Consistency of the Sleepy protocol of consensus with Markov chains

Matteo Vicari Prof. Daniele Venturi Prof. Giuseppe Di Luna

Department of Computer Science
Master degree in Cybersecurity

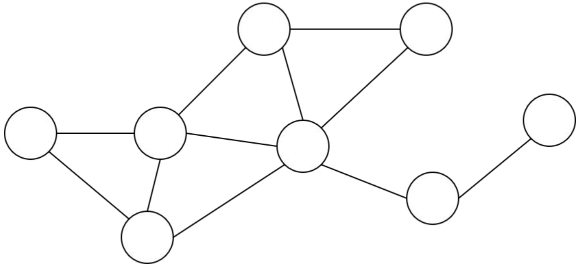
SAPIENZA
UNIVERSITÀ DI ROMA

Roadmap

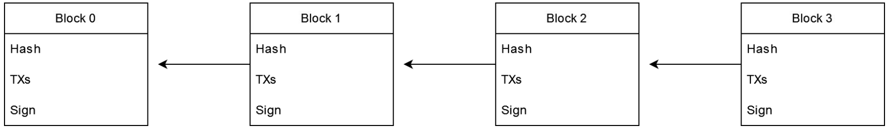
1. Blockchain Fundamentals
2. Sleepy Protocol
3. Consistency property
4. Convergence Opportunities
5. The new Markov Model
6. Sleepy Best Attack

Blockchain fundamentals

Peer to Peer network



Chain of blocks



Consensus protocol

Algorithm 1 Protocol $\Pi_{\text{sleepy}}(p)$

On input `init()` from $\mathcal{Z}$:
let $(pk, sk) := \mathfrak{s}.\text{gen}()$, register pk with $\mathcal{F}_{CA}$, let $chain := genesis$

On receive $chain'$:
assert $|chain'| > |chain|$ and $chain'$ is valid w.r.t. `eligible` and time t;
$chain := chain'$ and gossip $chain$

Every time step:

- receive input `transactions`(txs) from $\mathcal{Z}$
- let t be the current time, if $\texttt{eligible}^t(\mathcal{P})$ where $\mathcal{P}$ is the current node identifier:

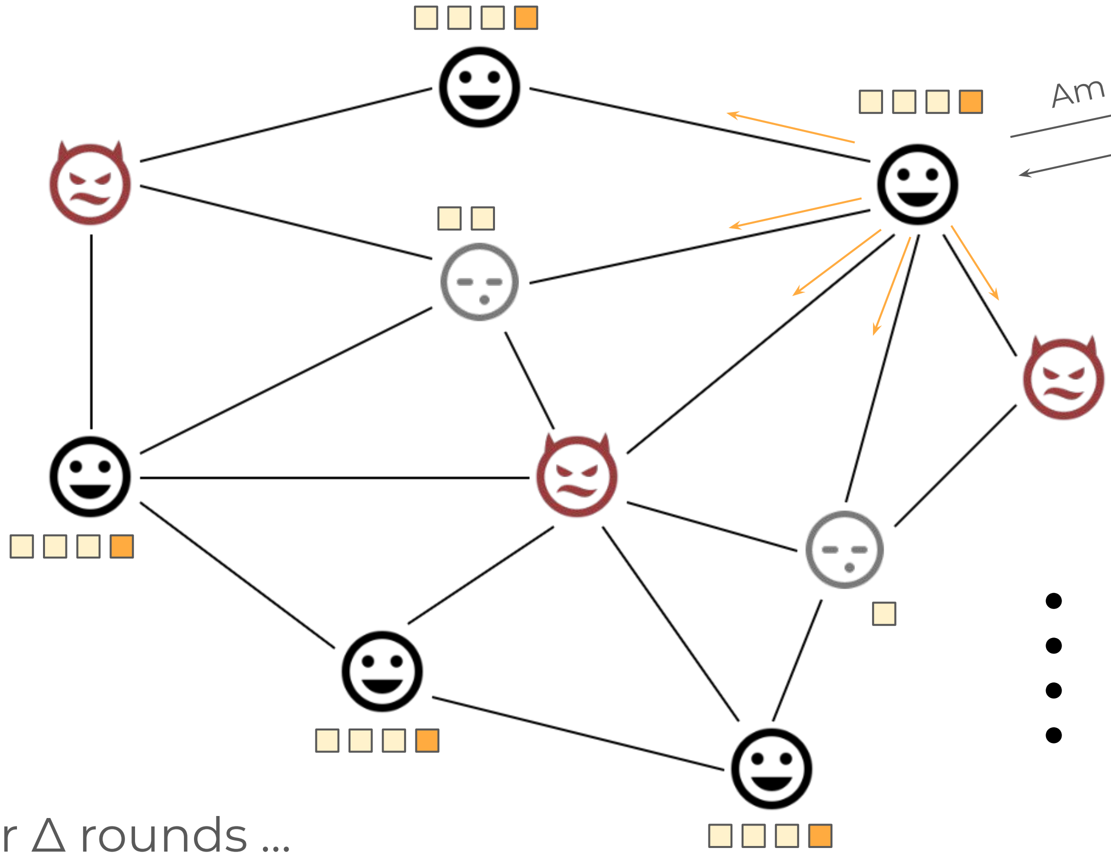
  let $\mathfrak{s} := \Sigma.\texttt{sign}(sk, chain[-1].\hbar, \text{txs}, t)$, $\hbar' := d(chain[-1].\hbar, \text{txs}, t, \mathcal{P}, \mathfrak{s})$,
  let $B := (chain[-1].\hbar, \text{txs}, t, \mathcal{P}, \mathfrak{s}, \hbar')$, let $chain := chain \| B$ and gossip $chain$
- output `extract`($chain$) to $\mathcal{Z}$ where `extract` outputs an ordered list of txs

