# Searching for Optimal Strategies in Proof-of-Stake Mining Games with Access to External Randomness

Author: Anthony Hein (‘22)

Advisers: Professor Matt Weinberg, Doctor Matheus V. X. Ferreira

Second Reader: Professor Mark Braverman

# Overview

1. **Motivation**
2. Game
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

# Proof-of-Work (PoW) Mining Protocol

**Proof-of-Work**

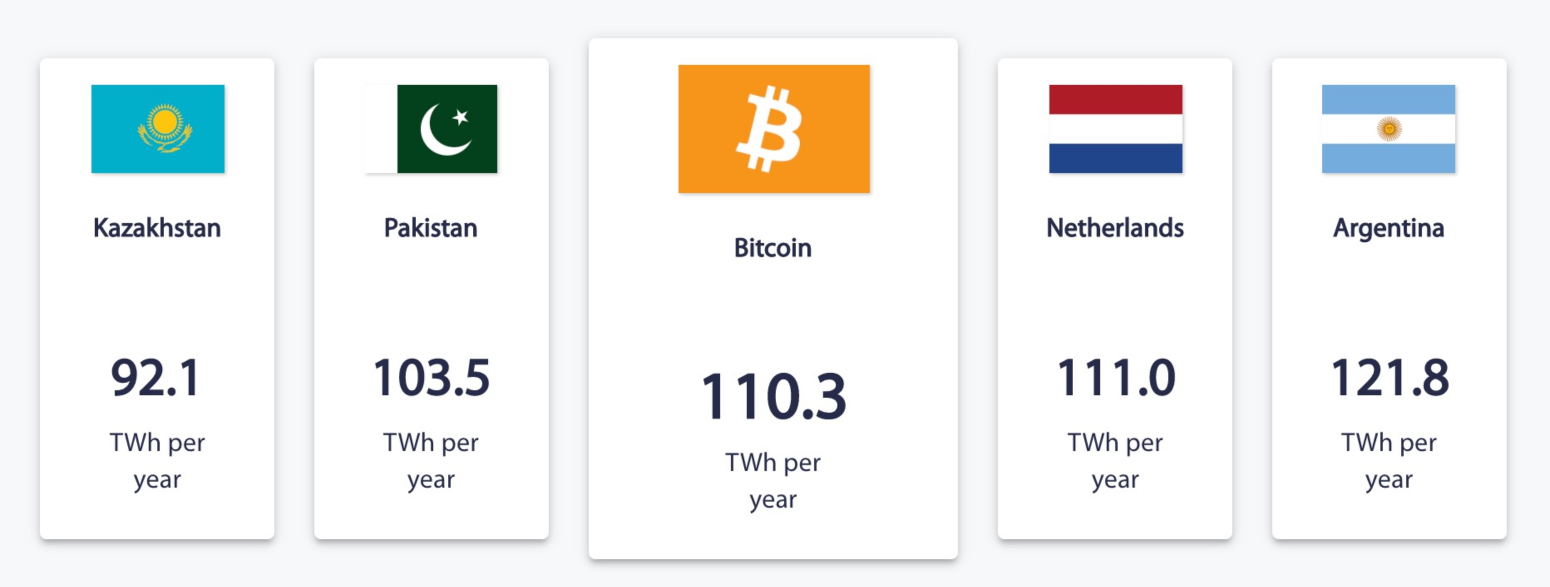
1. Present a string $s$ for which $H(s) < \text{target}$.
2. Mine a block of coins.

$H$ is non-invertible, so $s$ is a **needle in a haystack**.

Computing hashes over random strings consumes **electricity**.

# Proof-of-Work (PoW) Mining Protocol

*How much electricity does proof-of-work consume?*



| Kazakhstan | Pakistan | Bitcoin | Netherlands | Argentina |
|---|---|---|---|---|
| 92.1 | 103.5 | 110.3 | 111.0 | 121.8 |
| TWh per year | TWh per year | TWh per year | TWh per year | TWh per year |

[https://ccaf.io/cbeci/index/comparisons](https://ccaf.io/cbeci/index/comparisons)

# Proof-of-Stake (PoS) Mining Protocol

**Proof-of-Stake (w / External Randomness)**

1. External source chooses $x \in \{1, \text{total number of coins}\}$
2. If you own coin $x$, mine a block of coins.

Avoids millions of computations 🍃

# Project Goal

Investigate whether the PoS mining protocol is a viable alternative to the PoW mining protocol

# Overview

1. Motivation
2. **Game**
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

# Cryptocurrency Mining Game

Use a **2-player** game to model mining cryptocurrency under PoS.

Attacker has strength (probability of mining a block) $\alpha$.

Defender has strength (probability of mining a block) $1 - \alpha$.

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

# Cryptocurrency Mining Game: Demo

Current timestep is bolded.

Attacker hidden blocks:

Defender hidden blocks:

| Timestep | Miner |
|---|---|
| **0** | **N/A** |
| | |
| | |
| | |

# Cryptocurrency Mining Game: Demo

Current timestep is bolded.

Attacker hidden blocks:

Defender hidden blocks:

| Timestep | Miner |
|---|---|
| **0** | **N/A** |
| | |
| | |
| | |

Blockchain

(Longest path marked with heavy arrows.)

# Cryptocurrency Mining Game: Demo

Current timestep is bolded.

| Timestep | Miner |
|---|---|
| **0** | **N/A** |
| | |
| | |
| | |

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

0

## Game Transcript:

Game setup.

# Cryptocurrency Mining Game: Demo

Current timestep is bolded.

Attacker hidden blocks:

Defender hidden blocks: 1

| Timestep | Miner |
|---|---|
| 0 | N/A |
| **1** | **D** |
| | |
| | |

Blockchain (Longest path marked with heavy arrows.)

0

Game Transcript:

Defender mines block 1.

# Cryptocurrency Mining Game: Demo

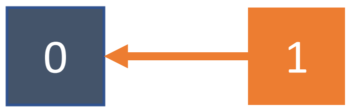
Current timestep is bolded.

Attacker hidden blocks:

Defender hidden blocks:

| Timestep | Miner |
|---|---|
| 0 | N/A |
| **1** | **D** |
| | |
| | |

Blockchain (Longest path marked with heavy arrows.)



Game Transcript:

Defender adds block 1 to the blockchain, pointing to 0.

# Cryptocurrency Mining Game: Demo

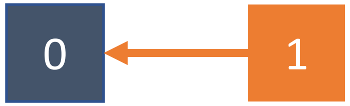
Current timestep is bolded.

Attacker hidden blocks: 2

Defender hidden blocks:

| Timestep | Miner |
|---|---|
| 0 | N/A |
| 1 | D |
| **2** | **A** |
| | |

Blockchain (Longest path marked with heavy arrows.)



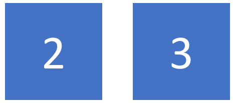
Game Transcript:

Attacker mines block 2.

# Cryptocurrency Mining Game: Demo

Current timestep is bolded.

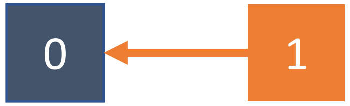
Attacker hidden blocks:



Defender hidden blocks:

| Timestep | Miner |
|---|---|
| 0 | N/A |
| 1 | D |
| 2 | A |
| **3** | **A** |

Blockchain (Longest path marked with heavy arrows.)



Game Transcript:

Attacker mines block 3.

# Cryptocurrency Mining Game: Demo

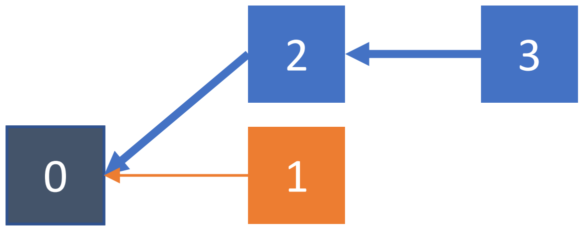
Current timestep is bolded.

| Timestep | Miner |
|---|---|
| 0 | N/A |
| 1 | D |
| 2 | A |
| **3** | **A** |

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)



Game Transcript:

Attacker adds blocks 2 and 3 to the blockchain, pointing 3 to 2 and 2 to 0.

# Cryptocurrency Mining Game: Demo

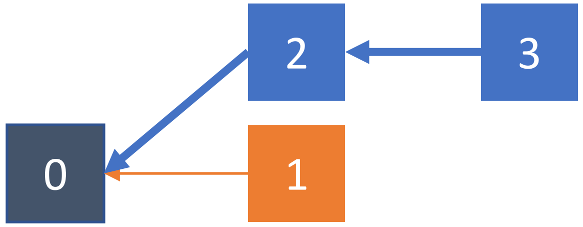
Attacker revenue: 1

Defender revenue: 0

Proportion of blocks they own in the **longest path** in the blockchain.

Blockchain

(Longest path marked with heavy arrows.)



# Honest Mining

Players are *supposed* to use the **honest mining strategy** (HONEST):

If you mine a block, publish it on the longest chain.

# Selfish Mining

Players can cheat and do better than HONEST.

Such **selfish mining** threatens the adoption of PoS.

# Robustness of PoS to Attack

Let **robustness** be the minimum strength $\alpha$ necessary to conduct an attack.

Denote this as $\alpha^{PoS}$.

# Project Goal

Investigate whether the PoS mining protocol is a viable alternative to the PoW mining protocol …

# Project Goal

Investigate whether the PoS mining protocol is a viable alternative to the PoW mining protocol …

by bounding $\alpha^{PoS}$, the robustness of the PoS mining protocol to an attack.

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

Blockchain

(Longest path marked with heavy arrows.)

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 1

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

0

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 1 2

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

0

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 1 2 3

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

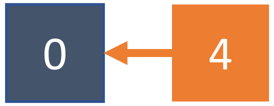
0

# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 1 2 3

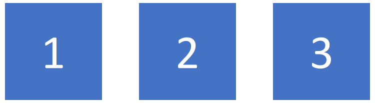
Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)



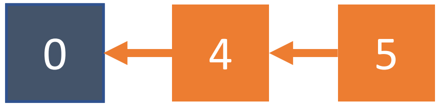
# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:



Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

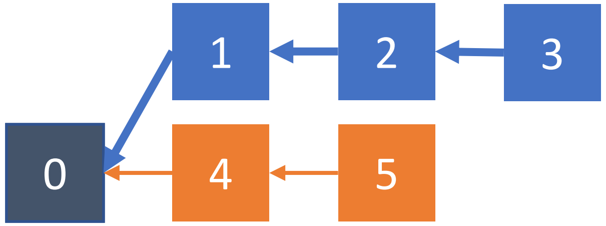


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

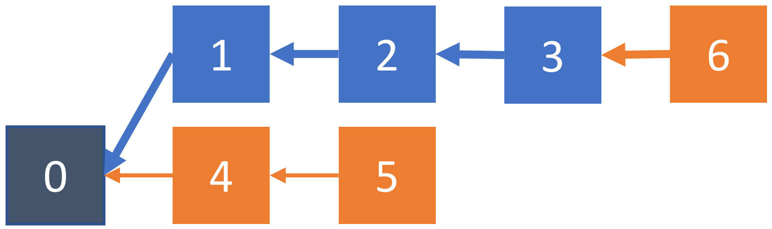


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

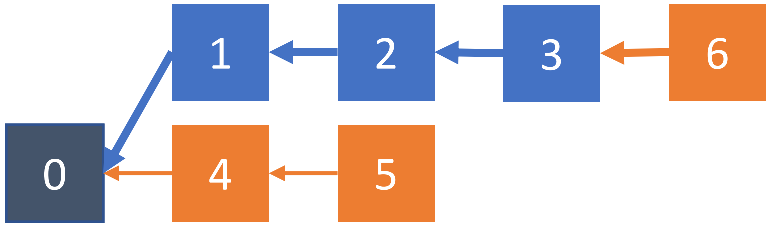


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 7

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

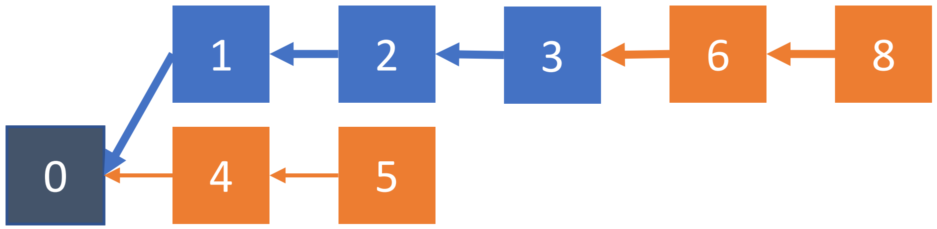


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 7

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

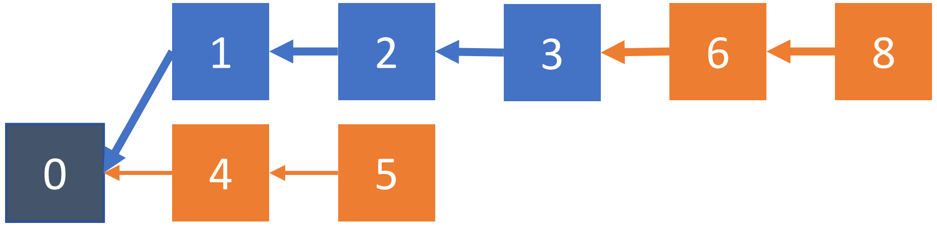


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks: 7 9

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

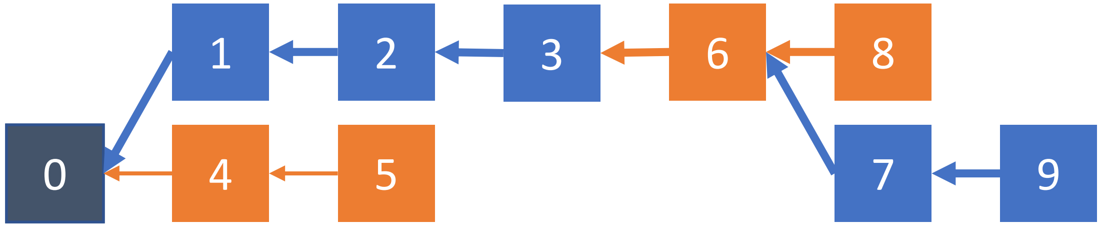


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

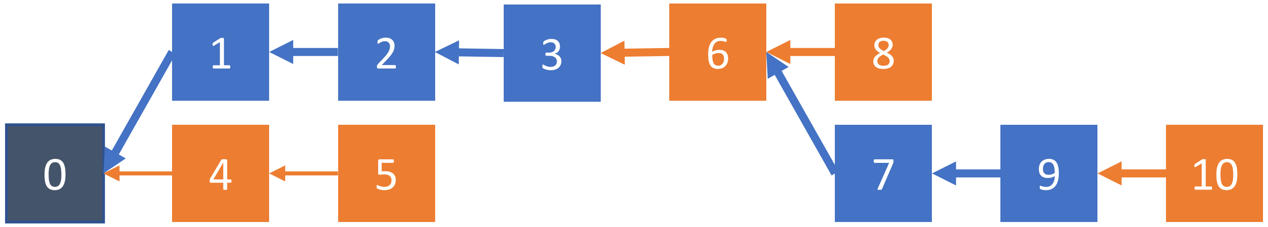


# Cryptocurrency Mining Game: Demo

Attacker hidden blocks:

Defender hidden blocks:

Blockchain (Longest path marked with heavy arrows.)

