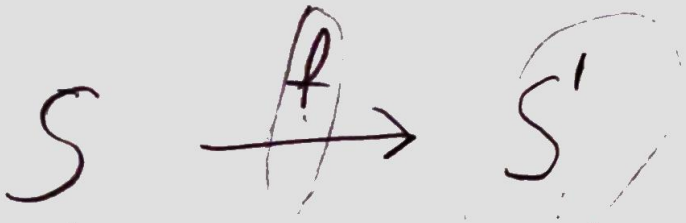
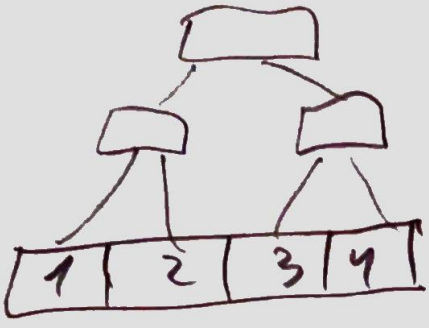
Data + Computations (state + transitions)



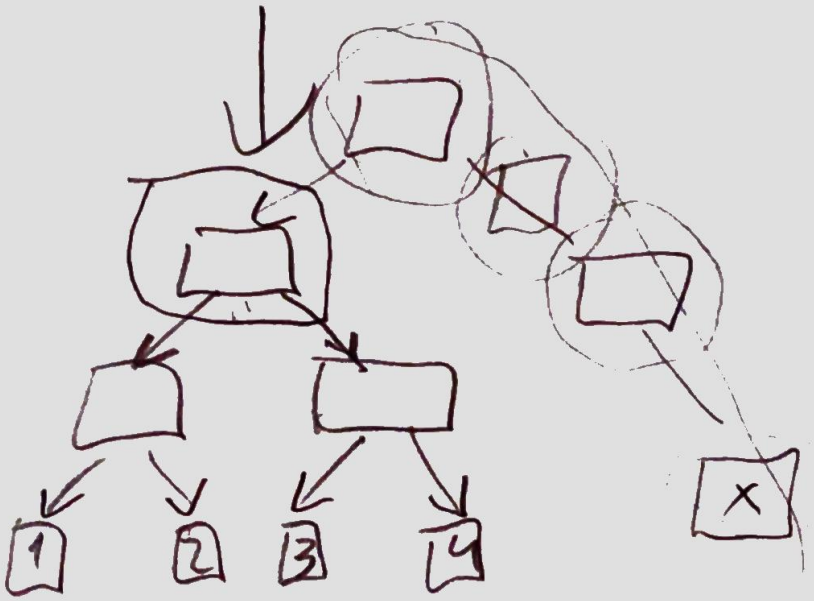
merkle hash ?trust

1. Pointer-based data structures



.append(x)

