Hyperproperties in Security Protocols

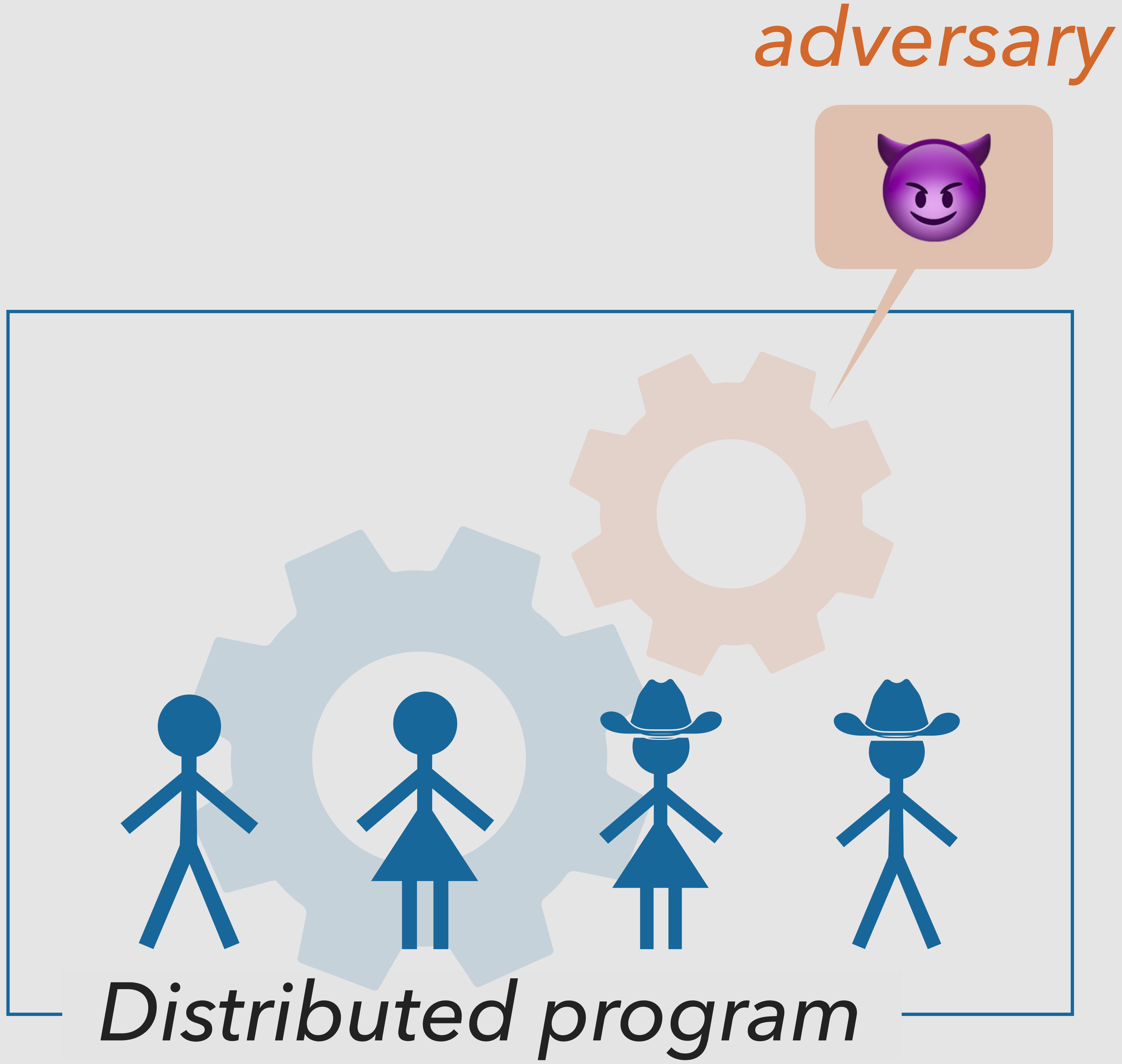
Summary of a coffee-break discussion