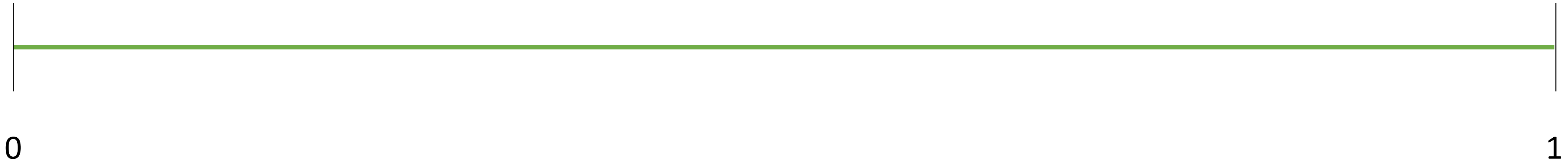


# Overview

1. Motivation
2. Game
3. **Prior Work**
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

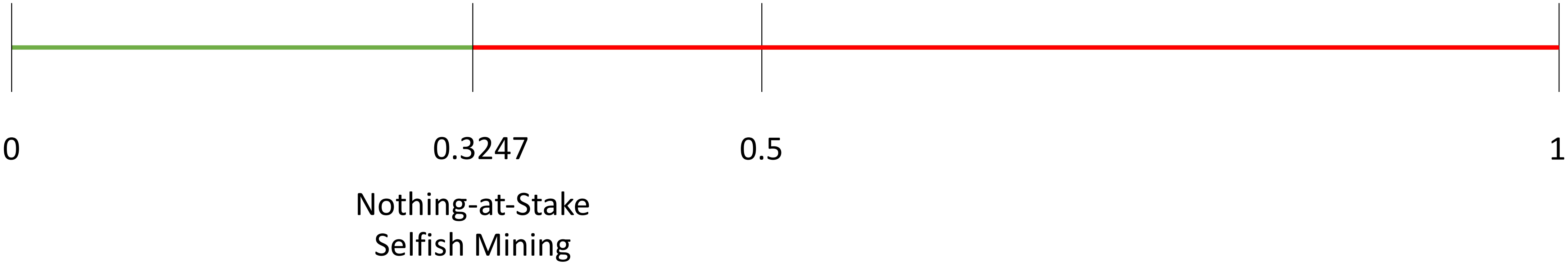
# Ferreira, M. V., & Weinberg, S. M. 2021.

$0 < \alpha^{PoS} < 1$



# Ferreira, M. V., & Weinberg, S. M. 2021.

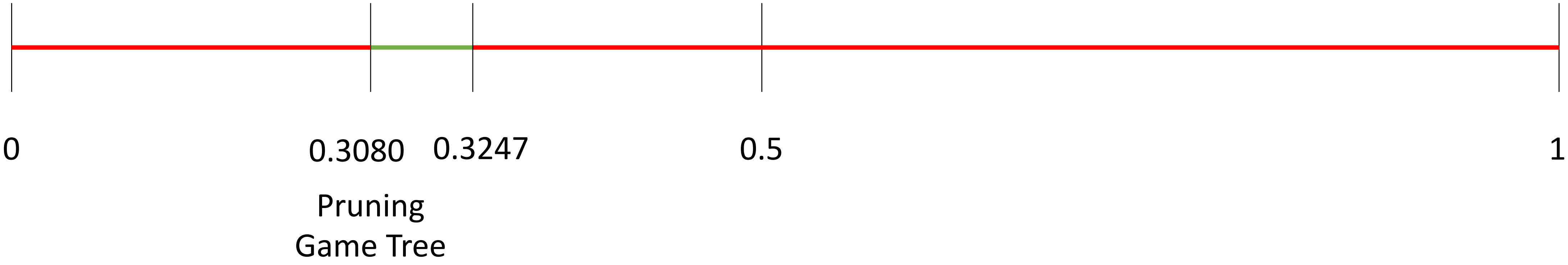
$0 \leq \alpha^{PoS} \leq 0.3247$



* Not drawn to scale.

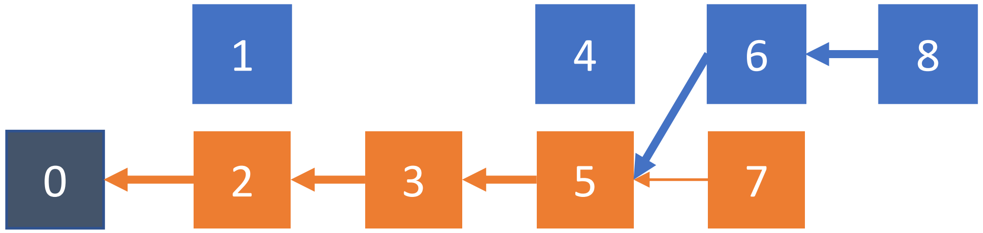
# Ferreira, M. V., & Weinberg, S. M. 2021.

$0.3080 \leq \alpha^{PoS} \leq 0.3247$

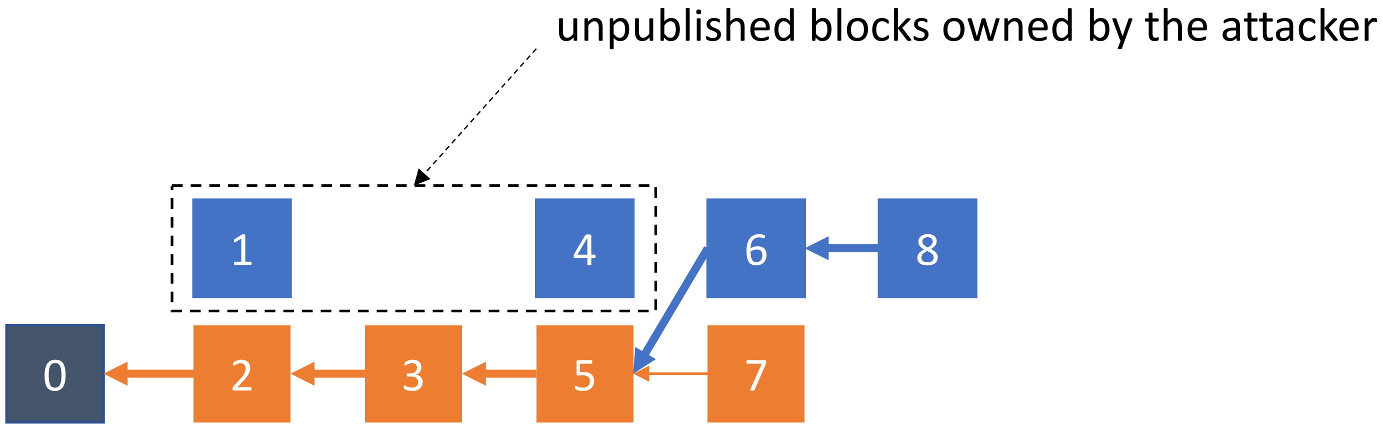


* Not drawn to scale.

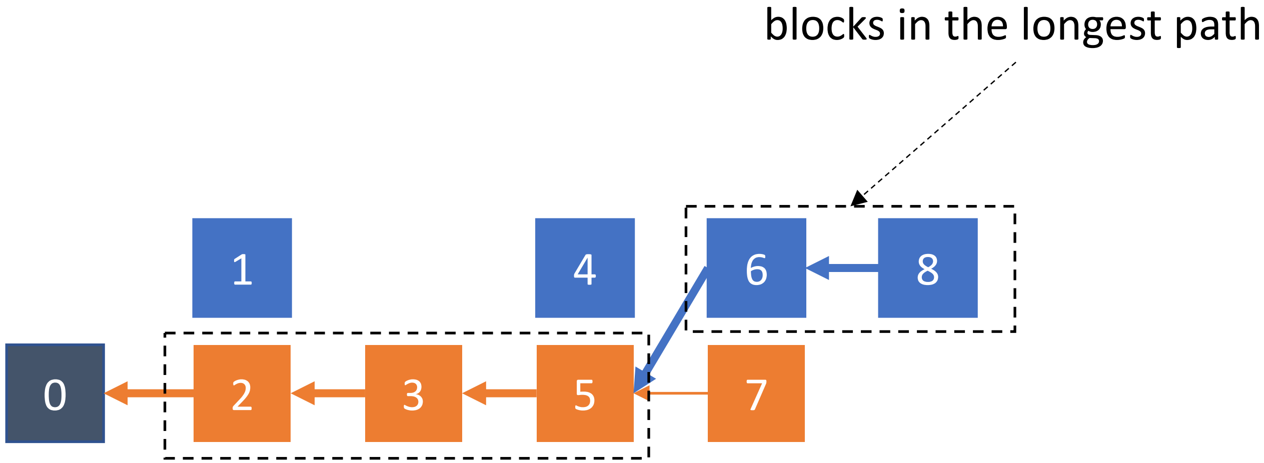
# Reading a State Diagram



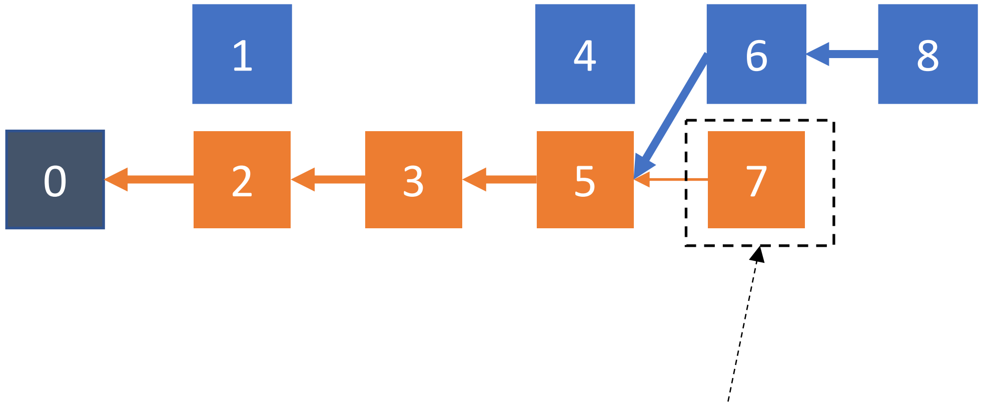
# Reading a State Diagram



# Reading a State Diagram



# Reading a State Diagram



orphaned block; block forked from the longest path

# Ferreira, M. V., & Weinberg, S. M. 2021.

**Legend**

Game State

○ optimal strategy unknown

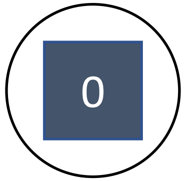
◯ optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

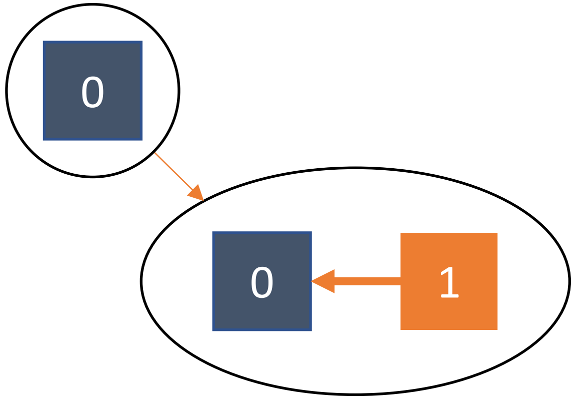
◯ optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

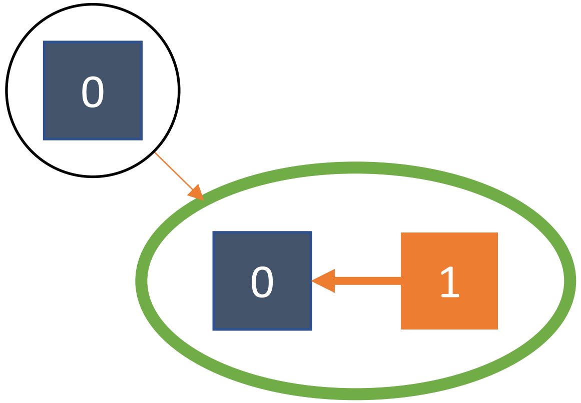
🟢 optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

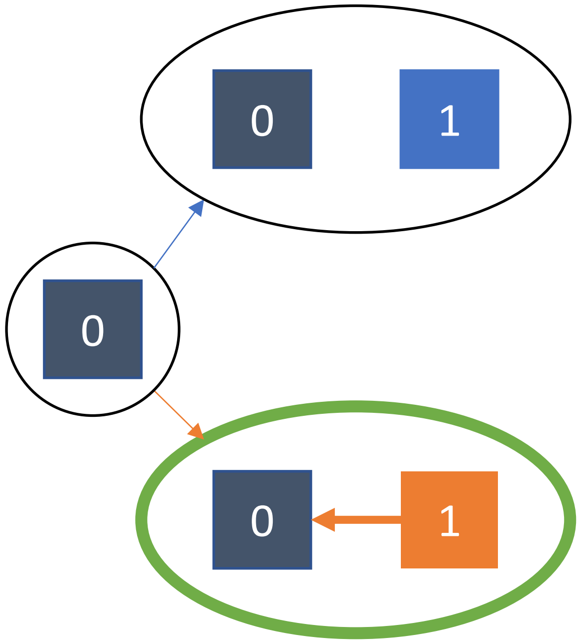
🟢 optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

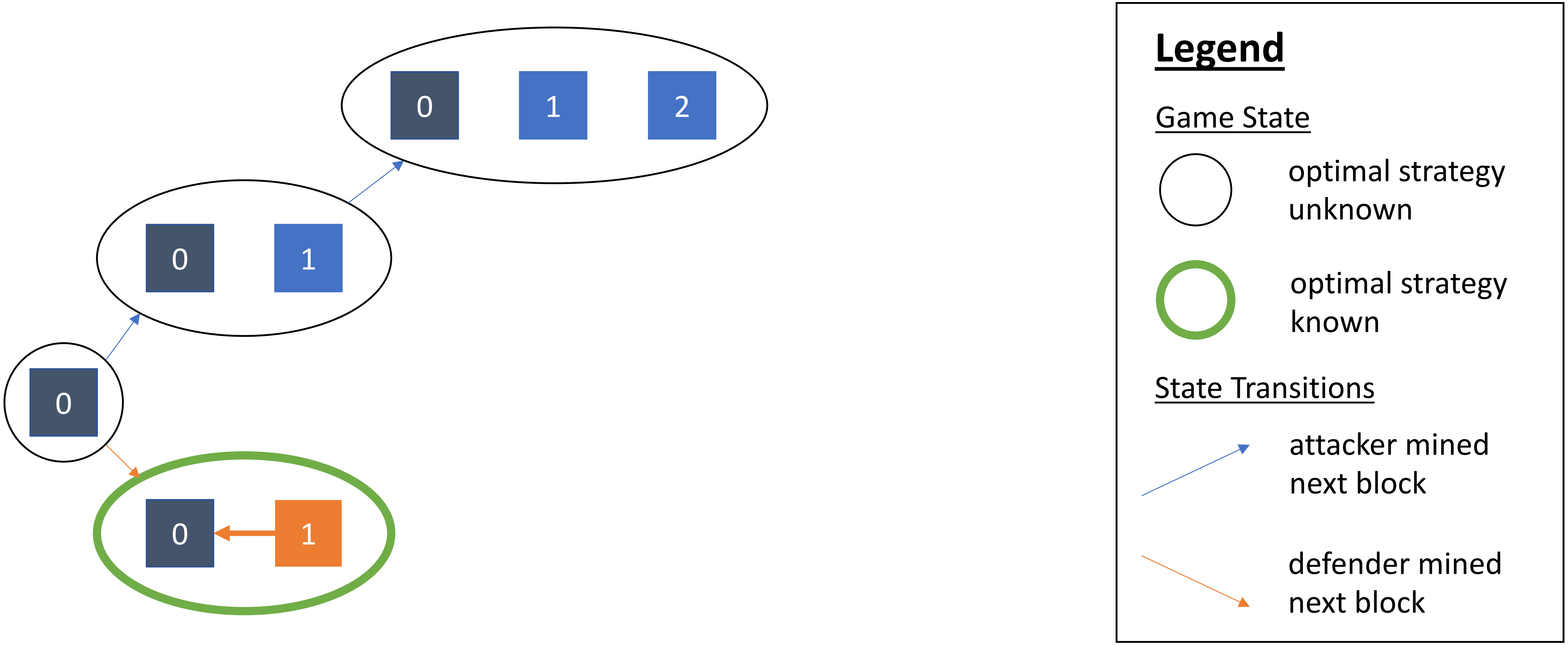
◯ optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