$S \xrightarrow{f} (S', M_{proof})$



$n^2 \log n$

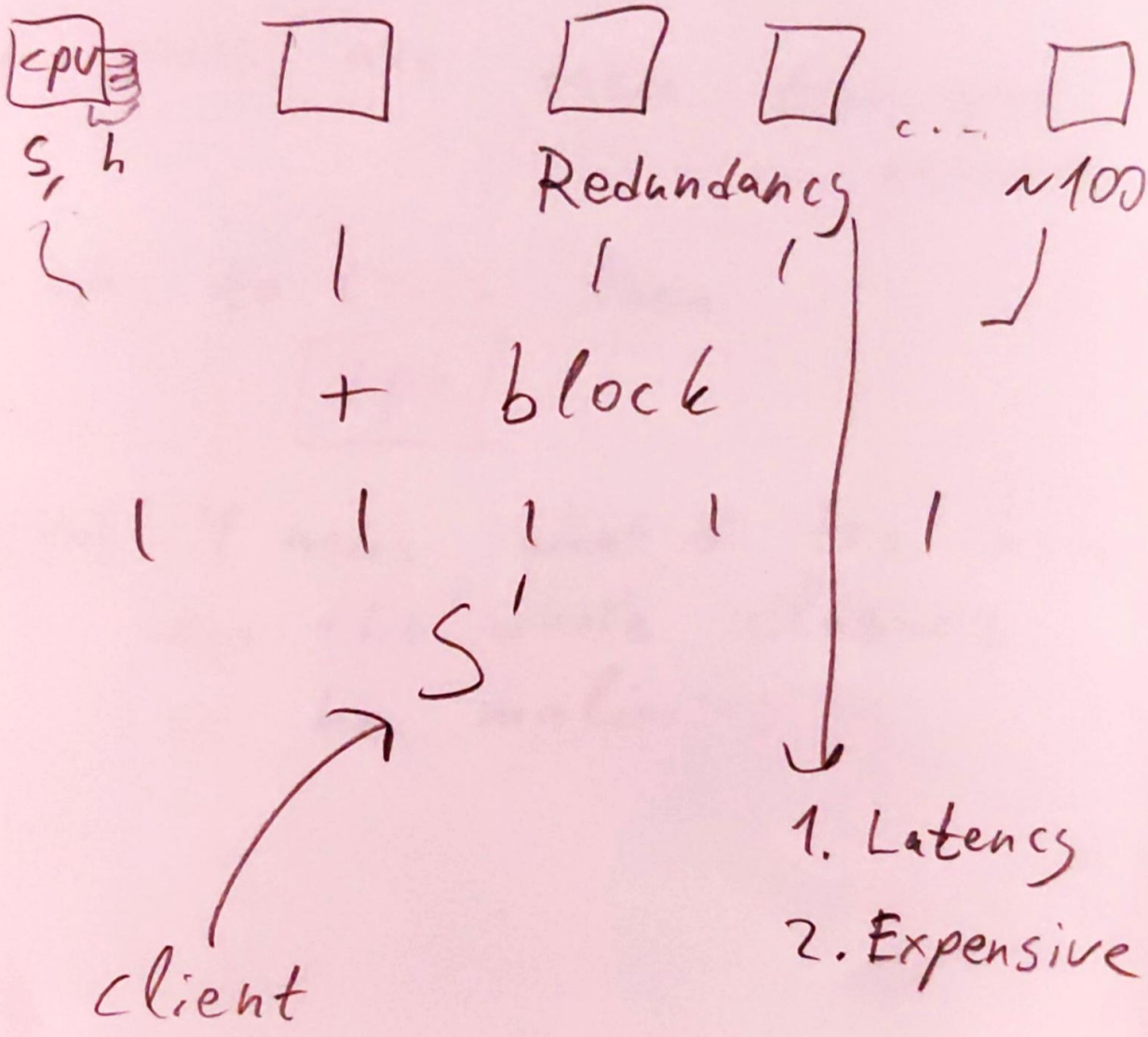
Comps on Client

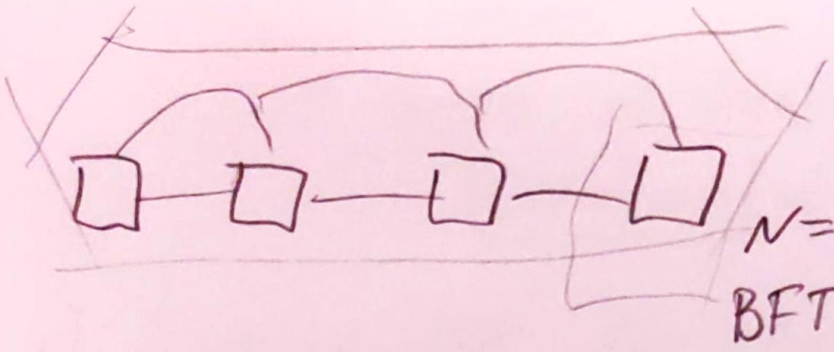
Châteauform'

2. Computation → bring to Data

Source of ? trust : blockchain

Majority appends block → block is valid





BFT consensus

if nodes are taken from open network

? why to trust them

[? pk]

? for 4 nodes, what is the chance for the whole cluster to be malicious

Trustworthy Party

Final Source of Trust

Ethereum ← WASM

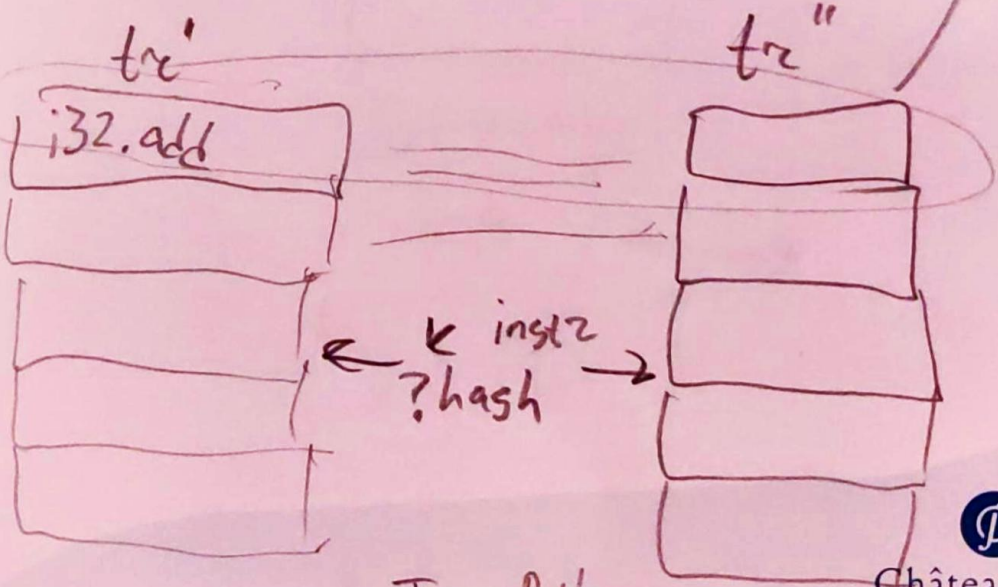
1) List of PK for Apps governed by Smart Contract

