8th Distributed Ledger Technology Workshop (DLT 2026)

Pula – June 6th, 2026

Looking for Stability in Proof-of-Stake Based Consensus Mechanisms

Alberto Leporati, Lorenzo Rovida

University of Milano-Bicocca

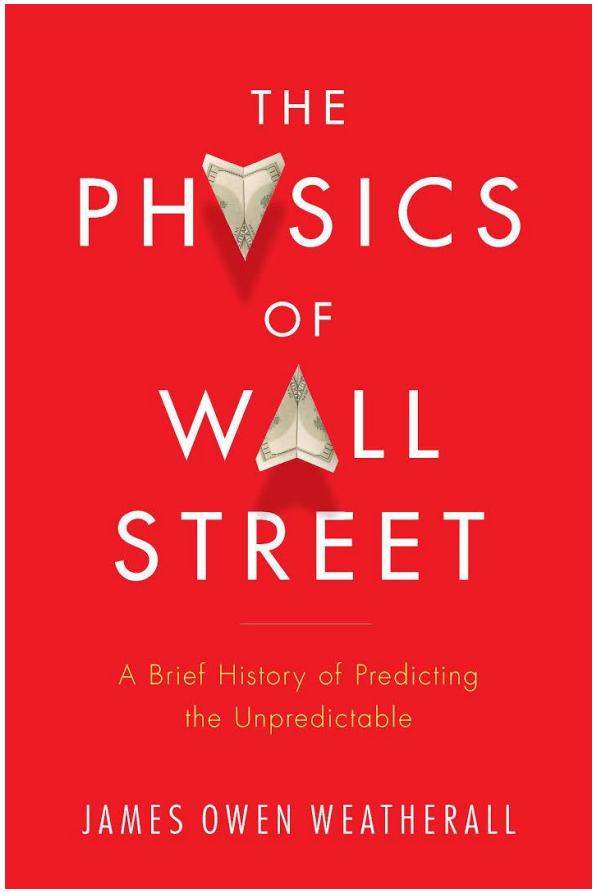
Department of Informatics, Systems, and Communication

alberto.leporati@unimib.it

Background

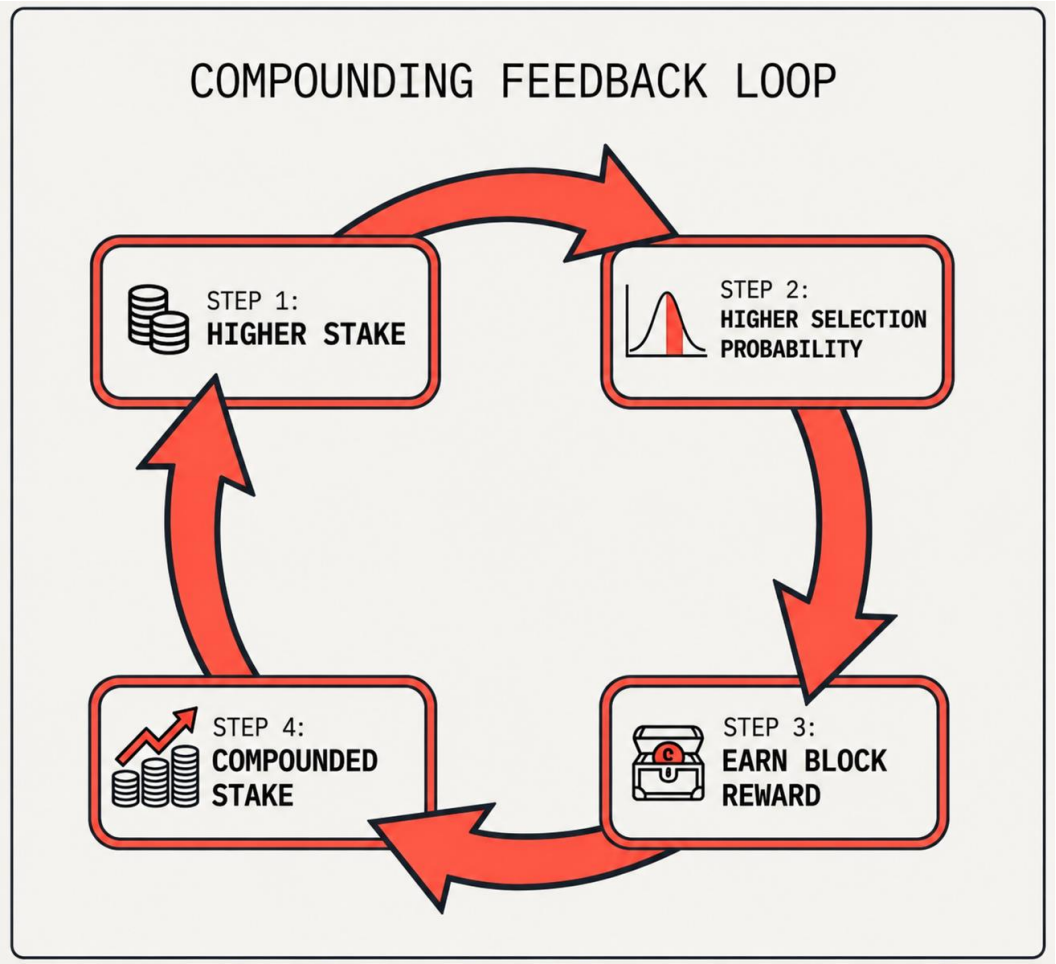
- A permissionless blockchain that
  - implements a cryptocurrency
  - is used to track cryptocurrency transactions