optimal strategy unknown

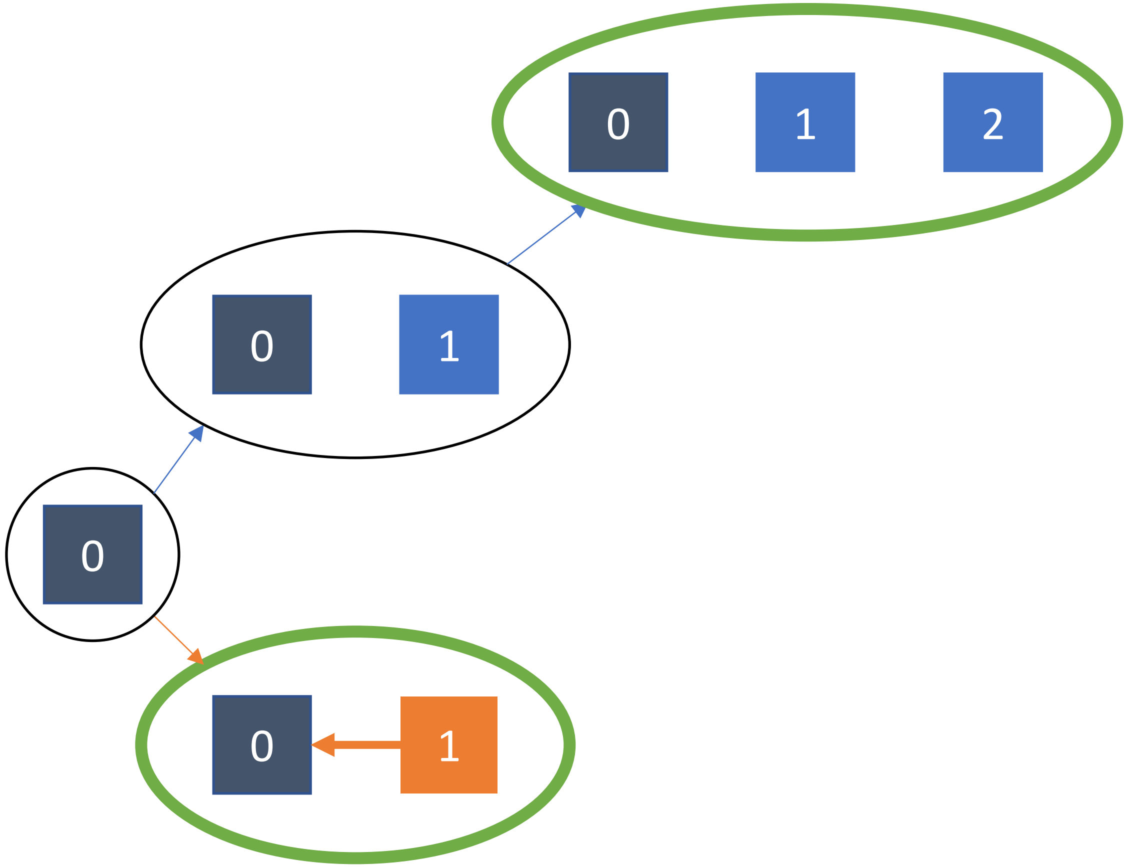
optimal strategy known

State Transitions

attacker mined next block

defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

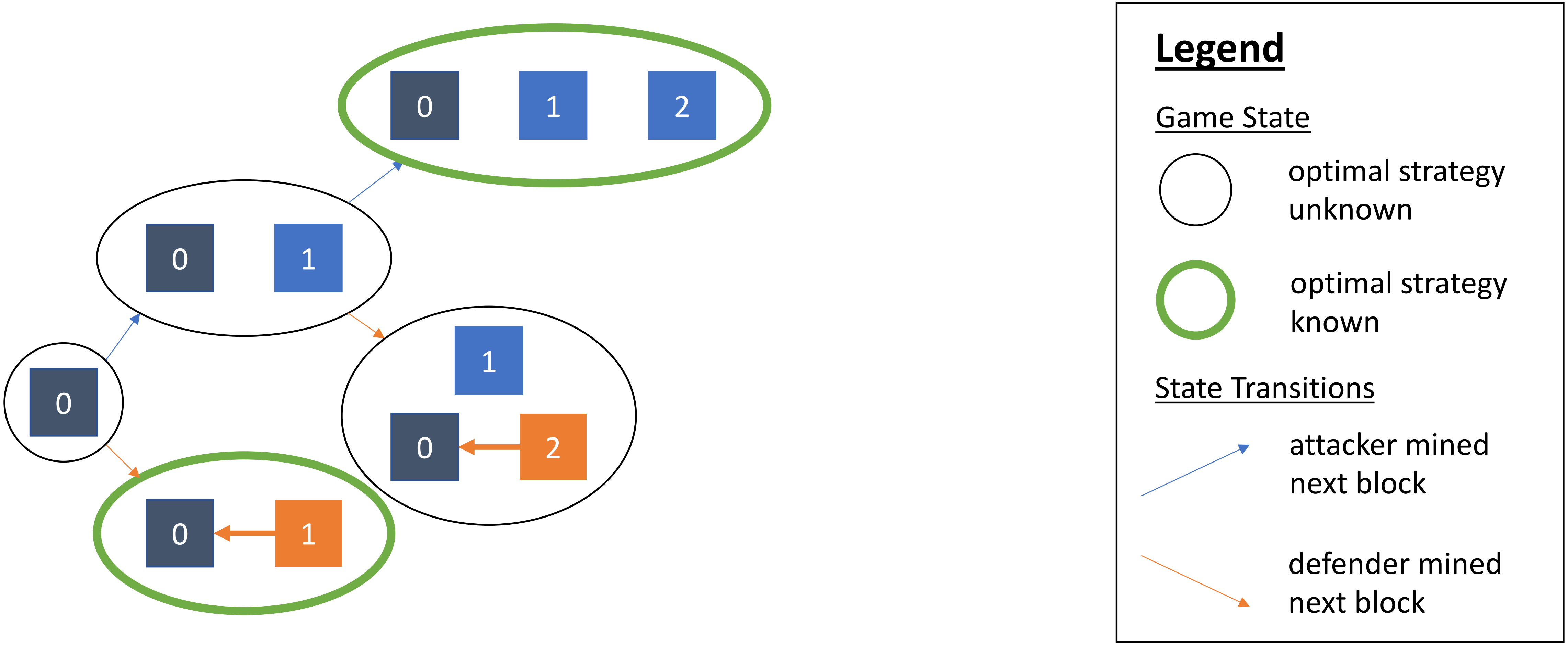
🟢 optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

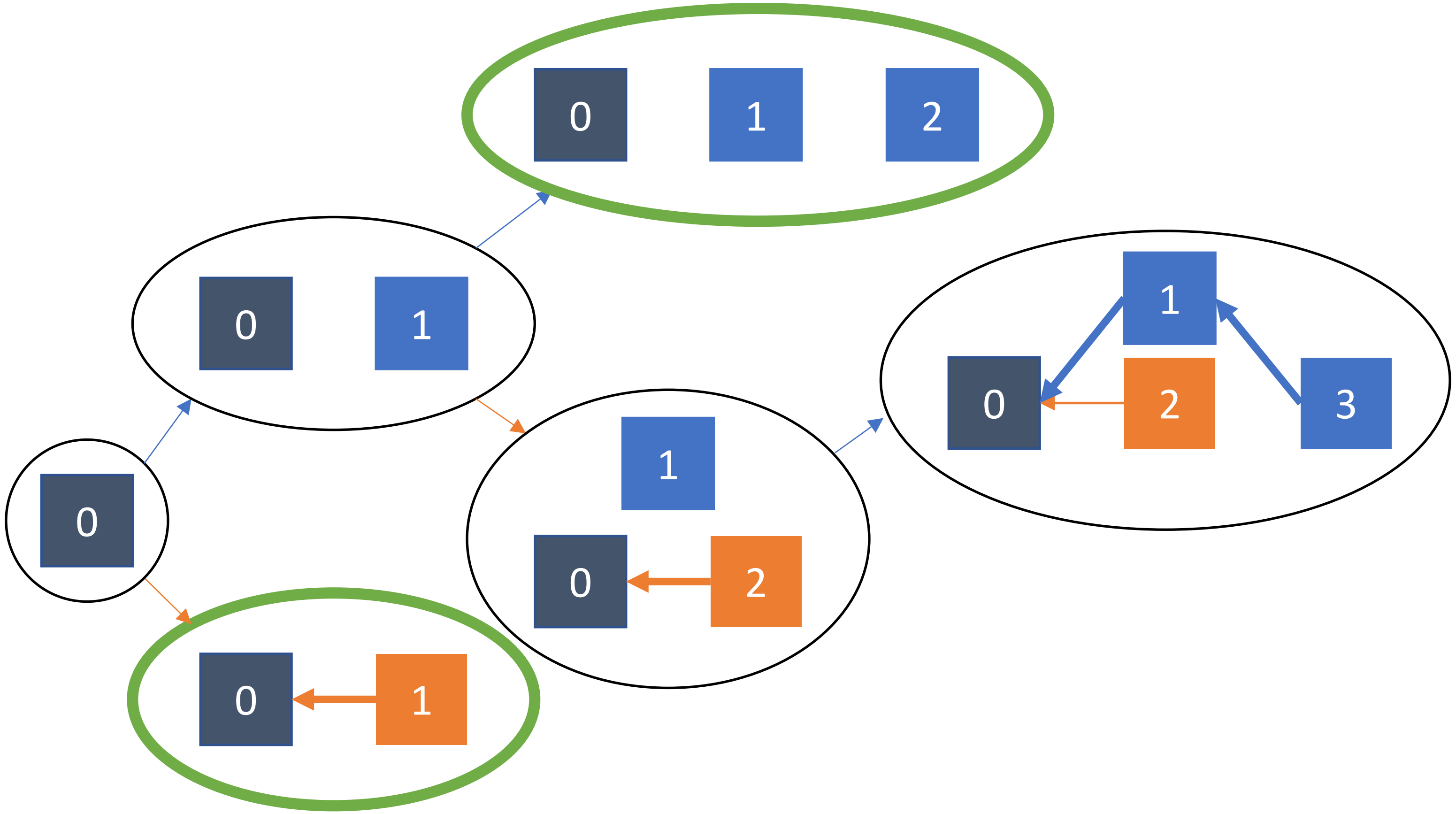
🟢 optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