2) Verification game "consensus"

$n_{1,2,3}$: $S \xrightarrow{t} S'$

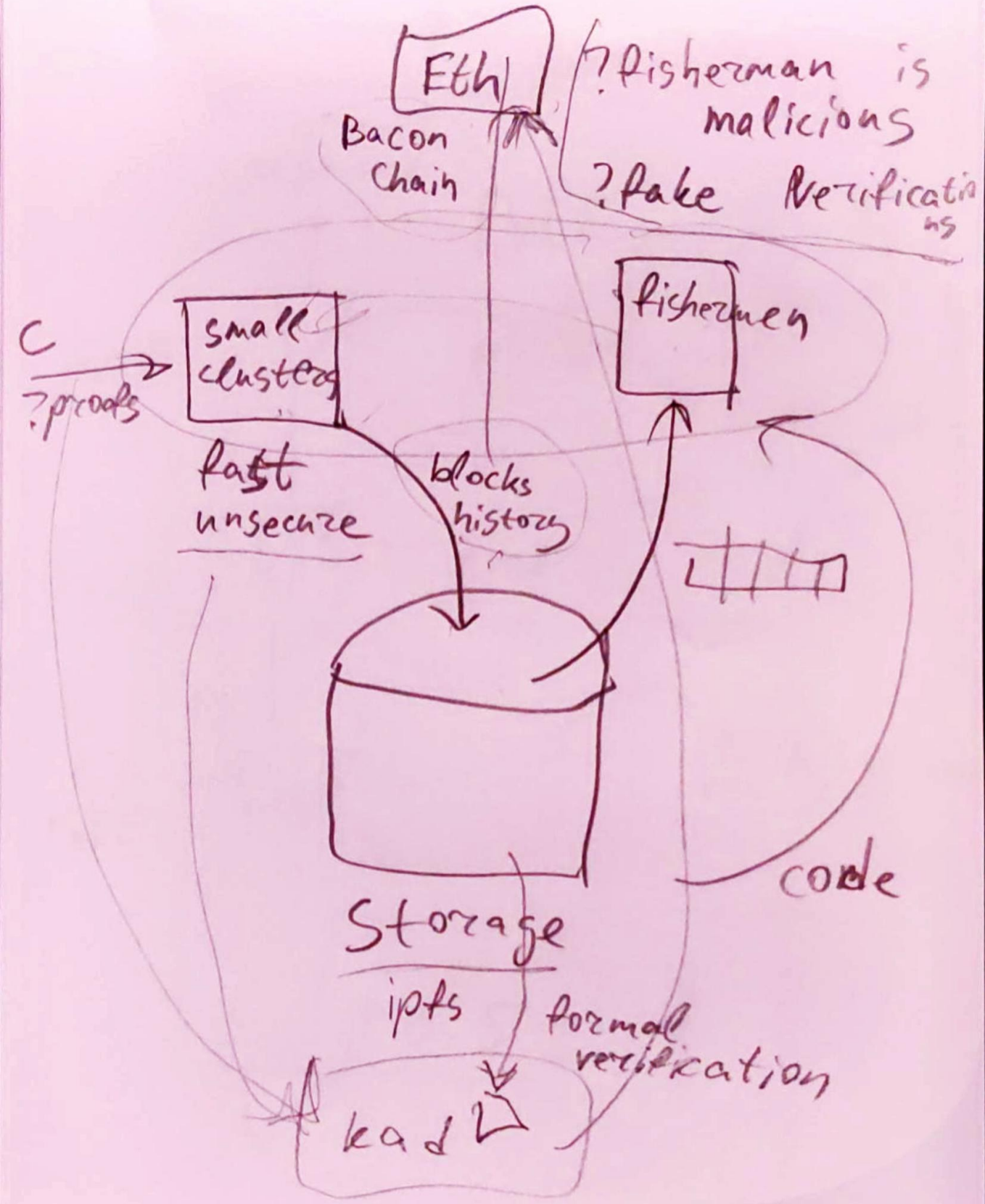
$\rightarrow n_4$: $S \xrightarrow{t} S''$

