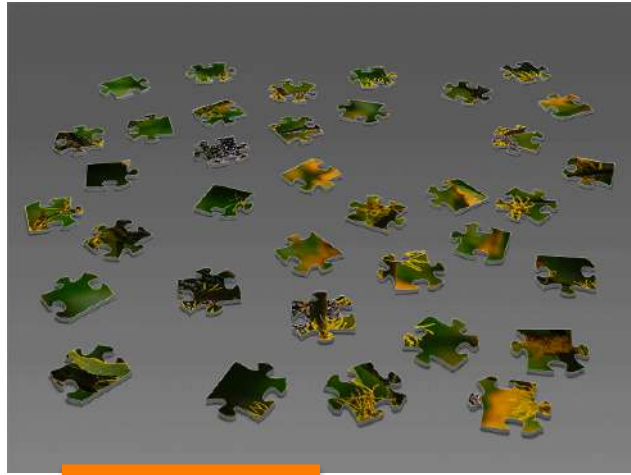
Thomas Arts
QuviQ



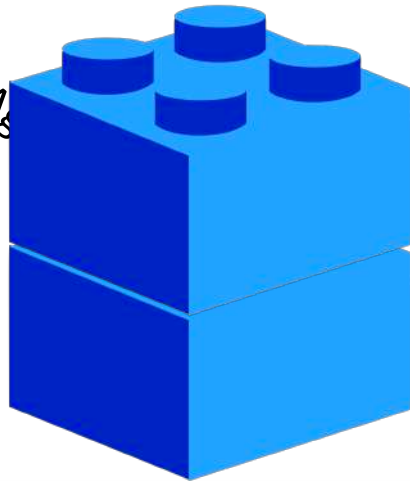
A node in a distributed network

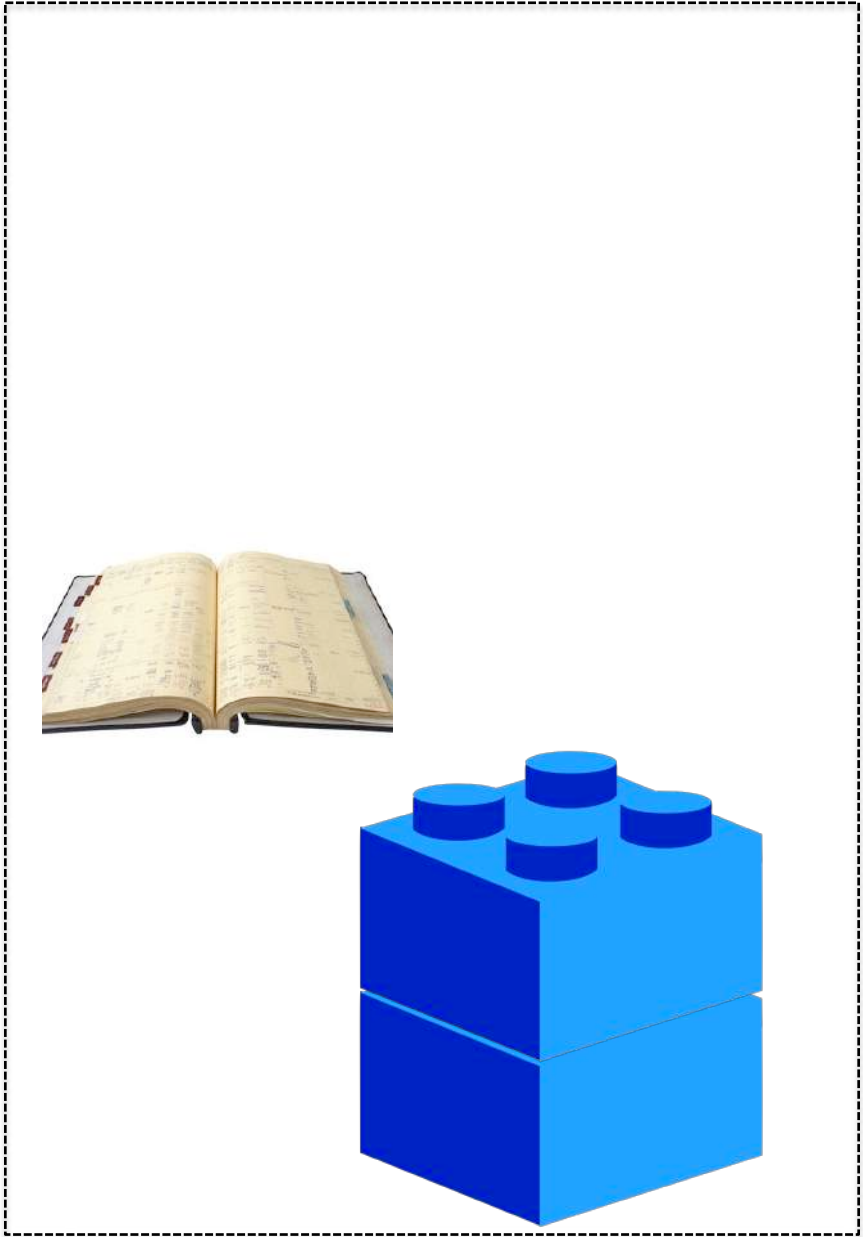


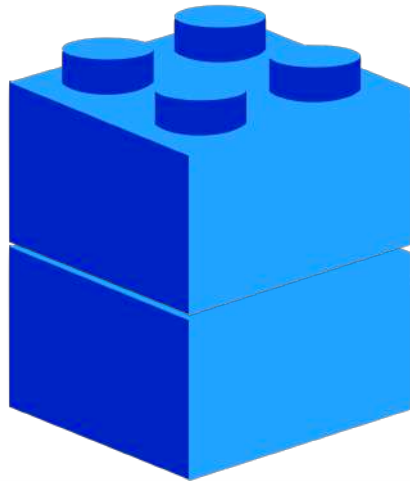


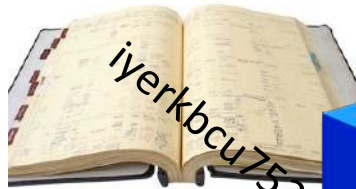
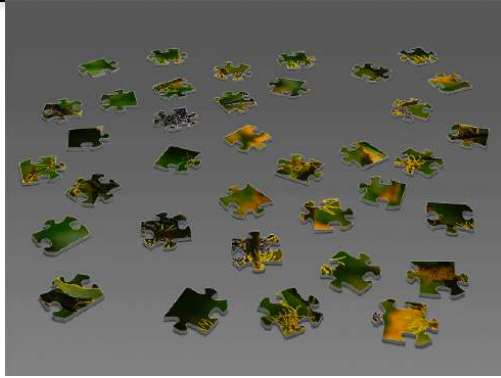