  can be seen as an economic market, where
  - some cryptocurrency is burned
  - some cryptocurrency is created, usually by minters/validators
- This economic market must be **trusted** and **sustainable** in the long term
- These topics are studied not only in Economics, but also in Mathematics and Physics



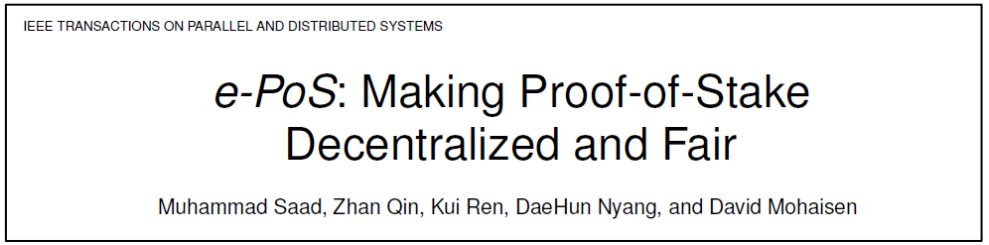
Proof-of-Stake

- We focus on the PoS consensus algorithm
- Several versions of PoS have been proposed
- PoS addresses the energy consumption problem of PoW
- PoS Proof-of-Stake (PoS) naturally behaves as a « Proof of Wealth ». It functions as an oligopoly where the mere act of validating blocks concentrates wealth over time, threatening the permissionless nature of the network



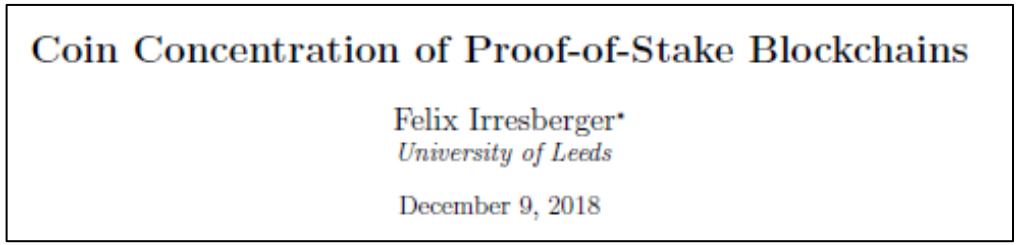
Proof-of-Stake: criticism

- In PoW, *miners* may possess a big amount of cryptocurrency, but they also spend a lot of (fiat) money to update the hardware and pay electricity bills
- No such expenses are associated with PoS: *stakers* put some cryptocurrency in the stake, get the rewards, and are not incentived to spend them
- In PoS, who is rich gets richer, by the compounding effect


IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS

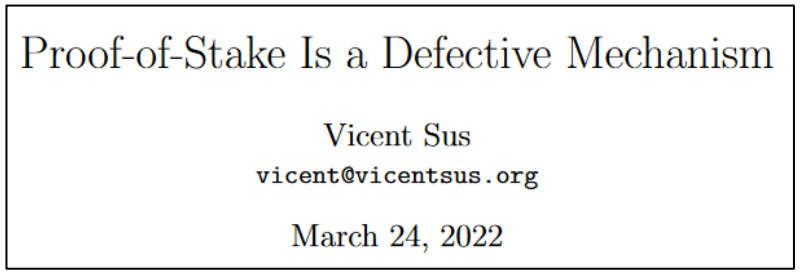
e-PoS: Making Proof-of-Stake Decentralized and Fair

Muhammad Saad, Zhan Qin, Kui Ren, DaeHun Nyang, and David Mohaisen


Coin Concentration of Proof-of-Stake Blockchains

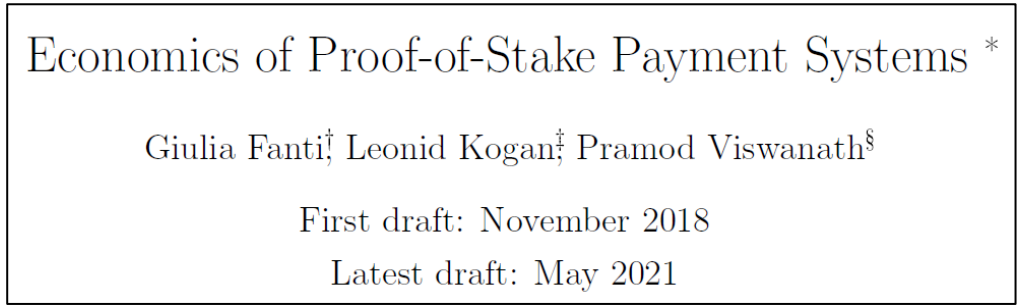
Felix Irresberger*
University of Leeds

December 9, 2018


Proof-of-Stake Is a Defective Mechanism

Vicent Sus
vicent@vicentsus.org

March 24, 2022


Economics of Proof-of-Stake Payment Systems *

Giulia Fanti†, Leonid Kogan‡, Pramod Viswanath§

First draft: November 2018
Latest draft: May 2021

Our question

> « Can we make PoS a **fair** and **sustainable** consensus mechanism? »

- This depends upon how PoS is implemented, not only on monetary policy
- Governing rules depend upon a number of parameters
- **Fair** to us means: no one should get richer or poorer by just validating blocks
- We measure wealth distribution by Gini coefficient
- **Sustainaible** means: users trust the system, hence they do not leave it
- The system must be perceived as trusted, not driven by an oligarchy, hence decentralized (both in terms of technical infrastructure and **wealth distribution**)

Our goal

- To study how the initial cryptocurrency supply, and the parameters that drive the PoS consensus mechanism, influence the (long term) wealth distribution …
- … by using a simulation approach
- **Note:** we do not focus on a particular implementation of PoS
- Other works in the literature address this problem from a **statistical** point of view (model based on Zipf's law)
- Instead, we consider the blockchain as a **complex system**, sensitive to the choice of parameter values and the initial state