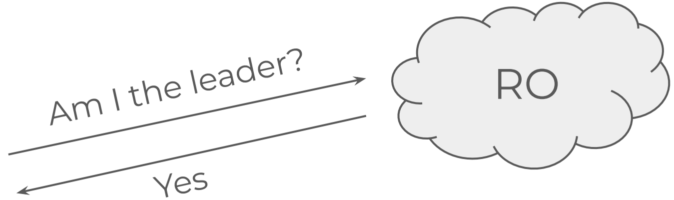
Subroutine $\text{eligible}^t(\mathcal{P})$:
return 1 if $H(\mathcal{P}, t) < D_p$ and $\mathcal{P}$ is a valid party of this protocol; else return 0

Sleepy protocol

(Weakly) Synchronous network ⇒ Δ maximum network delay (order of 10^{13})

Static corruption (μ, σ and ϱ are fixed)





$$\begin{cases} 1 & \text{with probability } p \\ 0 & \text{o.w.} \end{cases}$$

$$p = \frac{1}{\Delta c}$$

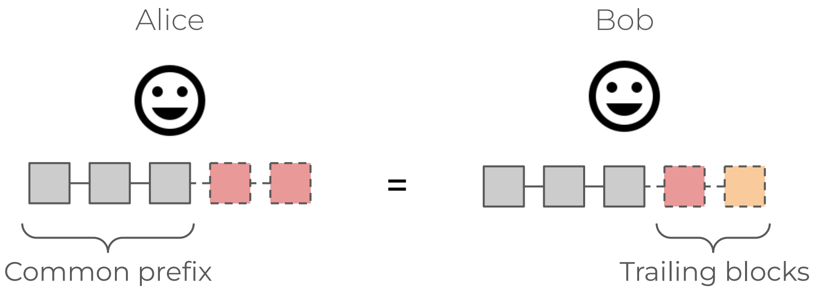
- Blocks are **signed** and **hashed**
- **Longest chain** wins
- c is the **chain speed**
- ϱ is the **corrupt fraction** of nodes

After Δ rounds ...

Consistency property

Common prefix

For every honest node:



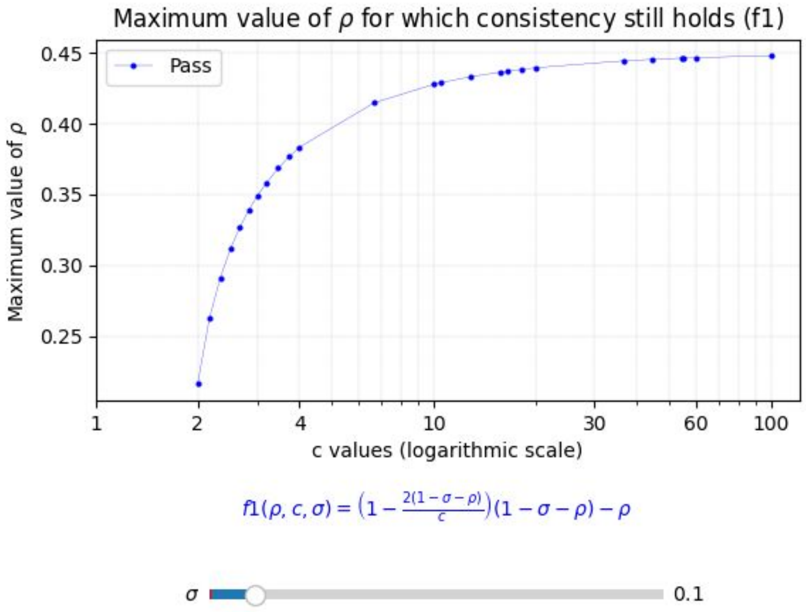
Future self consistency

Previous Sleepy consistency conditions:

$$\boxed{(1 - 2\alpha\Delta)\alpha > \beta}$$

$$\beta = p\rho N = \frac{\rho}{c\Delta}$$

$$\alpha = p\mu N = \frac{(1 - \sigma - \rho)}{c\Delta}$$

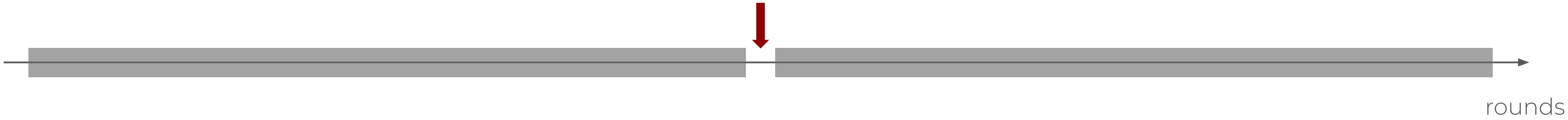


Consistency depends on c, ϱ and σ

Convergence opportunity

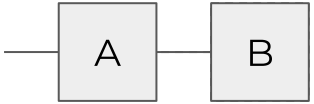
3 steps event:

Bob gets lucky and becomes leader
He builds and proposes to everyone **block B**

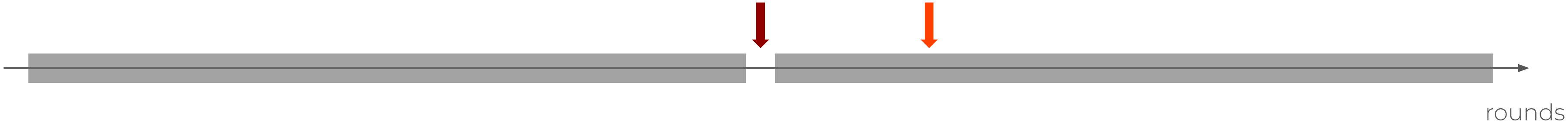


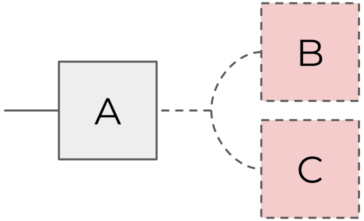
Δ rounds with no leader elected - Silent rounds
Every node in the network received the missing blocks
Everyone agrees on the last **block A**

Δ rounds with no leader elected - Silent rounds
Every node in the network received **block B**
The chain has increased by one and everyone agrees



What if Alice gets elected before reaching consensus and proposes **block C**?

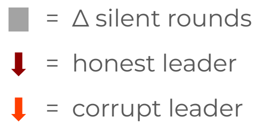


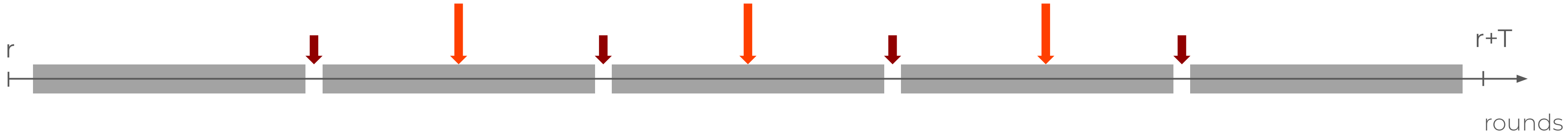


A **fork** occurs
Honest blocks cannot choose one of the two chains
Consensus is delayed