82hsbt2BBHA8

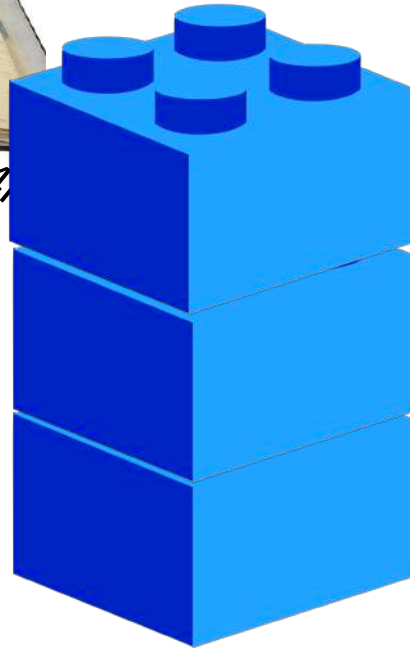


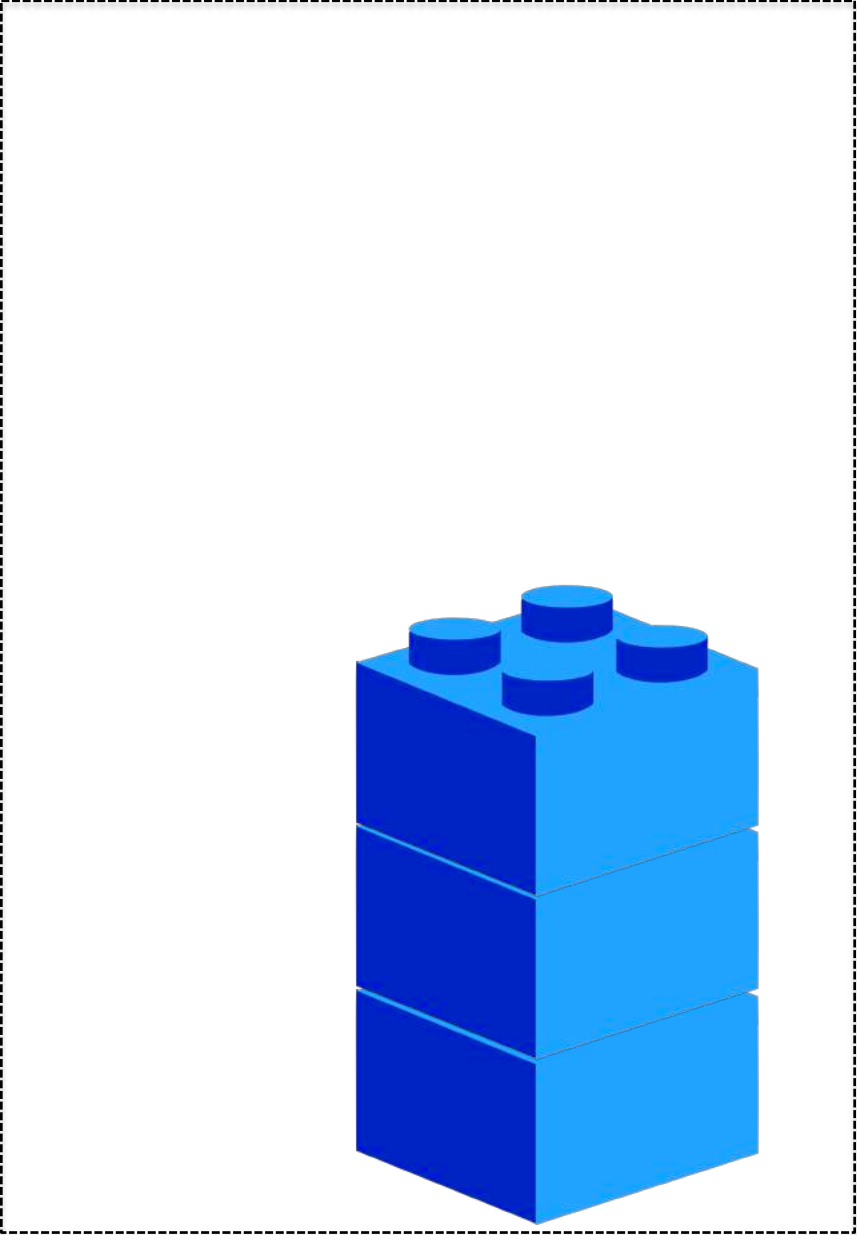




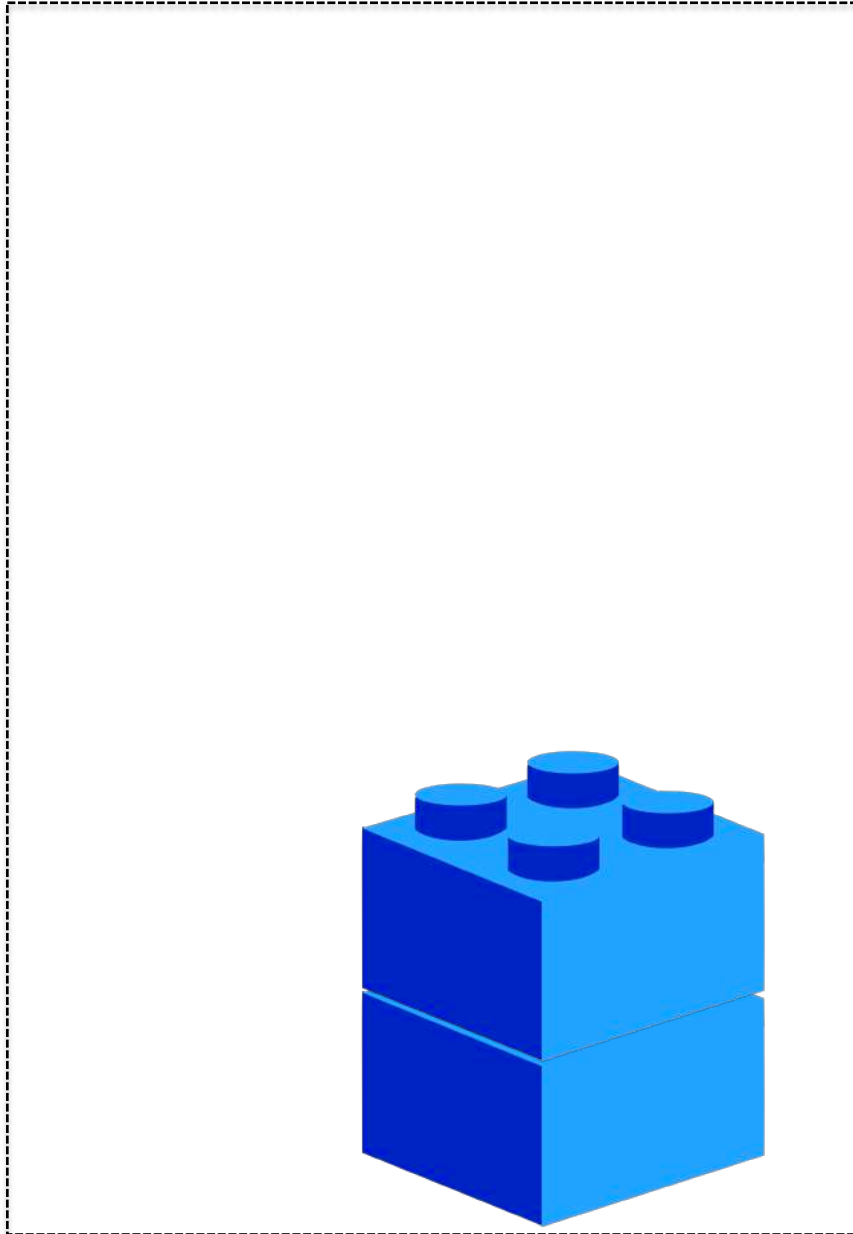