Itsaka Rakotonirina

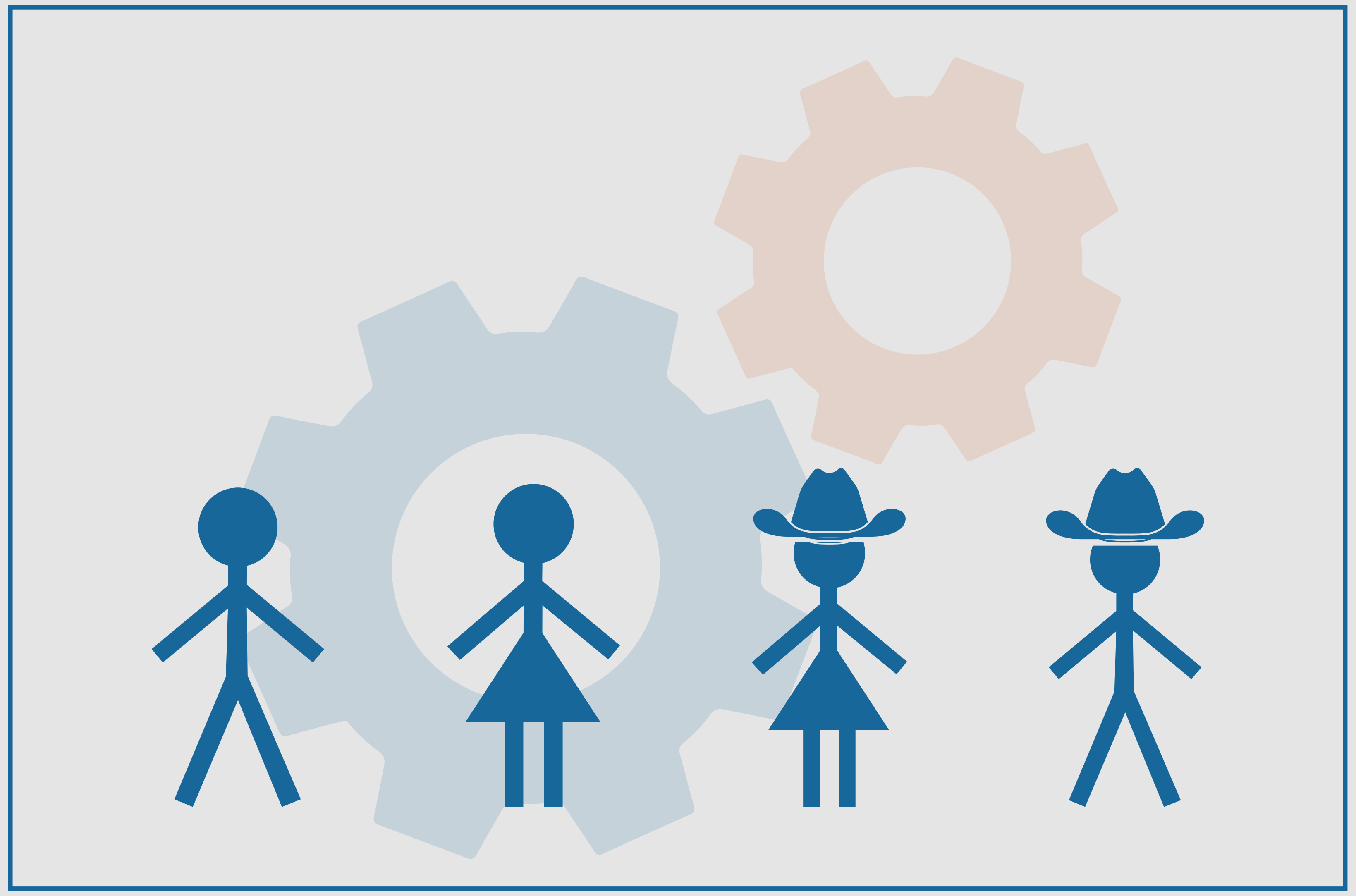
Security Protocols