⇒ Adversarial tactic

The adversary must break all convergence opportunities to deny consensus





If we call *adversarial slot*, then we want to make sure that

$$\underbrace{\mathbf{C}(view)[r, r+T]} > \underbrace{\mathbf{A}(view)[r, r+T]}$$

Challenging estimate to compute
Different techniques lead to values
with different accuracy levels

Very easy to calculate
It is just the expected number of leaders the
adversary will have in the time interval

New framework to study consistency on PoW
with Markov chains
[Kiffer, Rajaraman and Shelat, 2022]

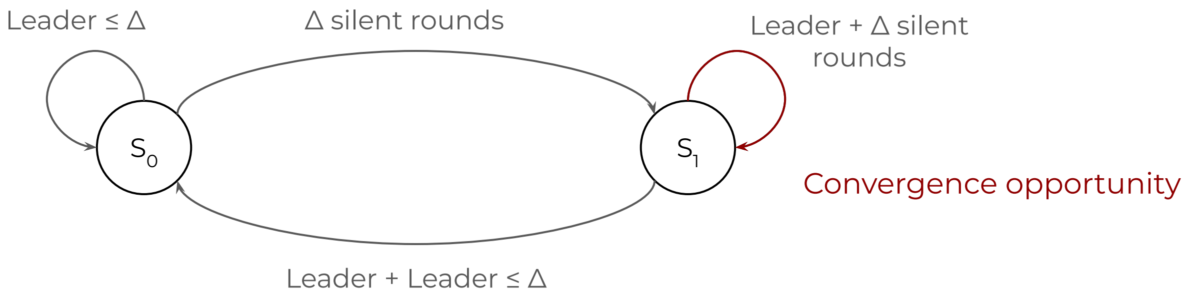
→

New estimate on convergence opportunities
New consistency condition

The new Markov model

S_0 = messy state

S_1 = ordered state



Events of interest

$$P_\Delta := (1-h)^\Delta$$

$$\mathcal{T} = \sum_{i,j} Pr[e_{ij}]\pi_i \ell_{ij}$$

Stationary distribution

$$\pi_0 = Pr[S_0] = 1 - P_\Delta$$

$$\pi_1 = Pr[S_1] = P_\Delta$$

New C.O. estimate

$$\mathbf{C} = \frac{P_\Delta^2}{\sum_{i,j} Pr[e_{ij}]\pi_i \ell_{ij}}$$

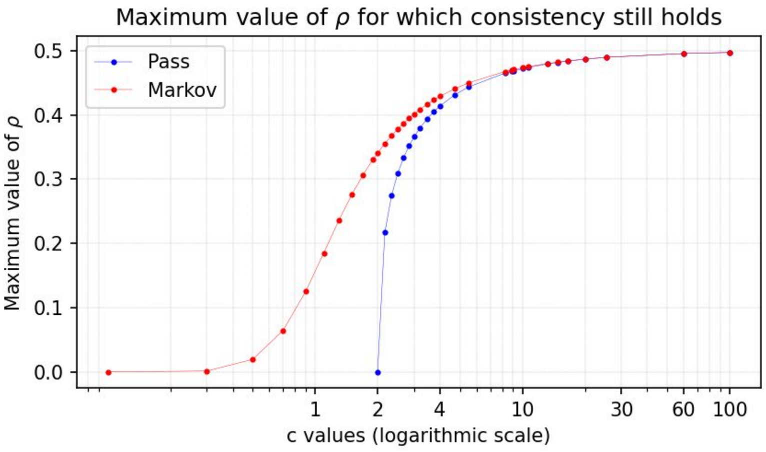
