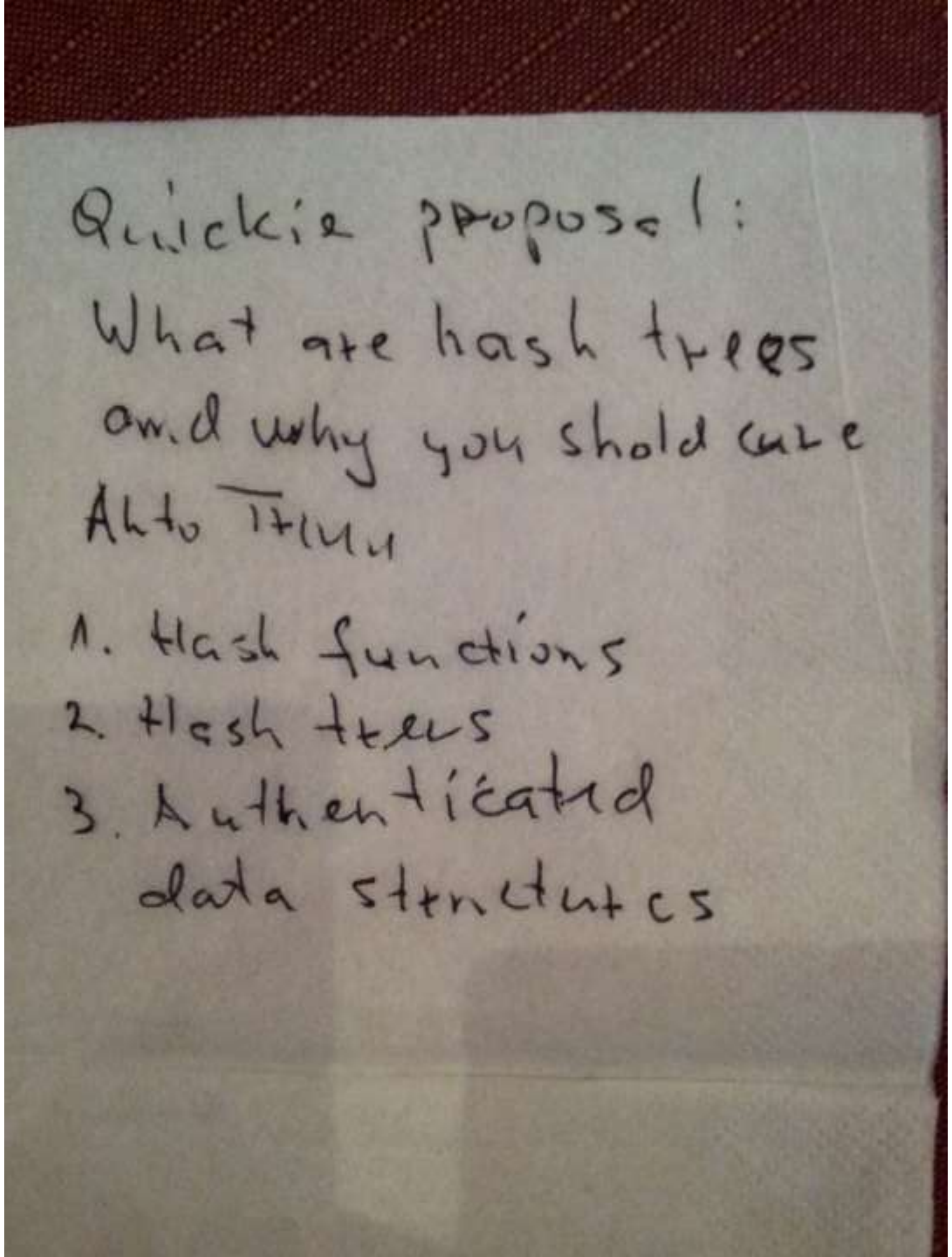
