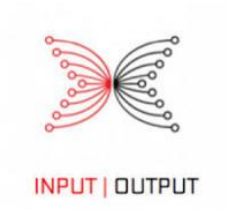
Practical Settlement Bounds for Longest-Chain Consensus

Peter Gaži
IOG

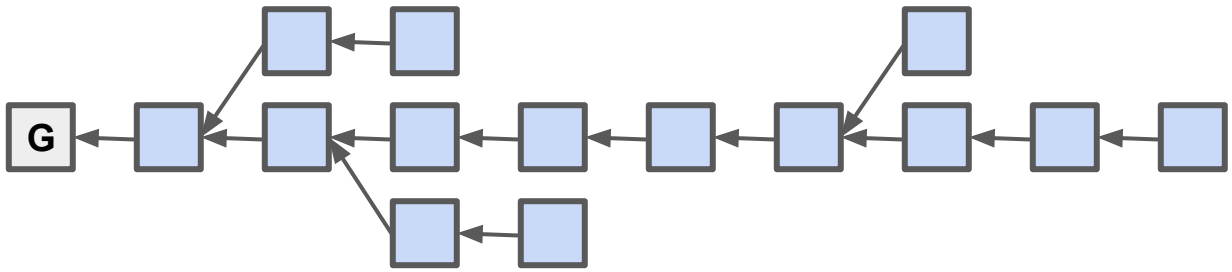
Ling Ren
University of Illinois
at Urbana-Champaign

Alexander Russell
University of Connecticut
and IOG



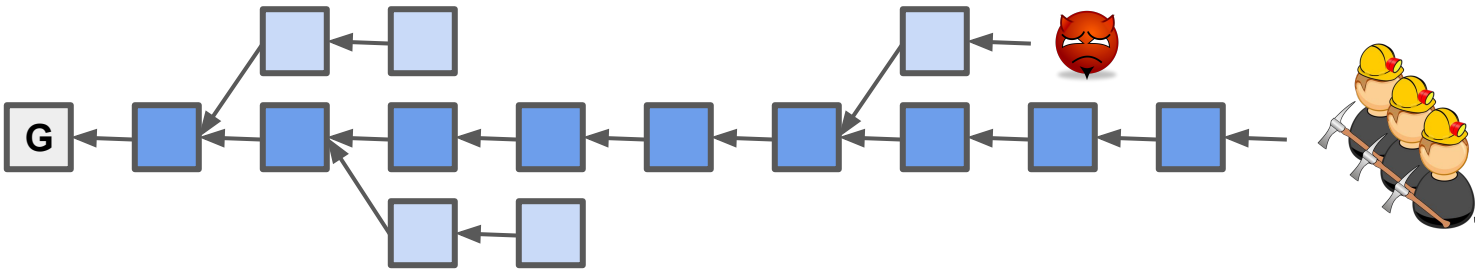
Longest-Chain Consensus

- transactions-carrying **blocks** appended in ever-growing **blocktree**
- blocks connected by hash links
- block-creation based on a **leadership lottery** (PoW/PoS)



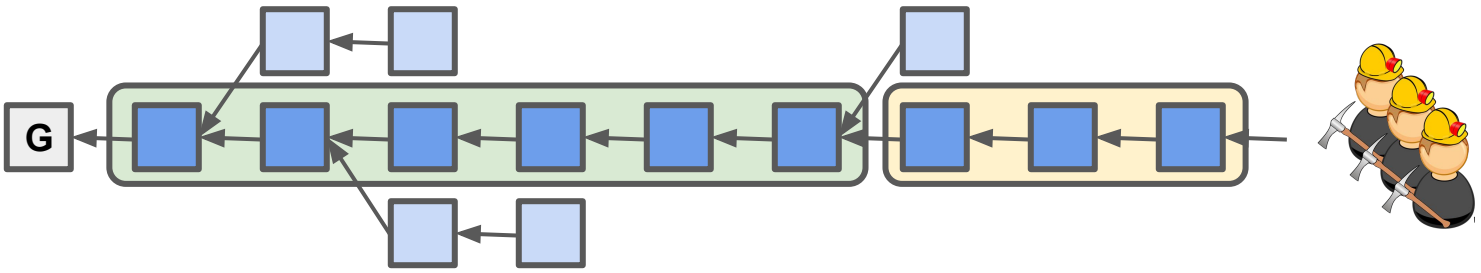
Longest-Chain Consensus

- transactions-carrying **blocks** appended in ever-growing **blocktree**
- blocks connected by hash links
- block-creation based on a **leadership lottery** (PoW/PoS)
- honest leaders extend **longest chain**, adversary extends arbitrarily



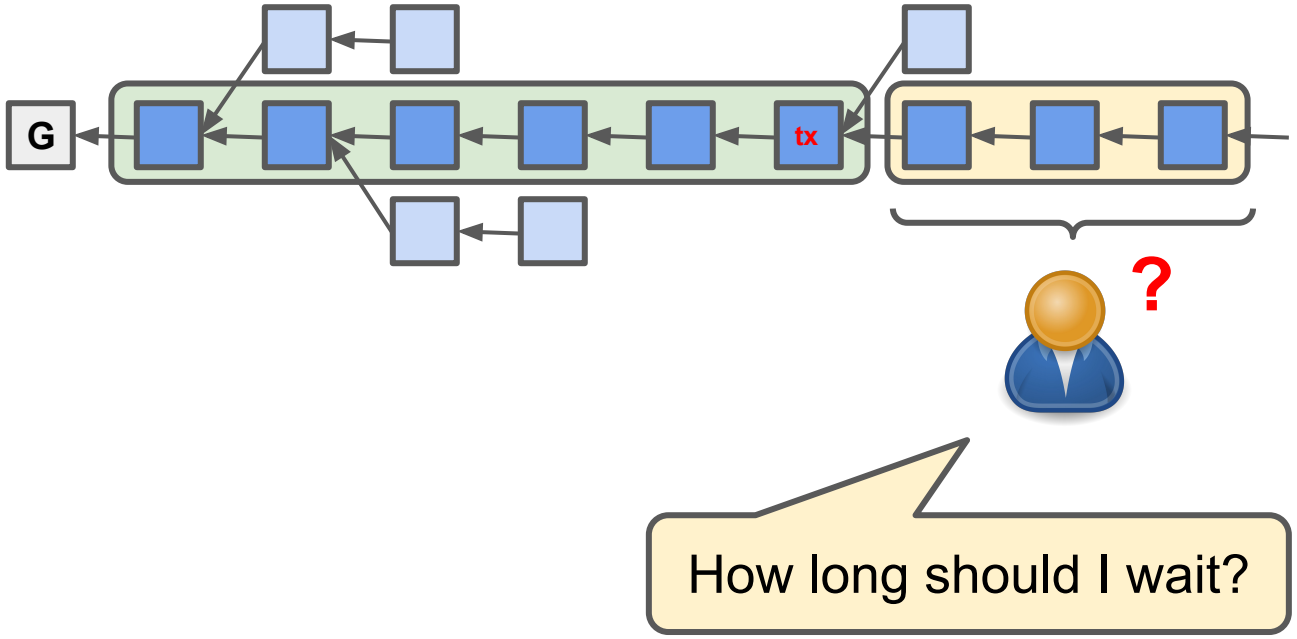
Longest-Chain Consensus

- transactions-carrying **blocks** appended in ever-growing **blocktree**
- blocks connected by hash links
- block-creation based on a **leadership lottery** (PoW/PoS)
- honest leaders extend **longest chain**, adversary extends arbitrarily
- **stable ledger state** : longest chain minus **unstable suffix**



Settlement is gradual and subjective!

How fast is longest-chain settlement?



Our Results

1. a rigorous method for obtaining settlement guarantees for longest-chain consensus:

Assuming
- some honest and adversarial power (hashing/stake)
- bound on message delays

how many blocks guarantee settlement except with acceptable error?

Our Results

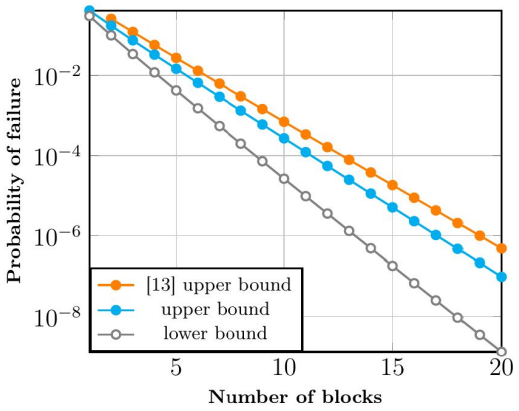
1. a rigorous method for obtaining settlement guarantees for longest-chain consensus:

Assuming
- some honest and adversarial power (hashing/stake)
- bound on message delays

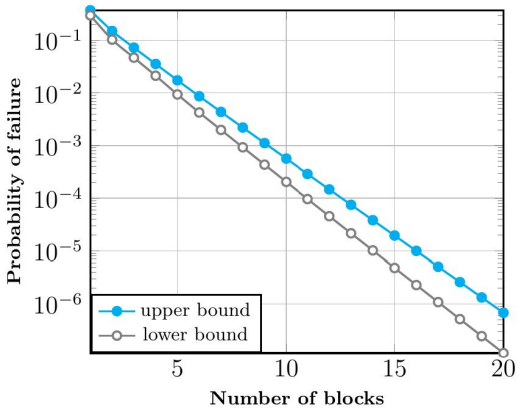
how many blocks guarantee settlement except with acceptable error?

2. concrete numerical results of practical interest:

PoW (Ethereum)



PoS (Cardano)

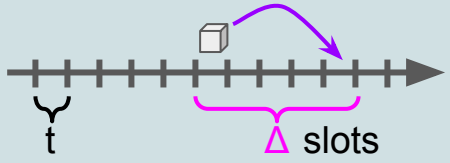


Our Model

Timeline and Message Delays:

Discrete model

- discrete slots of length t
- msgs delayed by: ≤ Δ slots



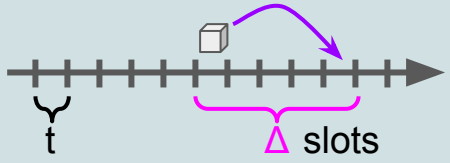
- natural for PoS
- good approximation for PoW (as $t \to 0$)

Our Model

Timeline and Message Delays:

Discrete model

- discrete slots of length t
- msgs delayed by: ≤ Δ slots



- natural for PoS
- good approximation for PoW (as $t \to 0$)

Leadership Lottery: independent Poisson processes with rates r_h and r_a

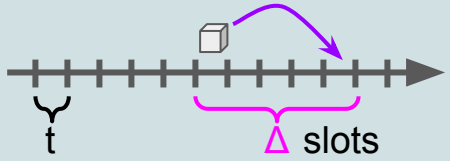
- exactly right for PoW
- good approximation for PoS

Our Model

Timeline and Message Delays:

Discrete model

- discrete slots of length t
- msgs delayed by: ≤ Δ slots



- natural for PoS
- good approximation for PoW (as $t \to 0$)

Leadership Lottery: independent Poisson processes with rates r_h and r_a

- exactly right for PoW
- good approximation for PoS

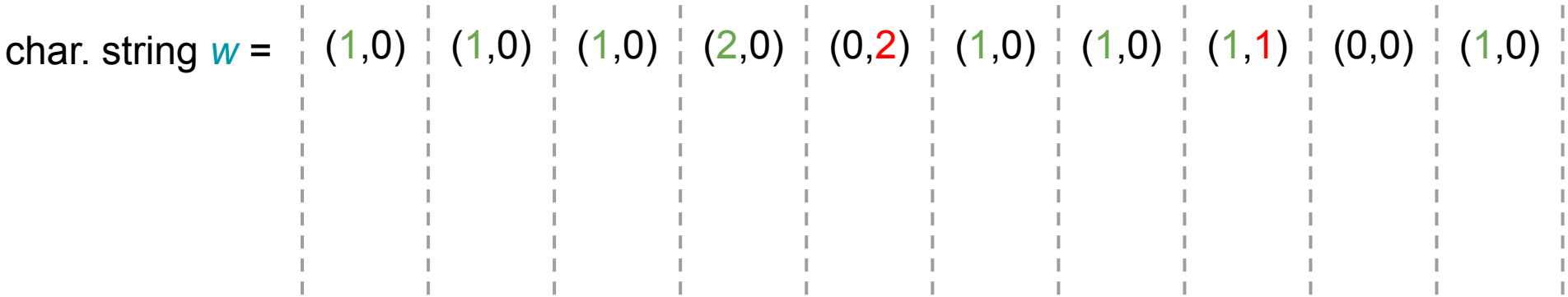
Adversary: arbitrary strategy

- cannot break hash function or the lottery

Tools: Characteristic Strings and Blocktrees

Tools: Characteristic Strings and Blocktrees

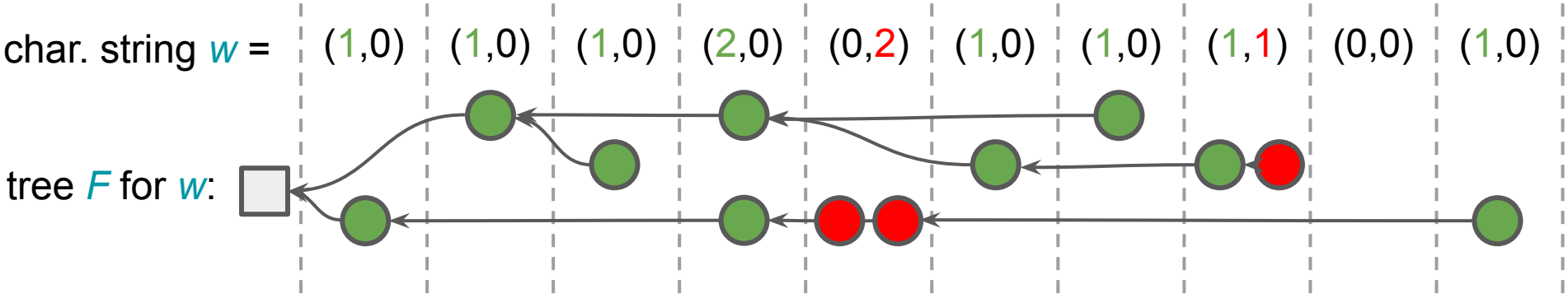
- **(characteristic) string *w***
  - numbers of honest/adversarial lottery successes in each slot



Tools: Characteristic Strings and Blocktrees

- **(characteristic) string *w***
  - numbers of honest/adversarial lottery successes in each slot

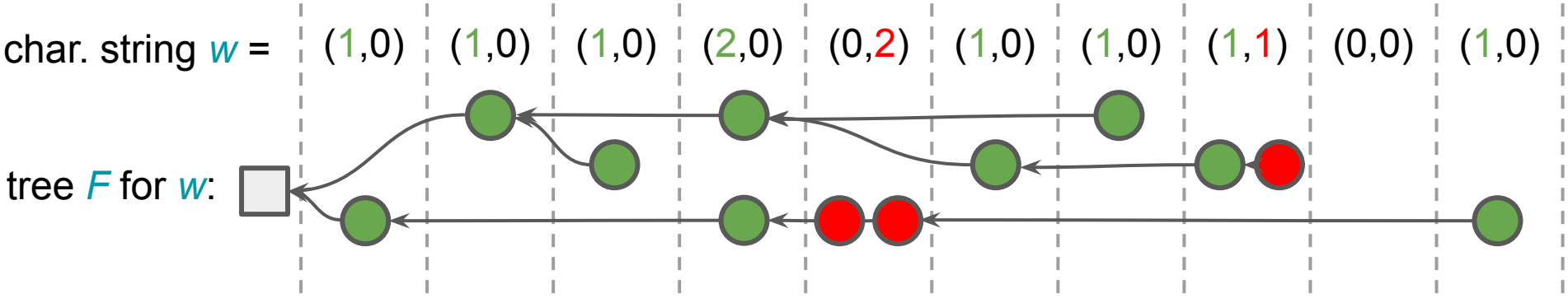
- **(block)tree *F* for *w***
  - all chains created in some valid execution compatible with *w*



Tools: Characteristic Strings and Blocktrees

- **(characteristic) string** *w*
  - numbers of honest/adversarial lottery successes in each slot