PoS simulator

- Written in the Julia language, for efficiency
- Source code available at https://github.com/lorenzorovida/PoS-Simulator
- We simulate an abstract version of PoS
- We simulate a closed system (no interaction with the external environment)
- The initial wealth distribution is chosen uniformly in a fixed range
- The percentage of tokens (coins) that are put in stake is the same for all peers
- … the same goes for the number of coins awarded
- … and the same holds for the percentage to be slashed

Some parameters

Parameter Name	Meaning
numberOfPeers	The number of participants in the blockchain. More precisely, the number of participants that aim to be selected as validators
numberOfCorruptedPeers	The number of peers that are corrupted, that is, that will be fined because they do not validate correctly the block
numberOfValidators	The number of peers that are chosen to validate a block
minNumberOfTokensPerPeer	The minimum number of tokens assigned to each peer during the distribution of the initial token supply
maxNumberOfTokensPerPeer	The maximum number of tokens assigned to each peer during the distribution of the initial token supply
stakeablePercentage	The percentage of tokens in the current supply of the peers, that can be put into the stake
numberOfRewardTokens	The number of tokens given as a reward to the validators that correctly validate the current block
percentageOfPenalty	The percentage of tokens removed from the amount of tokens staked by the corrupted validators
numberOfIterations	The number of iterations to be simulated, that corresponds to the number of blocks validated

Gini coefficient

- It can be defined in several ways, for example:

$$G = \frac{1}{2N} \sum_{i=1}^{N} \sum_{j=1}^{N} |x_i - x_j|$$

where N is the number of individuals in the population, and x_i is the monetary value associated with the i-th individual

- Invented to investigate and measure wealth/income distribution in populations
- Widely used in Economics and Social Statistics
- It takes values from 0 (complete decentralization) to 1 (absolute centralization)

  Less than 0.3: egalitarian distribution

  Greater than 0.5: dangerous and divisive

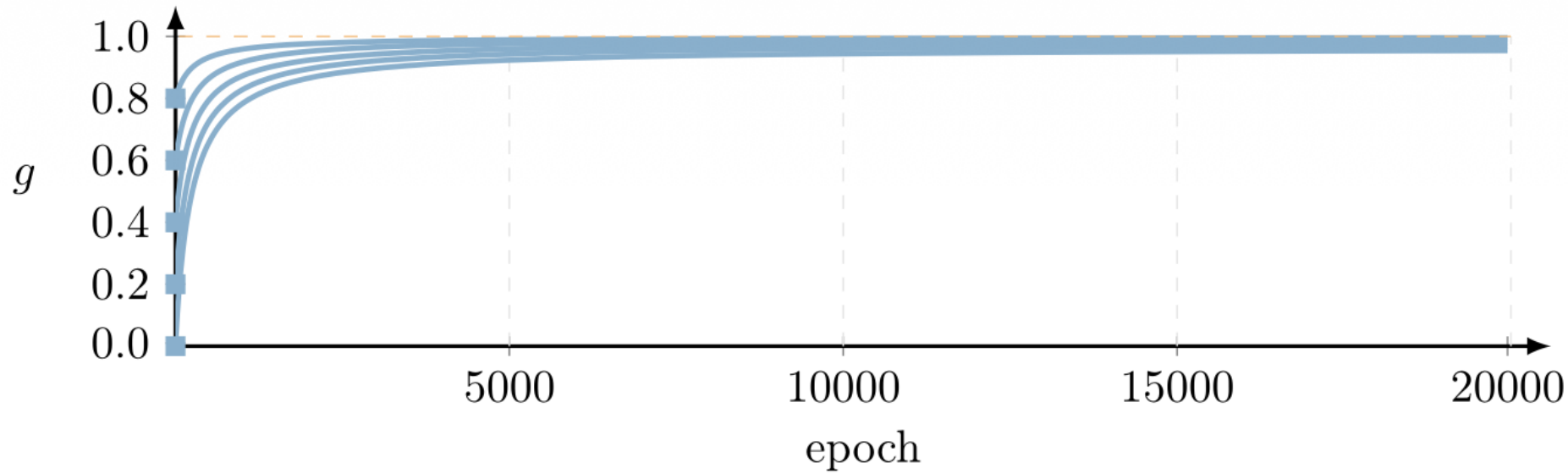
Experiments

- Inputs (variables):
  - Peers: 10.000
  - Initial stake volume: 5.000 – 50.000
  - Corrupted validators: parameterized
- Consensus type: variable
- Smoothing: variable
- Up to 4.000.000 epochs