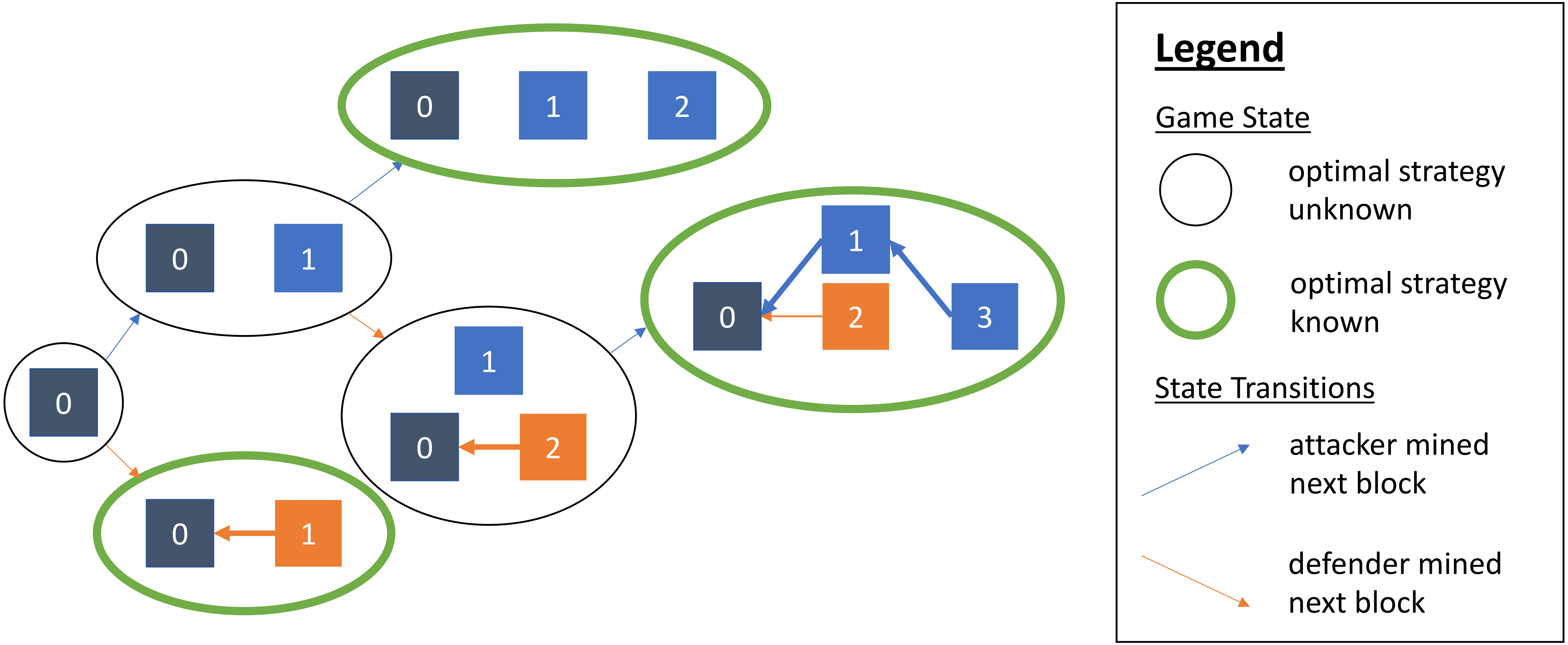
🟢 optimal strategy known

State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



**Legend**

Game State

○ optimal strategy unknown

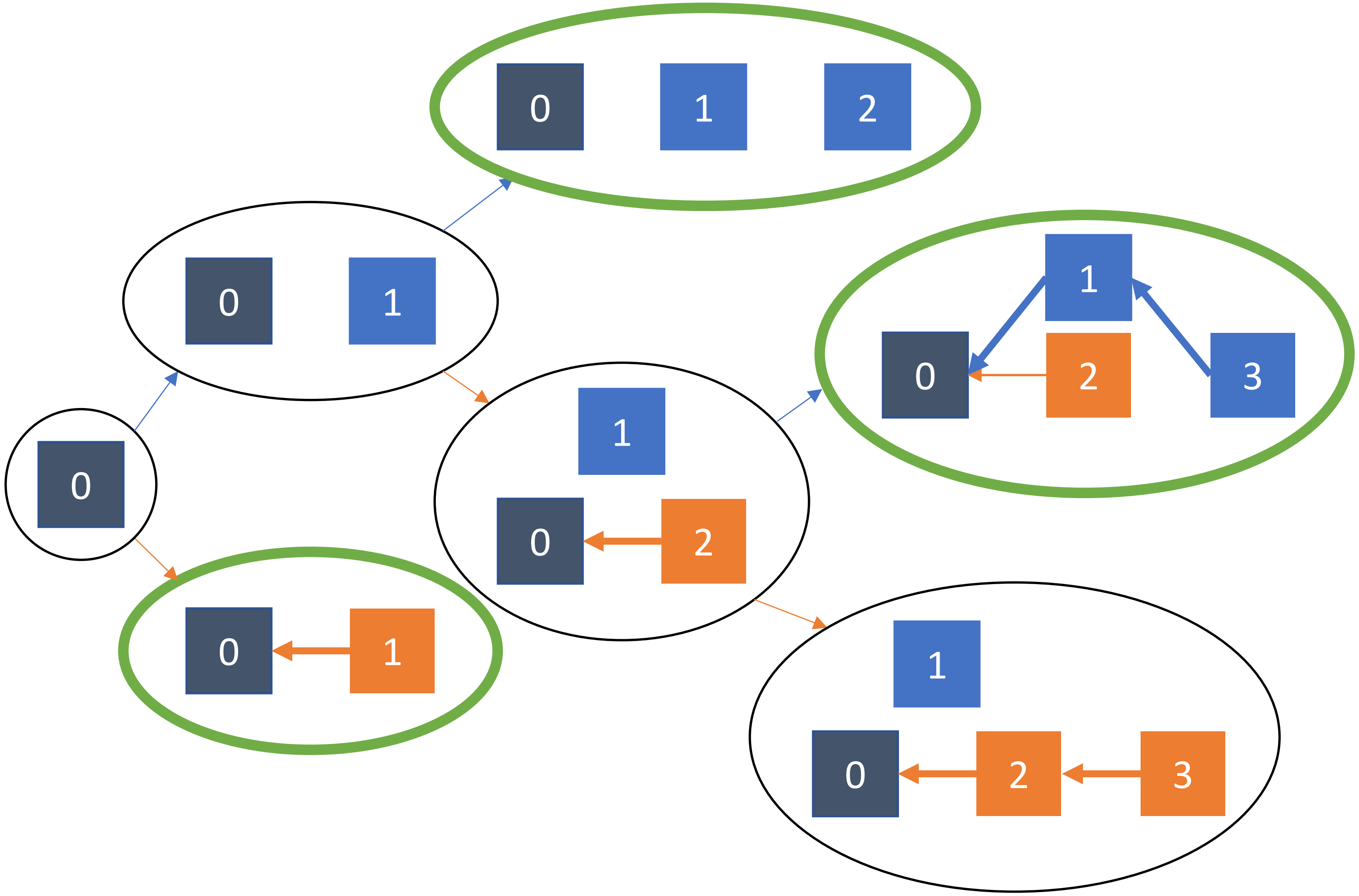
🟢 optimal strategy known

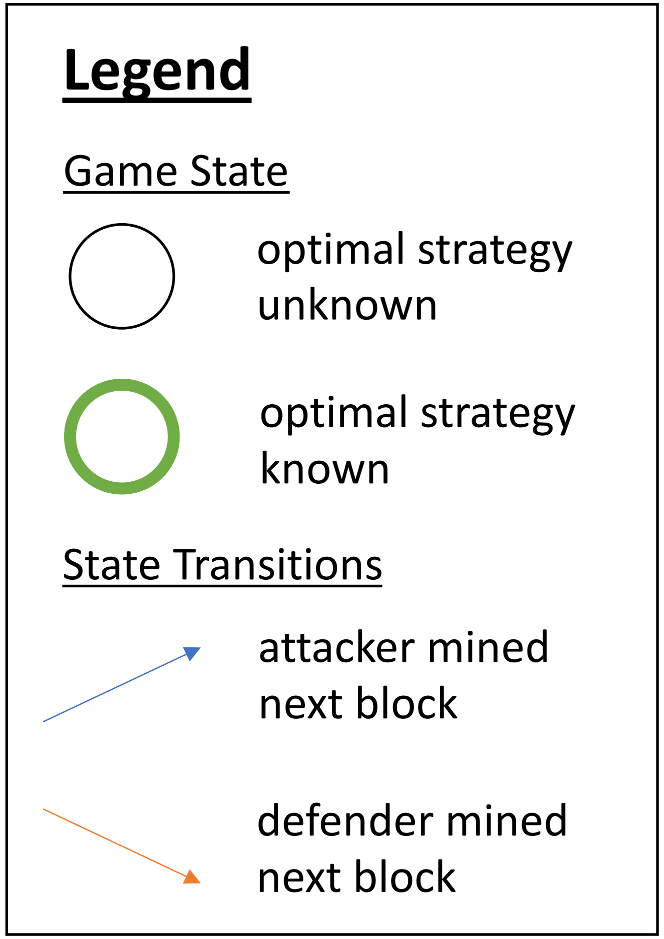
State Transitions

↗ attacker mined next block

↘ defender mined next block

# Ferreira, M. V., & Weinberg, S. M. 2021.



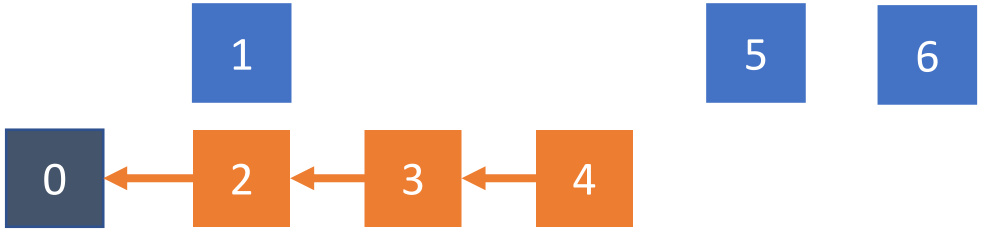


# Overview

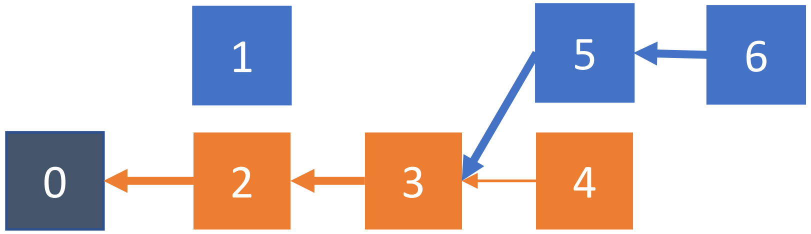
1. Motivation
2. Game
3. Prior Work
4. **Structured Strategies**
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

# Structured Strategies

Given state



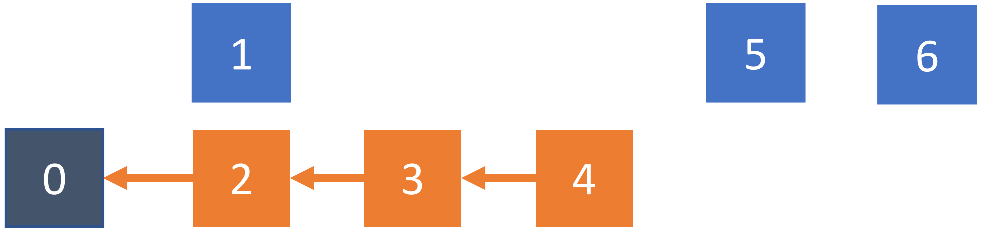
should a strategy take action



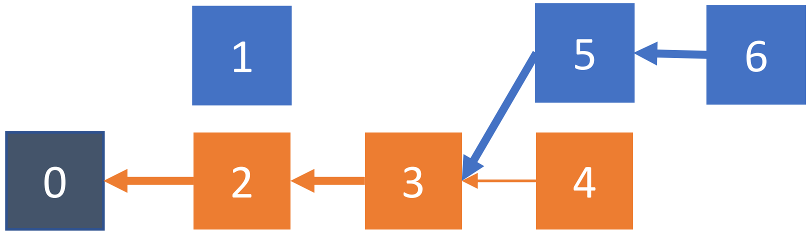
?

# Structured Strategies

Given state

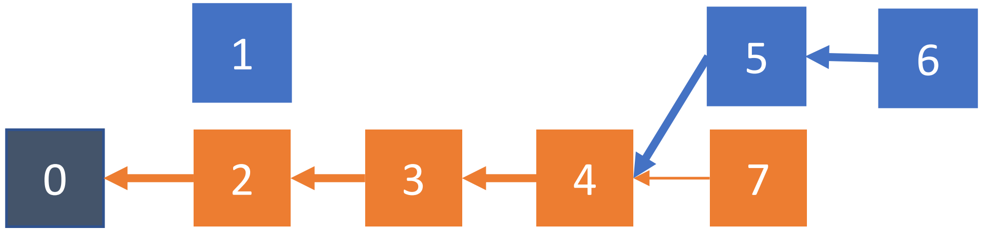


should a strategy take action



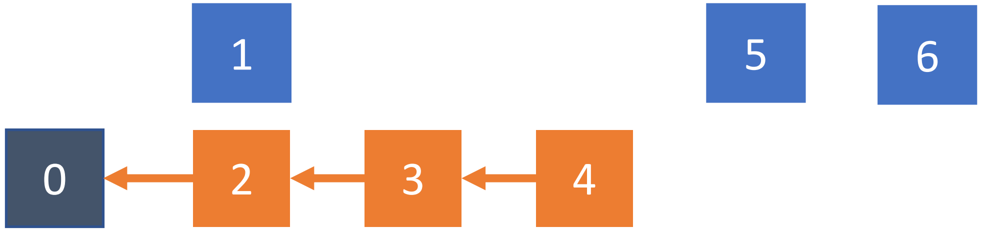
?

NO! Just wait... can still publish even in the worst-case scenario that defender mines the next block.

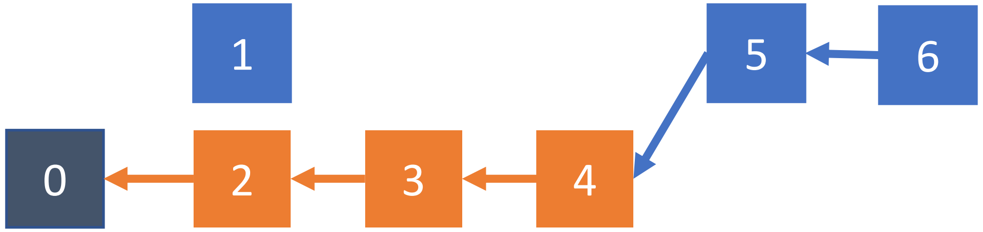


# Structured Strategies

Given state



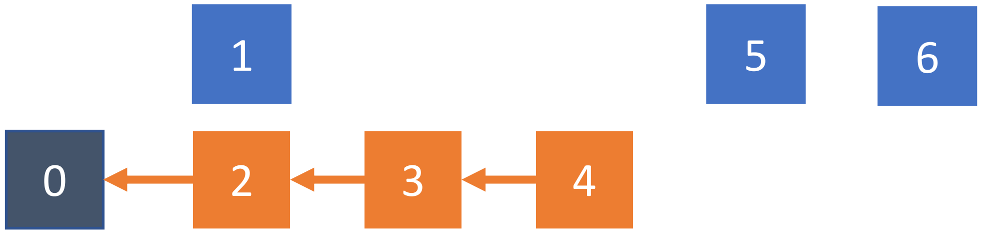
should a strategy take action



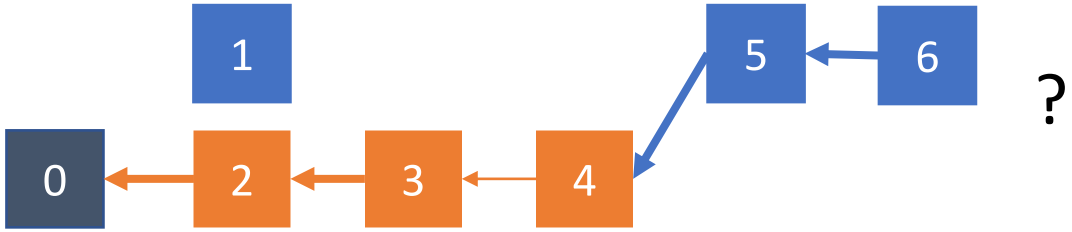
?

# Structured Strategies

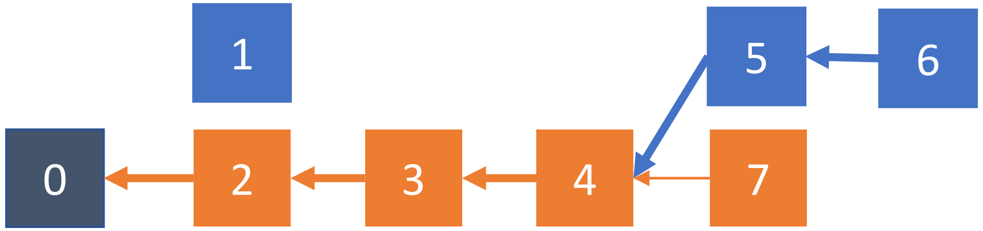
Given state



should a strategy take action

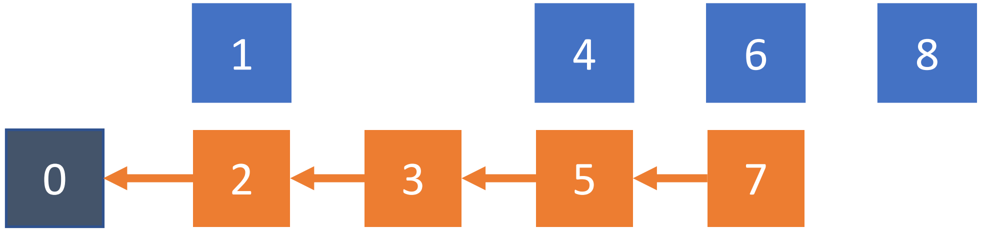


NO! Just wait... can still publish even in the worst-case scenario that defender mines the next block.

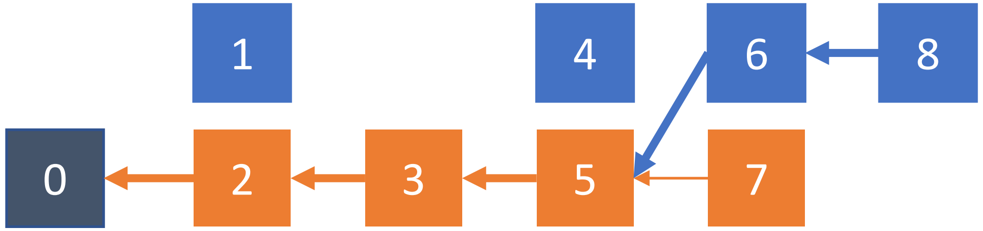


# Structured Strategies

Given state



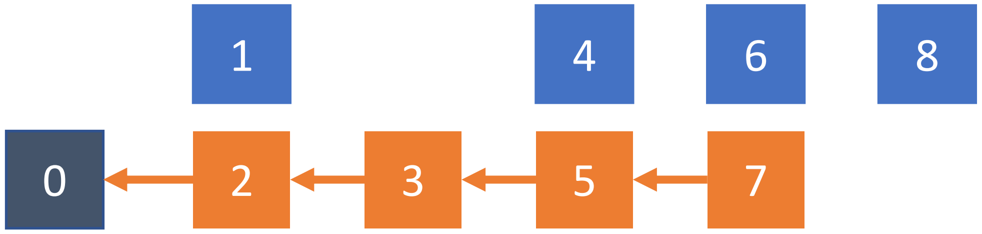
should a strategy take action



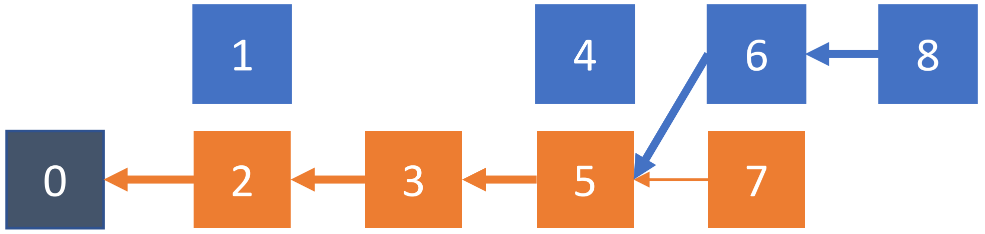
?

# Structured Strategies

Given state

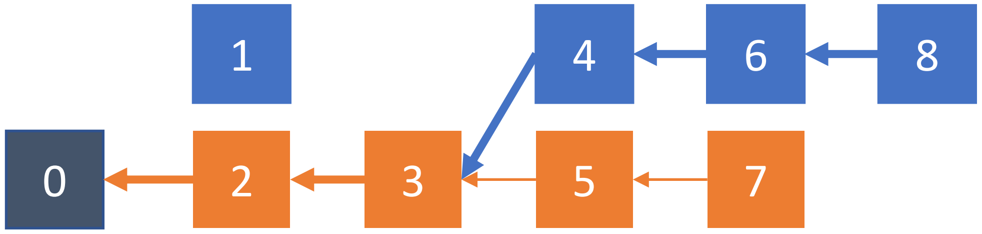


should a strategy take action



?

NO! Why wouldn't the strategy also publish block 4?



# Structured Strategies

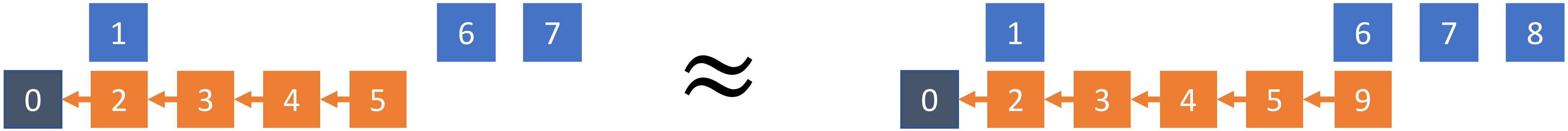
A *structured strategy* obeys these and several other “intuitive” properties so there are fewer actions to compare at any state.

Without loss of generality, an optimal strategy is *structured*.