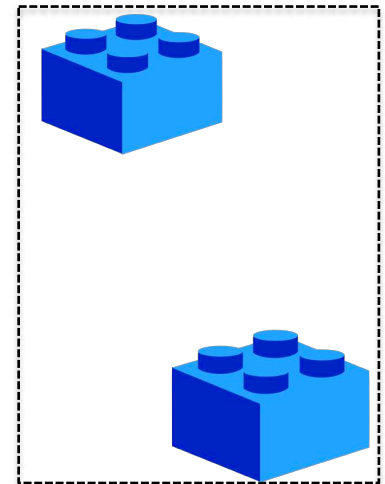
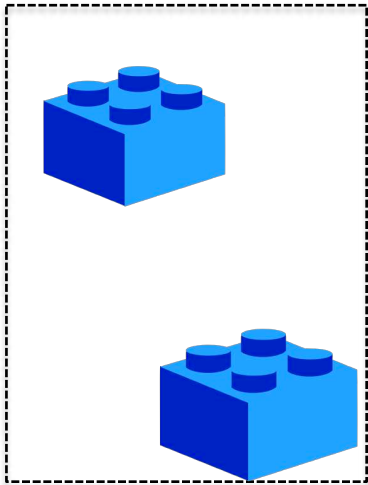
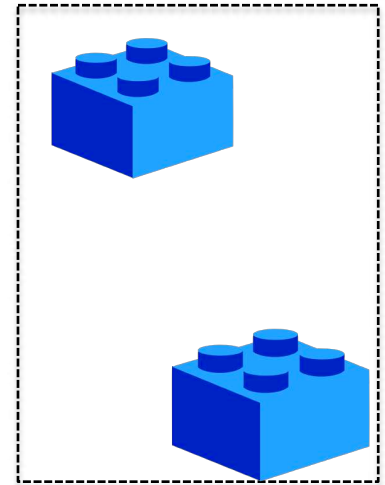
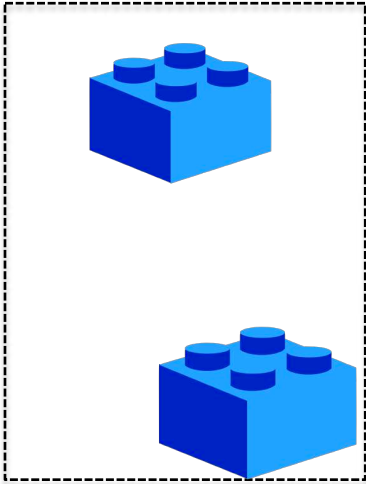