- deterministic computations
- final judge

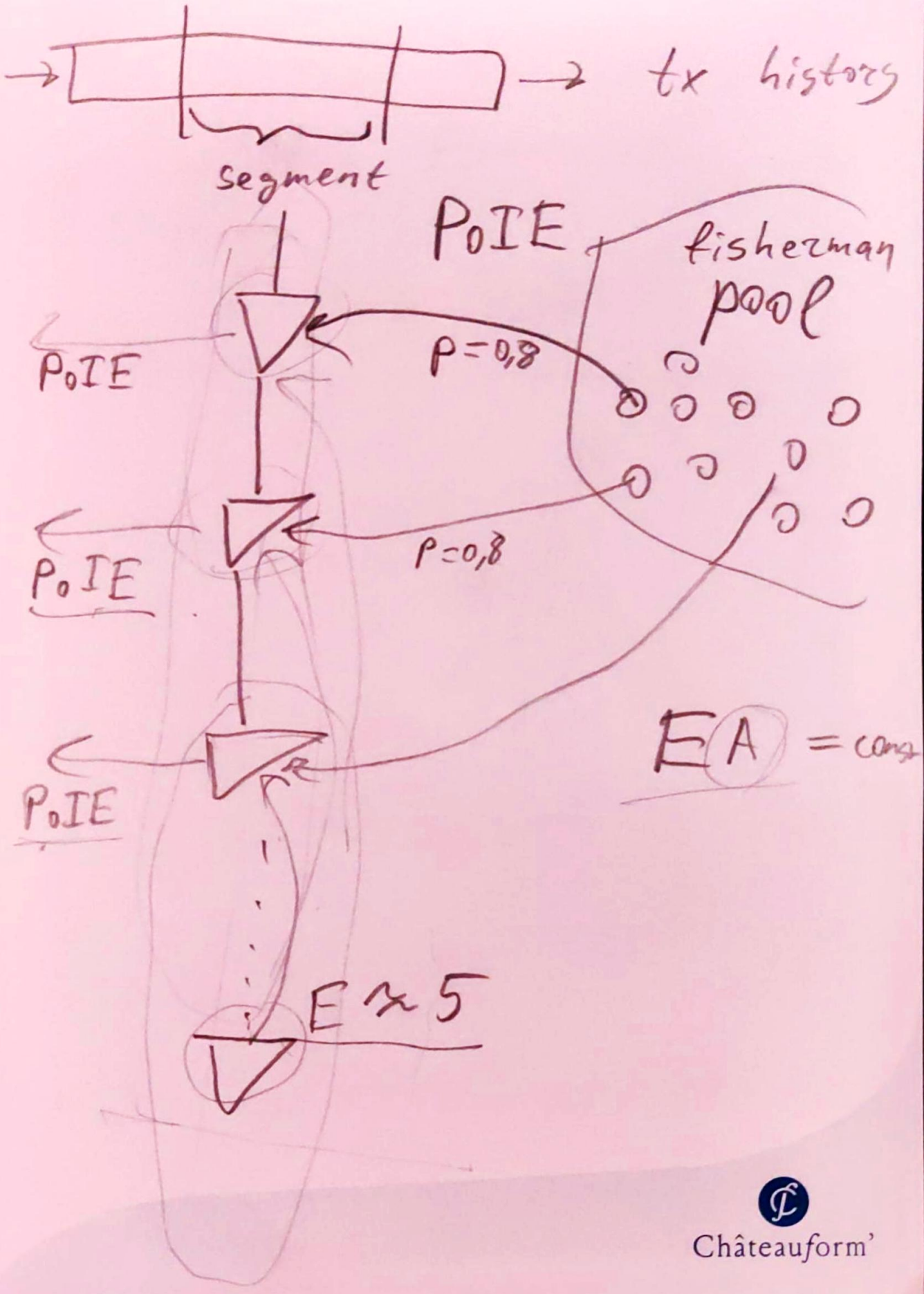


TrueBit

Châteauform'



Châteauform'



Châteauform'

Decoupling

Block Producer

from

Finality Gadget

3. zk-proofs
   ↳ good for small

4. CRDT
   ↳ good for p2p / local