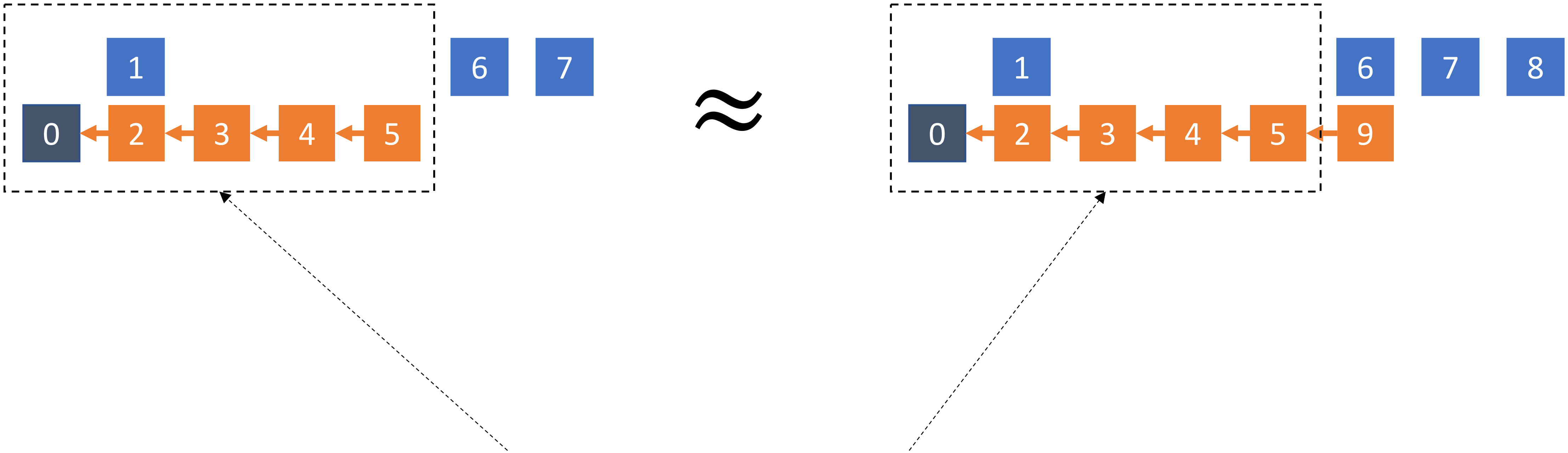
# Overview

1. Motivation
2. Game
3. Prior Work
4. Structured Strategies
5. **Symmetrical States**
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

# Symmetrical States

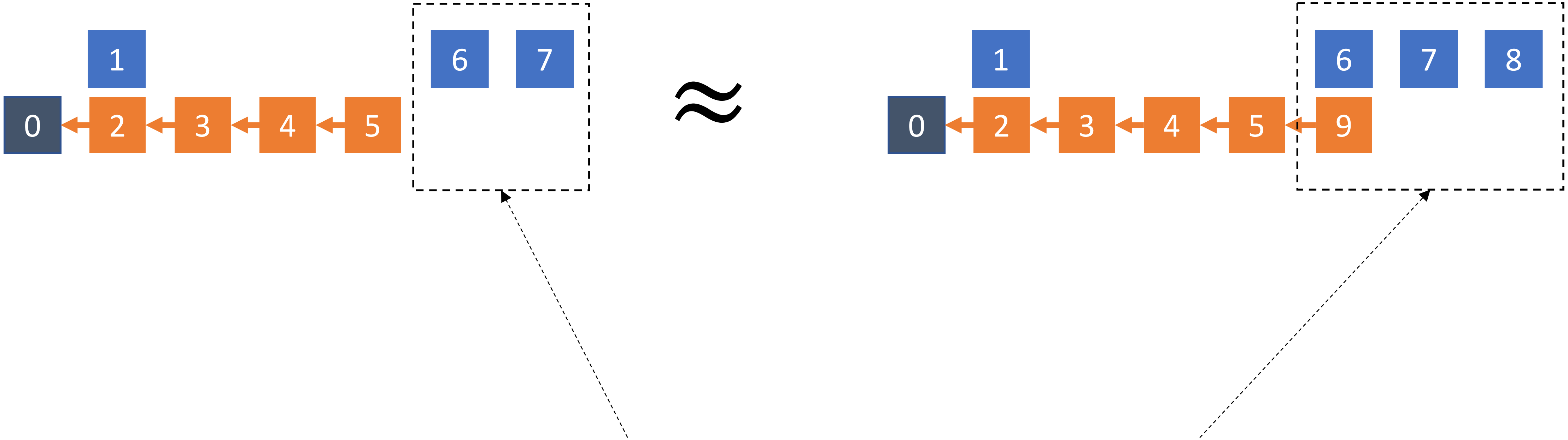


# Symmetrical States



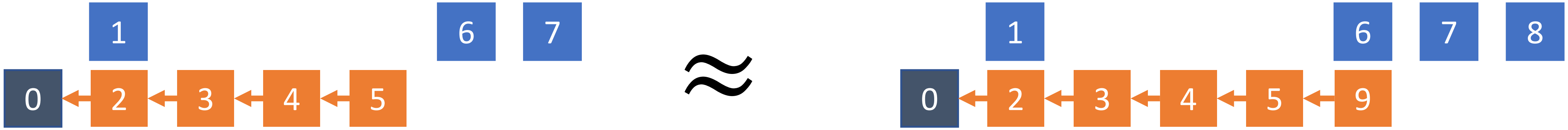
Same beginning state.

# Symmetrical States



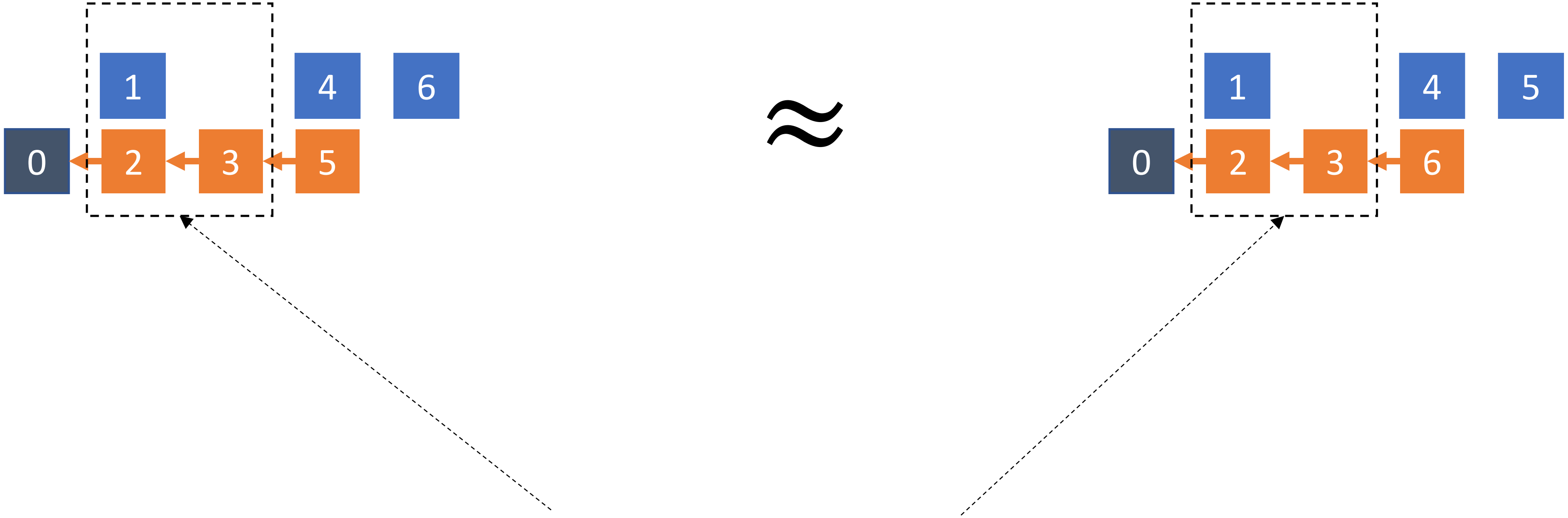
Same lead over the subsequent block.

# Symmetrical States



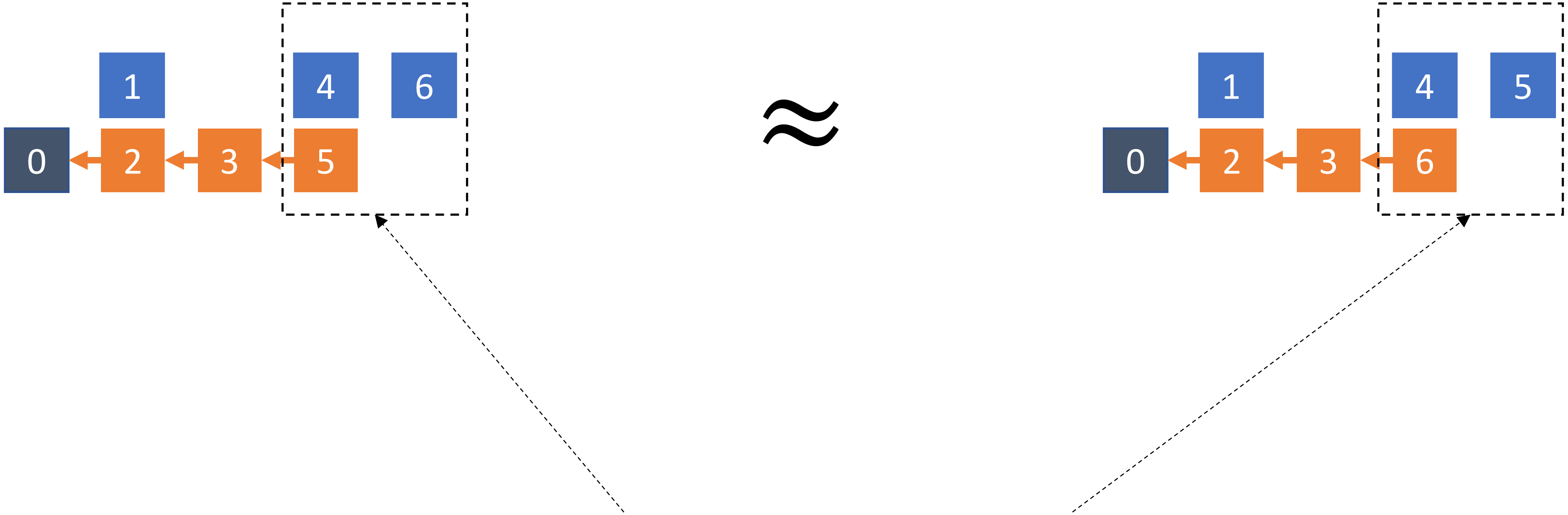
The values of these states are related by *exactly* the difference in the number of attacker blocks!

# Symmetrical States



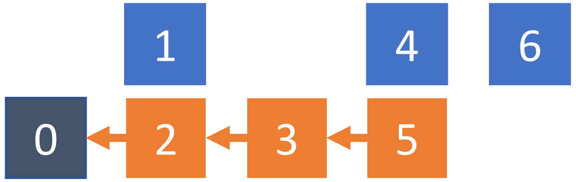
Same beginning state.

# Symmetrical States

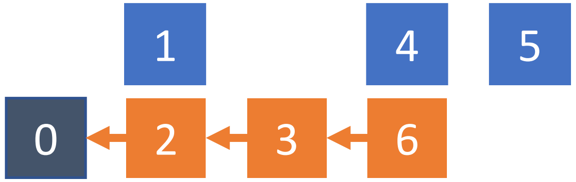


Only difference is 6 can never be published on 5,
but why would they want to do that anyways?

# Symmetrical States



≈



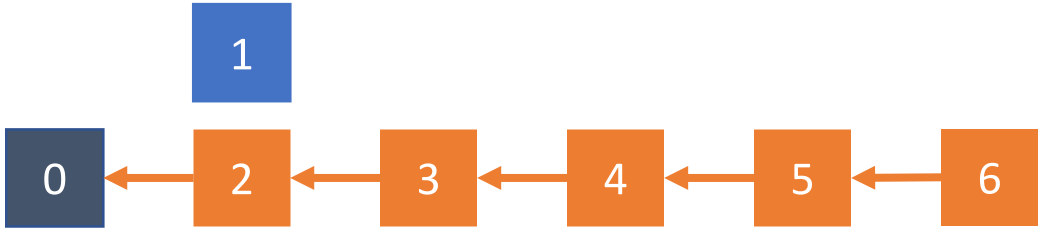
The values of these states are *exactly* equal!

# Overview

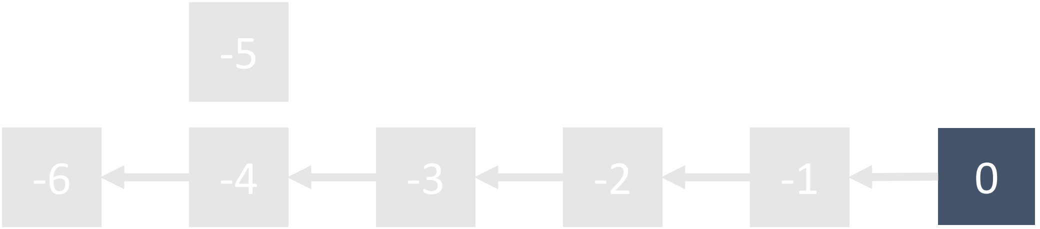
1. Motivation
2. Game
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. **Non-Checkpoint Finality**
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. Conclusion

# Non-Checkpoint Finality

If the game reaches

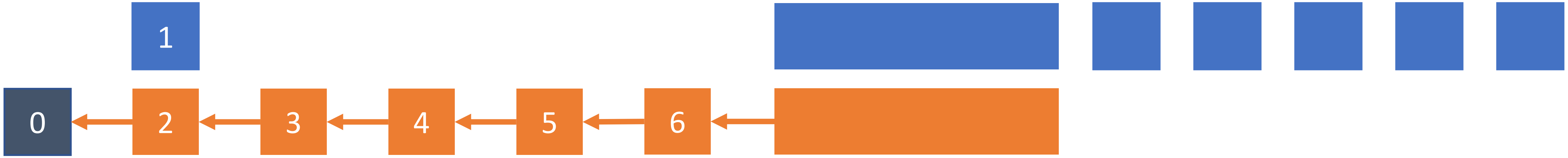


then the optimal strategy is to just "reset" the game, or



# Non-Checkpoint Finality

*Proof Sketch*: Suppose that the attacker ever has the chance to publish block 1 such that it enters the longest path. Then the game state looks something like



That is, the attacker has a lead of five blocks.

But, a lead of five blocks let's you do things which are *strictly better* than publishing block 1.

# Overview

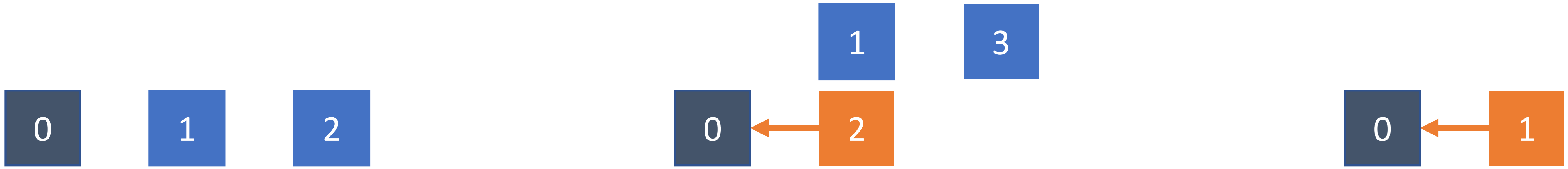
1. Motivation
2. Game
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. **n-Deficit Tolerance Family of Strategies**
8. Automating this Search
9. Conclusion

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.