New consistency condition

$$\frac{P_\Delta^2}{\sum_{i,j} Pr[e_{ij}]\pi_i \ell_{ij}} > \beta$$

Final analytical condition

$$(1-\sigma-\rho)e^{-\frac{2}{c}(1-\sigma-\rho)} - \rho > 0$$

Pass and Seeman condition VS New Markov condition

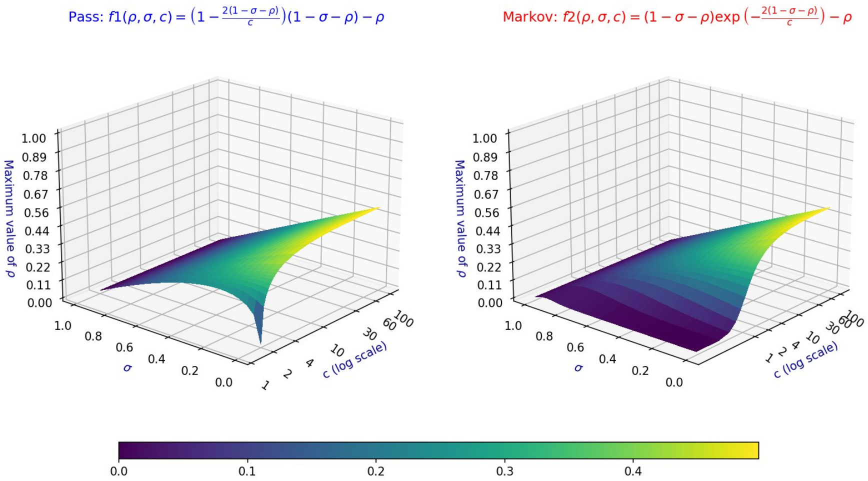


$$f1(\rho, c, \sigma) = \left(1 - \frac{2(1-\sigma-\rho)}{c}\right)(1-\sigma-\rho) - \rho$$

$$f2(\rho, c, \sigma) = (1-\sigma-\rho)e^{-\frac{2(1-\sigma-\rho)}{c}} - \rho$$

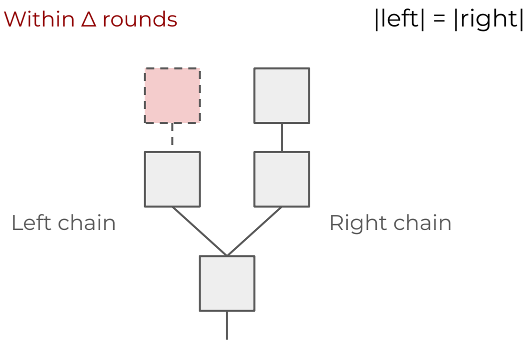
σ 0

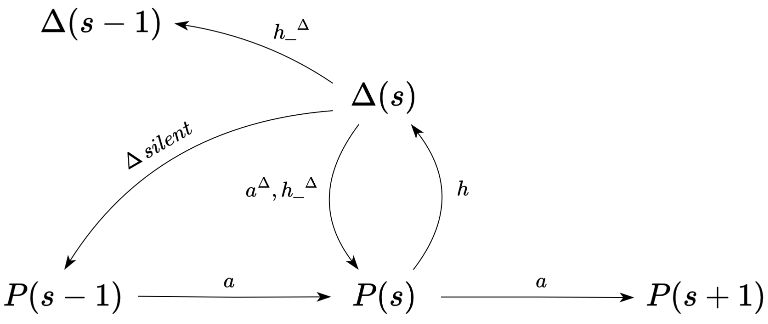
- Extended domain for c values
- Increased resistance to adversarial elective power ϱ



Sleepy best attack

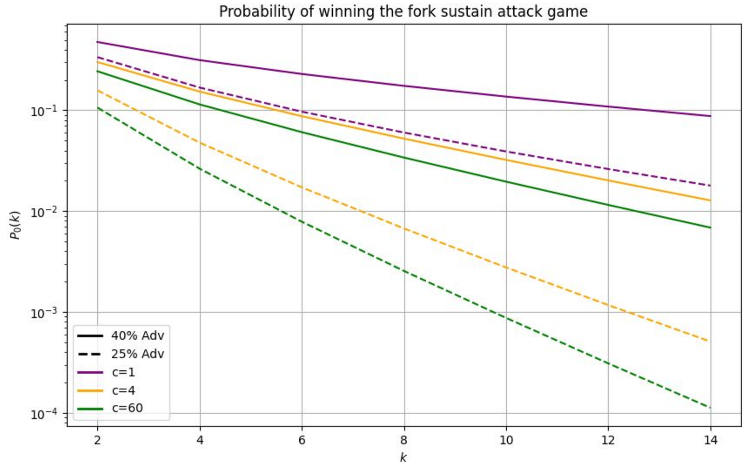
Fork sustain attack





- As long as the two chains have equal lengths, honest nodes cannot choose between the two

- As soon as one of the two chains is ahead for more than Δ rounds, the adversary loses



Even if consistency holds, the adversary is able to sustain a fork for *k* block with non negligible probability (in *k*)

Thank you for your attention!

Consult the paper here