iyerkbcu7524

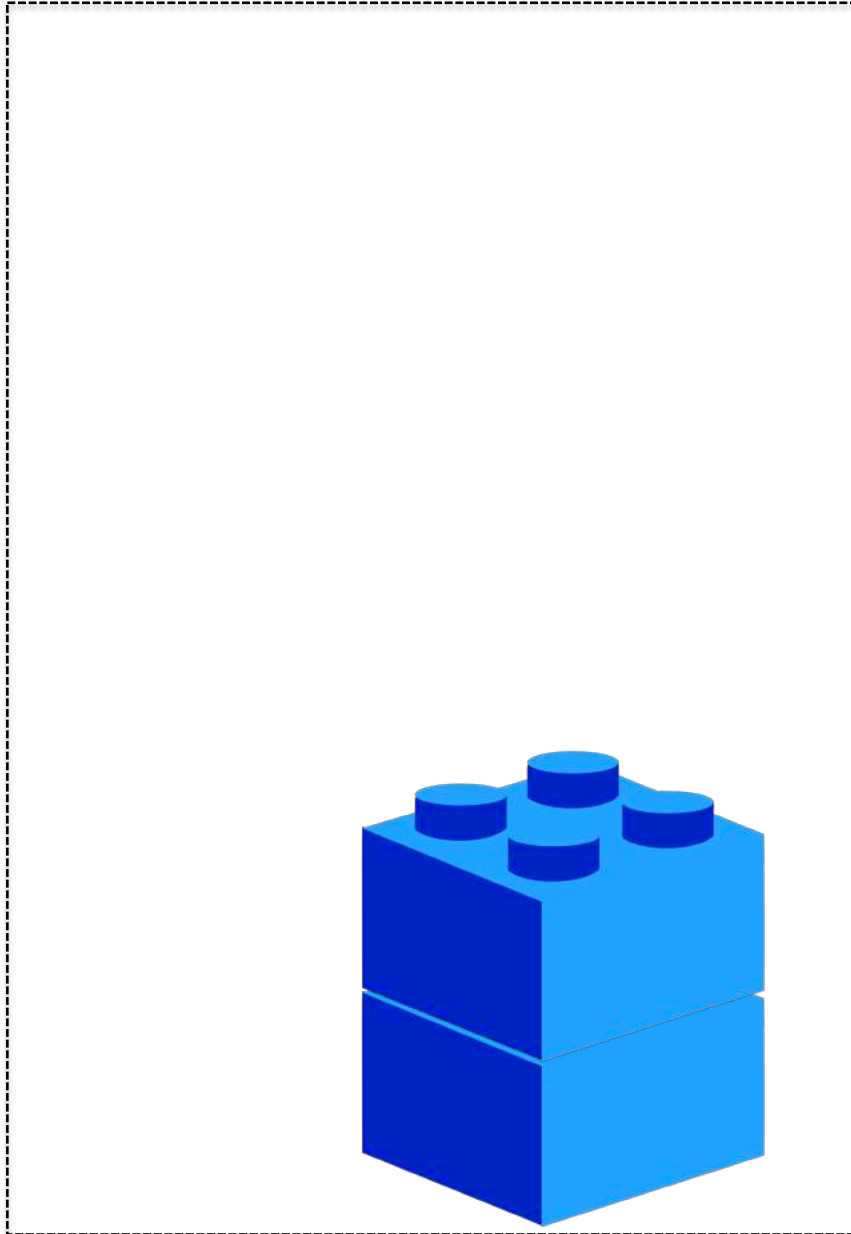
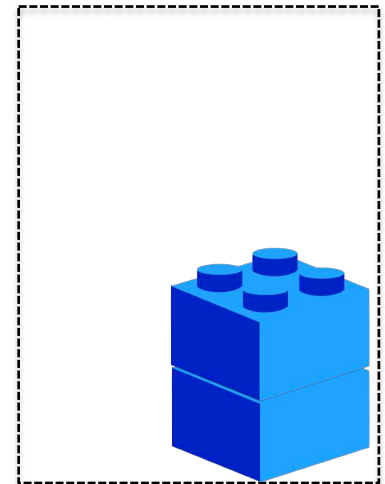
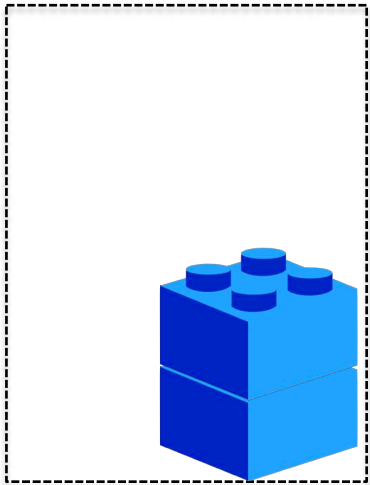
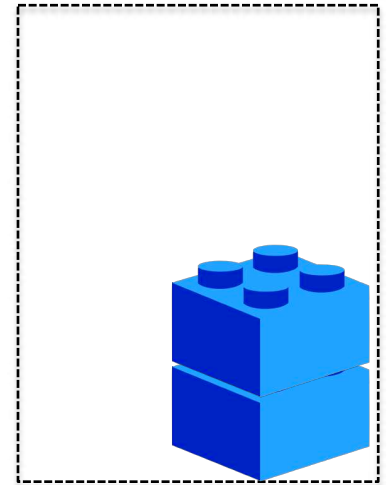
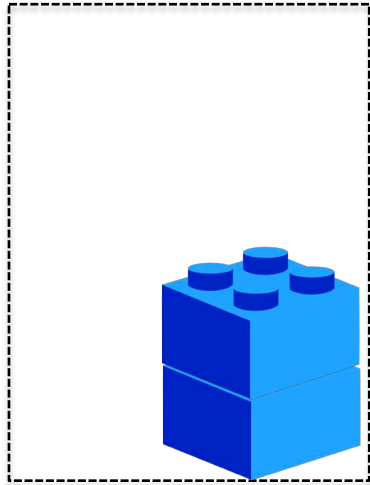