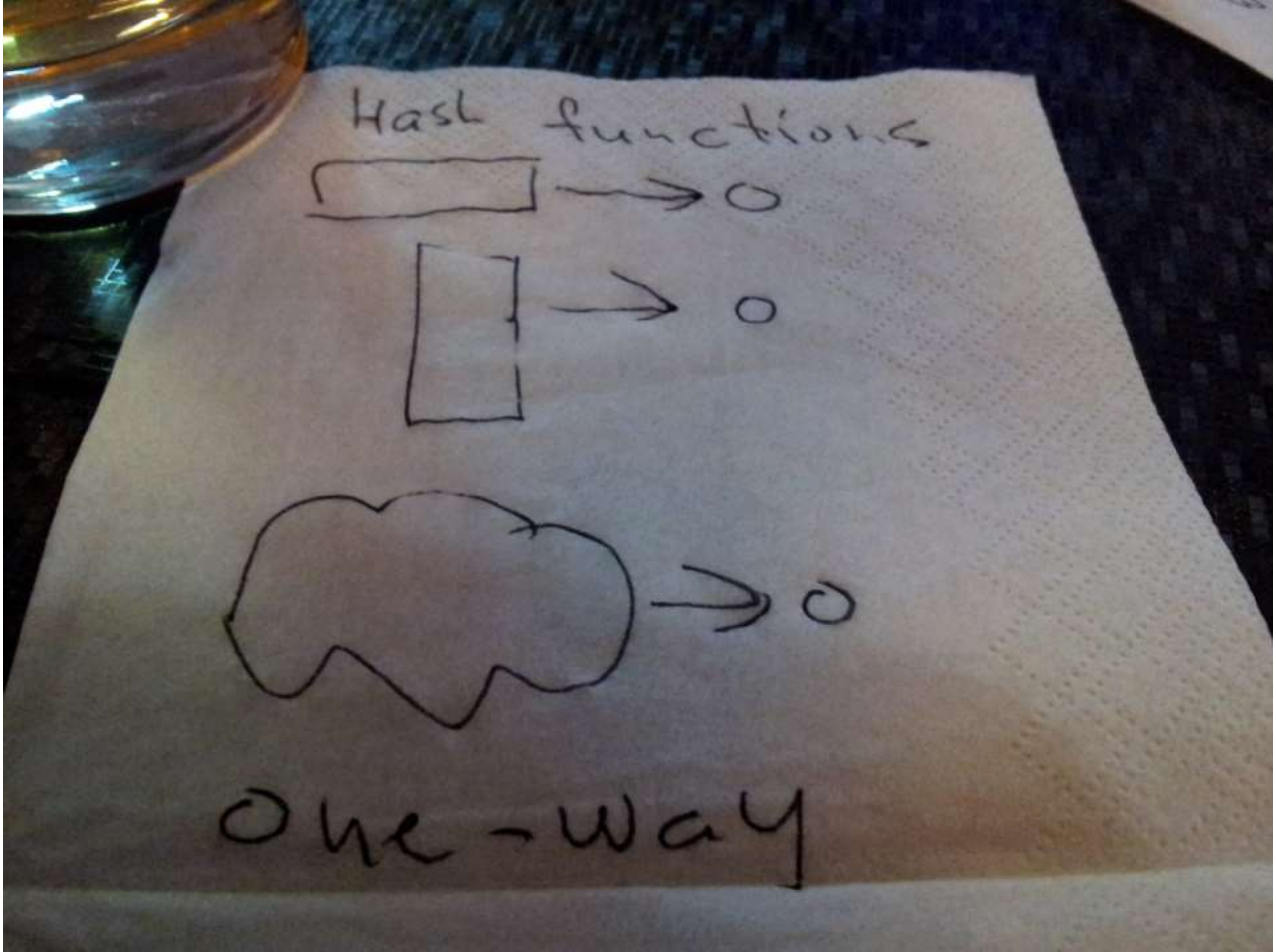