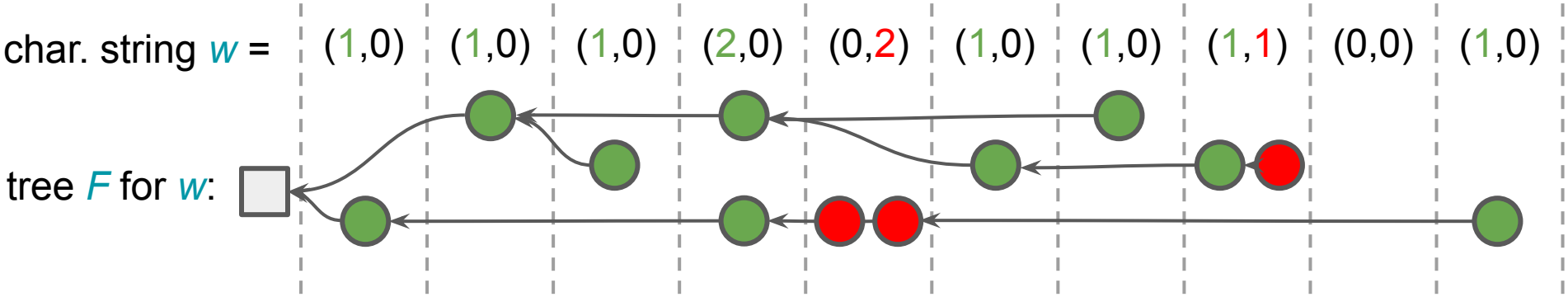
- **(block)tree** *F* **for** *w*
  - all chains created in some valid execution compatible with *w*
    - **honest depth property**: every honest block deeper than all Δ-old honest blocks



Tools: Characteristic Strings and Blocktrees

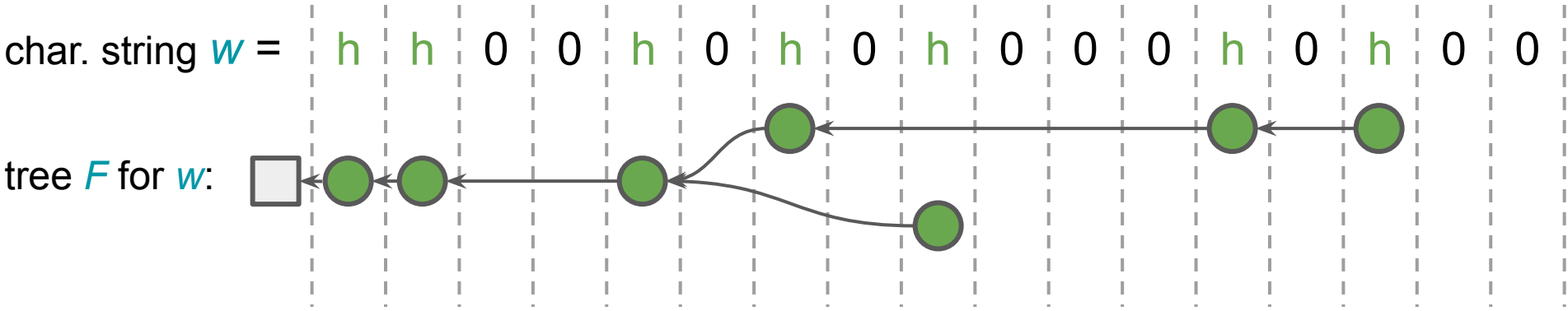
- **(characteristic) string** *w*
  - numbers of honest/adversarial lottery successes in each slot

- **(block)tree** *F* **for** *w*
  - all chains created in some valid execution compatible with *w*
    - **honest depth property**: every honest block deeper than all Δ-old honest blocks

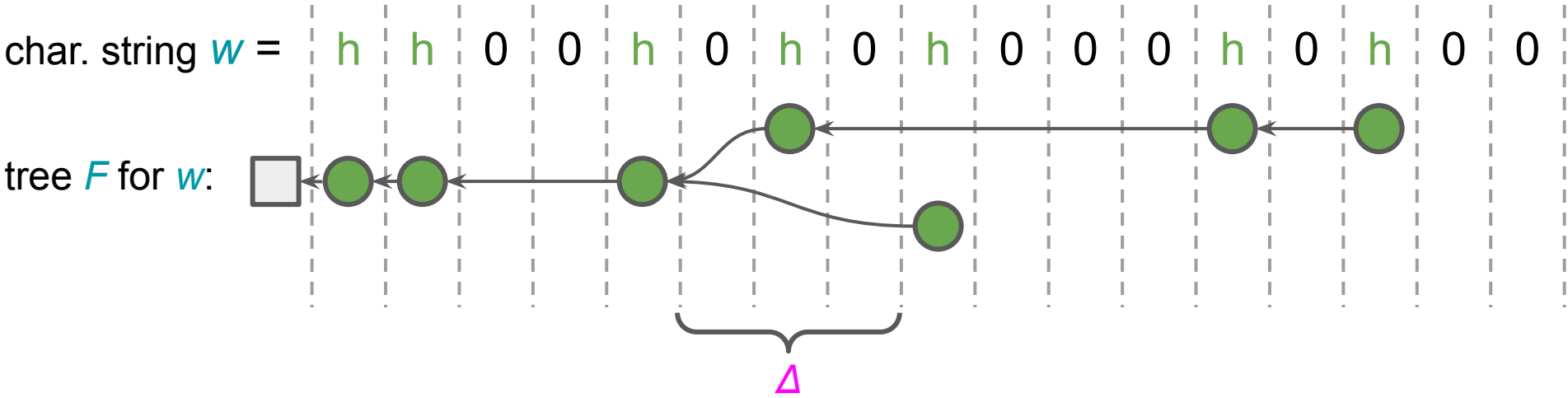


Does a string *w* admit a blocktree *F* with long diverging segments?

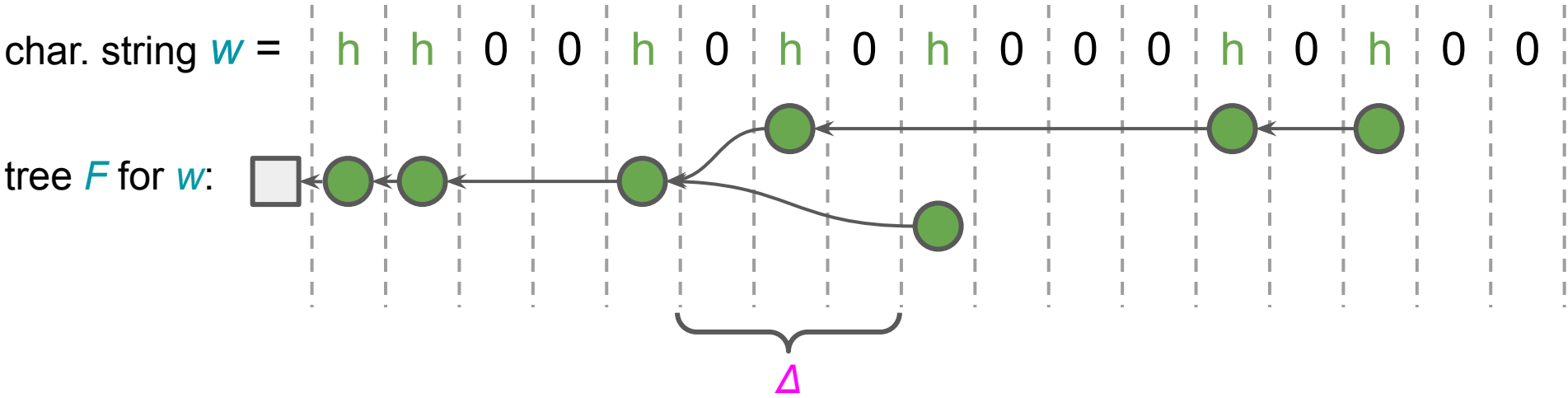
Characteristic Strings and Forks (Δ = 3)

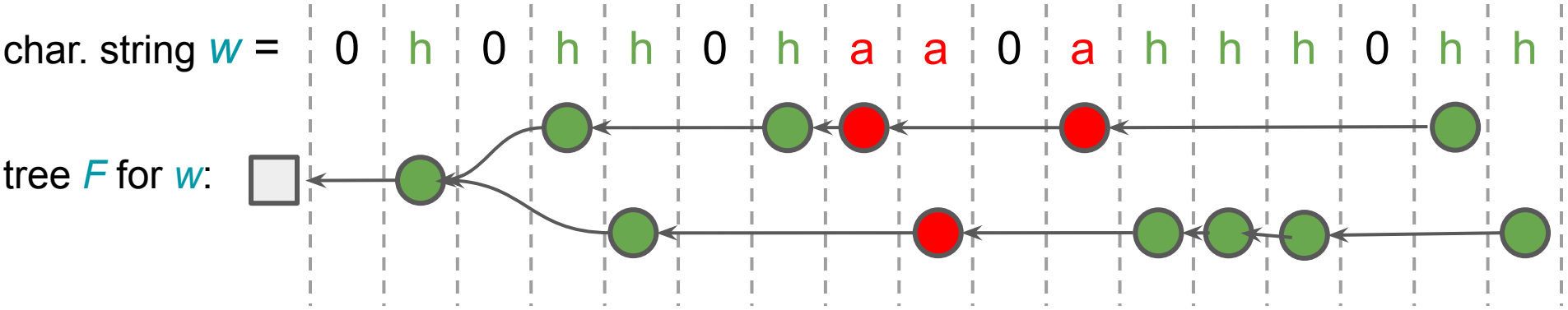


Characteristic Strings and Forks (Δ = 3)



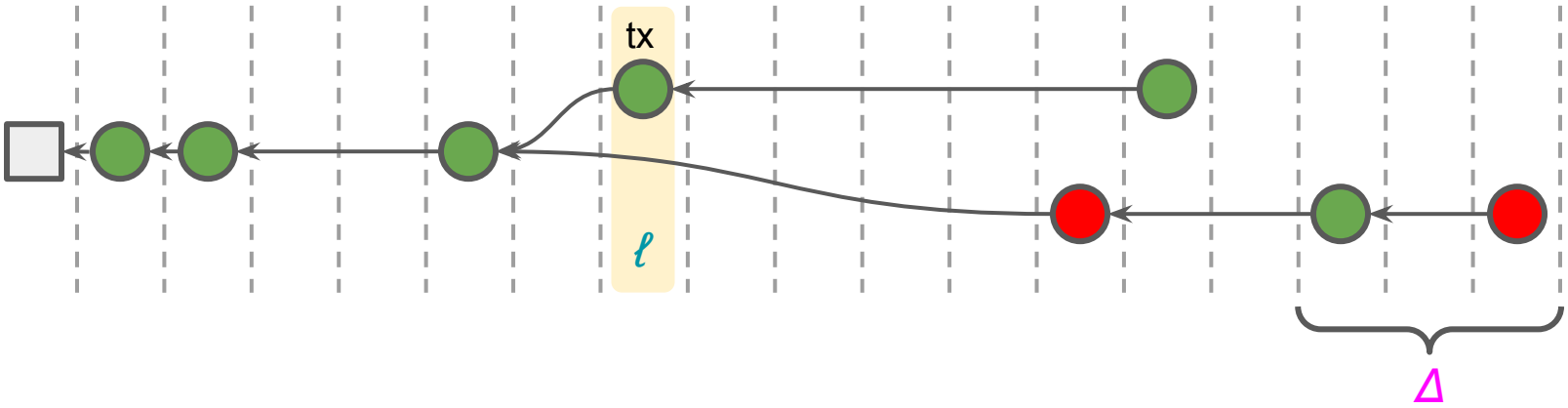
Characteristic Strings and Forks (Δ = 3)