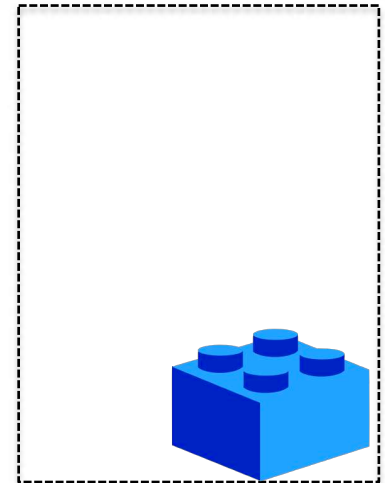
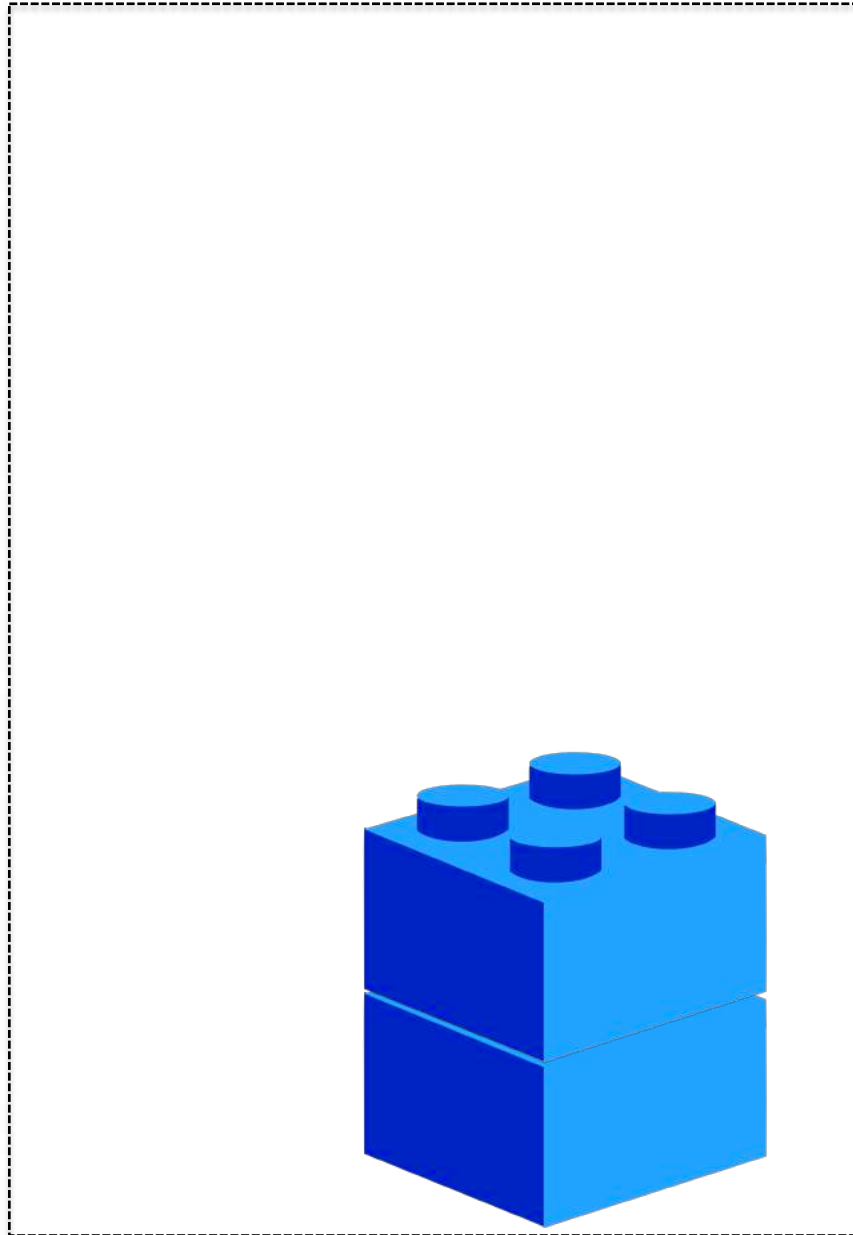
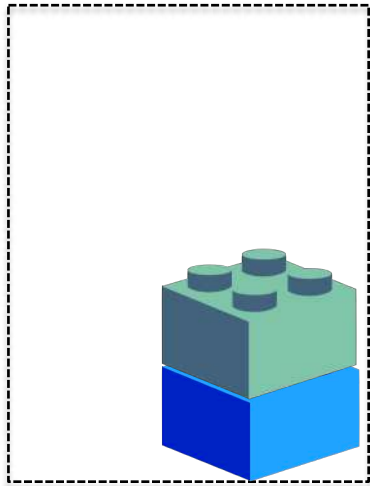
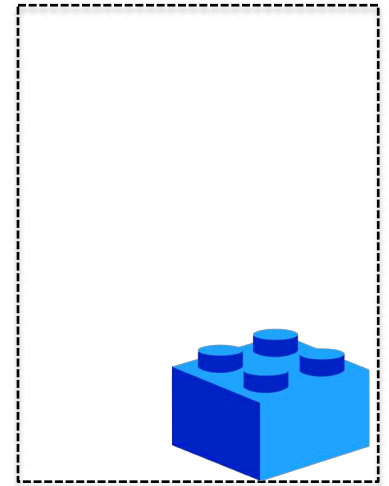
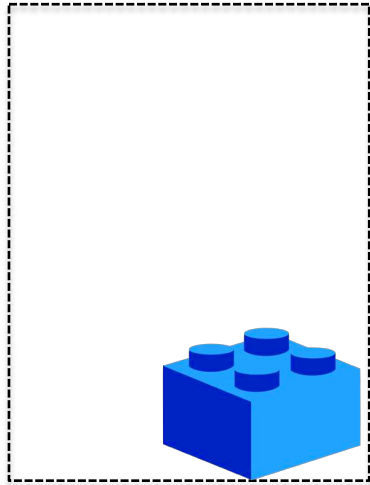
A node in a distributed network



