n, t are malicious, committing a single txn.

↳ Committing a single txn ⟹ many

↳ Notion of rounds; message delays

↳ fixed set of parties.

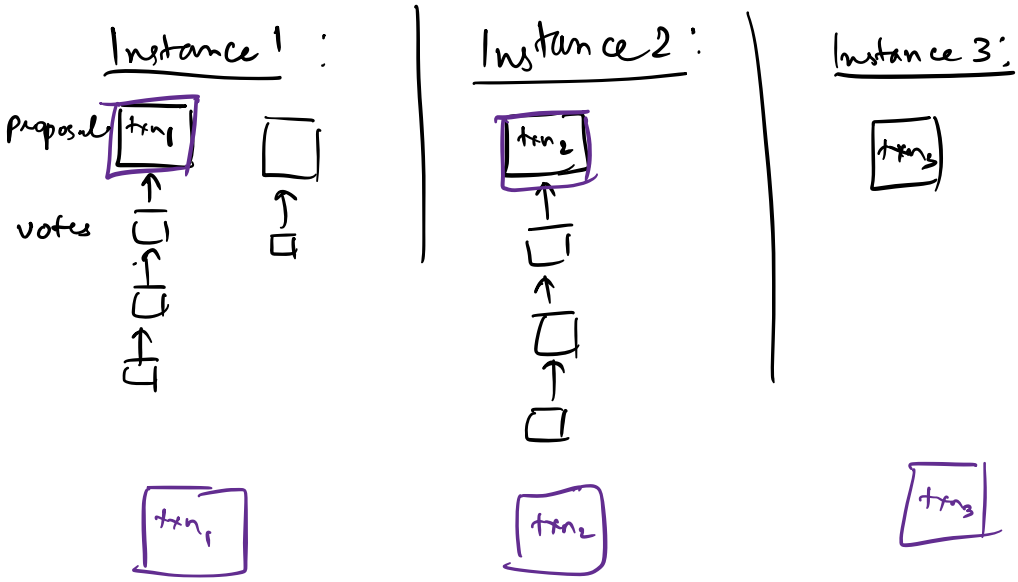
Committing a single txn to many txns:

Large blocks:

↳ we may not know of all txns.

↳ they take a lot of time to propagate.

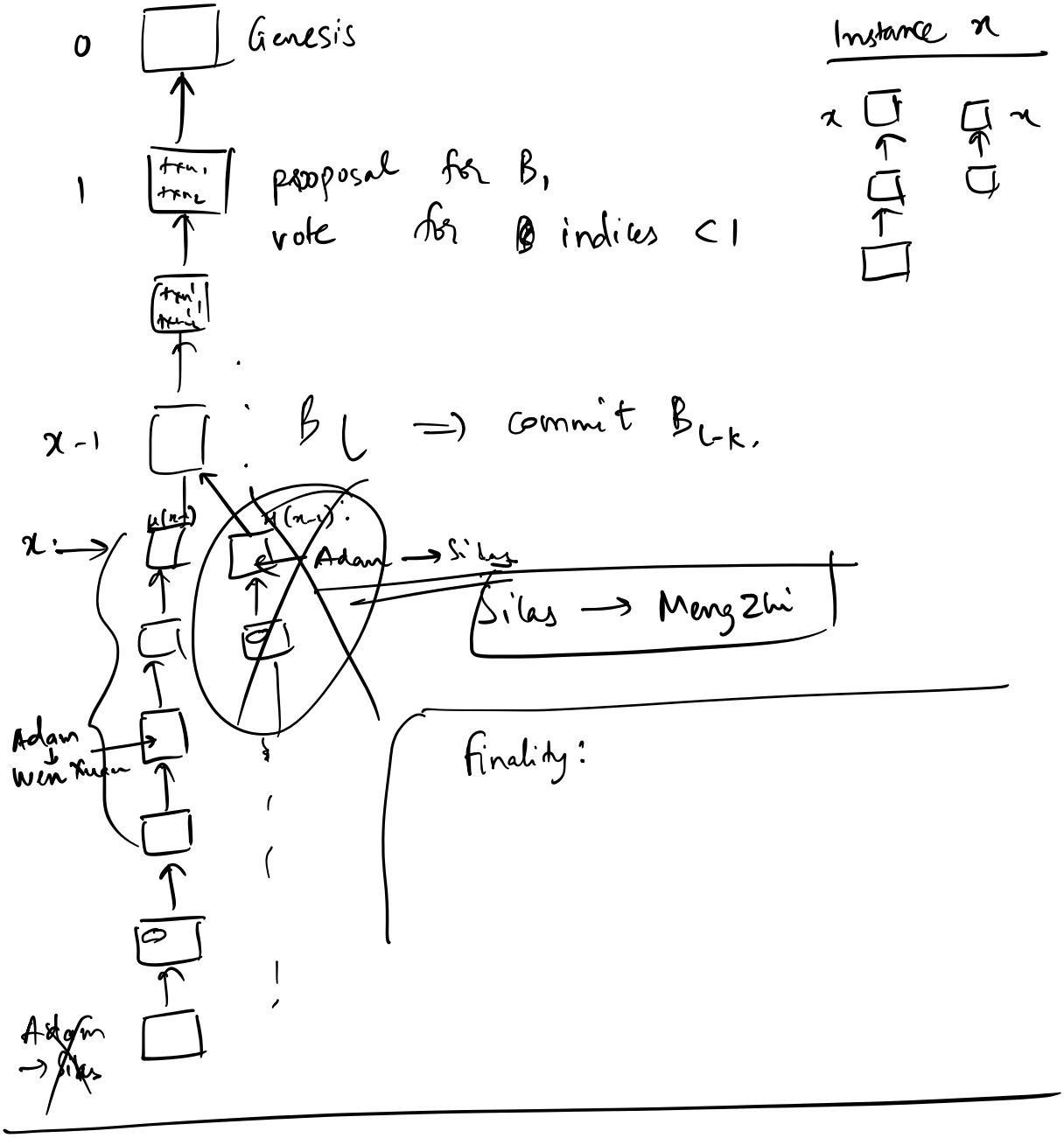
Run consensus protocol multiple times:



⟶ Each block contain some txns: 1MB (max).

↳ 4MB.

→ block chaining



n parties, t malicious:

X fixed set of parties. / do not know each other

— join or leave the system at any time.

"permissionless": no identities associated with them.

"pseudonyms".

"Bhargav": B123
B456
X579
⋮
} arbitrarily many parties.

<u>Assumption</u>: The resource held by any adversary is less than that held by honest parties.

resources.
- ↓ computation power (PoW)
- ↓ Proof-of-stake

<u>PoW</u>: Moderately hard puzzles

$H(\_\_\_\_ \mid r) \Longrightarrow y$. (infeasible).

r ↓ random.

y ↓ 256 bits.

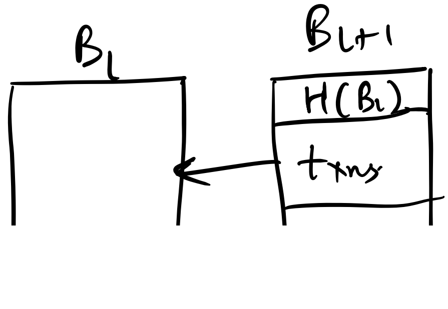
B_{l+1}

$0 \times \times \times \ldots$ ____

probabilistic: $H(\underline{txns} \mid nonce \mid r) \Rightarrow \underbrace{0\,0\,0\,0}_{\lambda}$ ____ 2^{λ}

nonce ↑

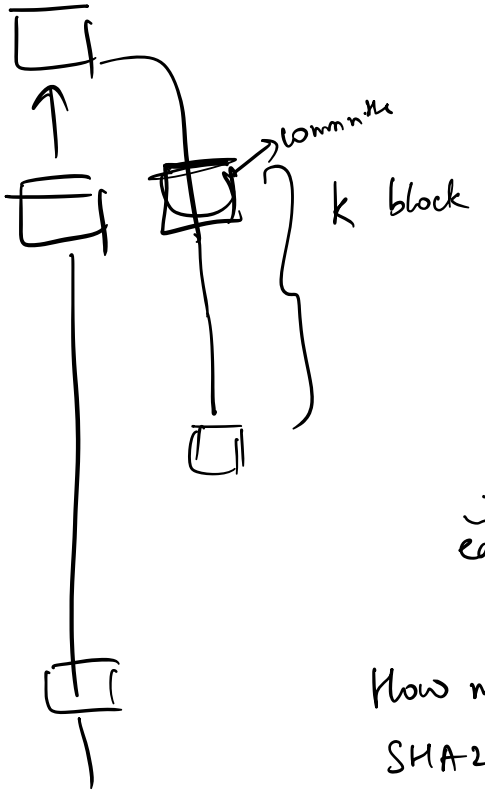
r ↓ $H(B_l)$

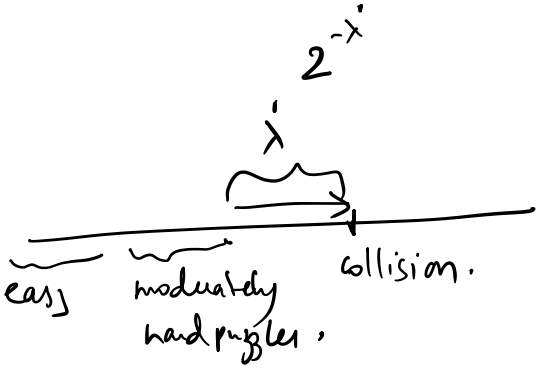


nonce.

$H(\text{pk.} \mid \text{Txns} \mid \text{nonce} \mid H(B_i)) \Rightarrow 0000\ldots$

keep changing.





How many zeros?

SHA256: collision?

After how many blocks, can

I think of SHA256 as being insecure?