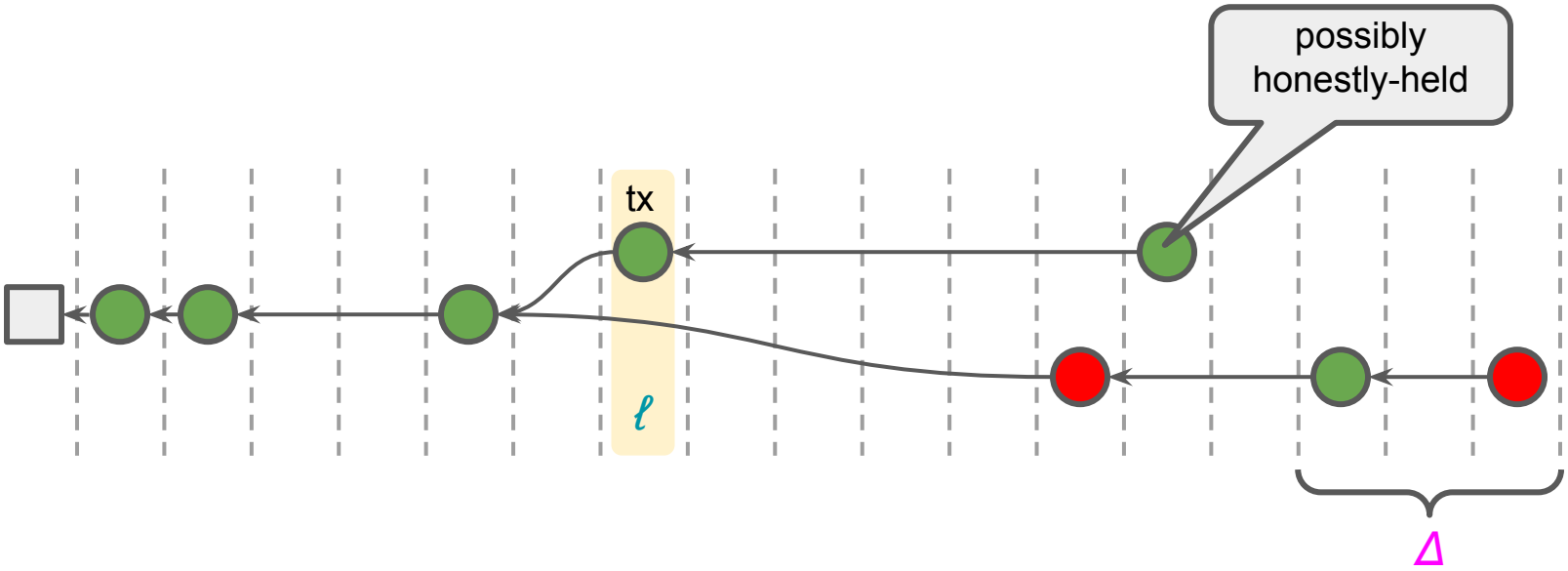


Tools: The Margin Quantity $\beta(.)$

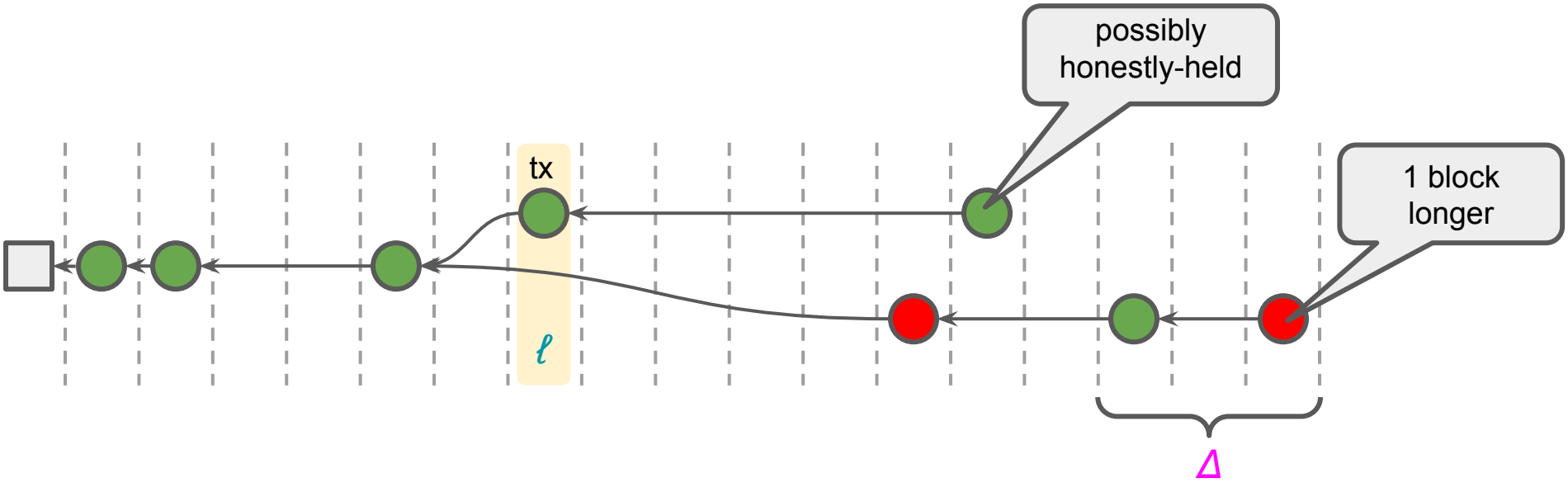
Tools: The Margin Quantity $\beta(.)$



Tools: The Margin Quantity $\beta(.)$

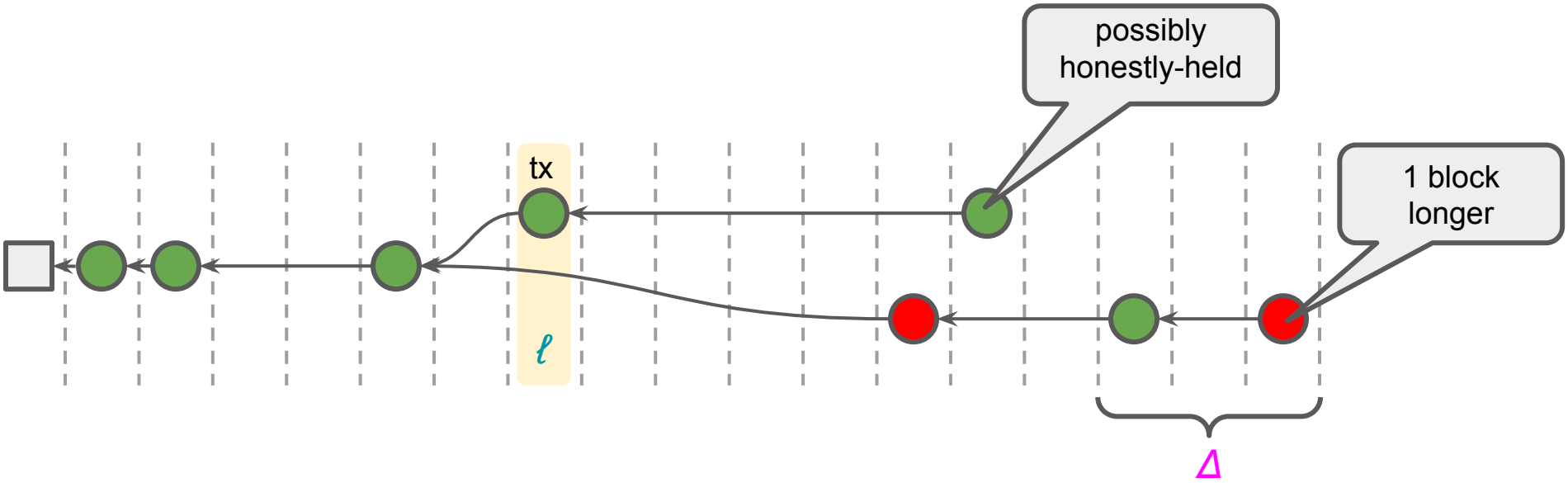


Tools: The Margin Quantity $\beta(.)$



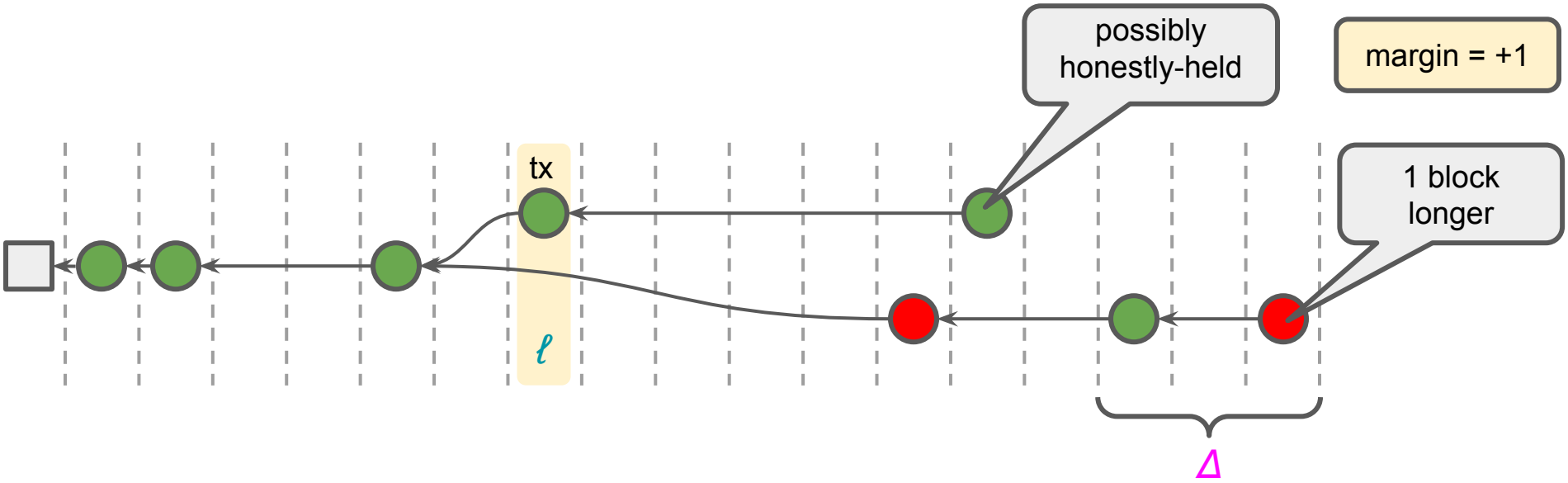
Tools: The Margin Quantity $\beta(.)$

- **margin of a tree**, $\beta_\ell(F)$
  - max. length advantage of a chain that differs from some "honest view" at ℓ



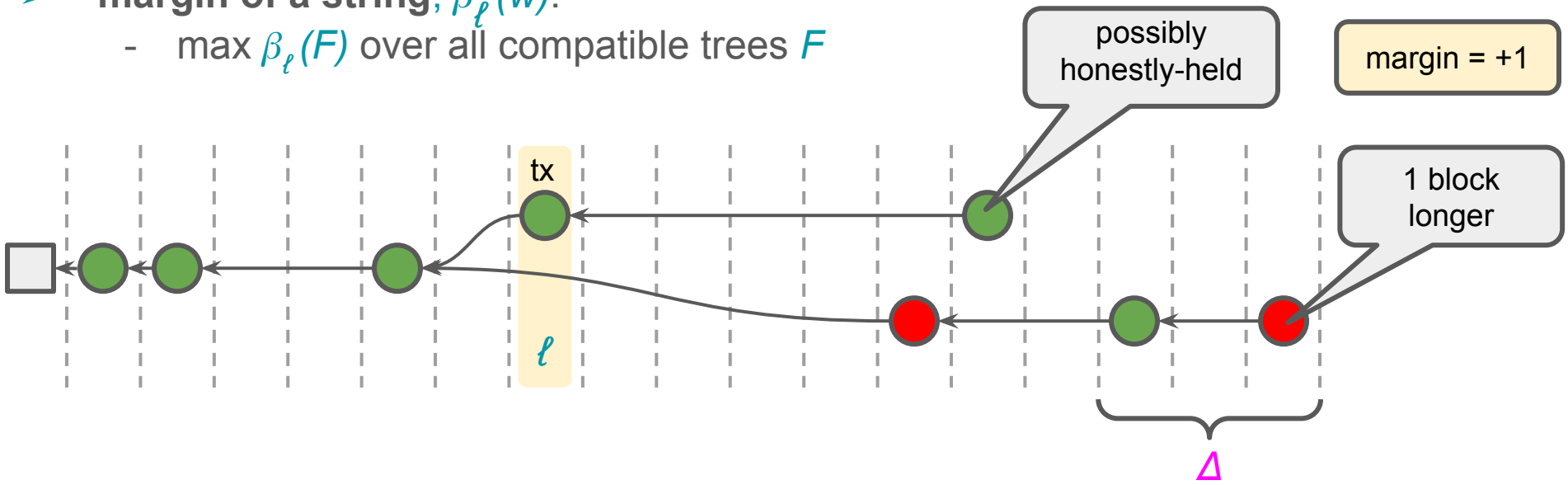
Tools: The Margin Quantity $\beta(.)$

- **margin of a tree**, $\beta_\ell(F)$
  - max. length advantage of a chain that differs from some "honest view" at ℓ



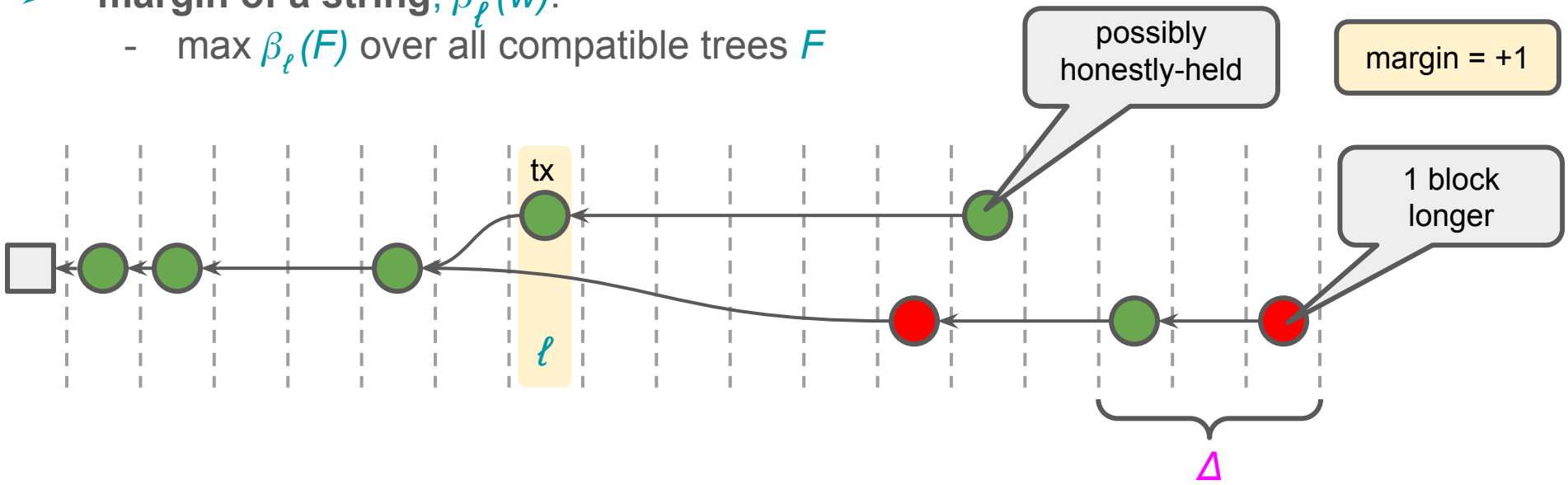
Tools: The Margin Quantity $\beta(.)$

- **margin of a tree**, $\beta_\ell(F)$
  - max. length advantage of a chain that differs from some "honest view" at ℓ
- **margin of a string**, $\beta_\ell(w)$:
  - max $\beta_\ell(F)$ over all compatible trees F



Tools: The Margin Quantity $\beta(.)$

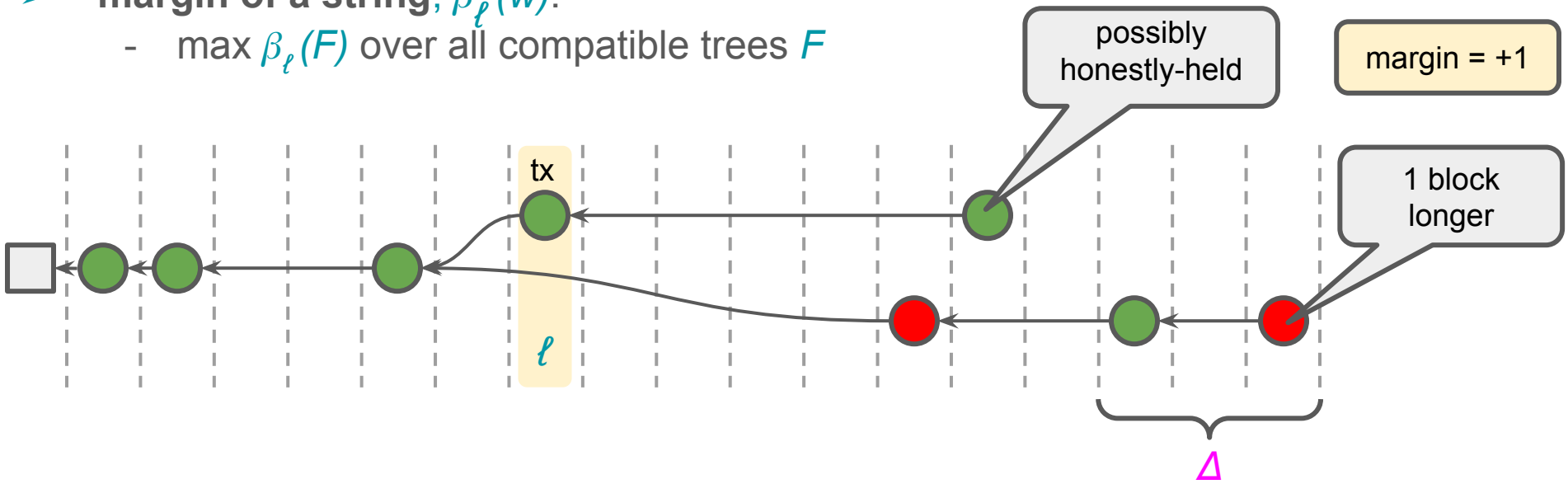
- **margin of a tree**, $\beta_\ell(F)$
  - max. length advantage of a chain that differs from some "honest view" at ℓ
- **margin of a string**, $\beta_\ell(w)$:
  - max $\beta_\ell(F)$ over all compatible trees F



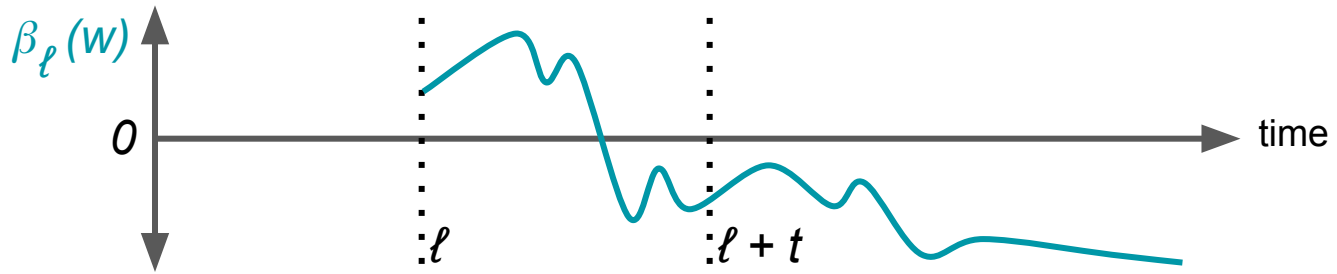
Crucial property: If $\beta_\ell(w) < 0$ then, after w, all honest parties' chains agree up to ℓ.

Tools: The Margin Quantity $\beta(.)$

- **margin of a tree**, $\beta_\ell(F)$
  - max. length advantage of a chain that differs from some "honest view" at ℓ
- **margin of a string**, $\beta_\ell(w)$:
  - max $\beta_\ell(F)$ over all compatible trees F



Crucial property: If $\beta_\ell(w) < 0$ then, after w, all honest parties' chains agree up to ℓ.



Detour: Longest-Chain Consistency Region

An easier but related question:

For which (r_h , r_a, Δ) do we get *any* eventual consistency?