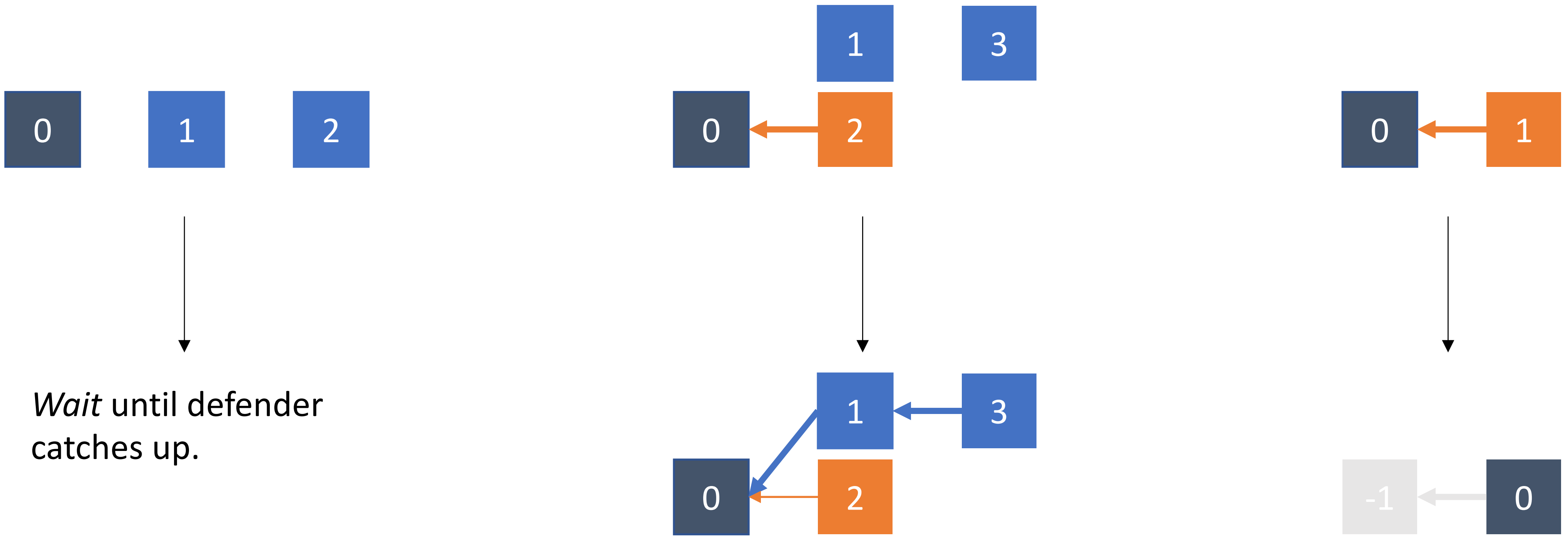
# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.



# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.



*Wait* until defender catches up.

# n-Deficit Tolerance Family of Strategies

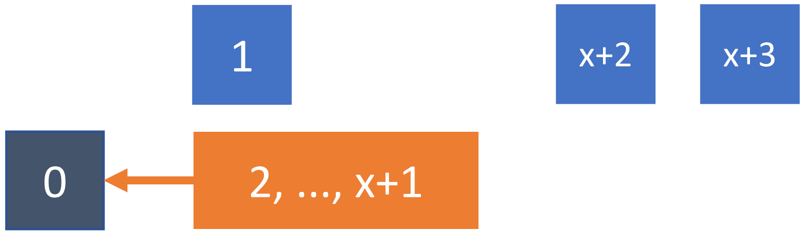
- Take optimal action at states where this is known.

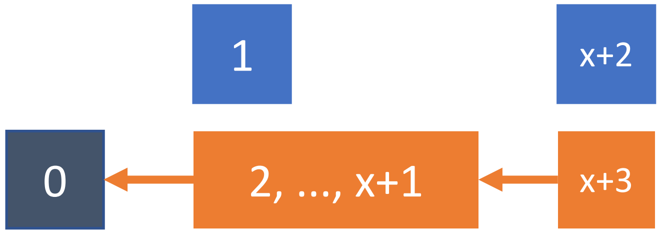
# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.

# n-Deficit Tolerance Family of Strategies

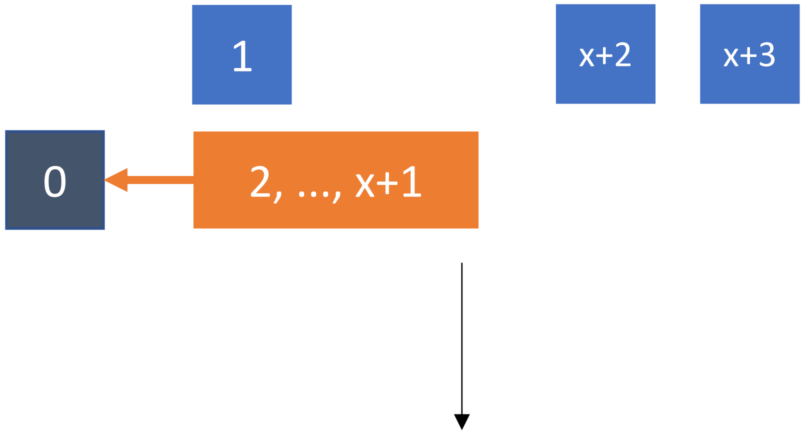
- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



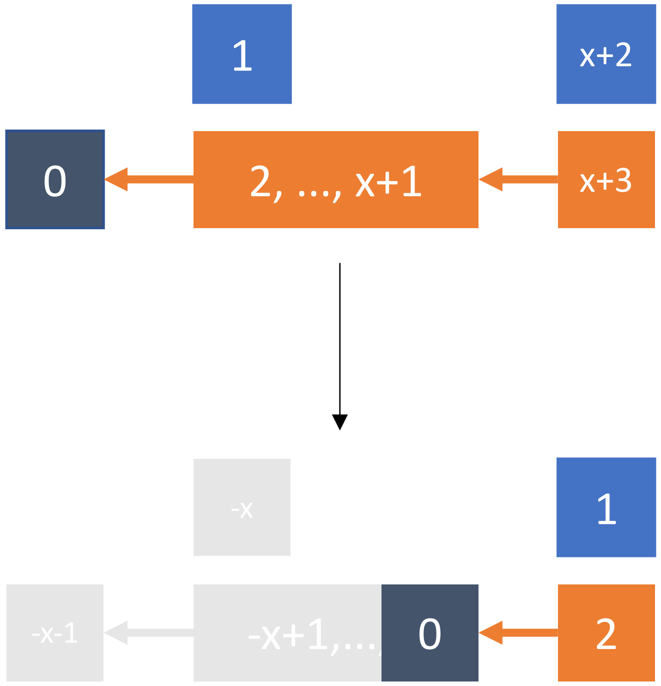


# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



*Wait* until defender catches up on blocks {x+2, x+3} or can recover block 1.



# n-Deficit Tolerance Family of Strategies

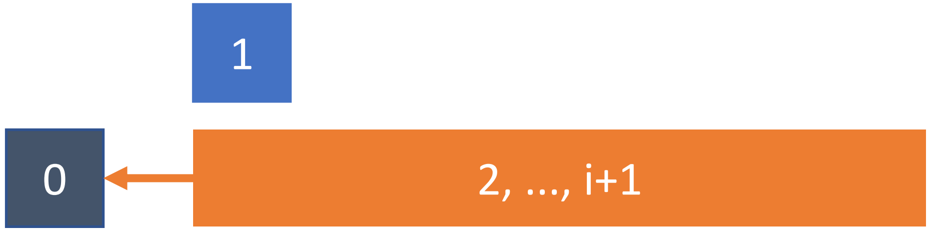
- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.

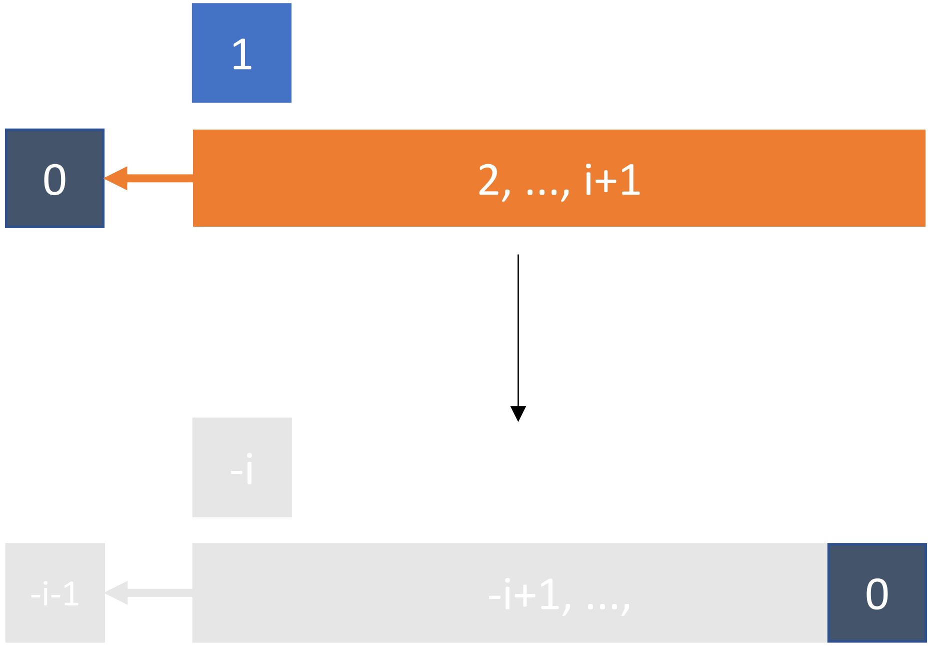
# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



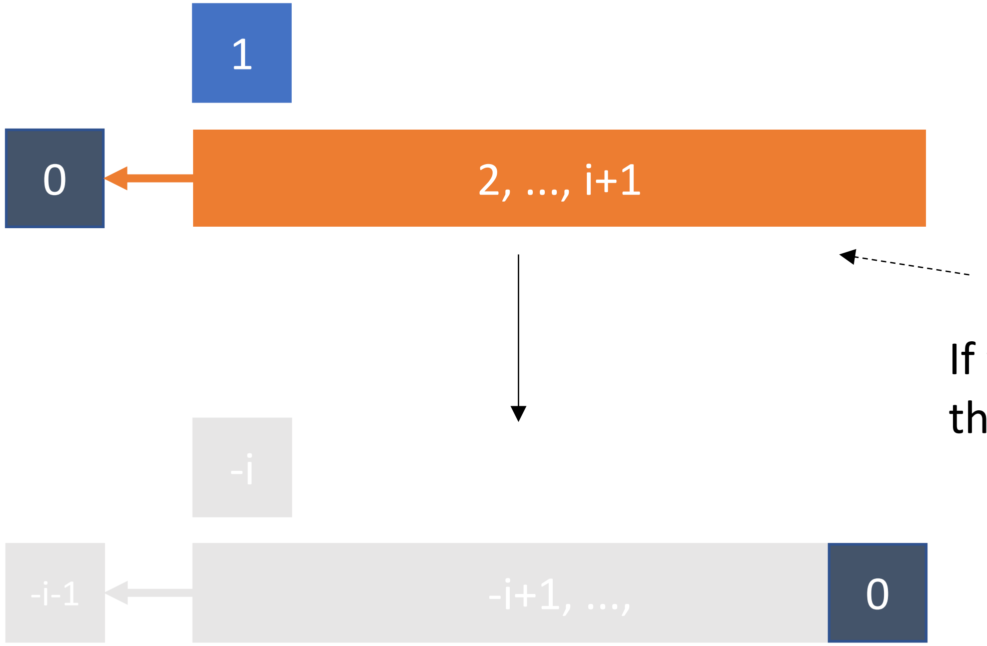
# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



# n-Deficit Tolerance Family of Strategies

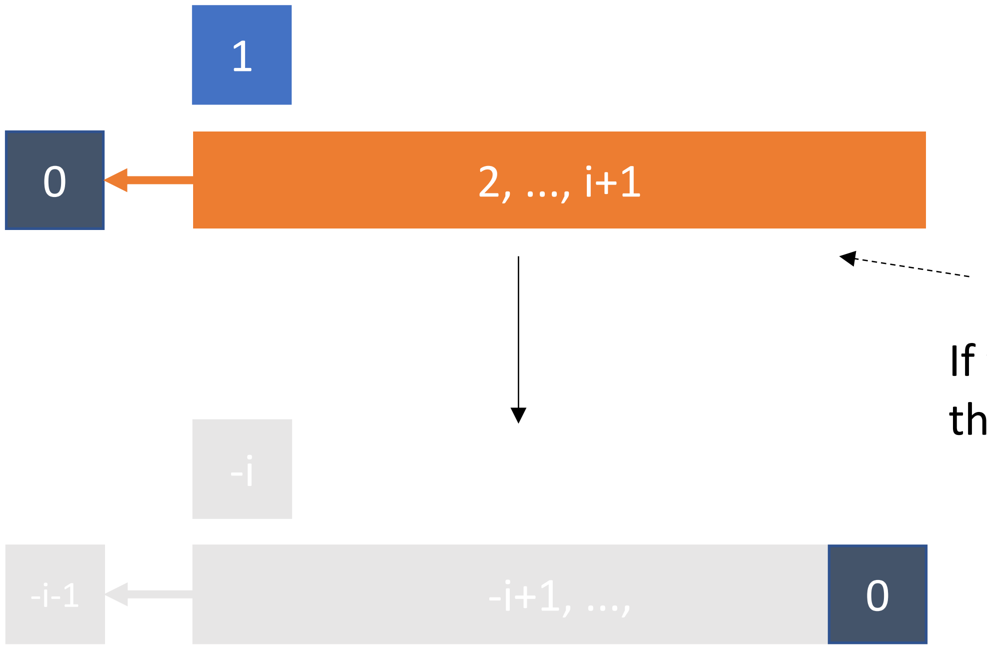
- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



If the strategy gives up at $i+1$ "deficit", then call it $i$-Deficit Tolerance.

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



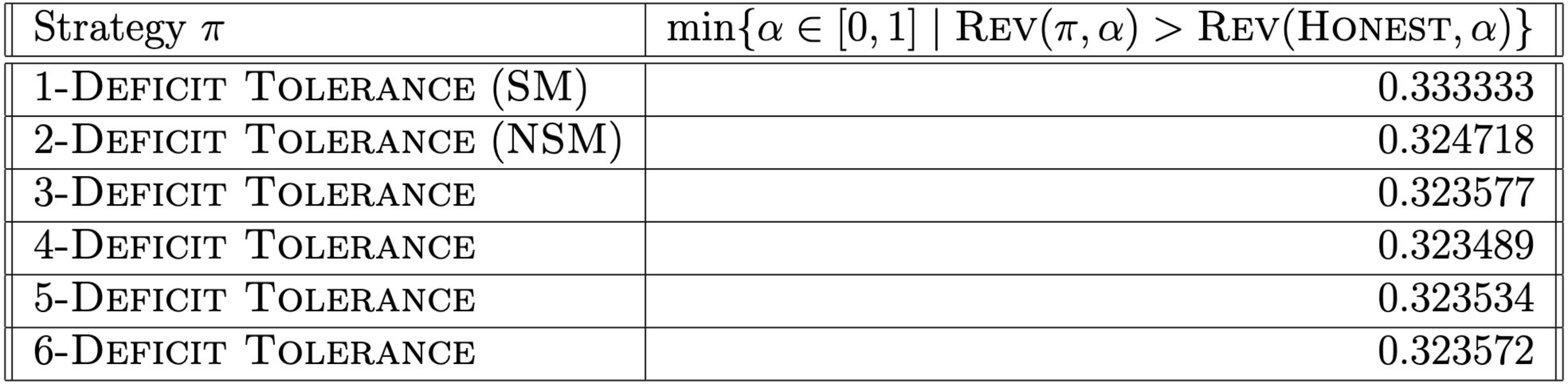
If the strategy gives up at $i+1$ "deficit", then call it $i$-Deficit Tolerance.

$$n\text{-}\textsc{Deficit Tolerance} = \bigcup_{i \in \mathbb{N}_+} \{i\text{-}\textsc{Deficit Tolerance}\}$$

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.
- Wait elsewhere.