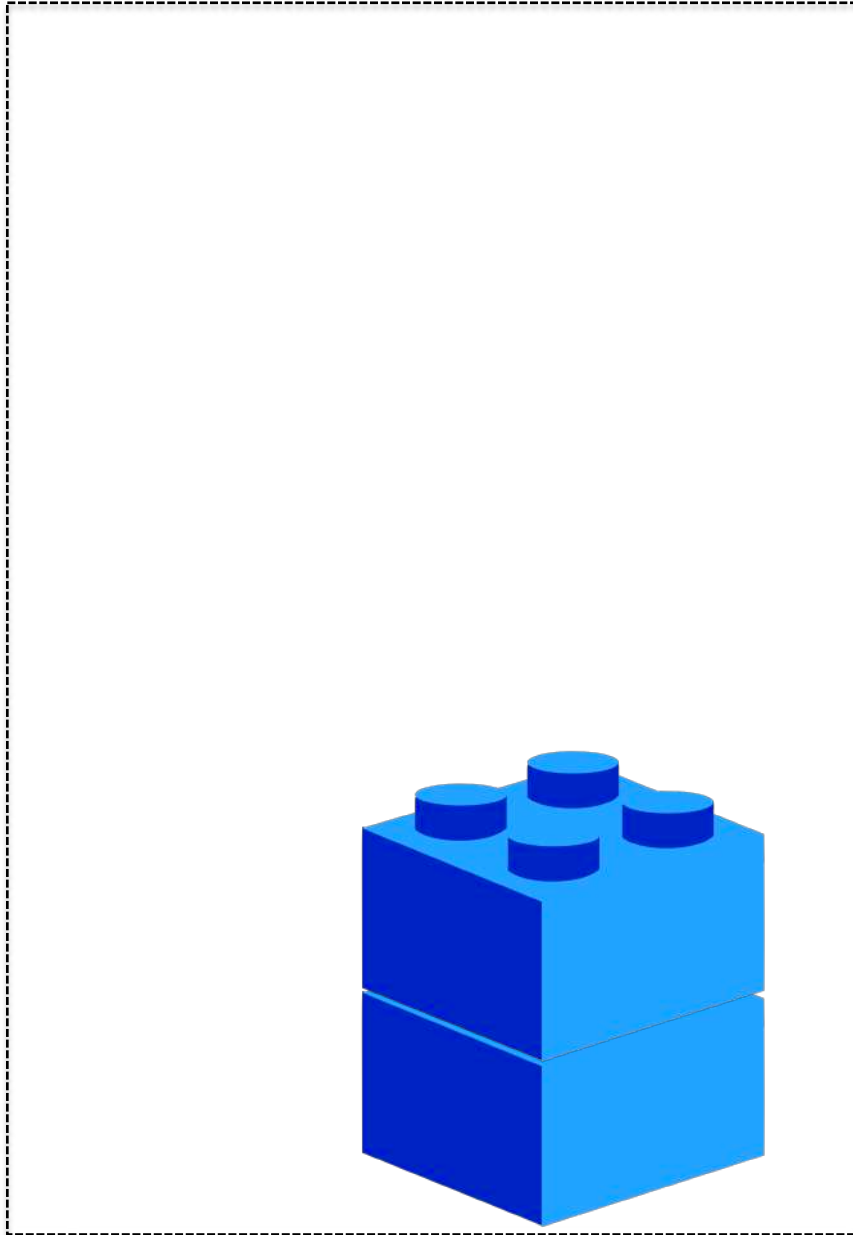
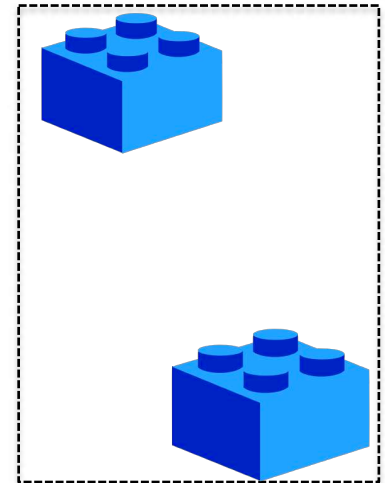
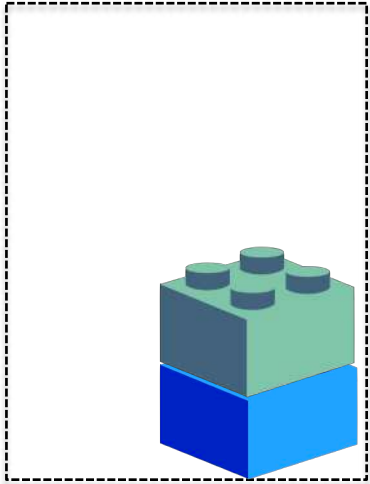
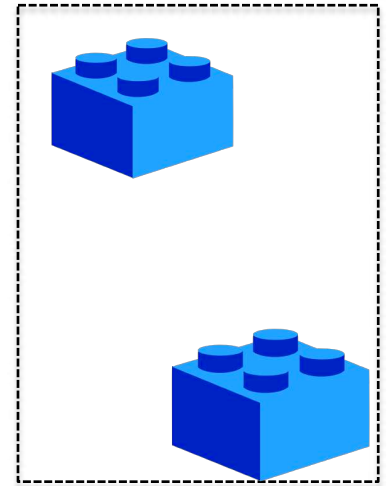
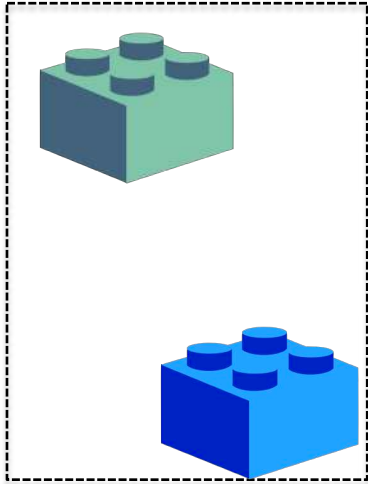
A node in a distributed network