Detour: Longest-Chain Consistency Region

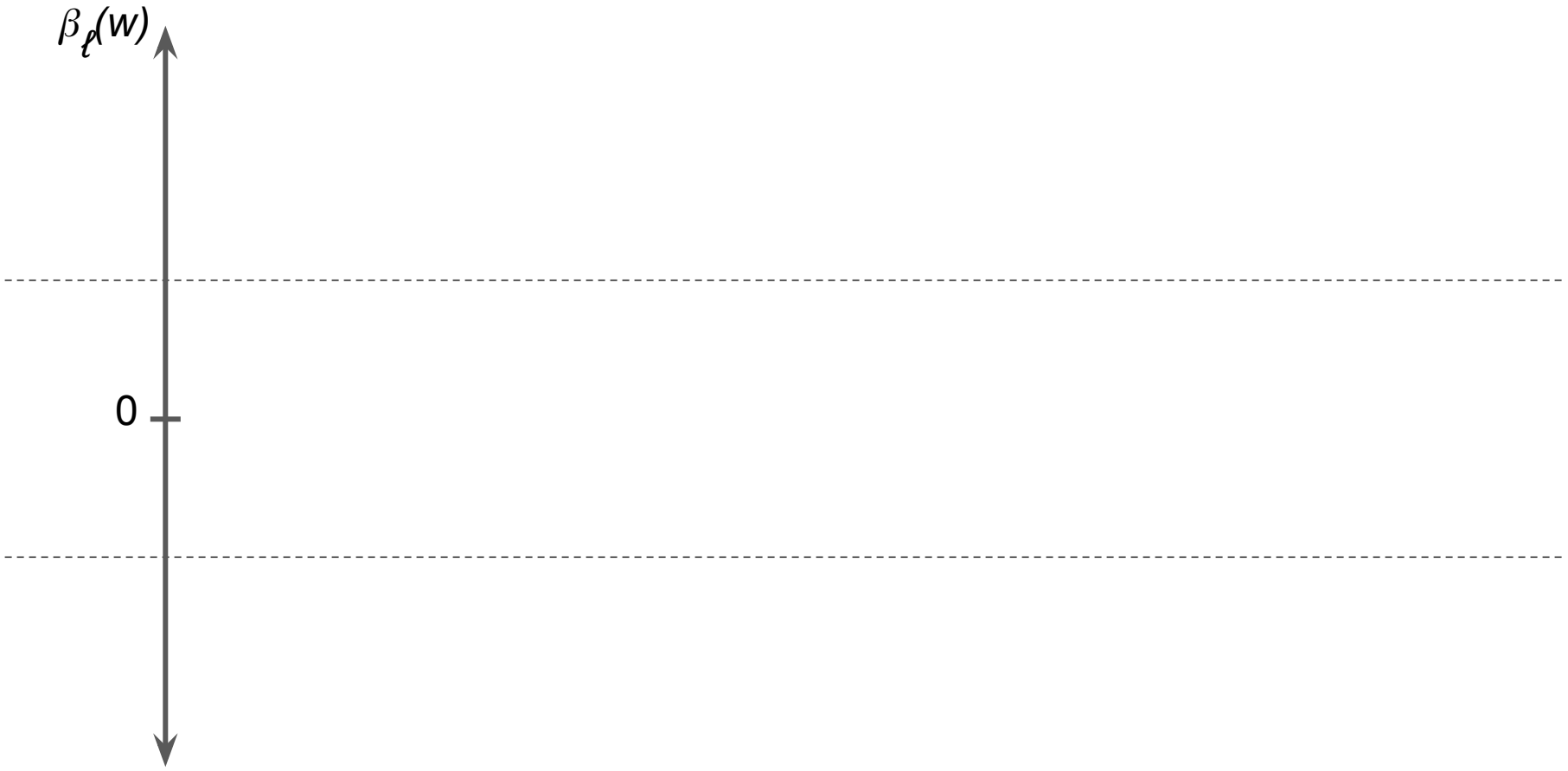
An easier but related question:

For which (r_h , r_a, Δ) do we get *any* eventual consistency?

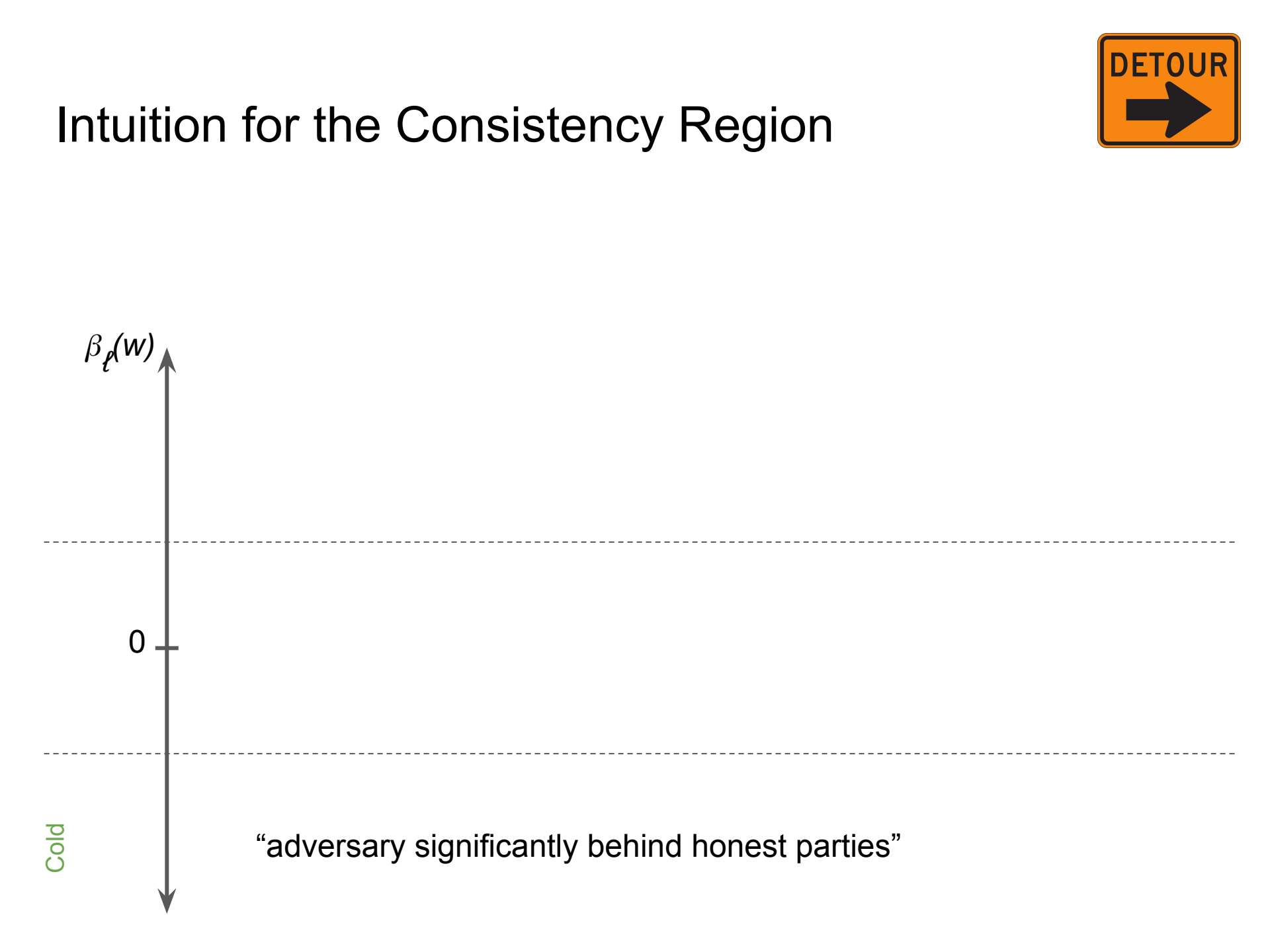
Fully answered in earlier work ([GKR,DKTTVWZ] @ CCS'20):

PoW/PoS longest-chain consensus is secure if $r_a < \frac{1}{\Delta + 1/r_h}$.

