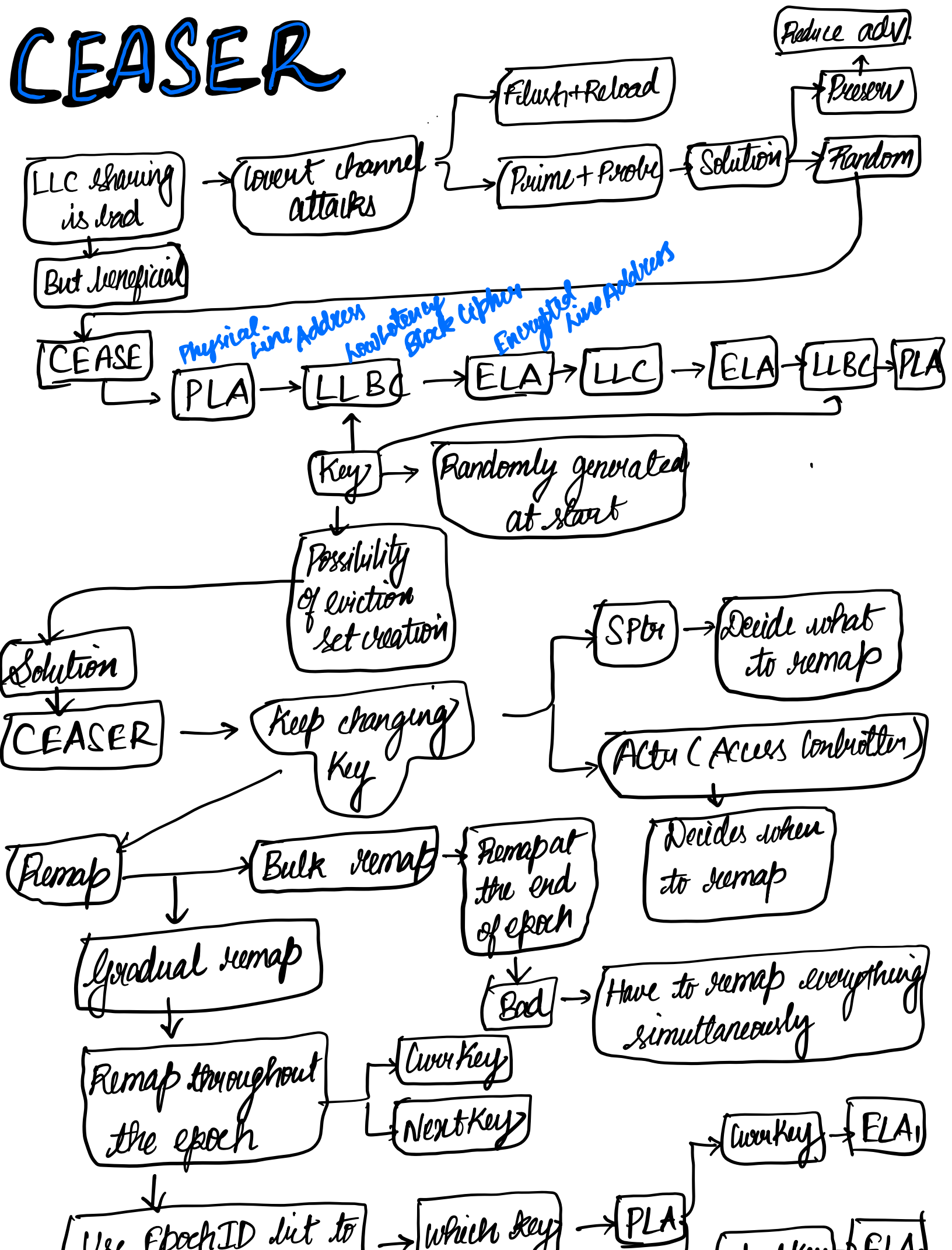
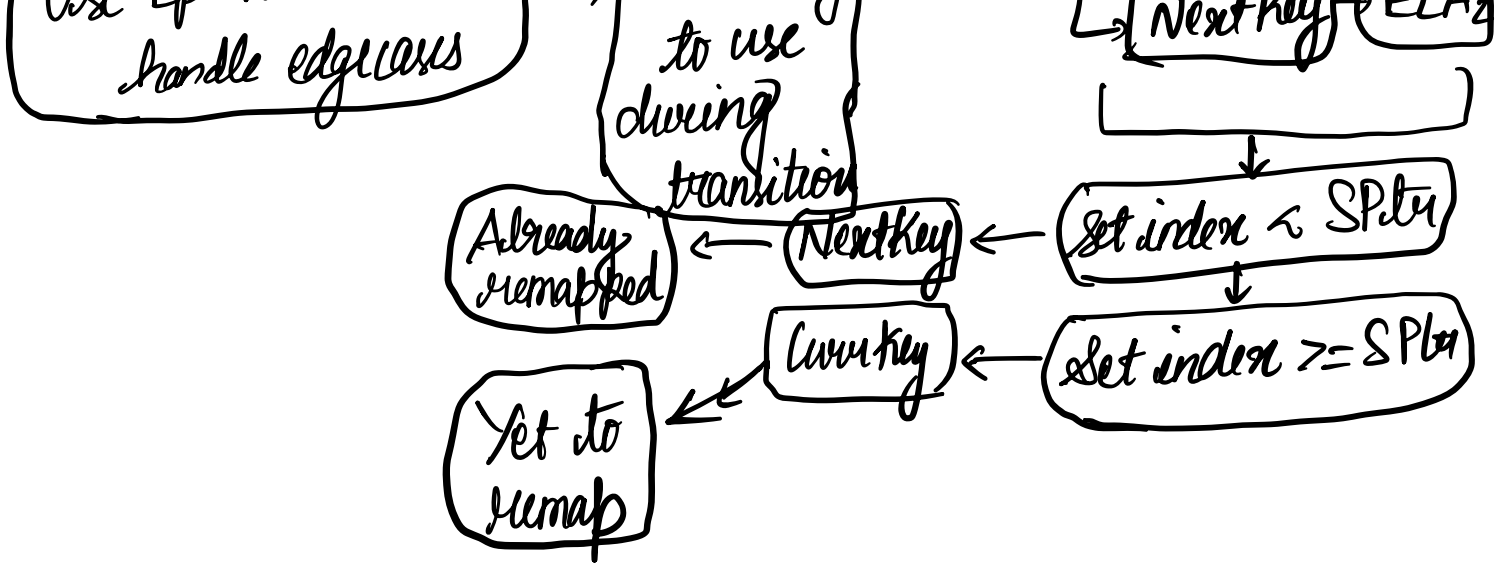
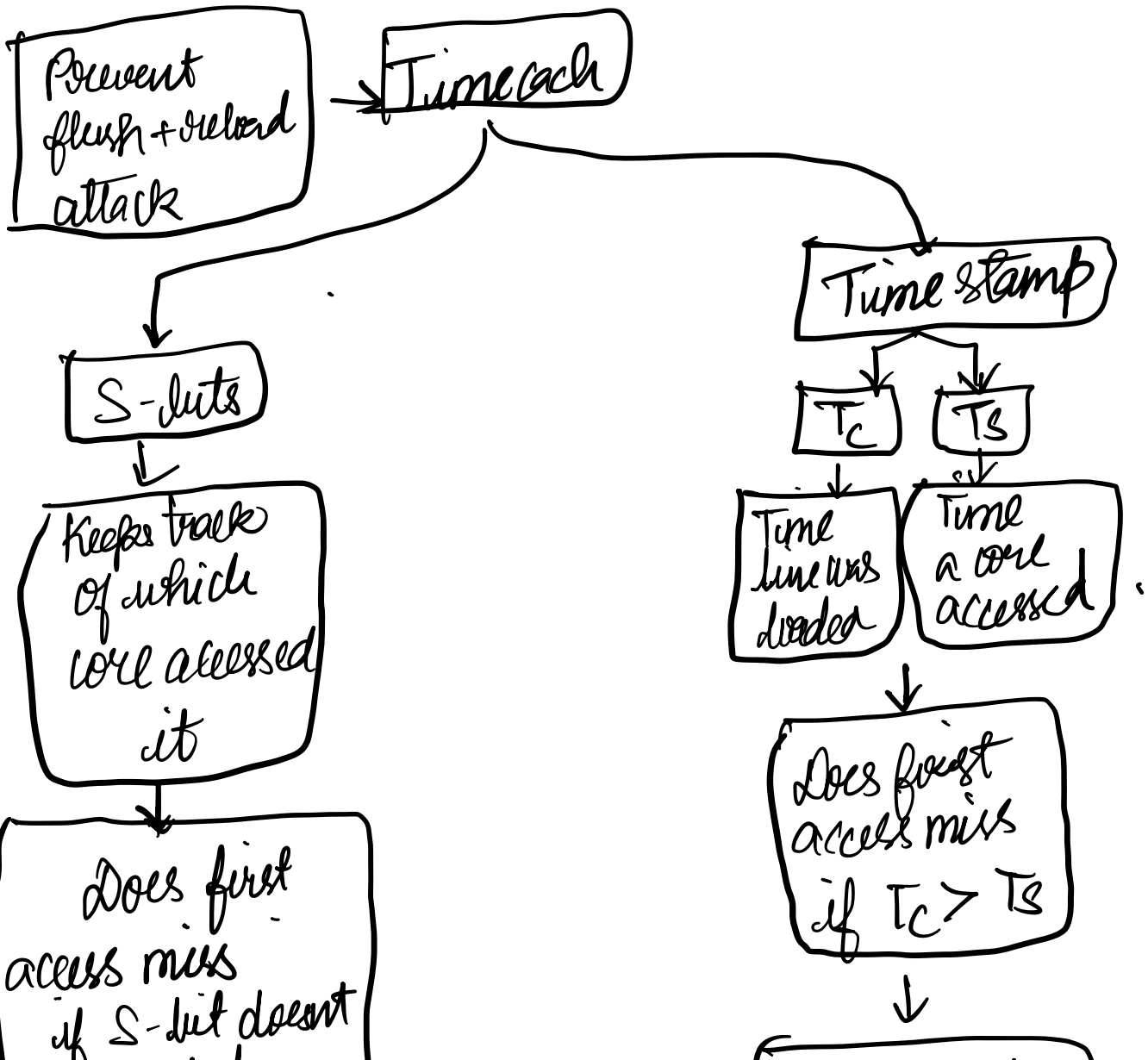
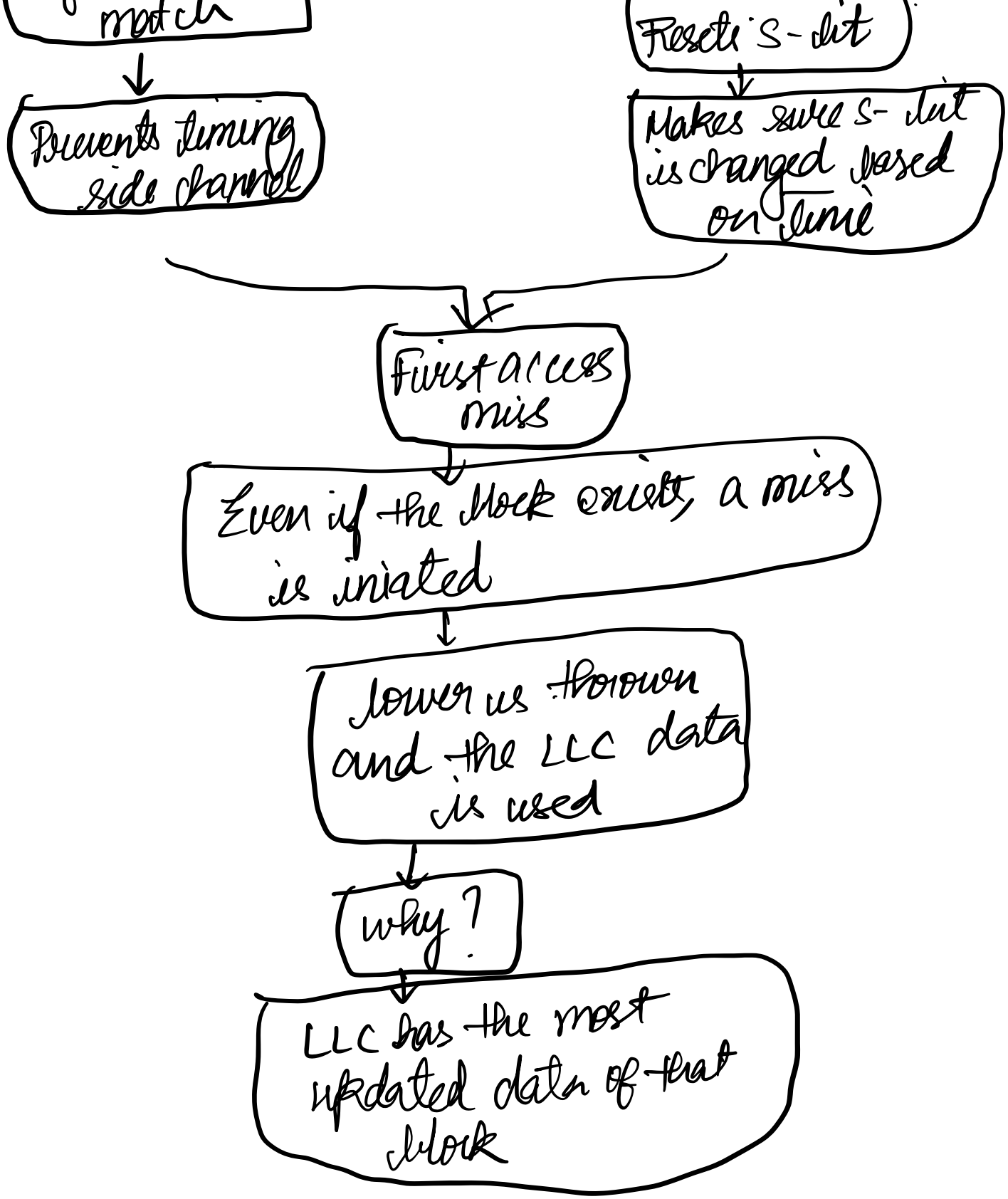
CEASER


Reduce adv.
Preserv
Flush+Reload
LLC sharing is bad
Covert channel attacks
Prime+Probe
Solution
Random
But beneficial
CEASE
Physical Line Address
Low latency Block Cipher
Encrypted Line Address
PLA
LLBC
ELA
LLC
ELA
LLBC
PLA
Key
Randomly generated at start
Possibility of eviction set creation
Solution
CEASER
Keep changing Key
SPtr
Decide what to remap
ACtr (Access Controller)
Decides when to remap
Remap
Bulk remap
Remap at the end of epoch
Bad
Have to remap everything simultaneously
Gradual remap
Remap throughout the epoch
CurrKey
NextKey
CurrKey
ELA
Use EpochID bit to
which key
PLA


handle edgecases
to use during transition
Already remapped
NextKey
Set index < SPtr
Yet to remap
CurrKey
Set index >= SPtr

TIMECACHE :


Prevent flush+reload attack
Timecach
S-bits
Keeps track of which core accessed it
Does first access miss if S-bit doesnt
Time stamp
Tc
Ts
Time linewas loaded
Time a core accessed
Does first access miss if Tc > Ts


mode
Prevents timing side channel
Resets S-bit
Makes sure S-bit is changed based on time
First access miss
Even if the block exists, a miss is initiated
lower us known and the LLC data is used
why?
LLC has the most updated data of that block