A node in a distributed network

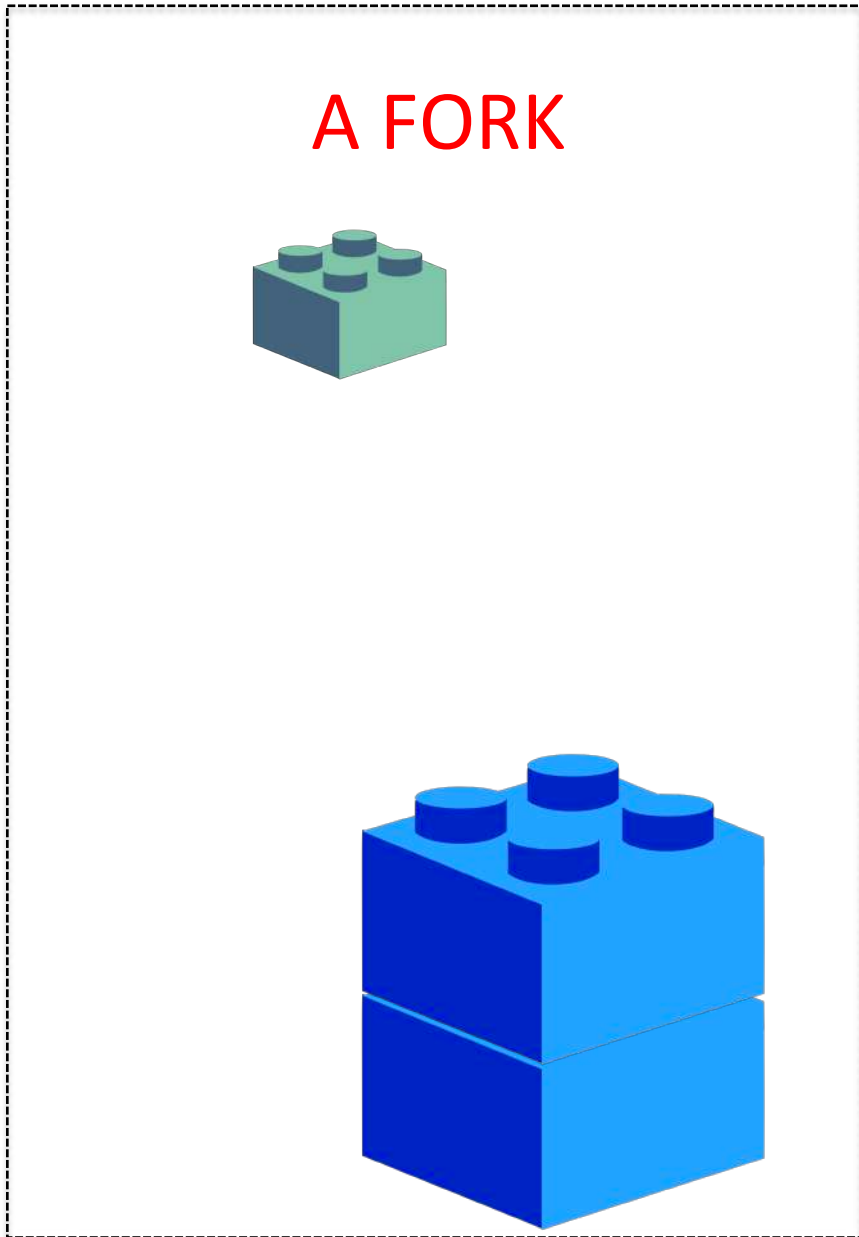
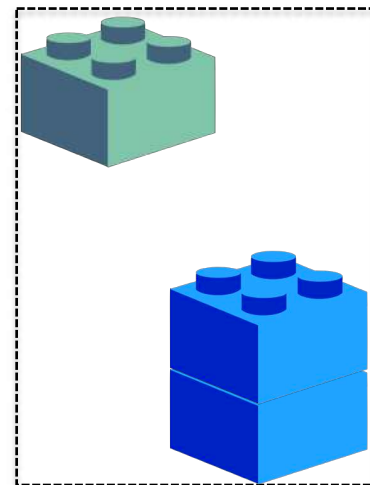
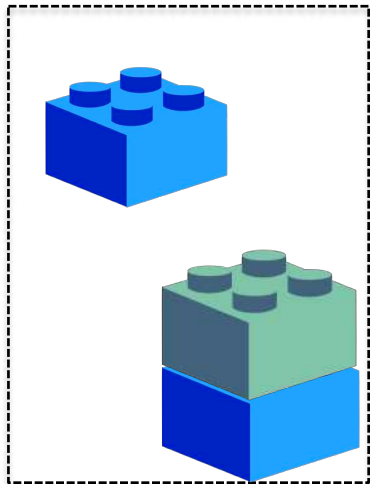
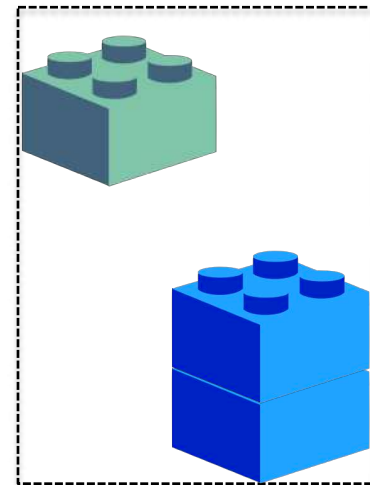
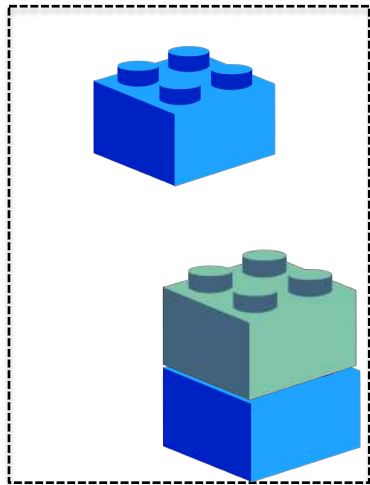


A node in a distributed network



A node in a distributed network

A FORK



Testing challenges

A complex distributed system, the usual challenge of infinitely many possible states

For example: synchronization, different kinds of transactions, unpredictable order of events, cryptography hard to mock, ...

QuickCheck

Instead of writing test cases....

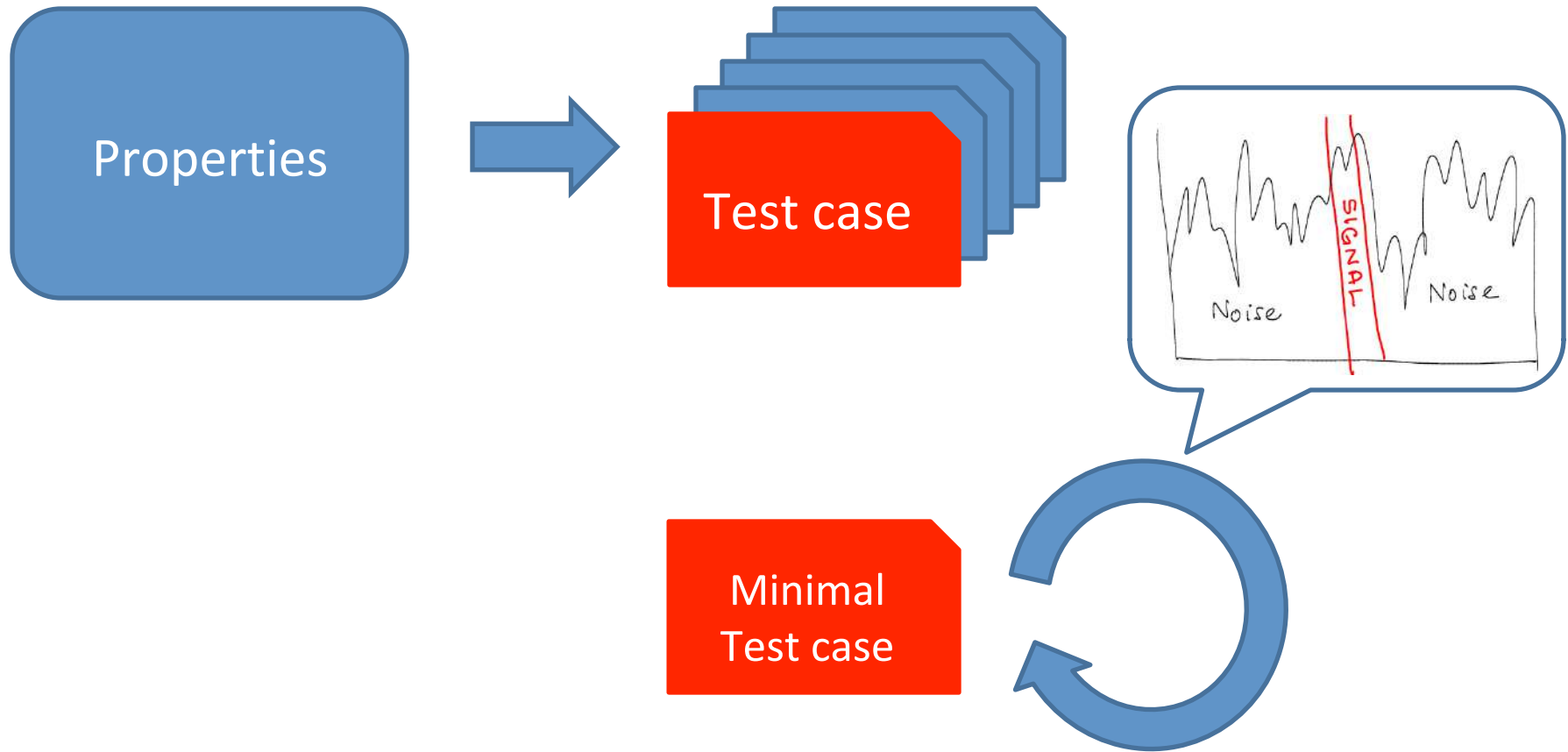
they are automatically generated from properties