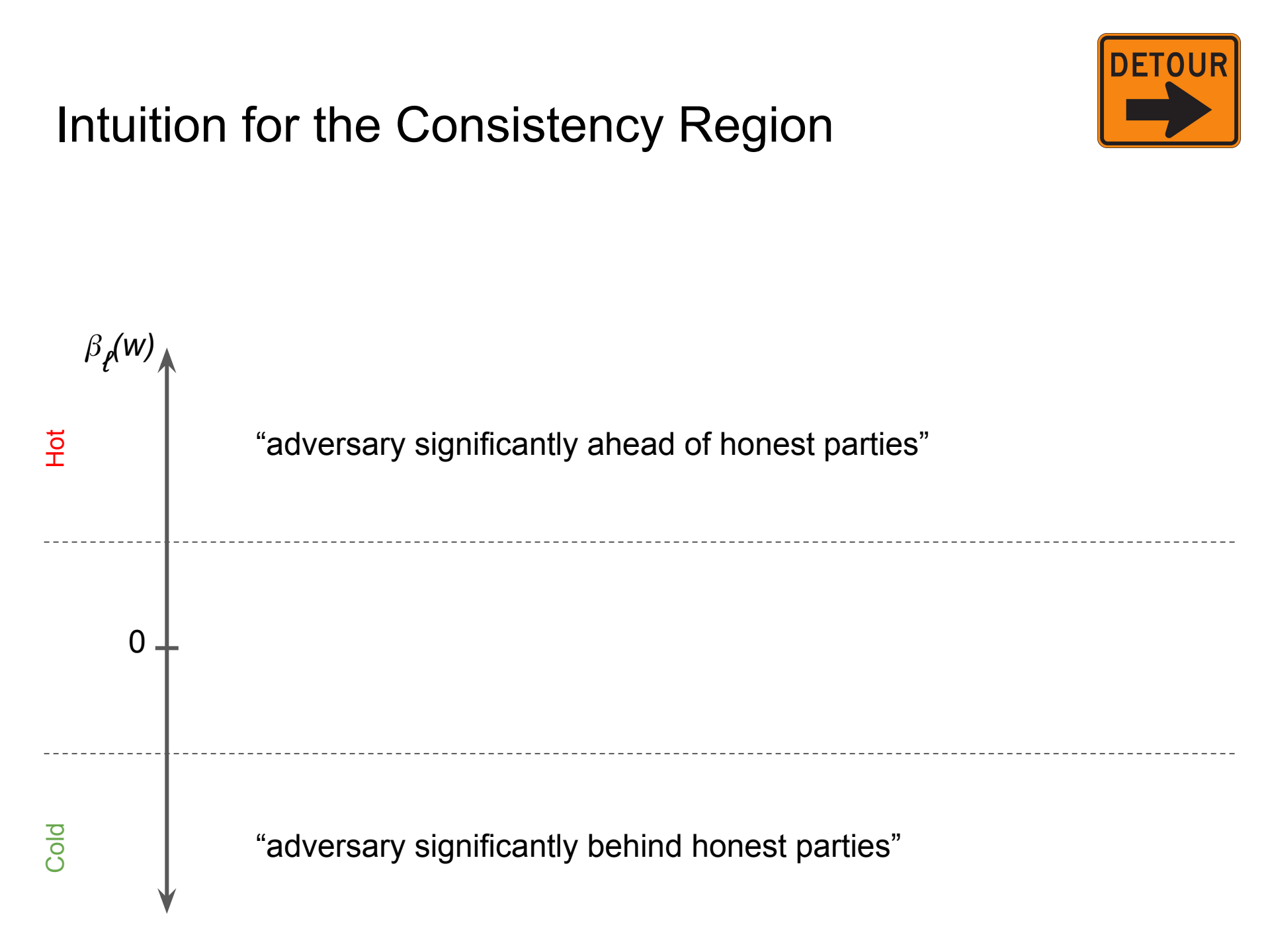
Intuition for the Consistency Region



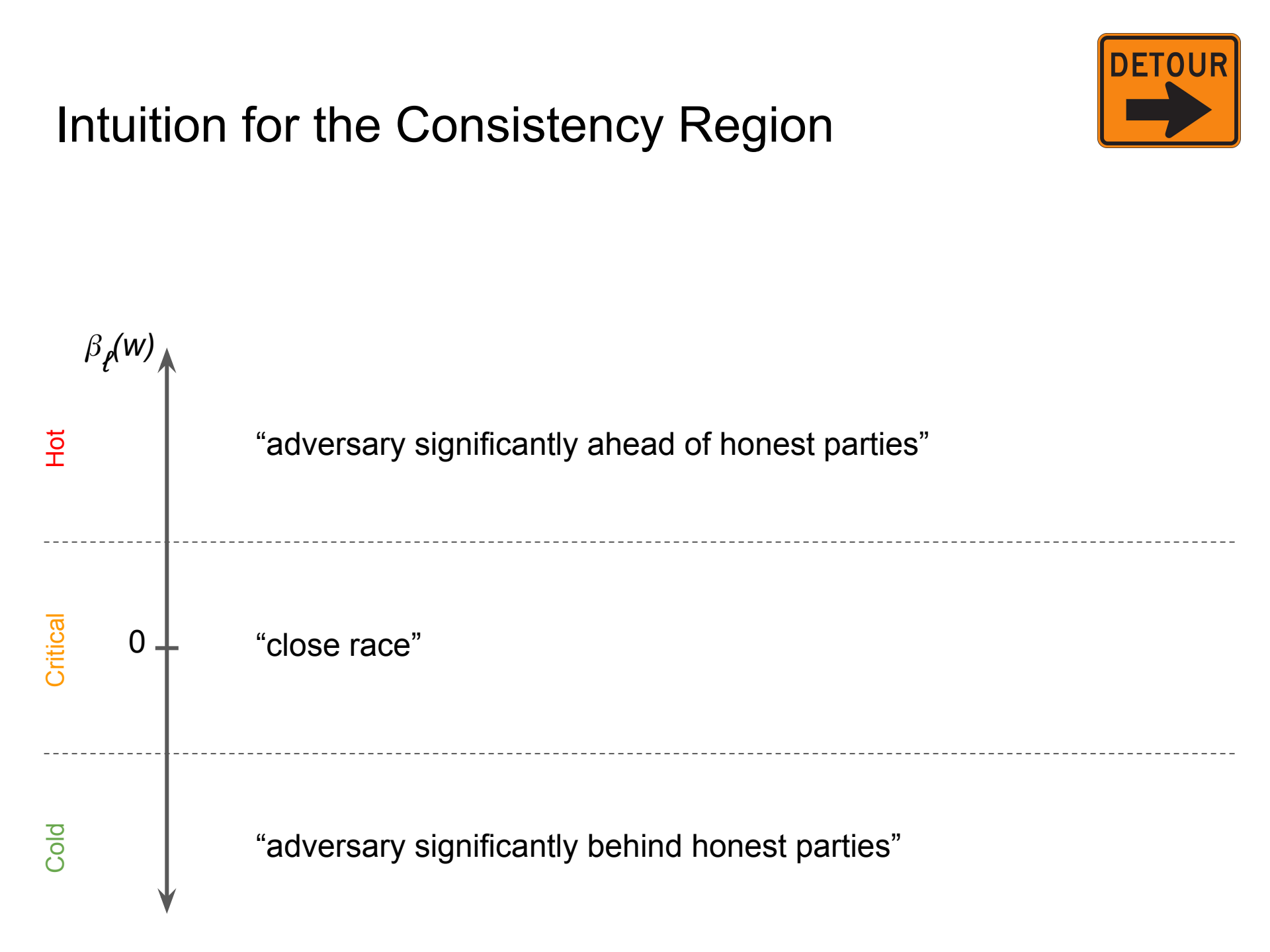
Intuition for the Consistency Region



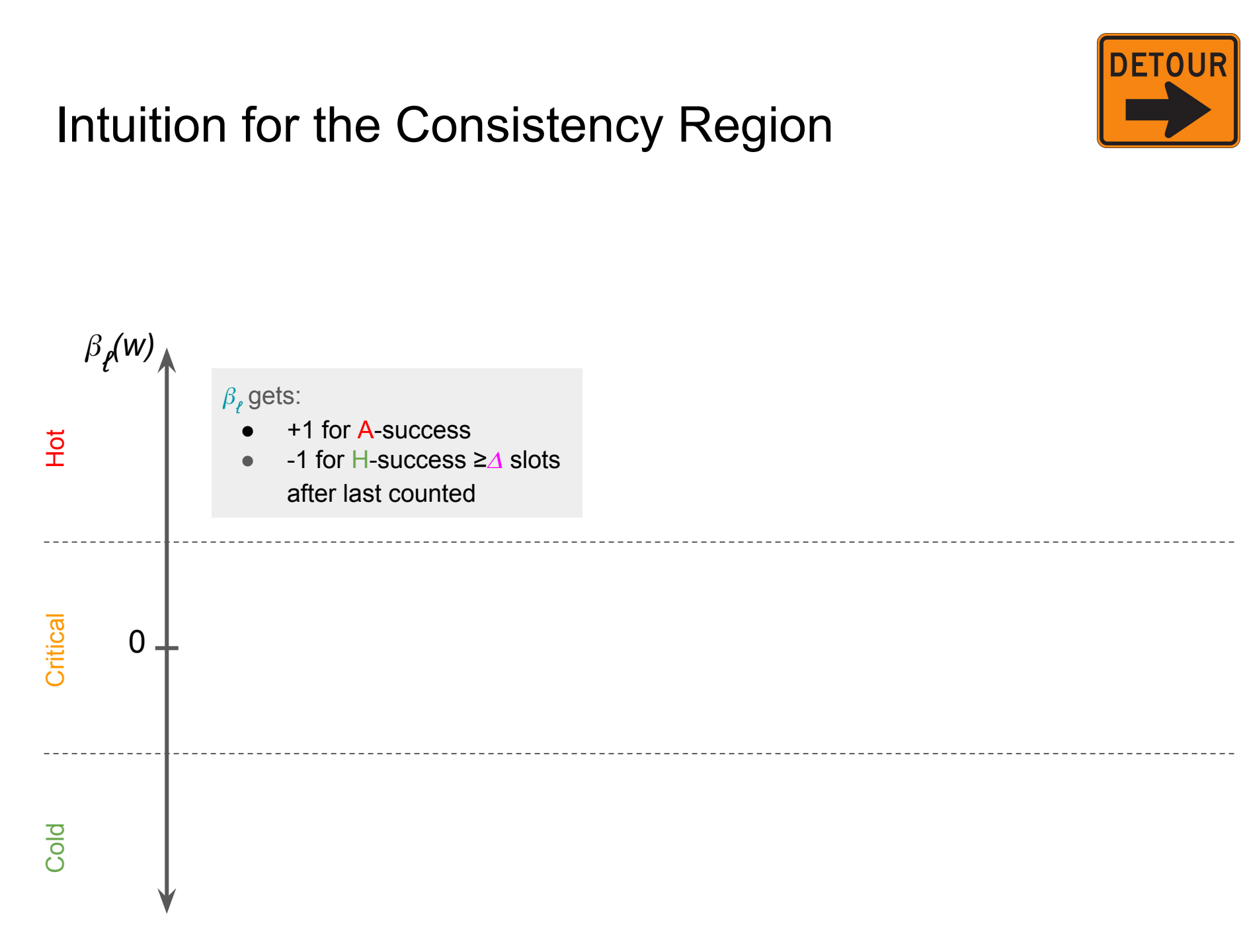
Intuition for the Consistency Region



Intuition for the Consistency Region

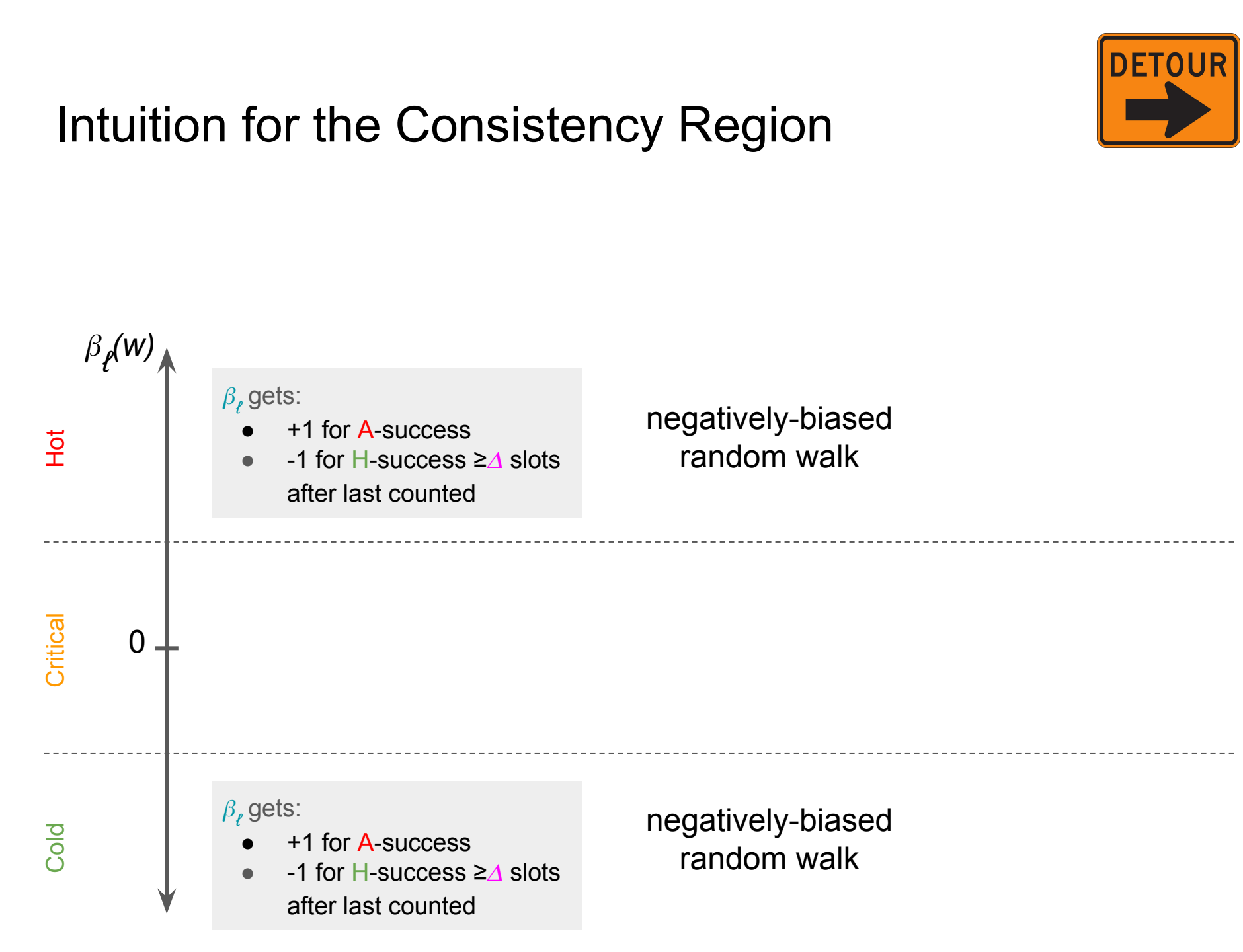


Intuition for the Consistency Region

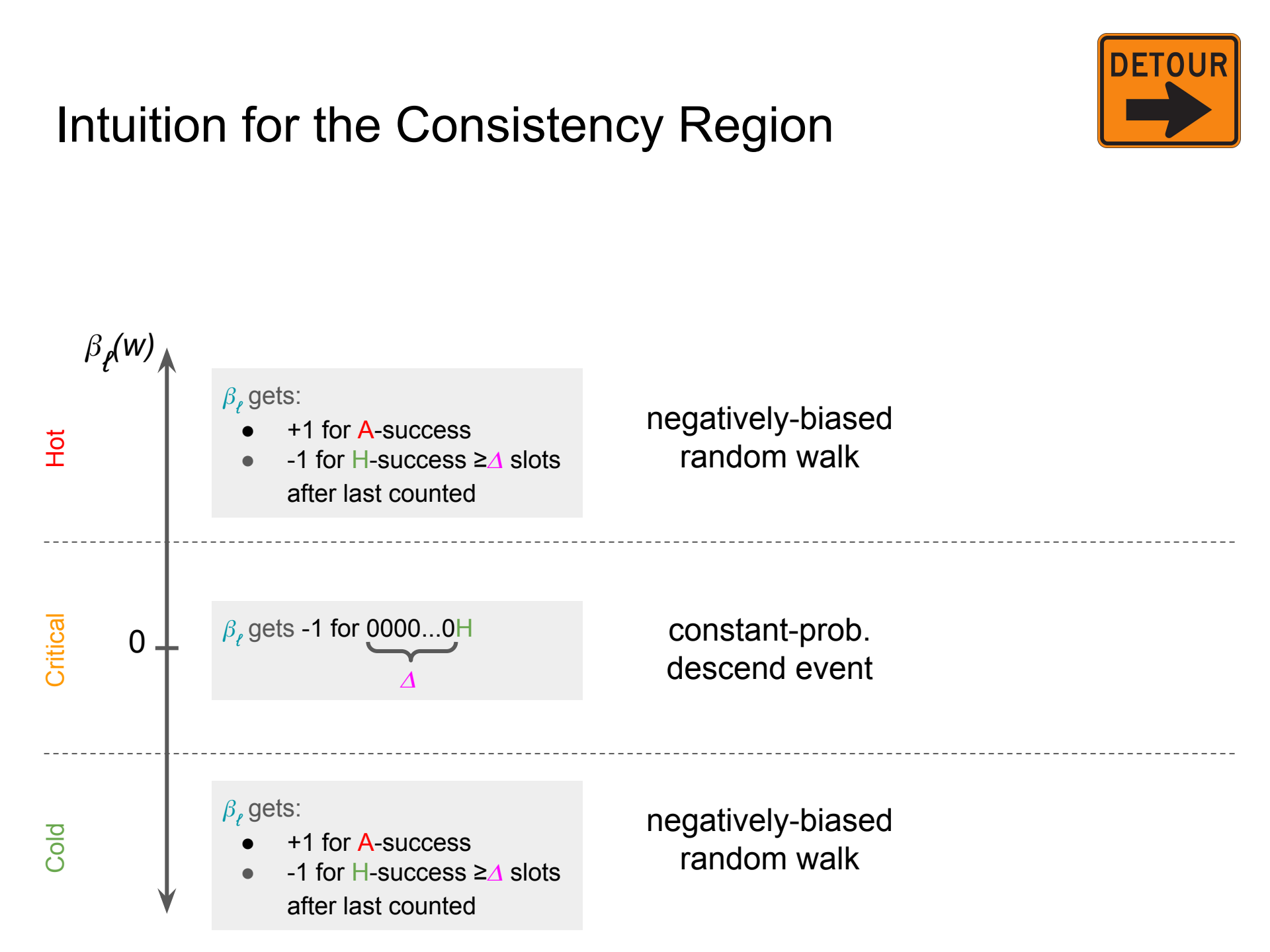


Intuition for the Consistency Region

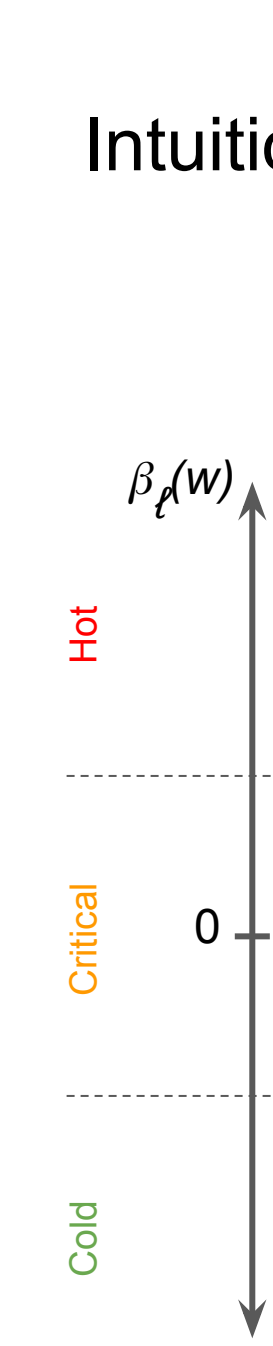
Intuition for the Consistency Region



Intuition for the Consistency Region



Intuition for the Consistency Region



β_ℓ gets:
- +1 for A-success
- -1 for H-success ≥Δ slots after last counted

negatively-biased random walk

- descends with certainty
- leaves quickly

β_ℓ gets -1 for $\underbrace{0000\ldots0}_{\Delta}$H

constant-prob. descend event

- descends with constant prob.
- leaves quickly

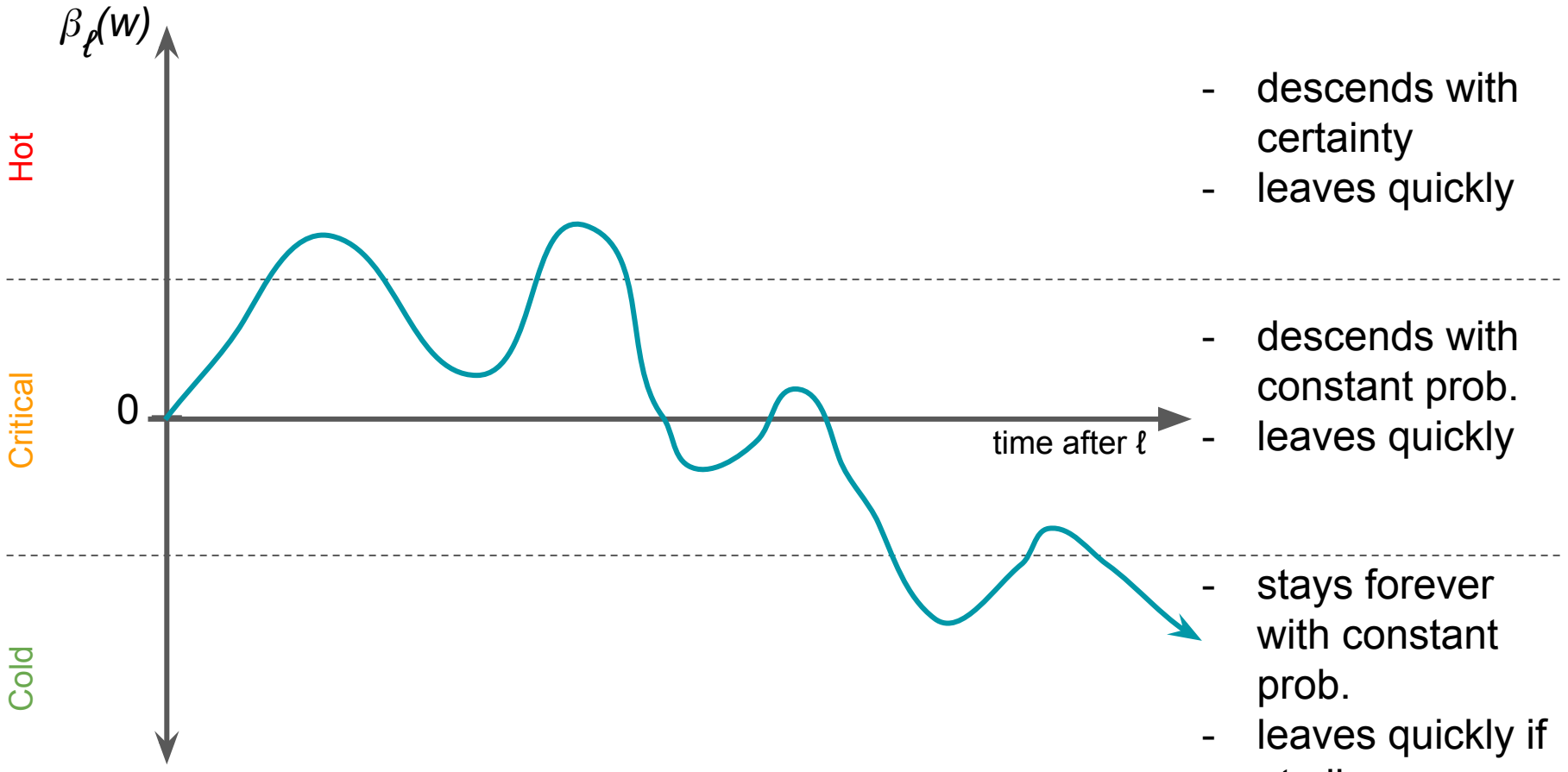
β_ℓ gets:
- +1 for A-success
- -1 for H-success ≥Δ slots after last counted

negatively-biased random walk

- stays forever with constant prob.
- leaves quickly if at all

Intuition for the Consistency Region

β_ℓ escapes to -∞ at a linear rate
(at time t is at position -Ω(t) except with probability exp(-Ω(t))