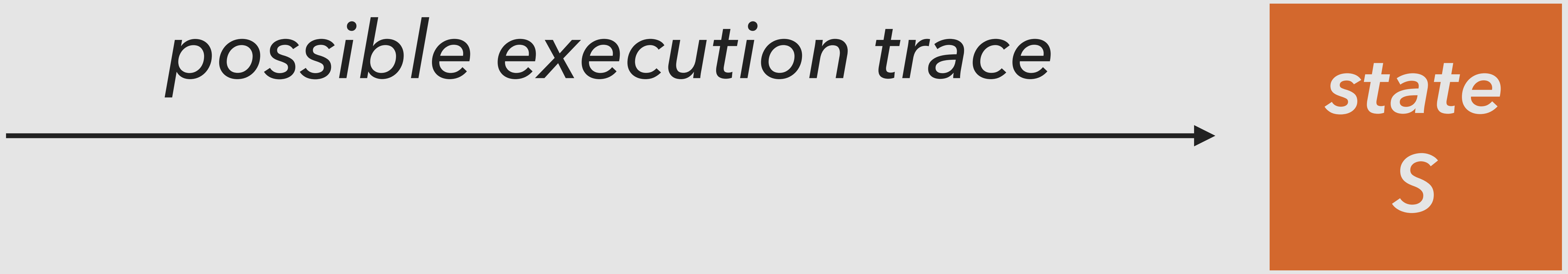
Distributed program

Security Protocols

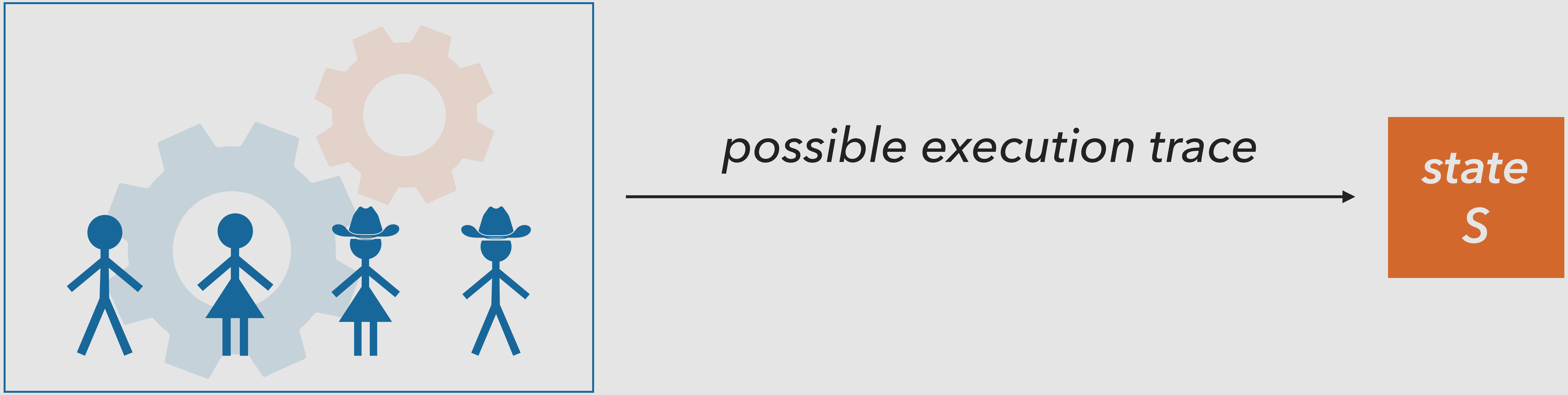