- Outputs:
  - Gini history
  - Wealth distribution

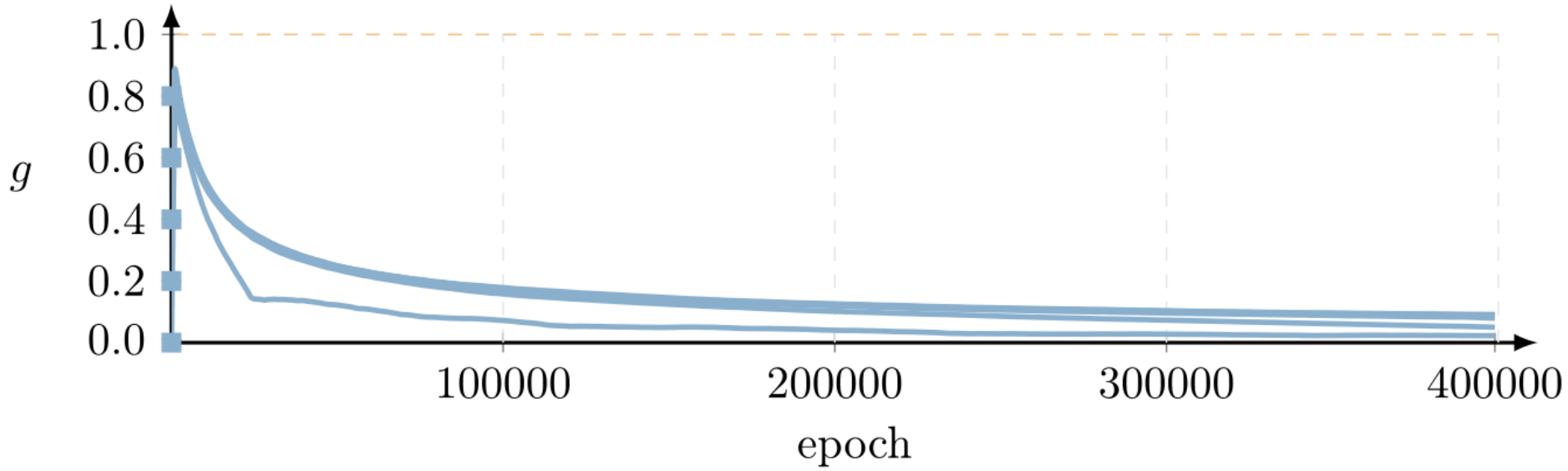
First scenario: Weighted PoS (the status quo)

- Probability strictly proportional to stake: $P_i = S_i \,/ \sum_j \, S_j$
- Result: after 20.000 epochs, 76.7% of peers fall below the average wealth threshold. The blockchain is monopolized by a shrinking oligarchy



Second scenario: Opposite-Weighted PoS (overcorrection)

- Probability inversely proportional to stake: $P_i = 1 - \left(S_i \,/\, \sum_j \; S_j\right)$
- Result: wealth becomes perfectly distributed. However, participants are completely disincentivized from staking coins, stripping the network of its security collateral