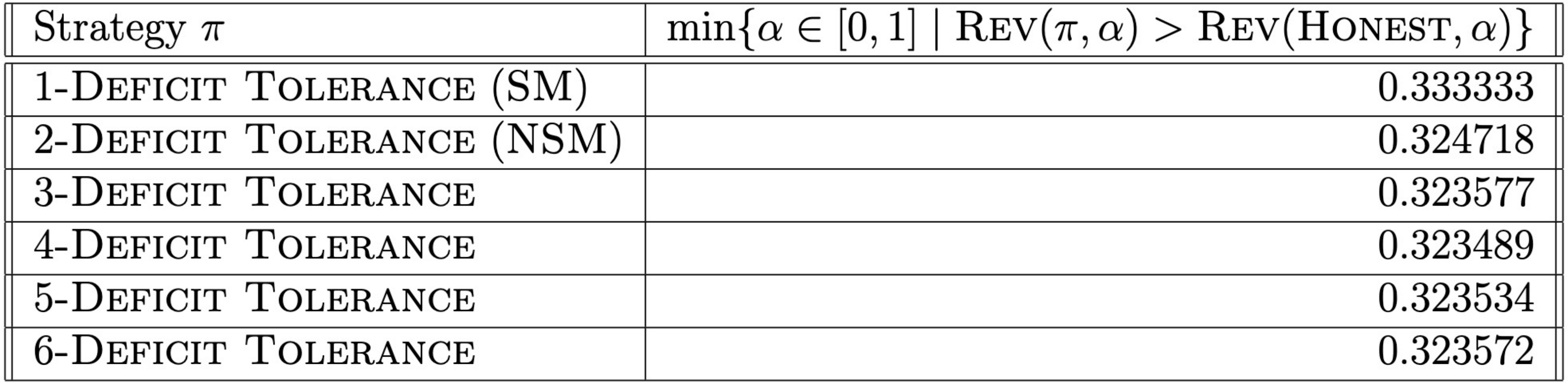
# n-Deficit Tolerance Family of Strategies



| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \textsc{Rev}(\pi,\alpha) > \textsc{Rev}(\textsc{Honest},\alpha)\}$ |
|---|---:|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

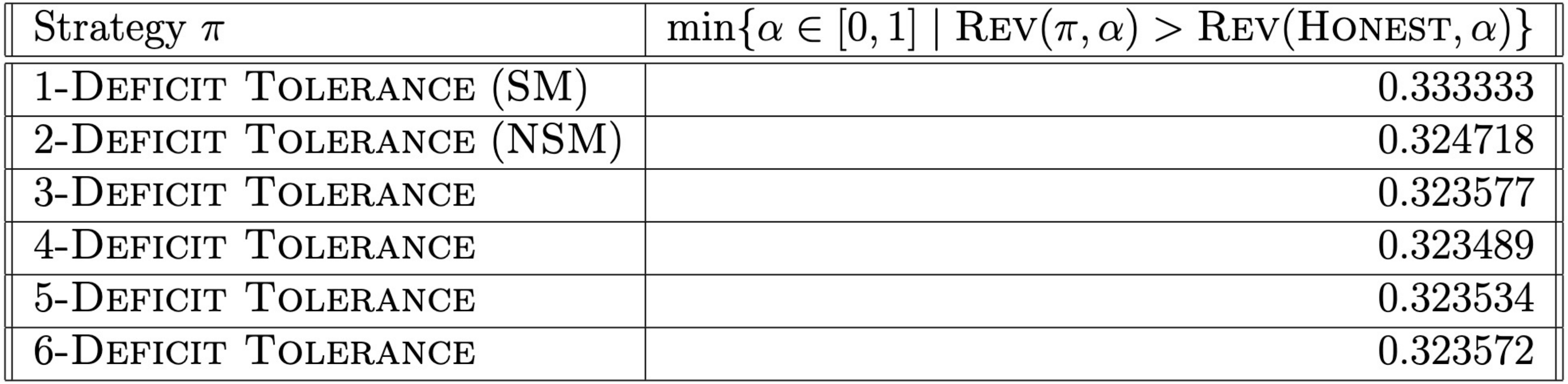
# n-Deficit Tolerance Family of Strategies

Smallest mining strength where it outperforms the honest strategy.



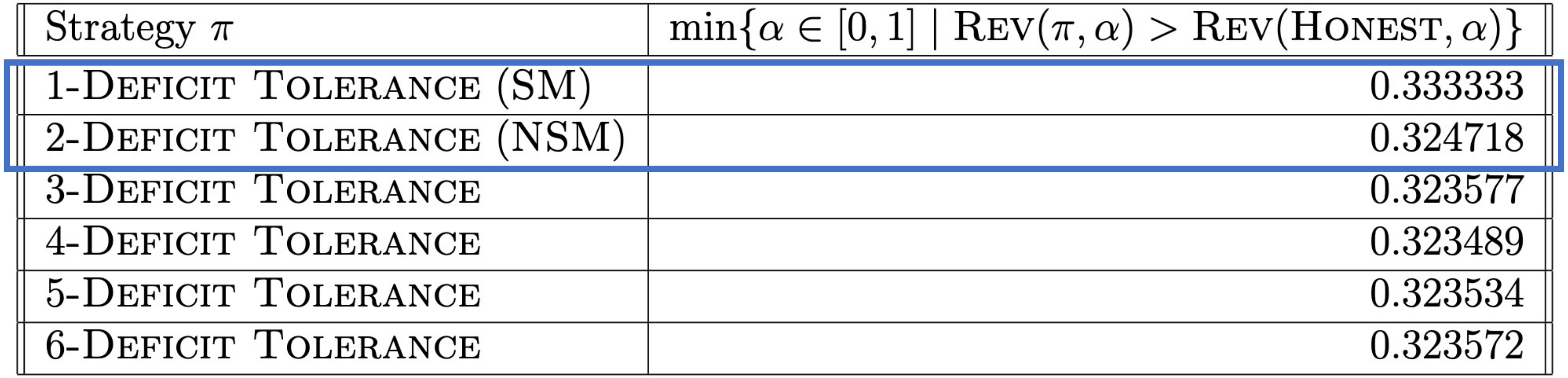
| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \textsc{Rev}(\pi, \alpha) > \textsc{Rev}(\textsc{Honest}, \alpha)\}$ |
|---|---:|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

# n-Deficit Tolerance Family of Strategies



| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \textsc{Rev}(\pi,\alpha) > \textsc{Rev}(\textsc{Honest},\alpha)\}$ |
|---|---:|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

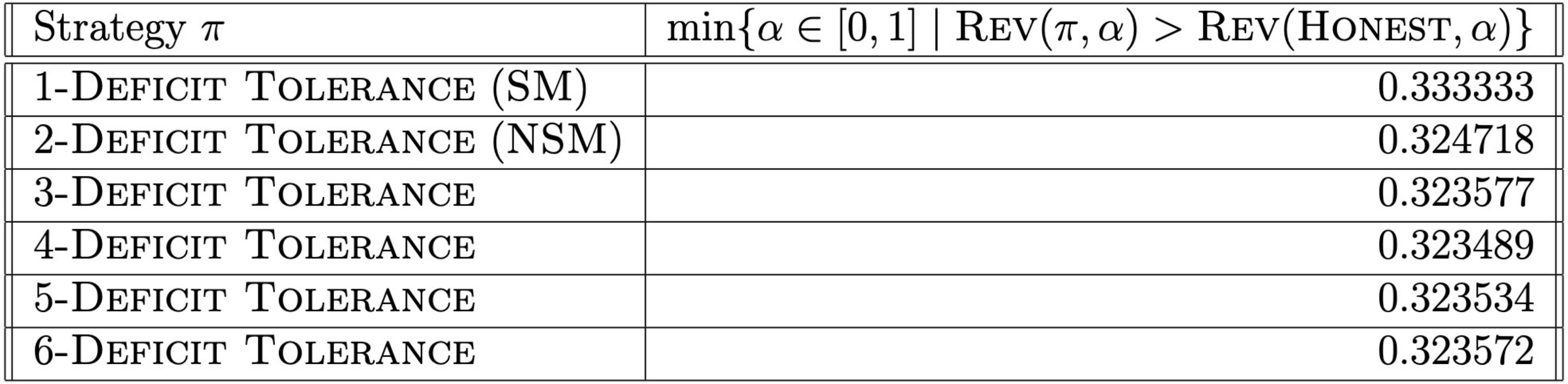
# n-Deficit Tolerance Family of Strategies



| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \textsc{Rev}(\pi,\alpha) > \textsc{Rev}(\textsc{Honest},\alpha)\}$ |
|---|---|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

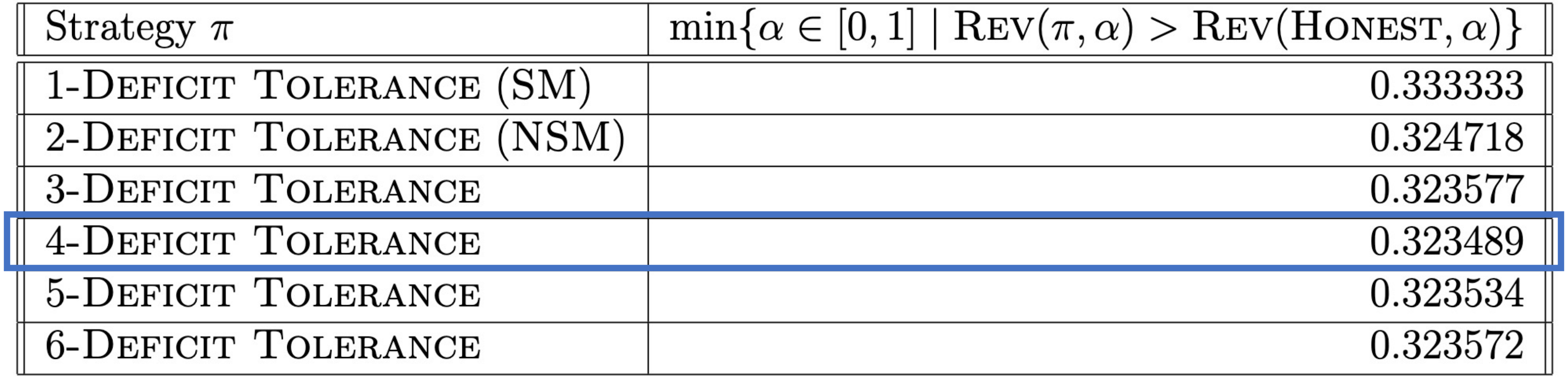
Prior work.

# n-Deficit Tolerance Family of Strategies



| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \mathrm{Rev}(\pi, \alpha) > \mathrm{Rev}(\mathrm{Honest}, \alpha)\}$ |
|---|---:|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

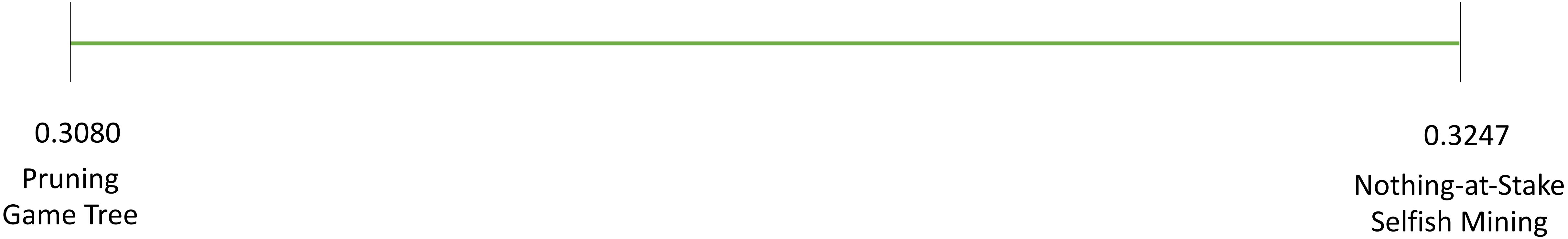
# n-Deficit Tolerance Family of Strategies



| Strategy $\pi$ | $\min\{\alpha \in [0,1] \mid \textsc{Rev}(\pi,\alpha) > \textsc{Rev}(\textsc{Honest},\alpha)\}$ |
|---|---:|
| 1-Deficit Tolerance (SM) | 0.333333 |
| 2-Deficit Tolerance (NSM) | 0.324718 |
| 3-Deficit Tolerance | 0.323577 |
| 4-Deficit Tolerance | 0.323489 |
| 5-Deficit Tolerance | 0.323534 |
| 6-Deficit Tolerance | 0.323572 |

# n-Deficit Tolerance Family of Strategies

$0.3080 \leq \alpha^{PoS} \leq 0.3247$



0.3080

Pruning
Game Tree

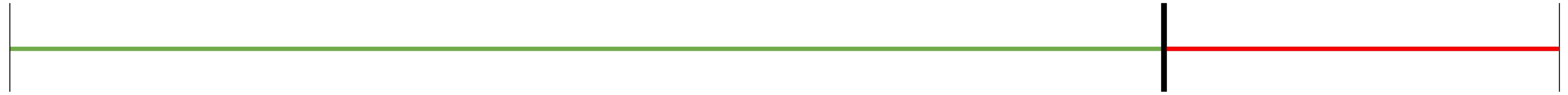
0.3247

Nothing-at-Stake
Selfish Mining

* Not drawn to scale.

# n-Deficit Tolerance Family of Strategies

$0.3080 \leq \alpha^{PoS} \leq 0.3235$



0.3080

Pruning Game Tree

0.3235

4-Deficit Tolerance

0.3247

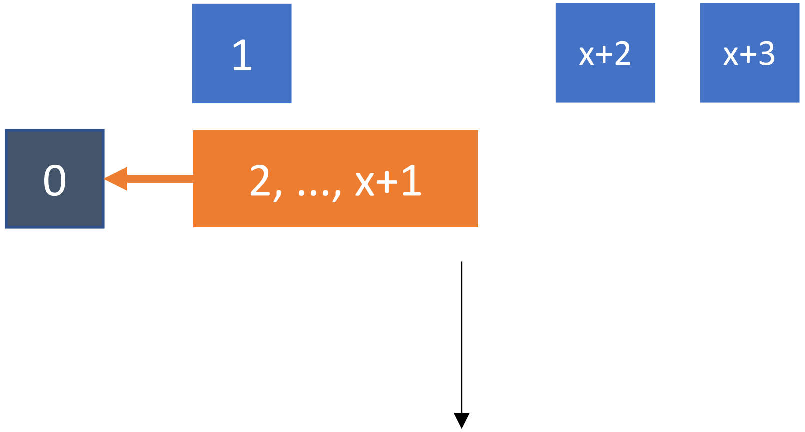
Nothing-at-Stake Selfish Mining

* Not drawn to scale.

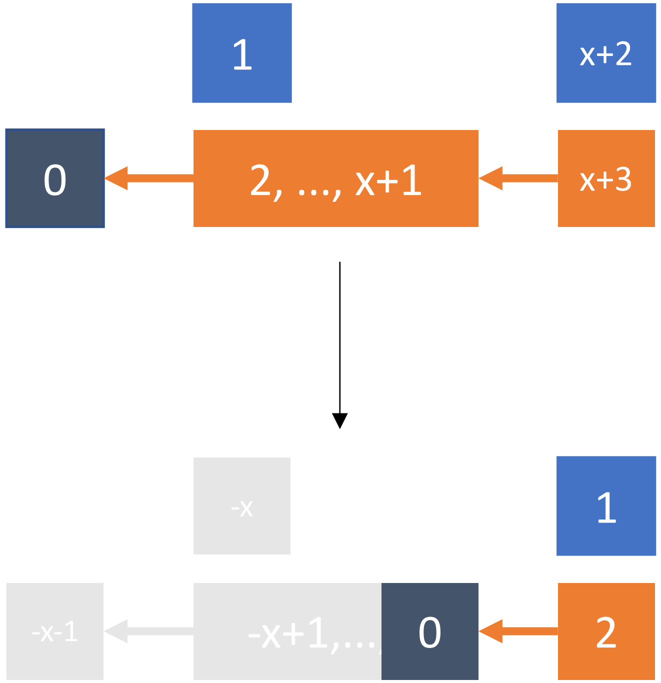
revisited

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



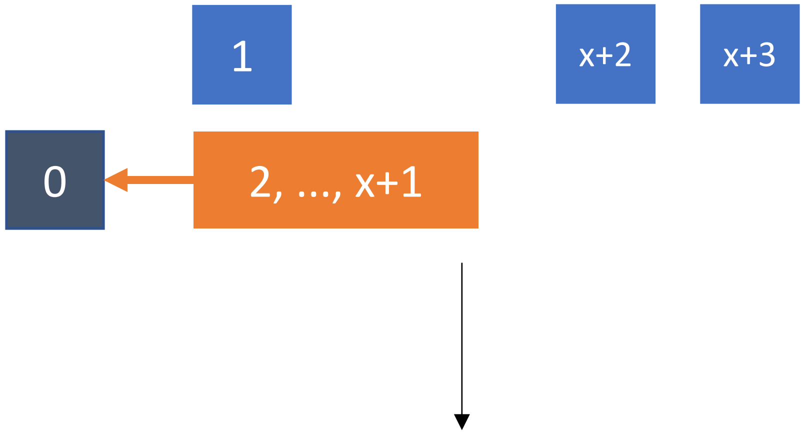
*Wait* until defender catches up on blocks {x+2, x+3} or can recover block 1.