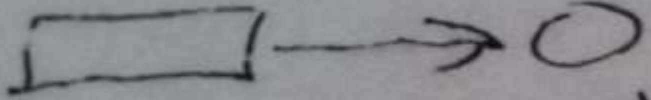
Quickie proposal:

What are hash trees and why you shold care

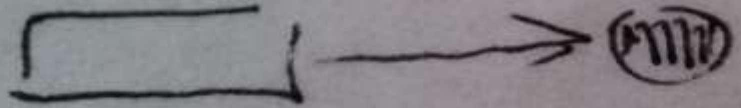
Ahto Truu

1. Hash functions
2. Hash trees
3. Authenticated data structures

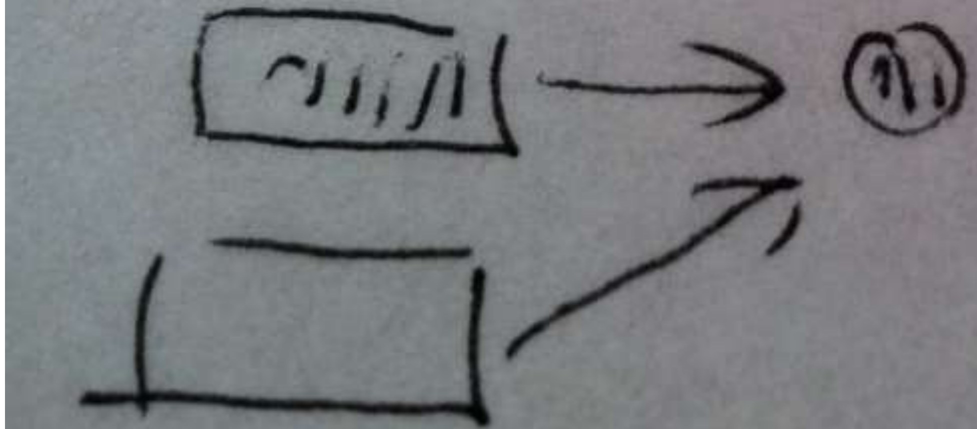

Hash functions
one-way

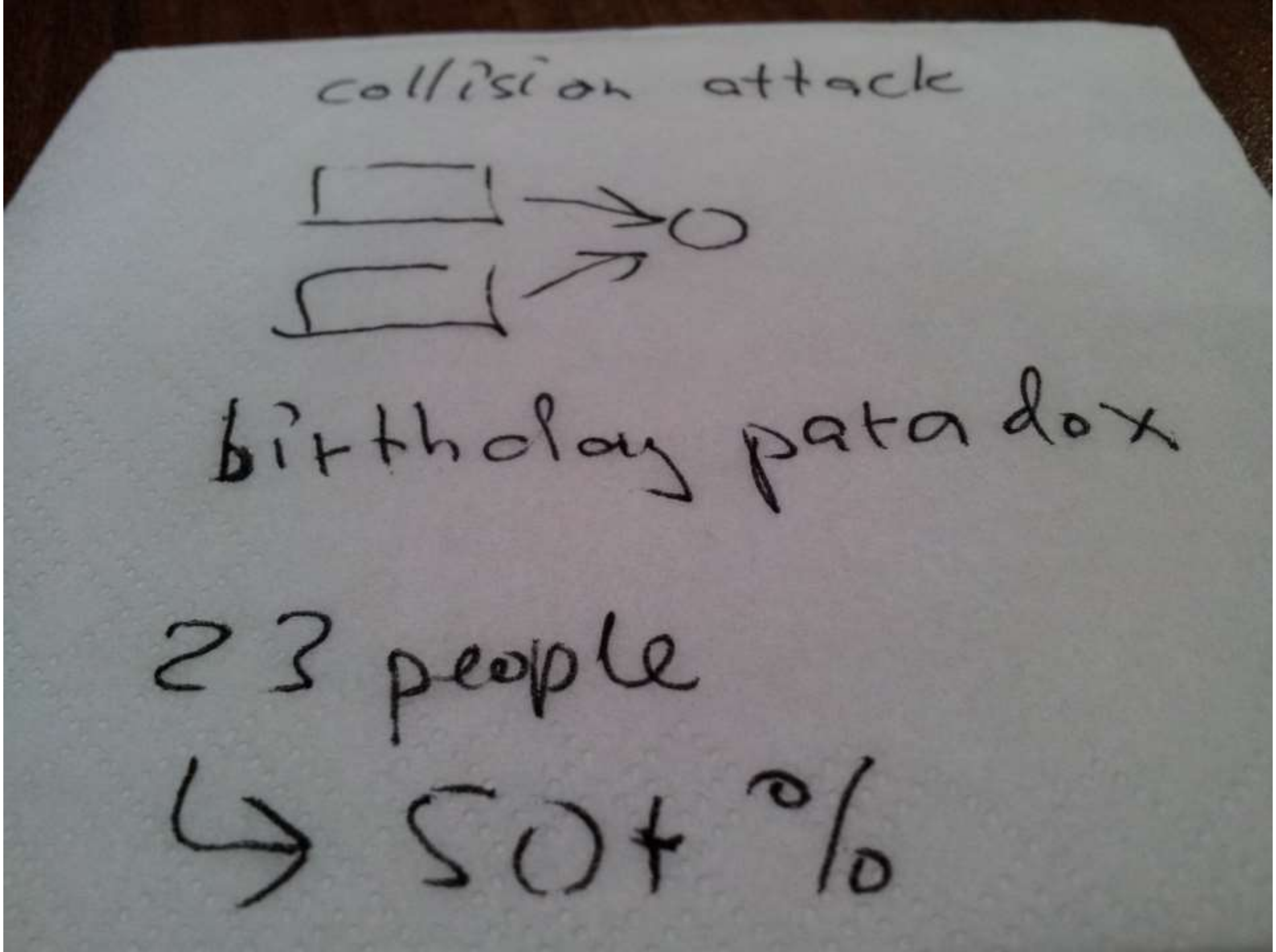