Useful for

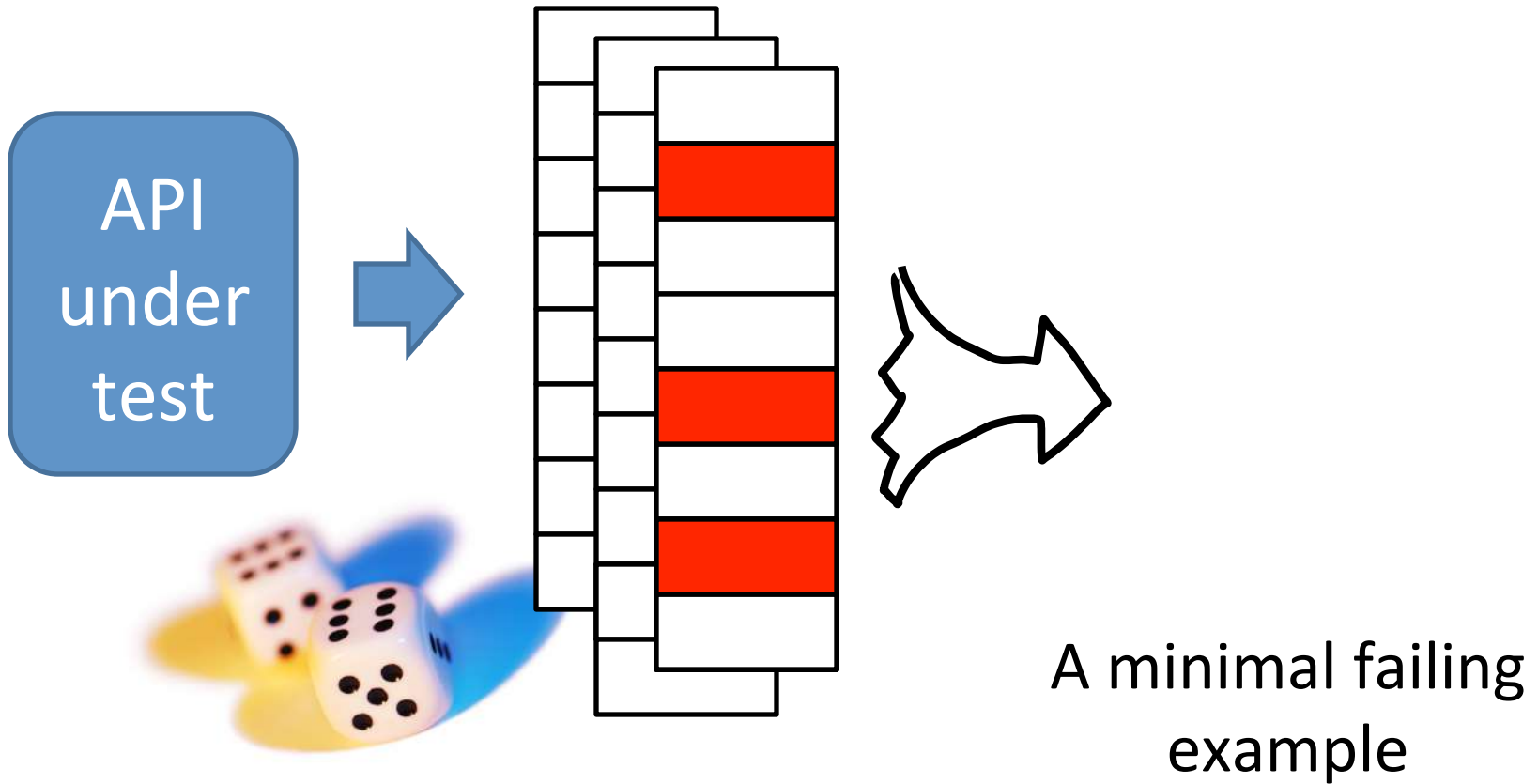
Unit Testing, Component Testing, System Testing

Less work, better testing, more fun

QuickCheck in a Nutshell



QuickCheck



DEMO

Property based testing

Blockchain properties

For all sequences of transactions: the total amount of tokens in the chain stays the same

Invalid transactions are not accepted on the chain (e.g. too low fee, too little in account, etc)

Property based testing

Distributed system

For all possible net-splits, crashes and forks, if network is stable long enough, nodes agree upon chain.

Conclusions

Blockchain testing

- generated tests found many corner cases
- on system level easy to add one feature and test thousands of new tests including feature
- hard to mock crypto

Questions

- <https://aeternity.com/>
- <https://github.com/aeternity/epoch/>
- <https://github.com/Quviq/epoch-eqc>

A node in a distributed network

synchronization