An algorithmic equilibrium

- We cannot rely on a static consensus formula, we need an adaptive mechanism
- Proposal:
  - when he network centralizes ($g > \theta$), the system autonomously shifts toward the Opposite-Weighted strategy
  - when it over-decentralizes ($g < \theta$), it shifts back toward the Weighted PoS

where:

g = Gini coefficient

θ = threshold

Gini-stabilized PoS

- The probability of choosing a peer as validator is:

$$P_i = \ell\left(P_w, 1 - P_w, t_j\right)$$

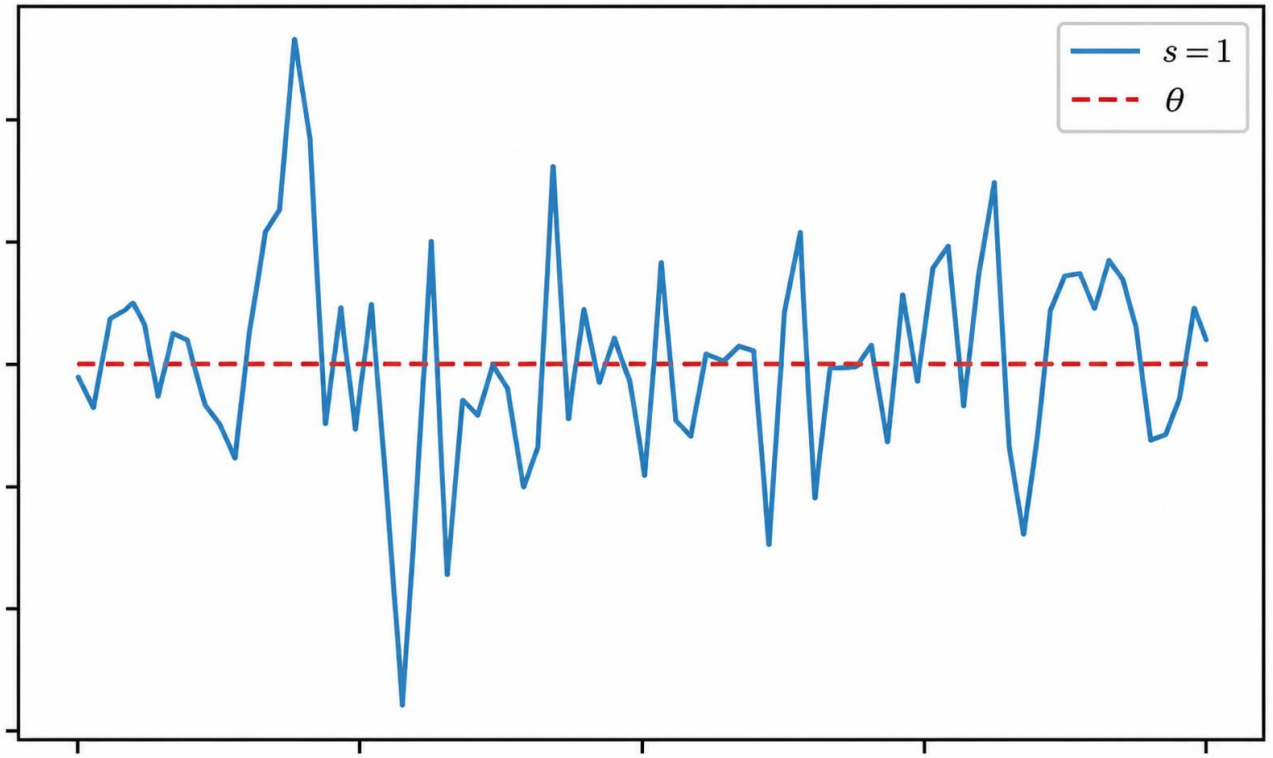
where:

- P_w = probability distribution as in Weighted PoS
- $\ell(x, y, t) = x + t(y - x)$ is an interpolation function
- t_j = adjustment factor based on the current Gini coefficient, defined as:

$$\begin{cases} t_0 = d(g, \theta) \\ t_j = \ell(t_{j-1}, d(g, \theta), s) \end{cases} \qquad d(g, \theta) = \frac{\operatorname{sgn}(g - \theta) + 1}{2}$$