pre-image attack



second pre image attack



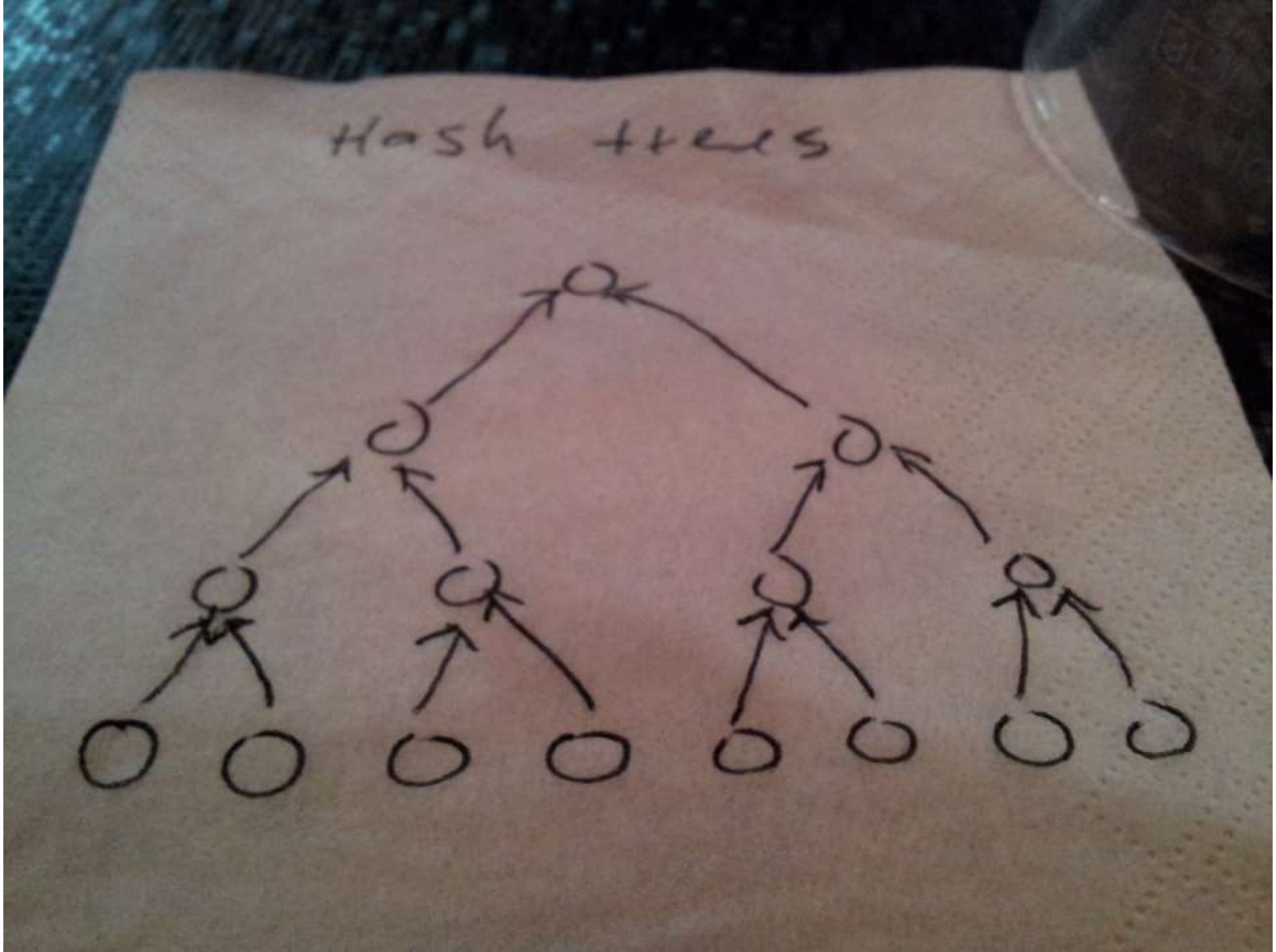


collision attack

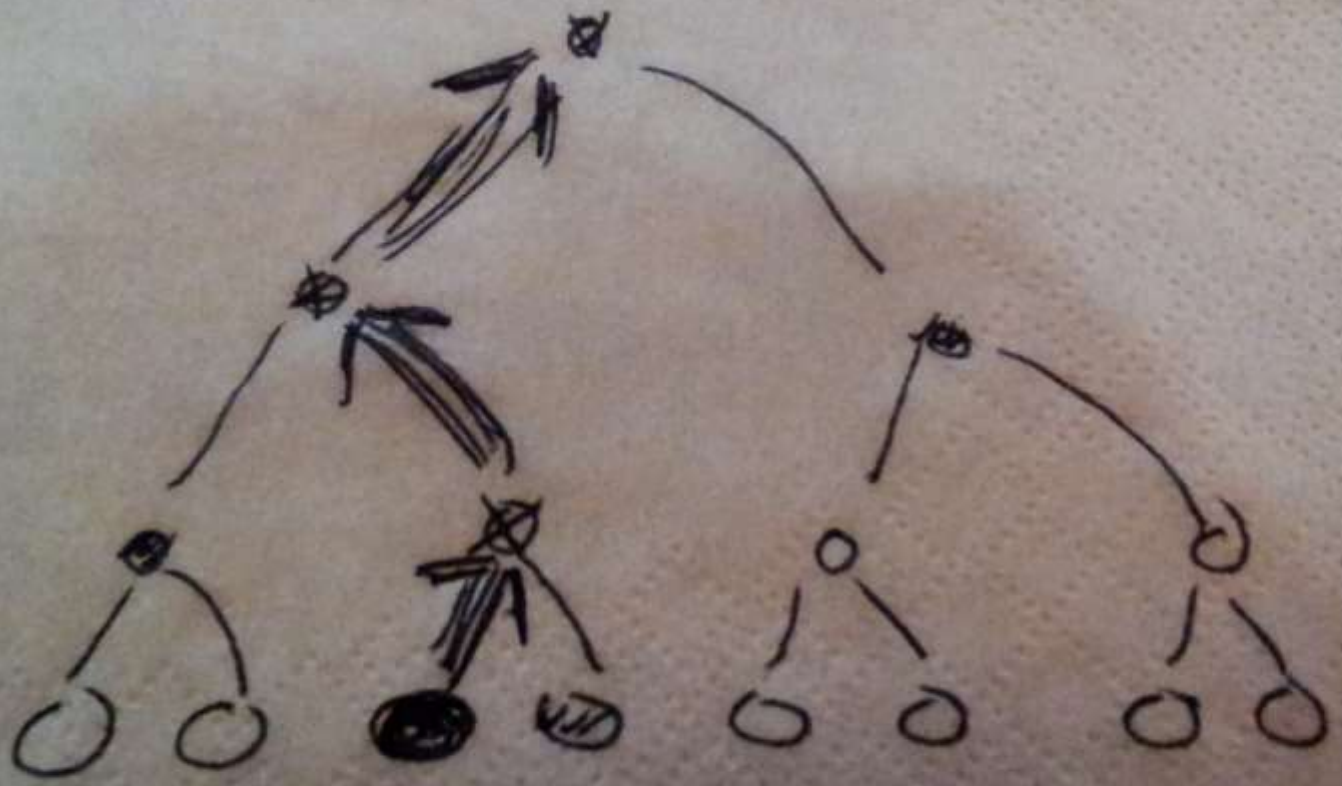