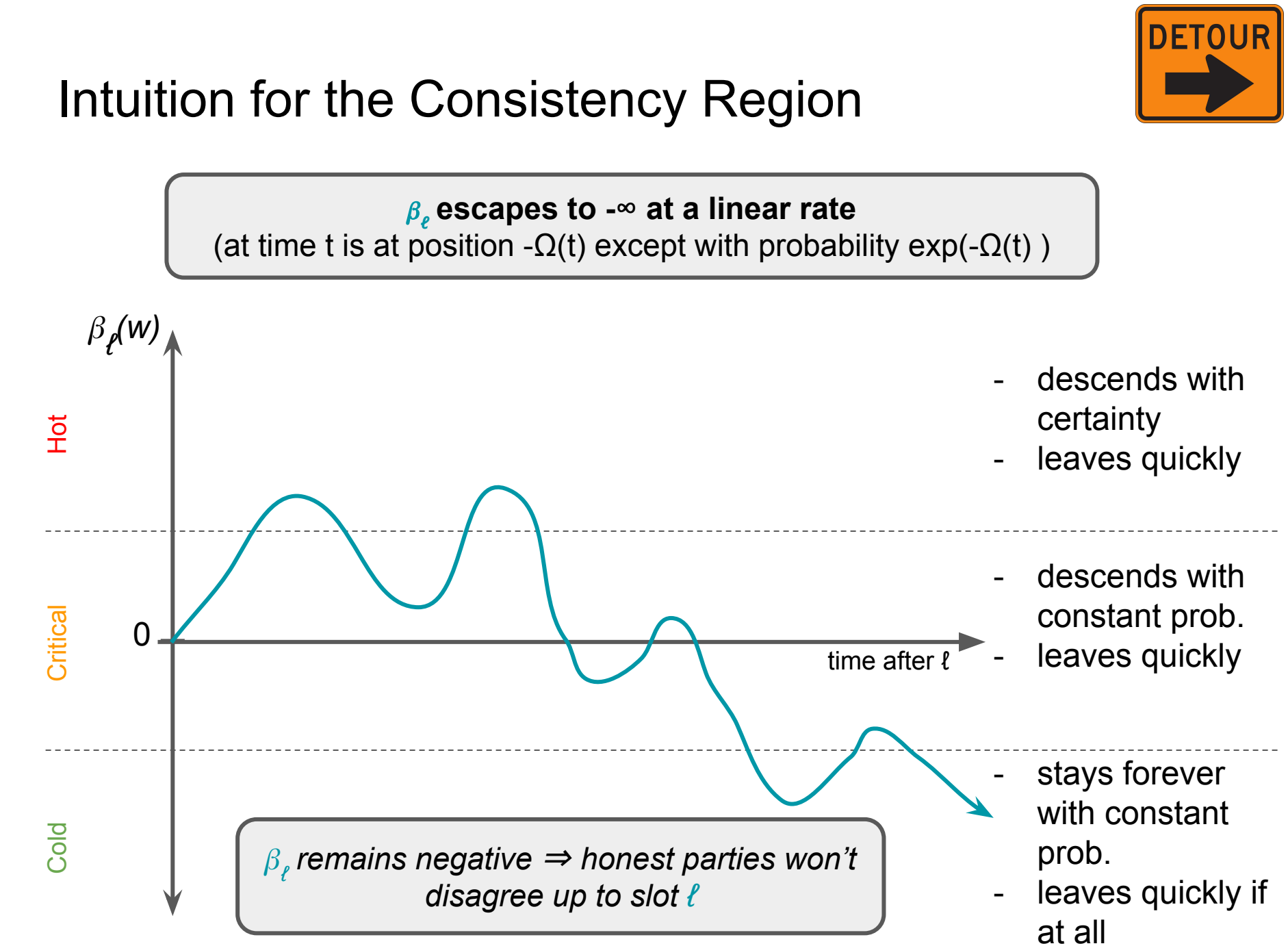


- descends with certainty
- leaves quickly

- descends with constant prob.
- leaves quickly

- stays forever with constant prob.
- leaves quickly if at all

Intuition for the Consistency Region



β_ℓ escapes to -∞ at a linear rate
(at time t is at position -Ω(t) except with probability exp(-Ω(t))

$\beta_\ell(w)$

Hot

Critical

Cold

0

time after ℓ

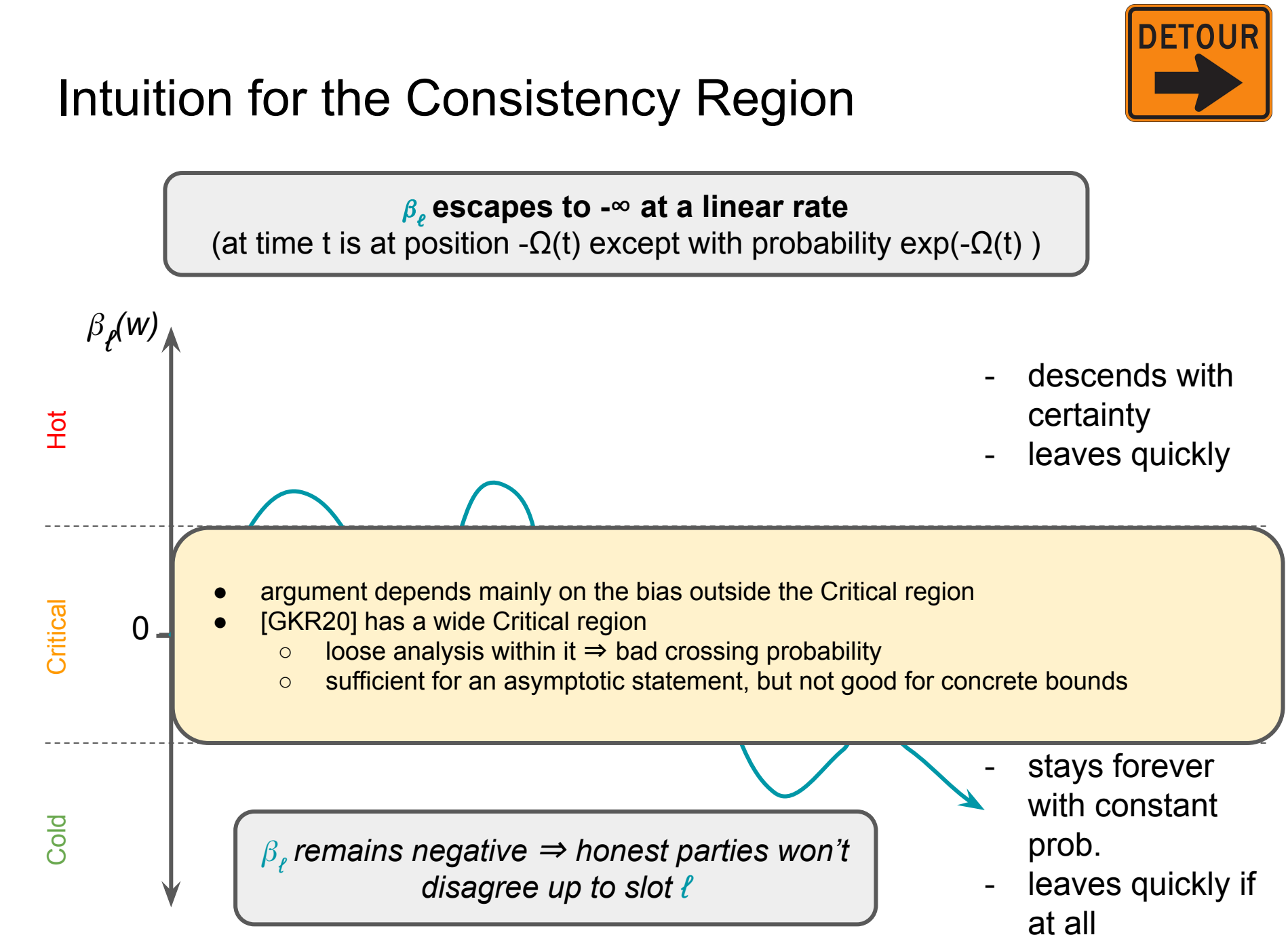
- descends with certainty
- leaves quickly

- descends with constant prob.
- leaves quickly

- stays forever with constant prob.
- leaves quickly if at all

β_ℓ remains negative ⇒ honest parties won't disagree up to slot ℓ

Intuition for the Consistency Region



β_ℓ escapes to -∞ at a linear rate
(at time t is at position -Ω(t) except with probability exp(-Ω(t))

$\beta_\ell(w)$

Hot

Critical

0

Cold

- descends with certainty
- leaves quickly

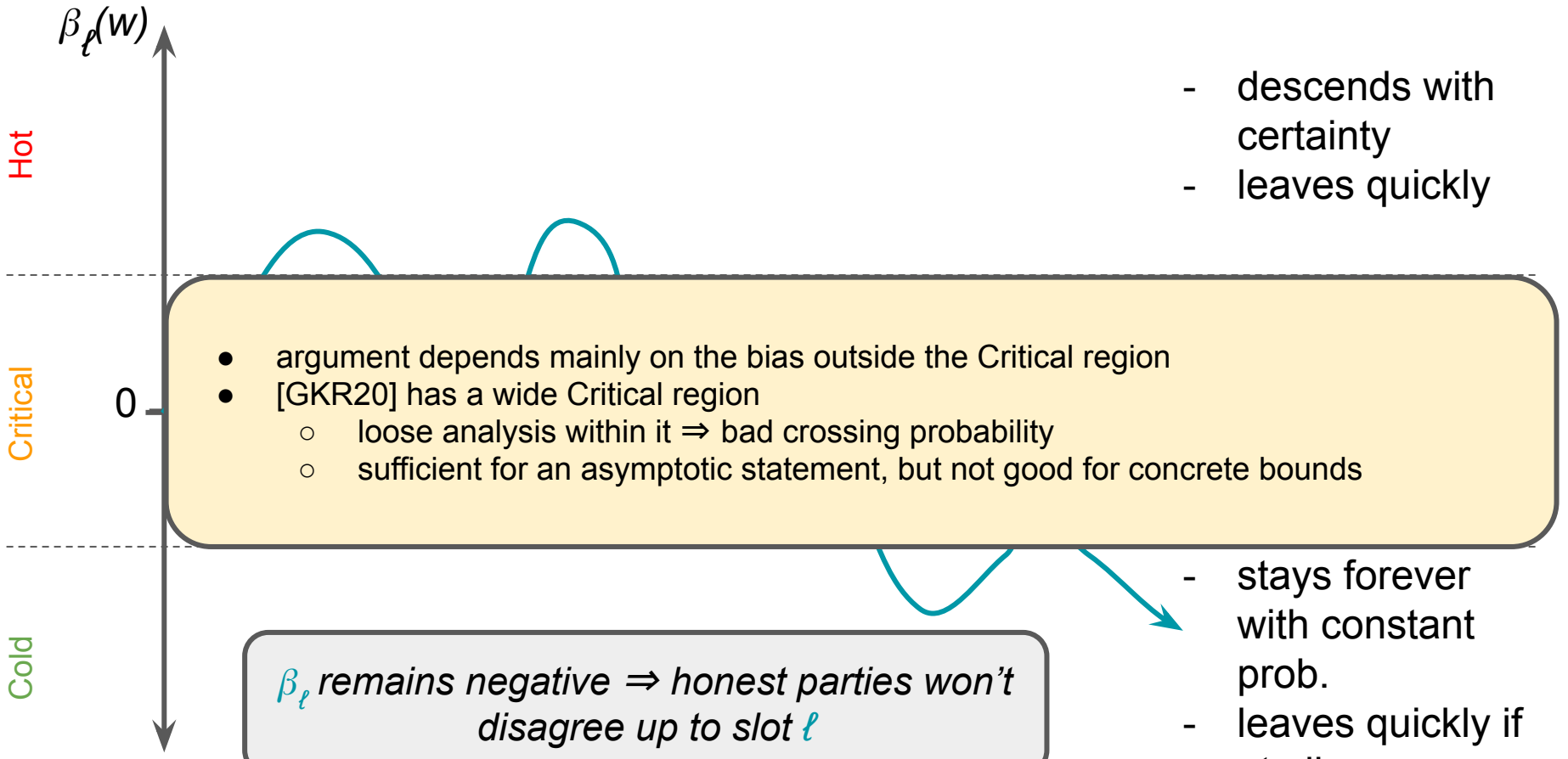
- argument depends mainly on the bias outside the Critical region
- [GKR20] has a wide Critical region
  - loose analysis within it ⇒ bad crossing probability
  - sufficient for an asymptotic statement, but not good for concrete bounds

- stays forever with constant prob.
- leaves quickly if at all

β_ℓ remains negative ⇒ honest parties won't disagree up to slot ℓ

Intuition for the Consistency Region

β_ℓ escapes to -∞ at a linear rate
(at time t is at position -Ω(t) except with probability exp(-Ω(t))



- descends with certainty
- leaves quickly

- argument depends mainly on the bias outside the Critical region
- [GKR20] has a wide Critical region
  - loose analysis within it ⇒ bad crossing probability
  - sufficient for an asymptotic statement, but not good for concrete bounds

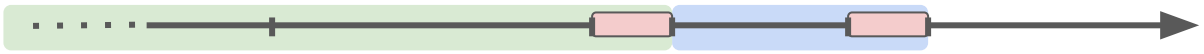
- stays forever with constant prob.
- leaves quickly if at all

β_ℓ remains negative ⇒ honest parties won't disagree up to slot ℓ

This Work: Technical Overview in a Nutshell

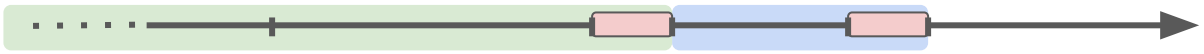
This Work: Technical Overview in a Nutshell

- a novel way to analyze the execution in larger chunks (“**phases**”)

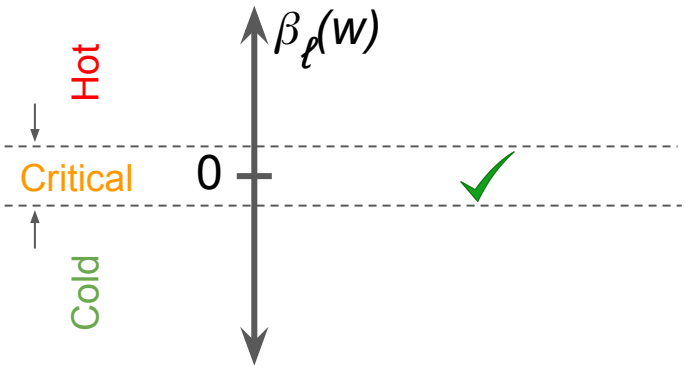


This Work: Technical Overview in a Nutshell

- a novel way to analyze the execution in larger chunks (“**phases**”)

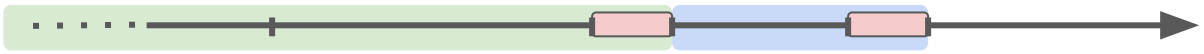


- allows for:
  - a narrow critical region
  - a practically tight analysis of margin while crossing it

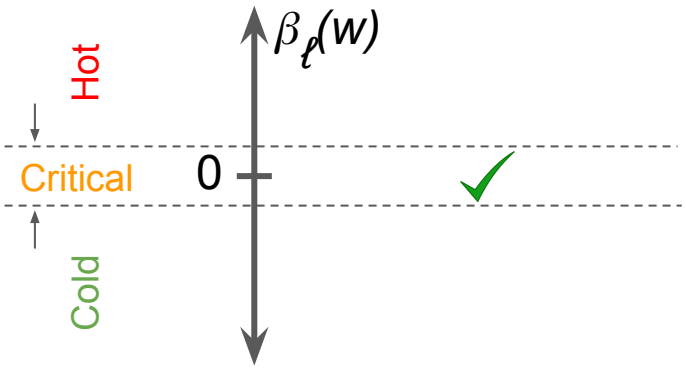


This Work: Technical Overview in a Nutshell

- a novel way to analyze the execution in larger chunks (“**phases**”)