- $d(g, \theta)$ controls the «direction» of the transition, and $0 < s \leq 1$ controls the «speed» of the transition

The «zig-zag» effect (constant smoothing, $s = 1$)



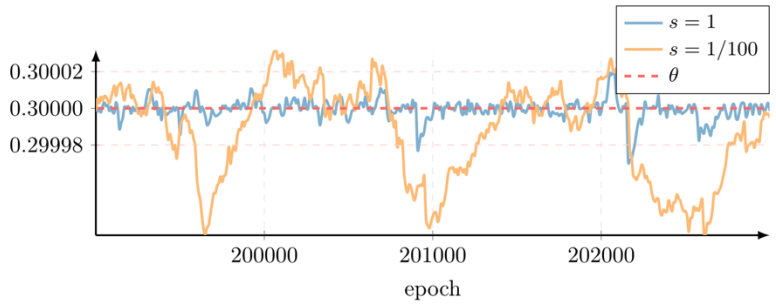
- A rigid interpolation factor $(s = 1)$ creates violent oscillation, because the networks instantly switches between Weighted Pos and Opposite-Weighted PoS as soon as the threshold θ is crossed
- We need a dynamic relaxation mechanism

Choosing the smoothing factor

Constant smoothing

$$s = k$$

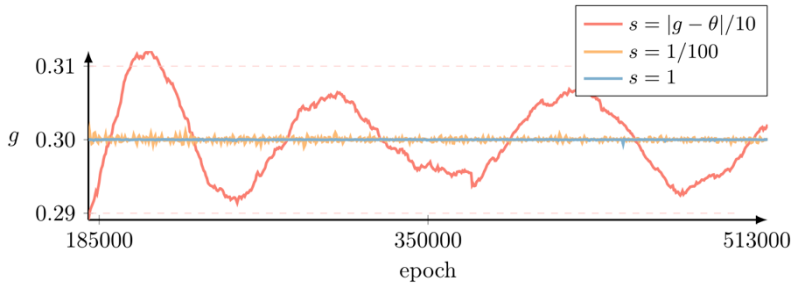
- Effect: violent, binary oscillation



Linear smoothing

$$s = \frac{|g - \theta|}{k}$$

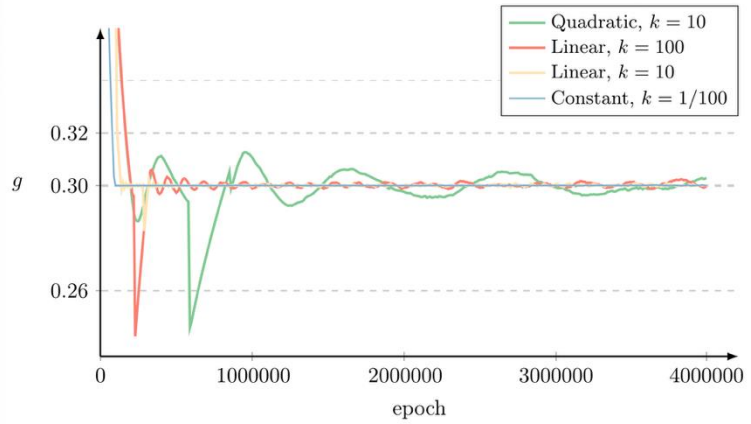
- Effect: Wavy, proportional correction. Amplitude decreases but frequency remains