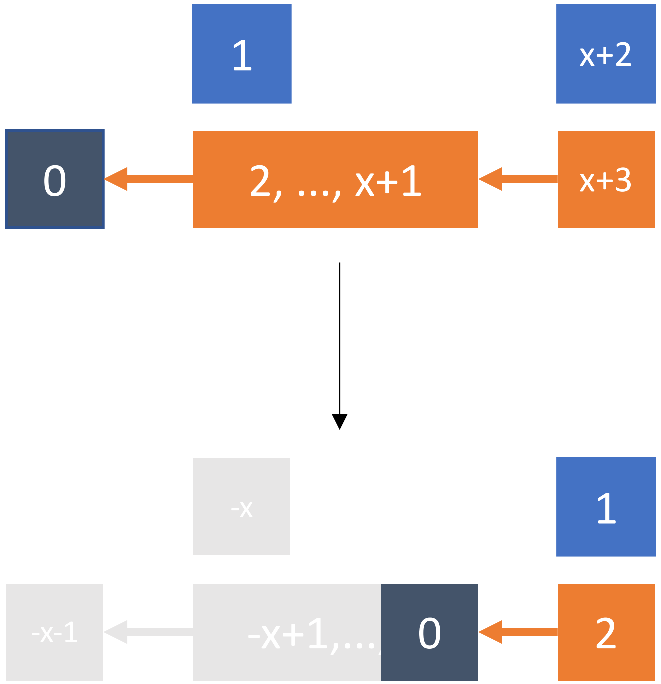
revisited

# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



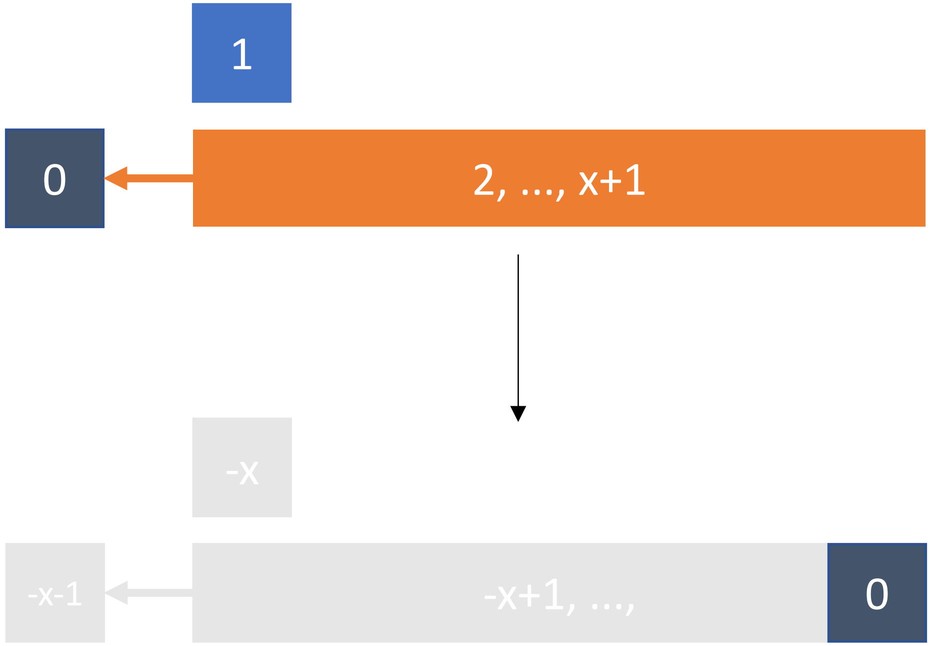
✓ *Wait* until defender catches up on blocks {x+2, x+3} or can recover block 1.



revisited

# n-Deficit Tolerance Family of Strategies

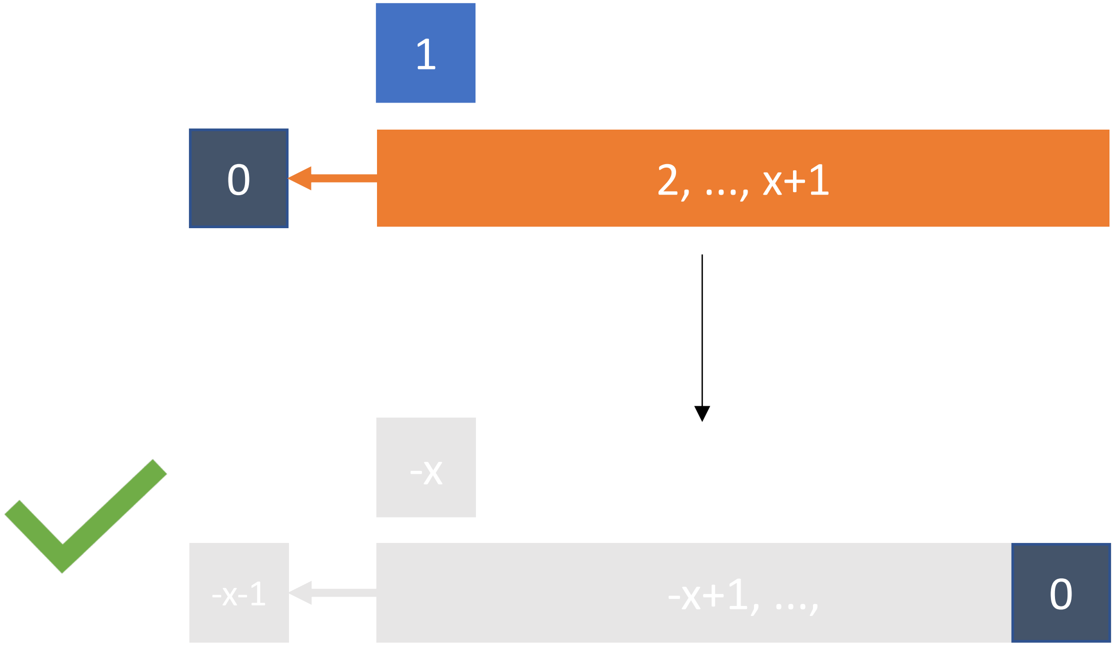
- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



revisited

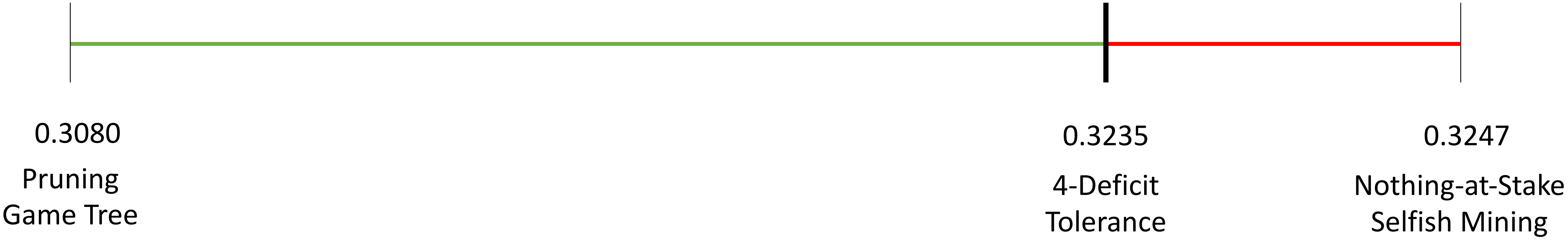
# n-Deficit Tolerance Family of Strategies

- Take optimal action at states where this is known.
- Take *reasonable* actions at other states that are interesting.



# n-Deficit Tolerance Family of Strategies

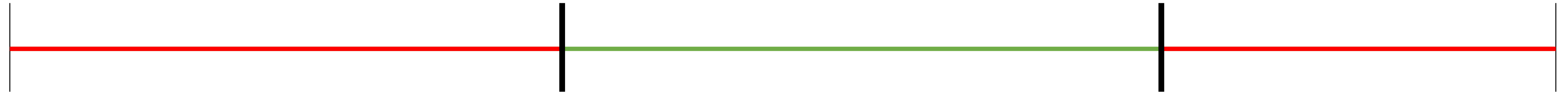
$0.3080 \leq \alpha^{PoS} \leq 0.3235$



* Not drawn to scale.

# n-Deficit Tolerance Family of Strategies

$0.3152 \leq \alpha^{PoS} \leq 0.3235$



0.3080

Pruning
Game Tree

0.3152

Further Pruning
Game Tree

0.3235

4-Deficit
Tolerance

0.3247

Nothing-at-Stake
Selfish Mining

* Not drawn to scale.

# Overview

1. Motivation
2. Game
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. **Automating this Search**
9. Conclusion

# Automating this Search

Algorithm:

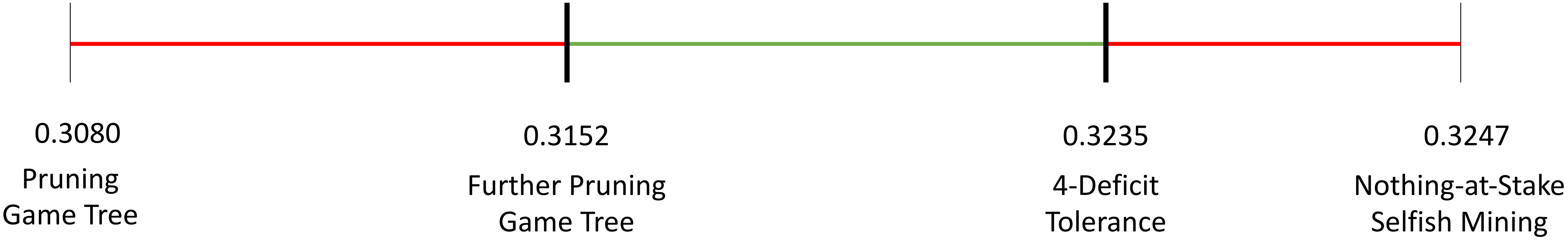
1. Simulate all reachable states with at most $n$ blocks.
2. Lower and upper bound the value of all states with $n$ blocks.
3. For $i = n - 1, \ldots, 0$:
    a. Lower and upper bound the value of all states with $i$ blocks.

The above results on structured strategies, symmetrical states, and non-checkpoint finality, make this *computationally feasible*.

https://thesis.anthonyhein.com/materials/code-results/index.html

# Automating this Search

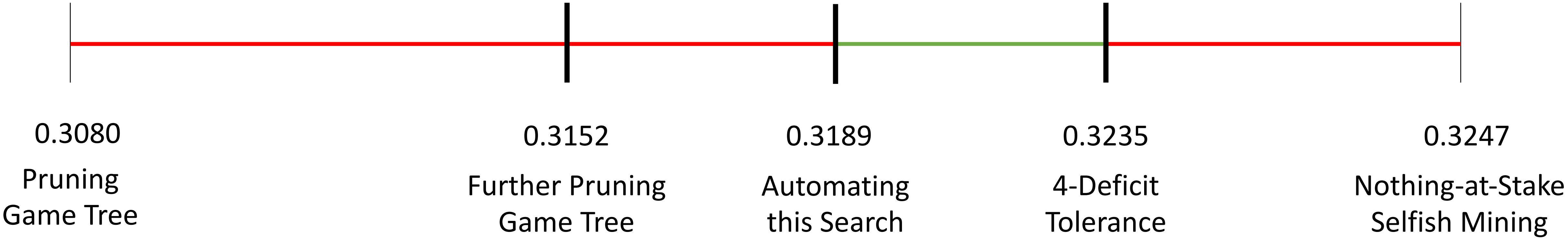
$0.3152 \leq \alpha^{PoS} \leq 0.3235$



* Not drawn to scale.

# Automating this Search

$0.3189 \leq \alpha^{PoS} \leq 0.3235$



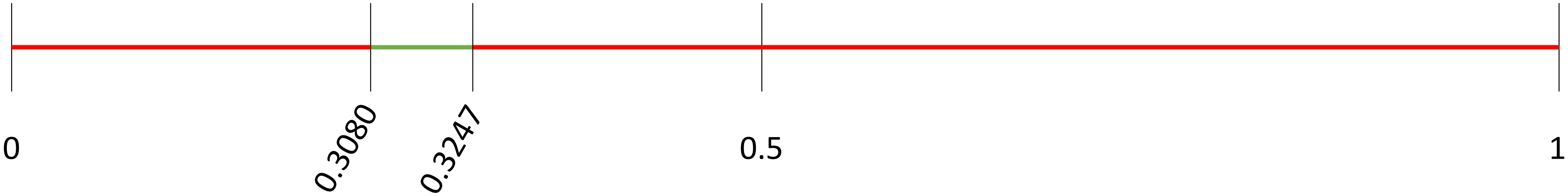
* Not drawn to scale.

# Overview

1. Motivation
2. Game
3. Prior Work
4. Structured Strategies
5. Symmetrical States
6. Non-Checkpoint Finality
7. n-Deficit Tolerance Family of Strategies
8. Automating this Search
9. **Conclusion**

# Conclusion

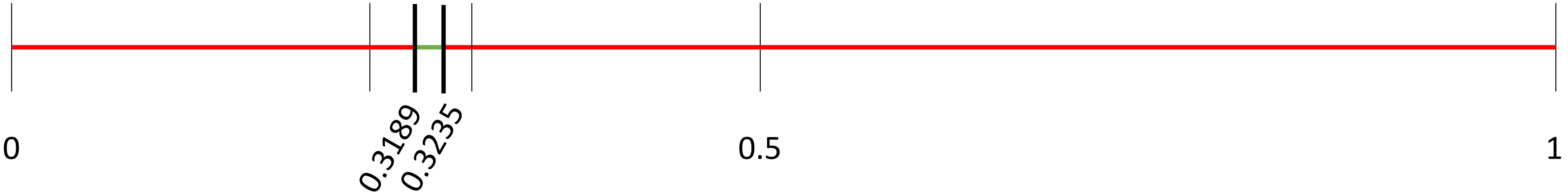
$0.3080 \leq \alpha^{PoS} \leq 0.3247$



* Not drawn to scale.

# Conclusion

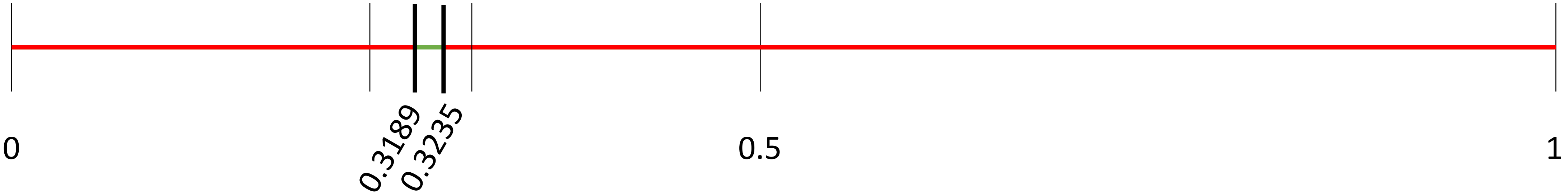
$0.3189 \leq \alpha^{PoS} \leq 0.3235$



* Not drawn to scale.

# Conclusion

Assuming a Bitcoin-like cryptocurrency, increasing mining strength by 0.001 costs $900,000,000.



* Not drawn to scale.

# Acknowledgements

Professor Matt Weinberg

Doctor Matheus V. X. Ferreira

Professor Mark Braverman

Briana Macedo

# Materials

All materials can be found at [https://thesis.anthonyhein.com](https://thesis.anthonyhein.com)

Username: princeton

Password: pledge-my-honor

# Questions?

Please email one of

- anhein@princeton.edu
- anhein@cs.princeton.edu
- anthonynhein@gmail.com