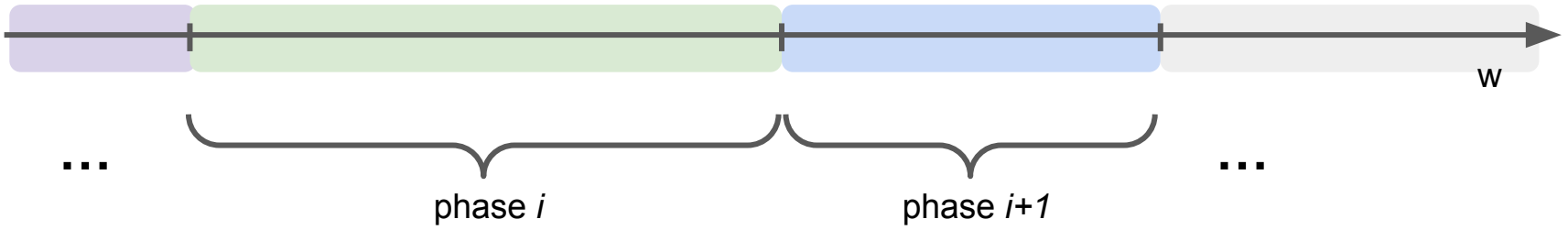
- allows for:
  - a narrow critical region
  - a practically tight analysis of margin while crossing it



- margin recurrences that can be simulated for practical settlement bounds

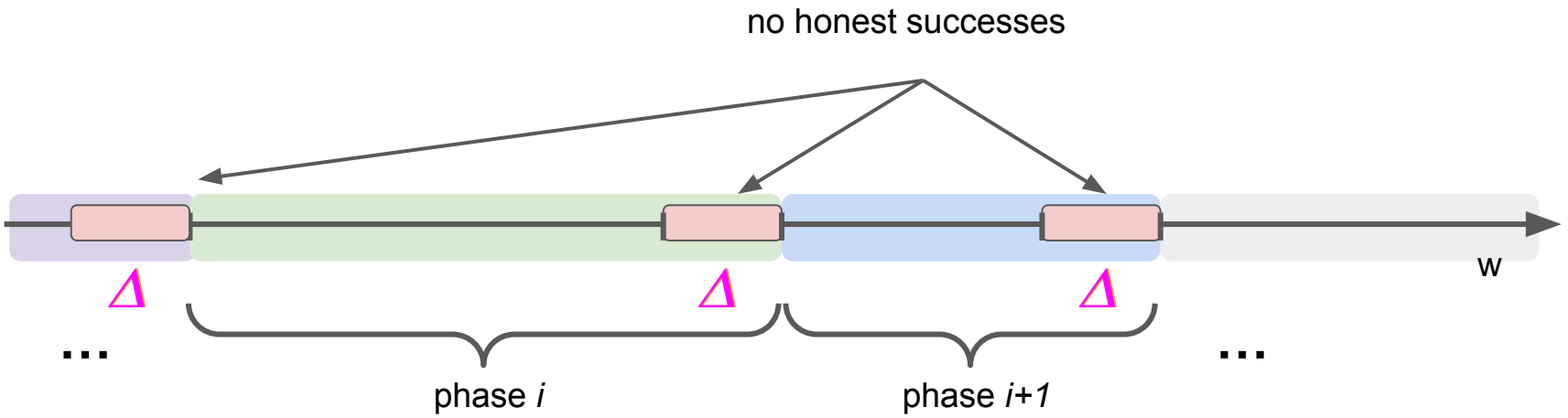
Splitting Execution into Phases

- consecutive, non-overlapping slot sequences
- **Goal:** honest party producing a block is aware of all honest blocks produced in all previous phases

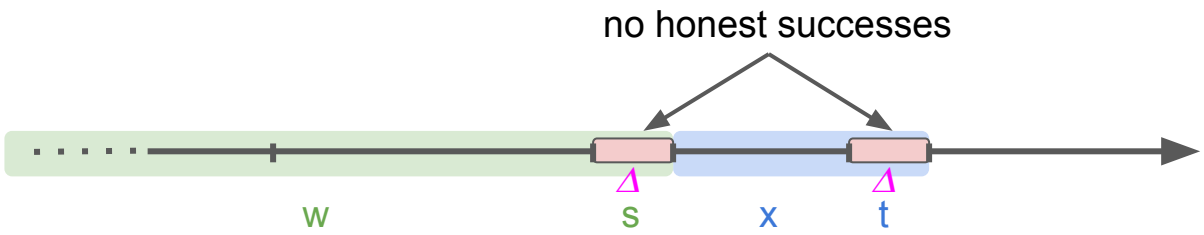


Splitting Execution into Phases

- consecutive, non-overlapping slot sequences
- **Goal:** honest party producing a block is aware of all honest blocks produced in all previous phases
- **Definition:** phase ends with Δ-long honest silence



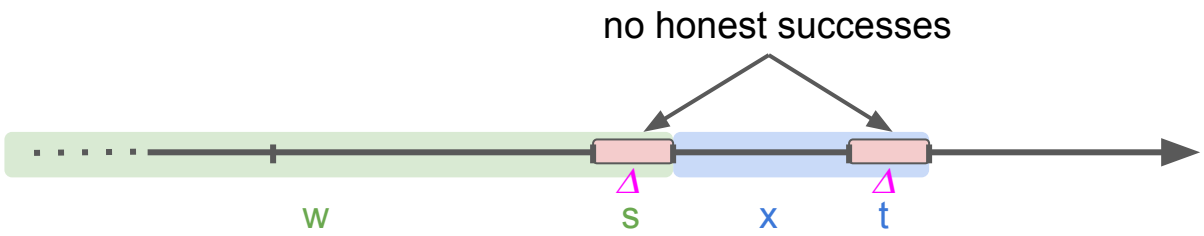
Analysis Plan: Phase Recurrences



1. Devise recurrences upper-bounding β_ℓ(wsxt) based on
   - β_ℓ(ws)
   - some properties of xt

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + F(\text{xt})$$

Analysis Plan: Phase Recurrences



1. Devise recurrences upper-bounding β_ℓ(wsxt) based on
   - β_ℓ(ws)
   - some properties of xt

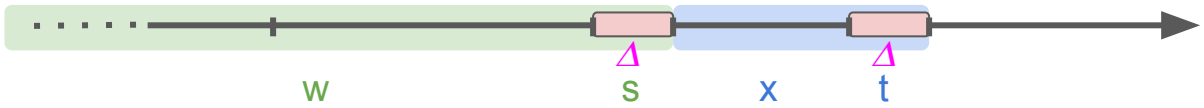
$$\beta_\ell(\text{wsxt}) \leq \beta_\ell(\text{ws}) + F(\text{xt})$$

2. Iteratively upper-bound $\beta_\ell(.)$ throughout the full execution

PoW Phase Recurrences: Intuition

- “ideal” recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \ldots - \ldots$$

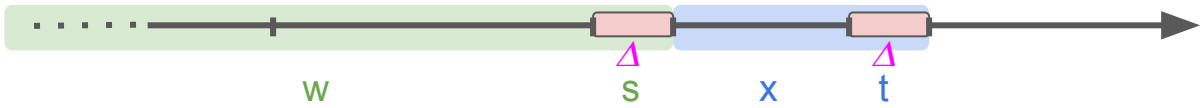


PoW Phase Recurrences: Intuition

- “ideal” recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - \ldots$$

+1 for each adversarial success



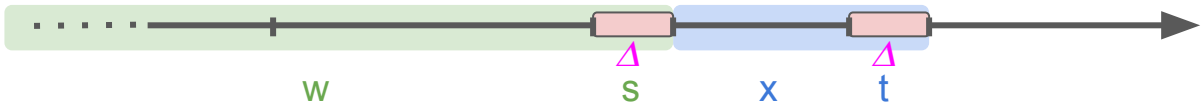
PoW Phase Recurrences: Intuition

- “ideal” recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each “honest depth” increase



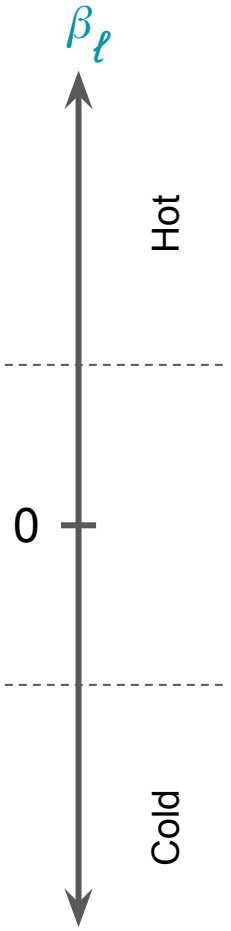
PoW Phase Recurrences: Intuition

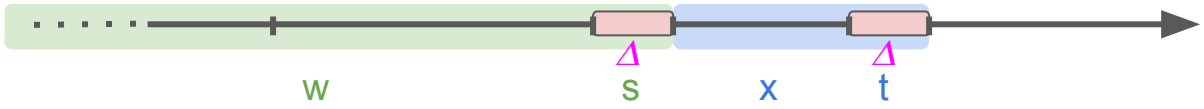
- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase





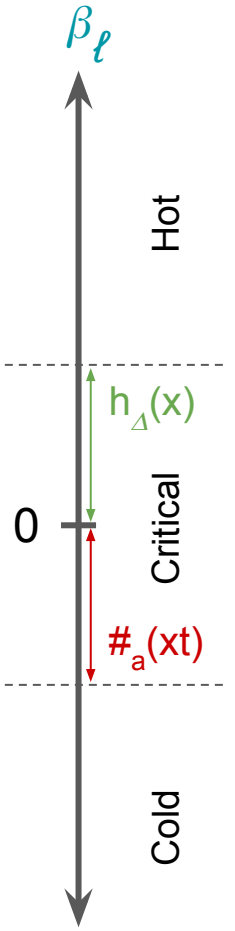
PoW Phase Recurrences: Intuition

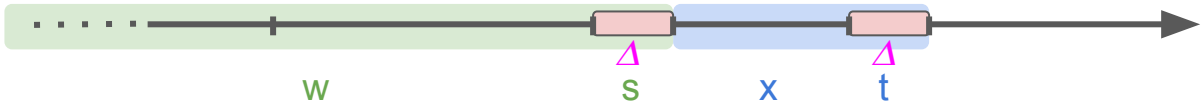
- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase





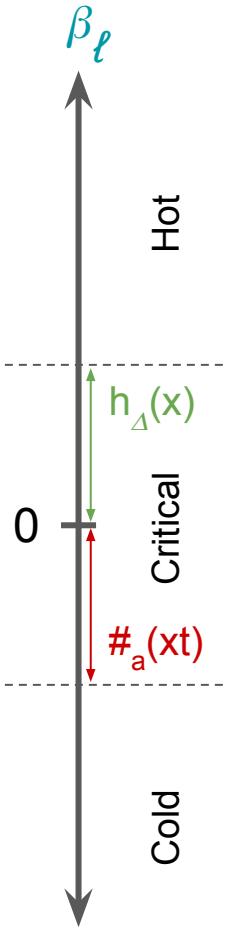
PoW Phase Recurrences: Intuition

- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

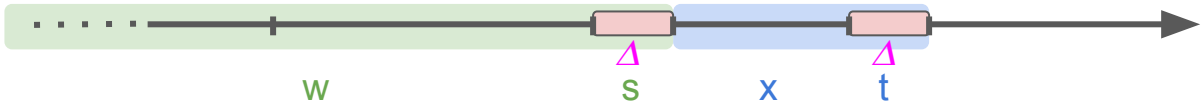
-1 for each honest depth increase



- **Critical region:** two upper bounds

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + \#_a(\text{xt})$$

$$\beta_\ell(\text{wsxt}) \le \#_a(\text{xt})$$



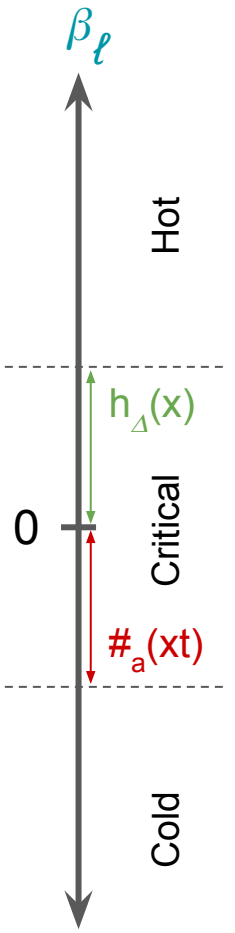
PoW Phase Recurrences: Intuition

- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase

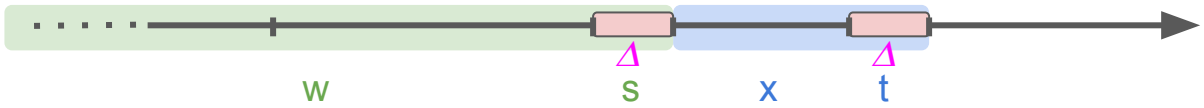


- **Critical region:** two upper bounds

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + \#_a(\text{xt})$$

Negative $\beta_\ell(\text{ws})$: as if honest successes don't count

$$\beta_\ell(\text{wsxt}) \le \#_a(\text{xt})$$



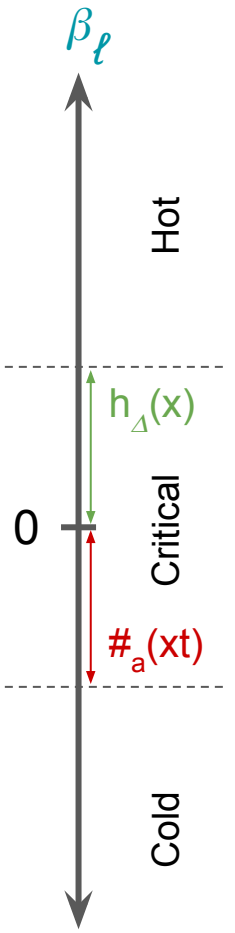
PoW Phase Recurrences: Intuition

- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase



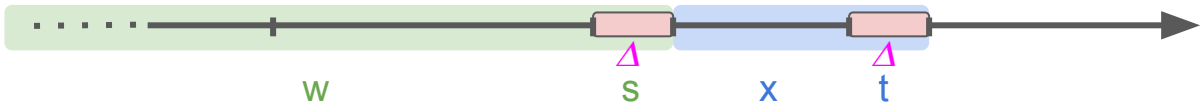
- **Critical region:** two upper bounds

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + \#_a(\text{xt})$$

Negative $\beta_\ell(\text{ws})$: as if honest successes don't count

$$\beta_\ell(\text{wsxt}) \le \#_a(\text{xt})$$

Positive $\beta_\ell(\text{ws})$: as if honest successes don't count after reaching 0



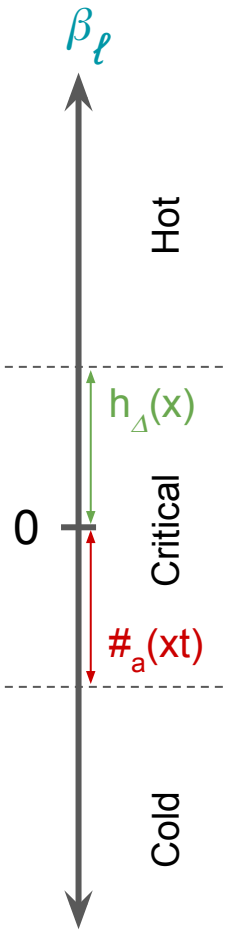
PoW Phase Recurrences: Intuition

- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase



- **Critical region:** two upper bounds

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + \#_a(\text{xt})$$

Negative $\beta_\ell(\text{ws})$: as if honest successes don't count

$$\beta_\ell(\text{wsxt}) \le \#_a(\text{xt})$$

Positive $\beta_\ell(\text{ws})$: as if honest successes don't count after reaching 0

- **Crossing zero:** If $\beta_\ell(\text{ws}) = 0$ then $\beta_\ell(\text{ws}0^\Delta\text{h}) = -1$.