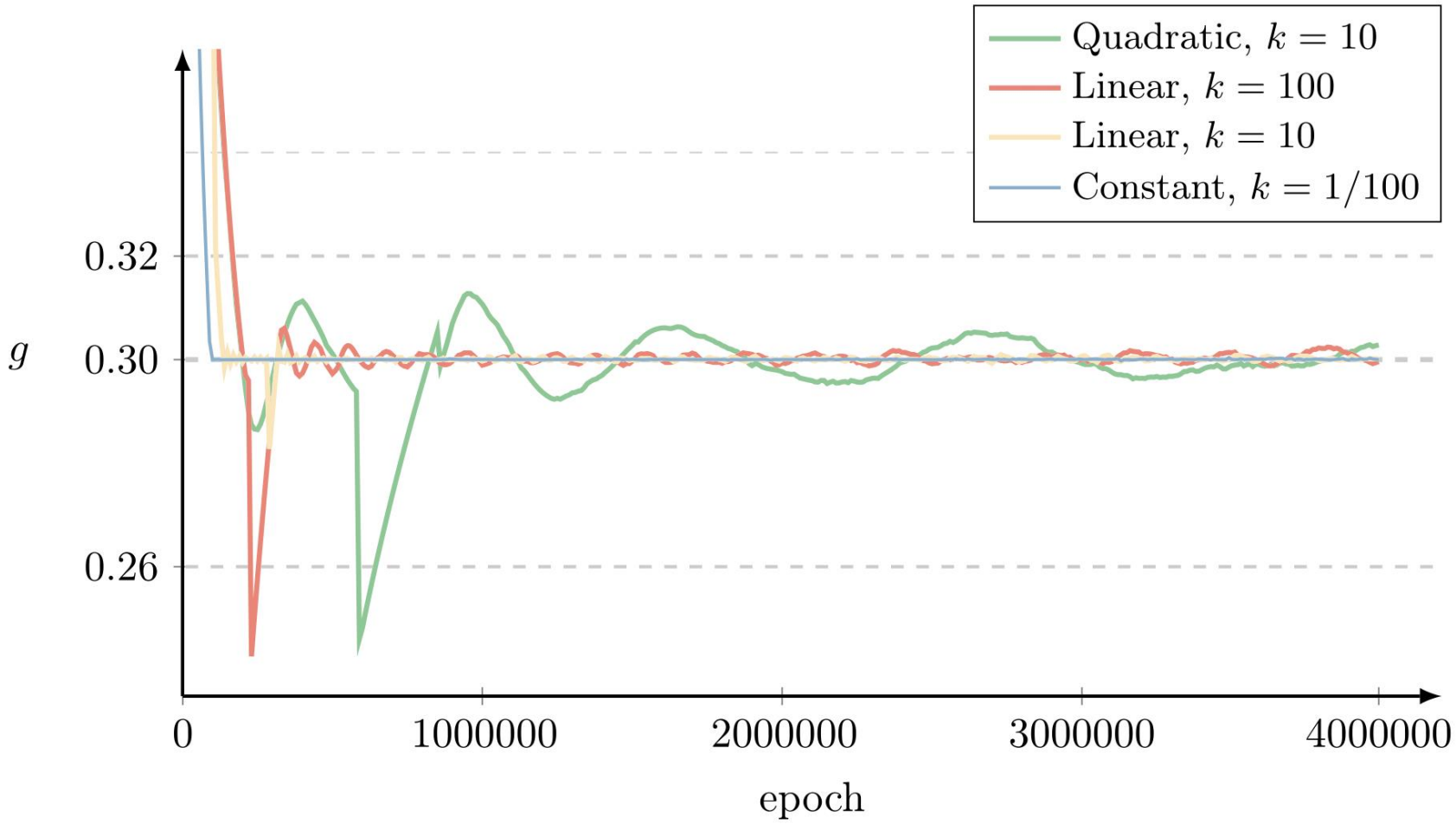
Quadratic smoothing

$$s = \frac{|g - \theta|^2}{k}$$

- Effect: Rapid dampening. The system goes smoothly into a flat, stable line



Achieving equilibrium (4.000.000 epochs)



Quadratic smoothing, with $k = 10$, rapidly dampens variance

Thank you for your attention !

Gràtzias a totus po s'atentzione