birthday paradox

23 people

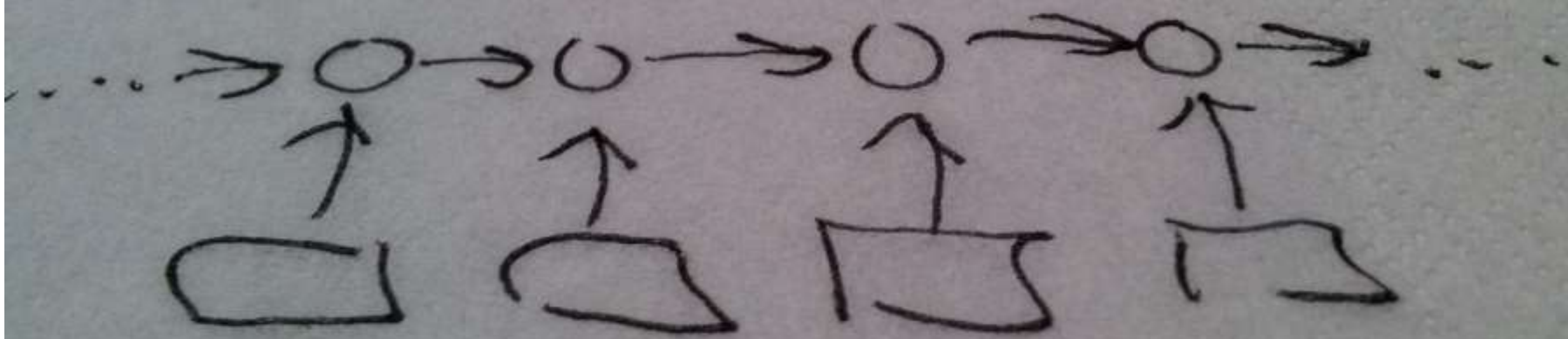
↳ 50+ %


Hash trees

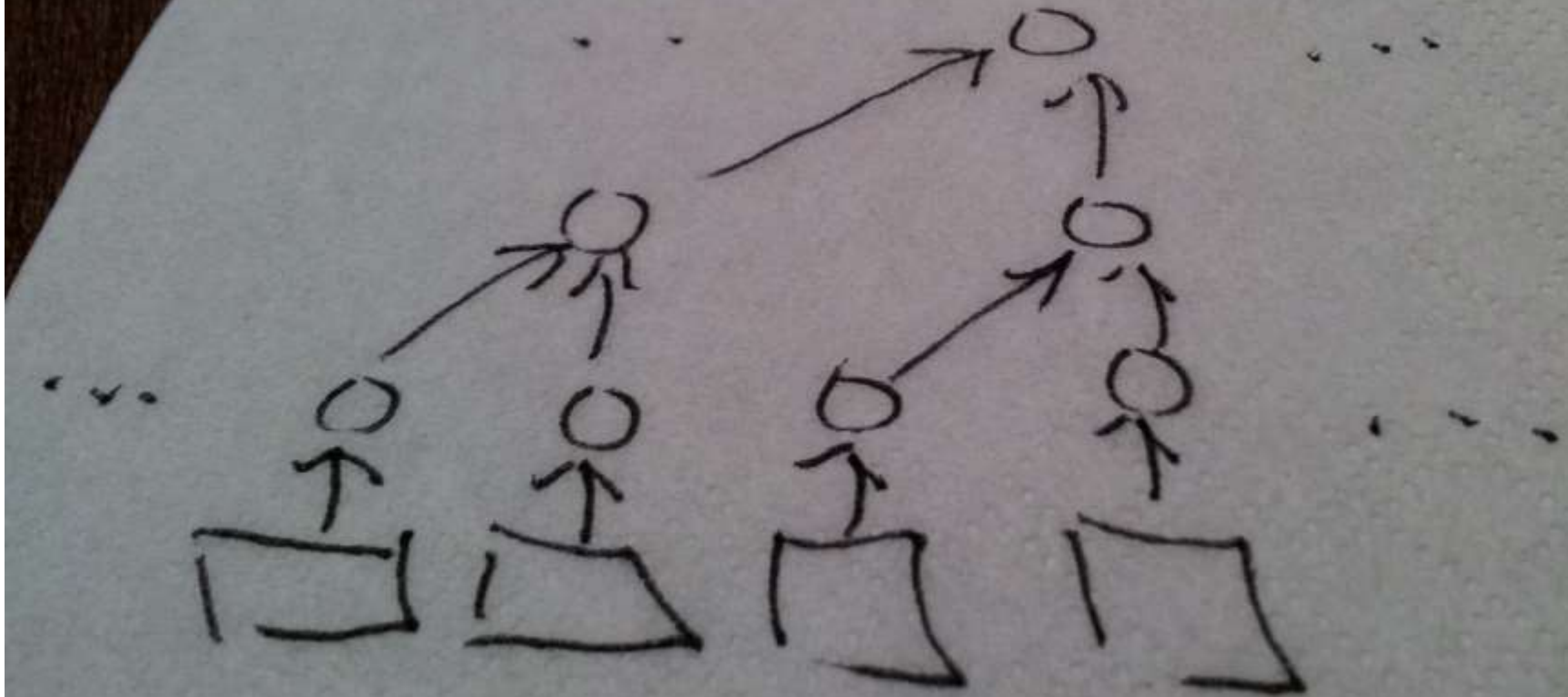
Hash chains