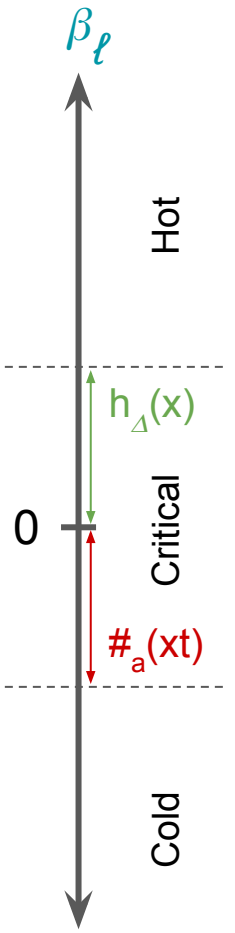
PoW Phase Recurrences: Intuition

- **Hot & cold regions:** "ideal" recurrence

$$\beta_\ell(\text{wsxt}) = \beta_\ell(\text{ws}) + \#_a(\text{xt}) - h_\Delta(\text{x})$$

+1 for each adversarial success

-1 for each honest depth increase



- **Critical region:** two upper bounds

$$\beta_\ell(\text{wsxt}) \le \beta_\ell(\text{ws}) + \#_a(\text{xt})$$

Negative $\beta_\ell(\text{ws})$: as if honest successes don't count

$$\beta_\ell(\text{wsxt}) \le \#_a(\text{xt})$$

Positive $\beta_\ell(\text{ws})$: as if honest successes don't count after reaching 0

- **Crossing zero:** If $\beta_\ell(\text{ws}) = 0$ then $\beta_\ell(\text{ws}0^\Delta\text{h}) = -1$.

Proofs: Tree surgery.

PoS Complications

PoS Complications

- different **tree** notion
  - single (adversarial) success allows extending many chains

PoS Complications

- different **tree** notion
  - single (adversarial) success allows extending many chains

- two intertwined characteristic quantities
  - **reach**: the maximal “potential” length of a chain
    - simpler than margin
  - **margin**: analogous to the PoW margin
    - more complicated than in PoW, as it depends on reach

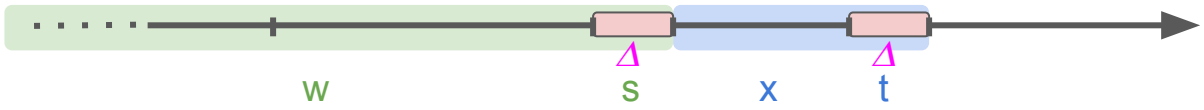
PoS Complications

- different **tree** notion
  - single (adversarial) success allows extending many chains

- two intertwined characteristic quantities
  - **reach**: the maximal “potential” length of a chain
    - simpler than margin
  - **margin**: analogous to the PoW margin
    - more complicated than in PoW, as it depends on reach

- the recurrence must compute these in tandem
  - determine both values for wsxt based on both values on ws

$$Q(wsxt) \leq Q(ws) + F(xt)$$



PoW vs. PoS Phase Recurrences

$$Q(wsxt) \leq Q(ws) + F(xt)$$

- PoW recurrences simpler
  - single quantity
  - outside Critical: a simple race between adversarial successes and honest depth
  - crossing zero easier: does not depend on another quantity

PoW vs. PoS Phase Recurrences

$$Q(wsxt) \leq Q(ws) + F(xt)$$

- PoW recurrences simpler
  - single quantity
  - outside Critical: a simple race between adversarial successes and honest depth
  - crossing zero easier: does not depend on another quantity

- both recurrences can be numerically simulated
  - albeit, PoW easier

PoW vs. PoS Phase Recurrences

$$Q(wsxt) \leq Q(ws) + F(xt)$$

- PoW recurrences simpler
  - single quantity
  - outside Critical: a simple race between adversarial successes and honest depth
  - crossing zero easier: does not depend on another quantity

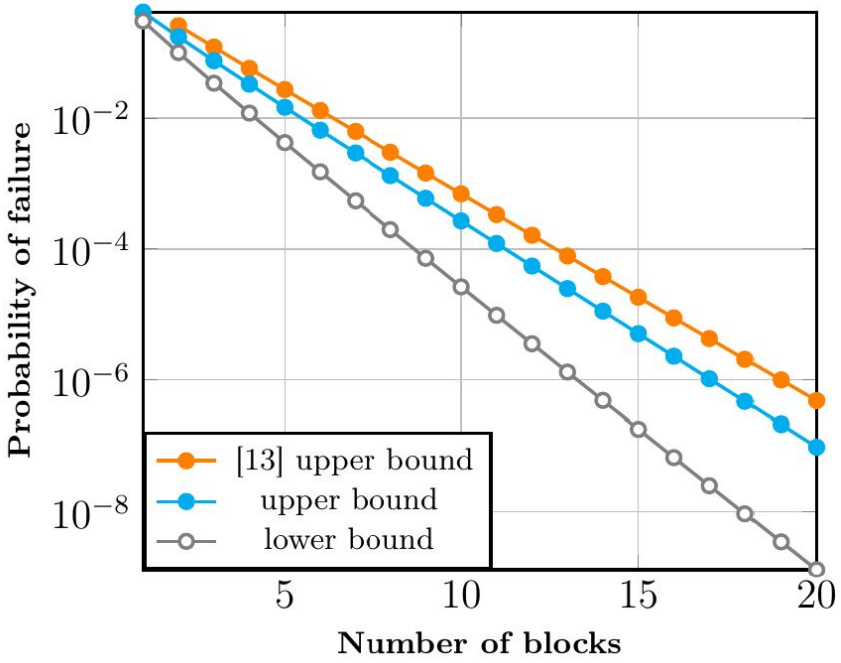
- both recurrences can be numerically simulated
  - albeit, PoW easier

- PoW recurrences give slightly faster settlement

Explicit Results

Explicit Results

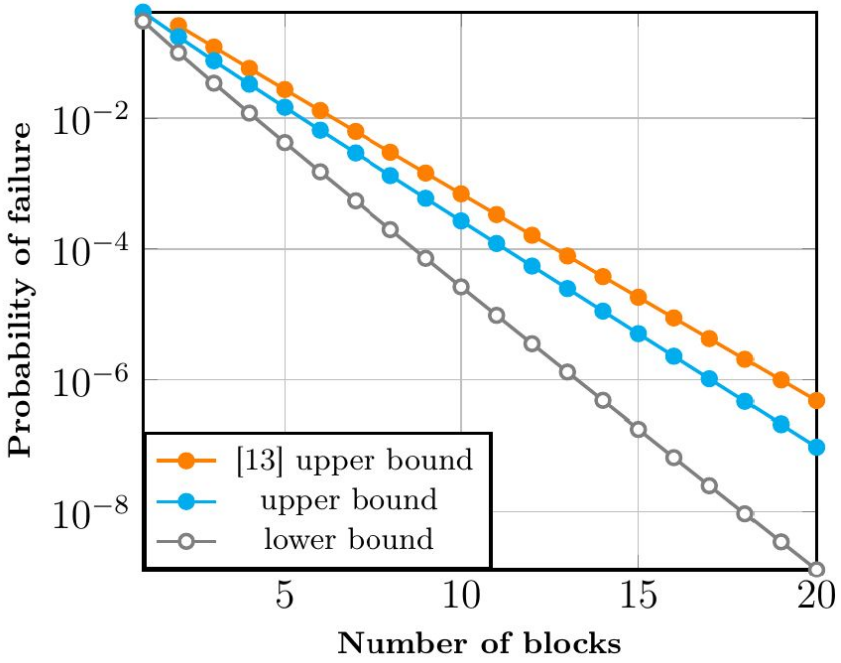
Ethereum (PoW)



- block time: 13 seconds
- Δ = 2 seconds
- adversarial mining power: 10%

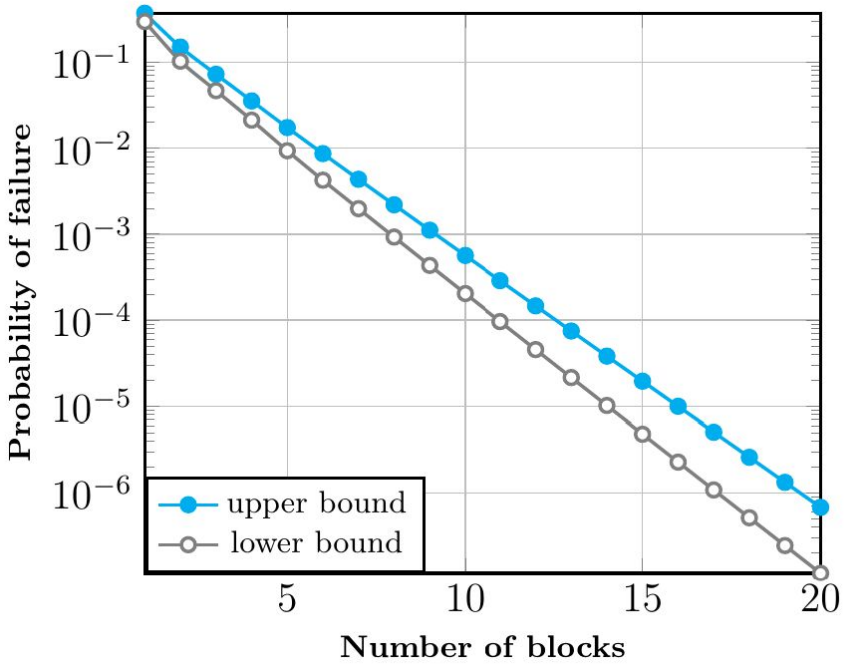
Explicit Results

Ethereum (PoW)



- block time: 13 seconds
- Δ = 2 seconds
- adversarial mining power: 10%

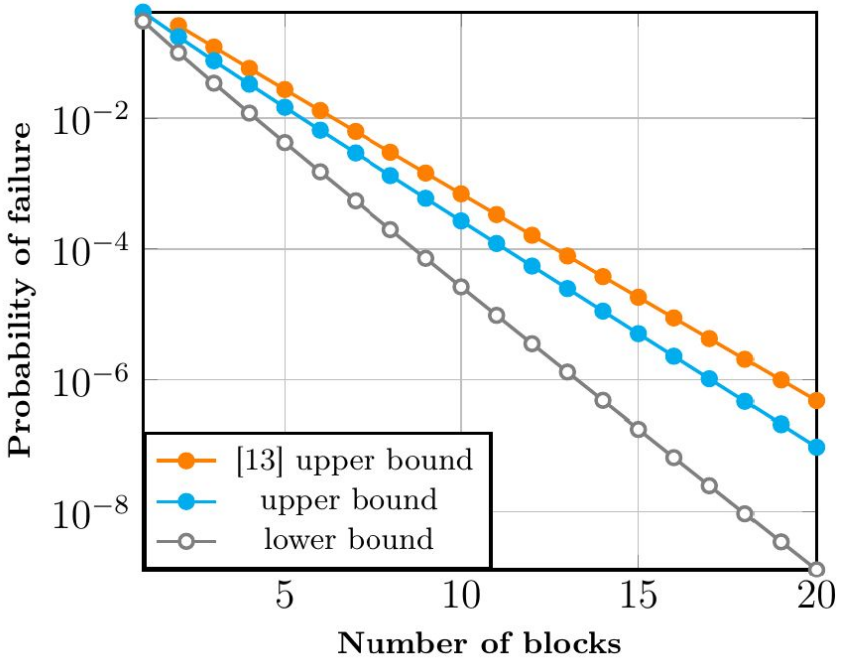
Cardano (PoS)



- block time: 20 seconds
- Δ = 2 seconds
- adversarial stake: 10%

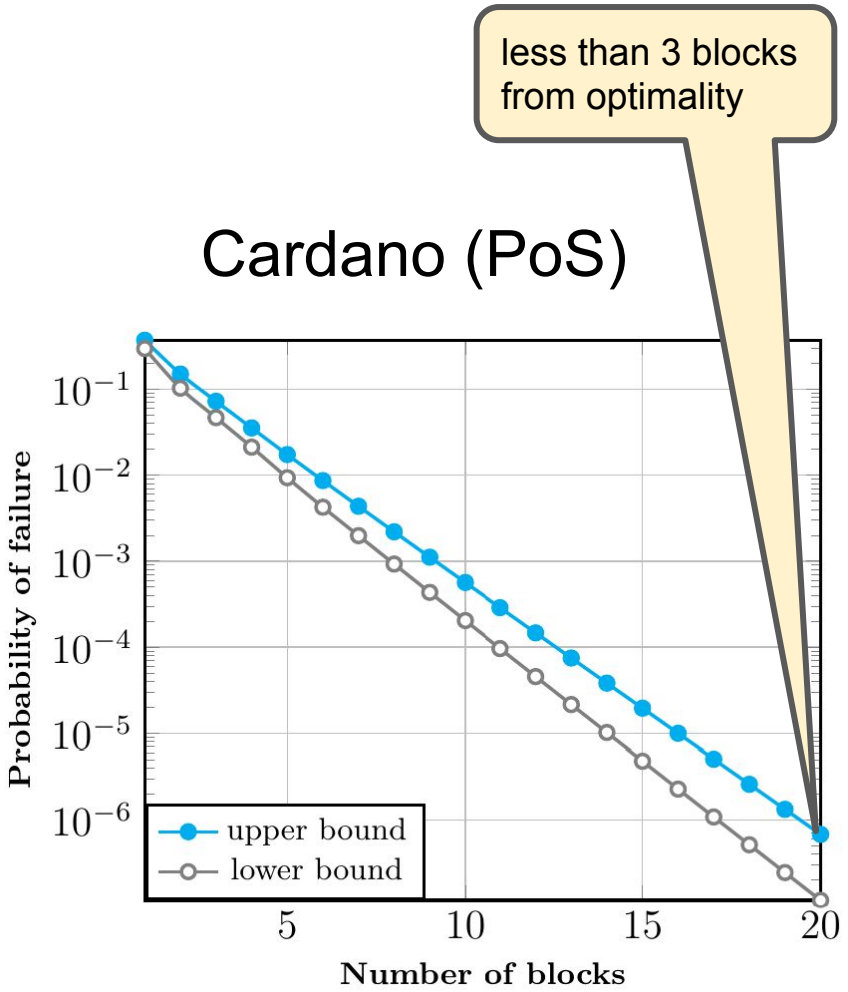
Explicit Results

Ethereum (PoW)



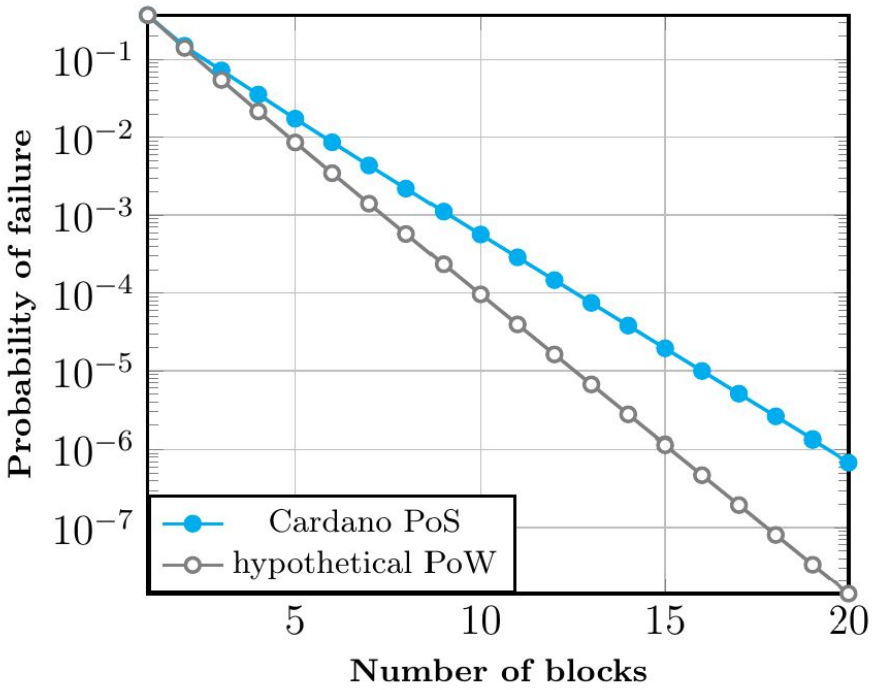
- block time: 13 seconds
- Δ = 2 seconds
- adversarial mining power: 10%

Cardano (PoS)



- block time: 20 seconds
- Δ = 2 seconds
- adversarial stake: 10%

Explicit Results: Comparing PoW to PoS



- block time: 13 seconds
- Δ = 2 seconds
- adversarial mining power/stake: 10%

Thank you for your attention!