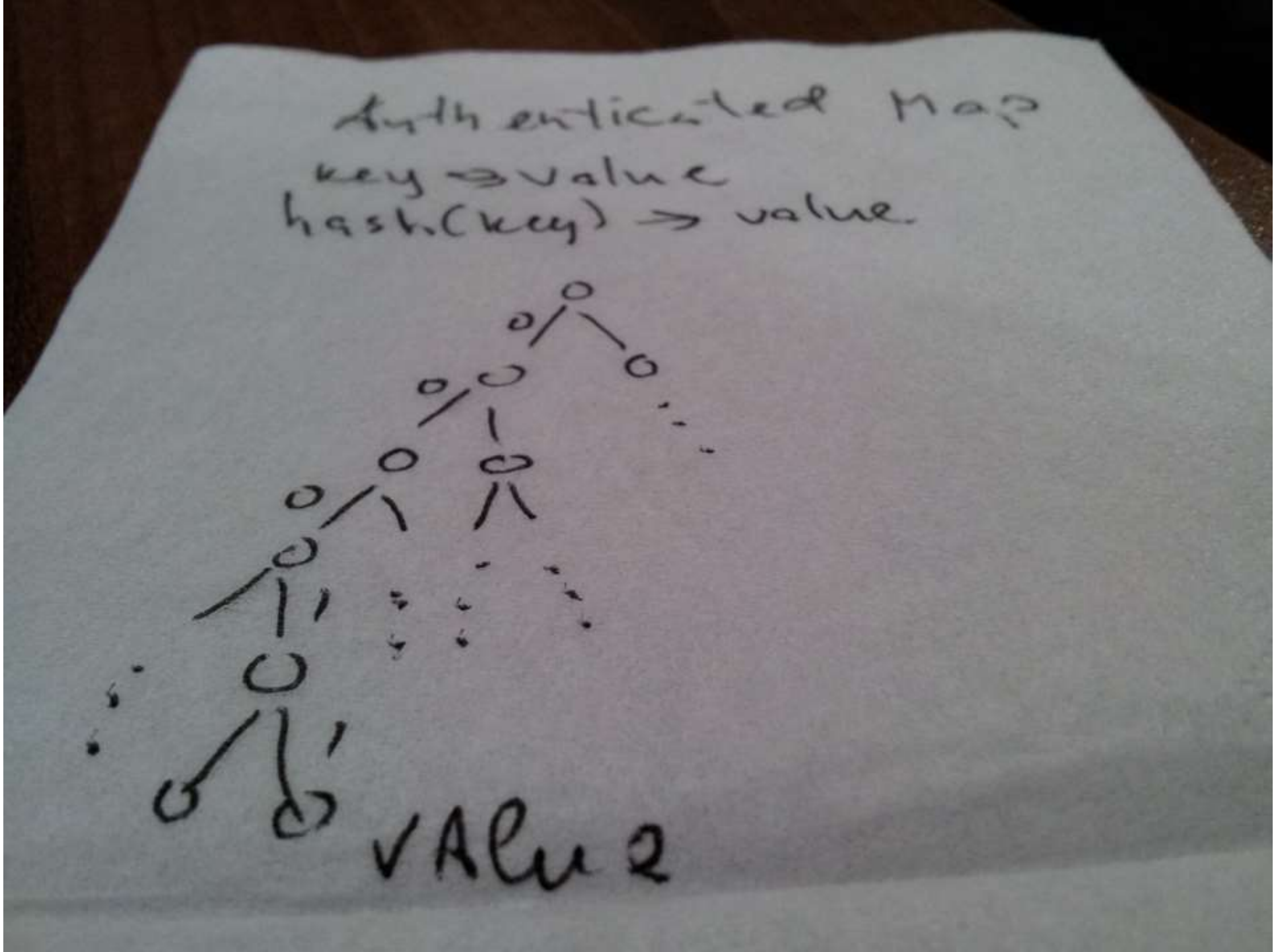


Authenticated log
naive a.k.a. blockchain



Authenticated log
tree - based



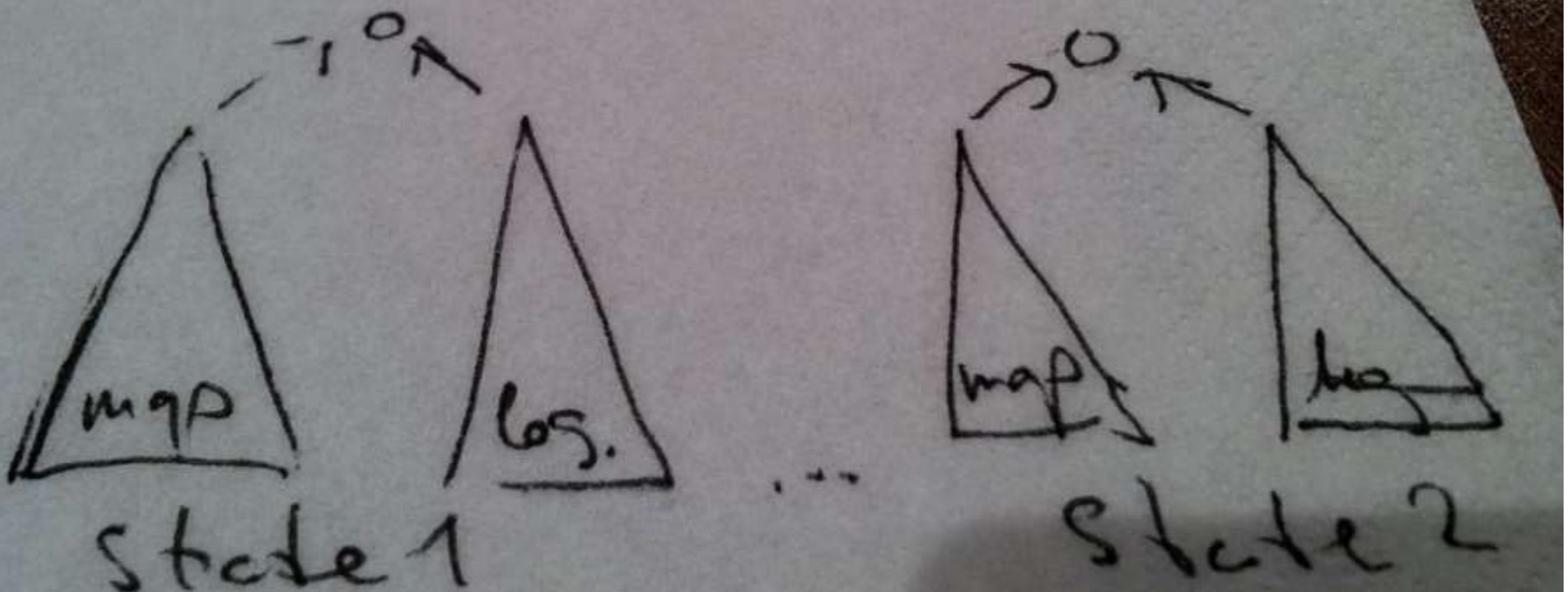


Authenticated Map

key → value

hash(key) → value

Authenticated Map
with modification
history a.k.a.
auth. log-backed map


map
log.
...
map
log
state 1
state 2