Reachability





Reachability



possible execution trace

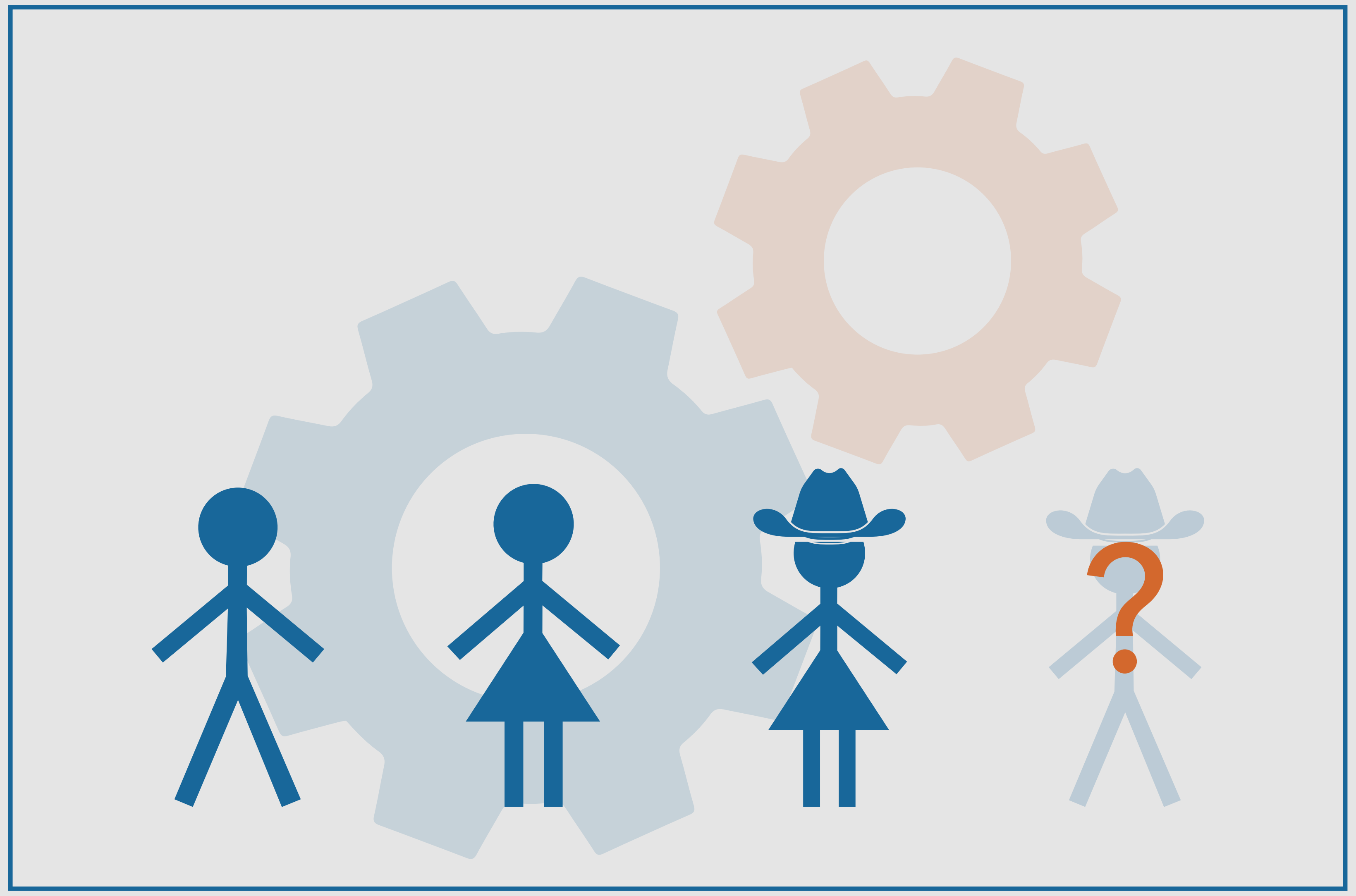
state S

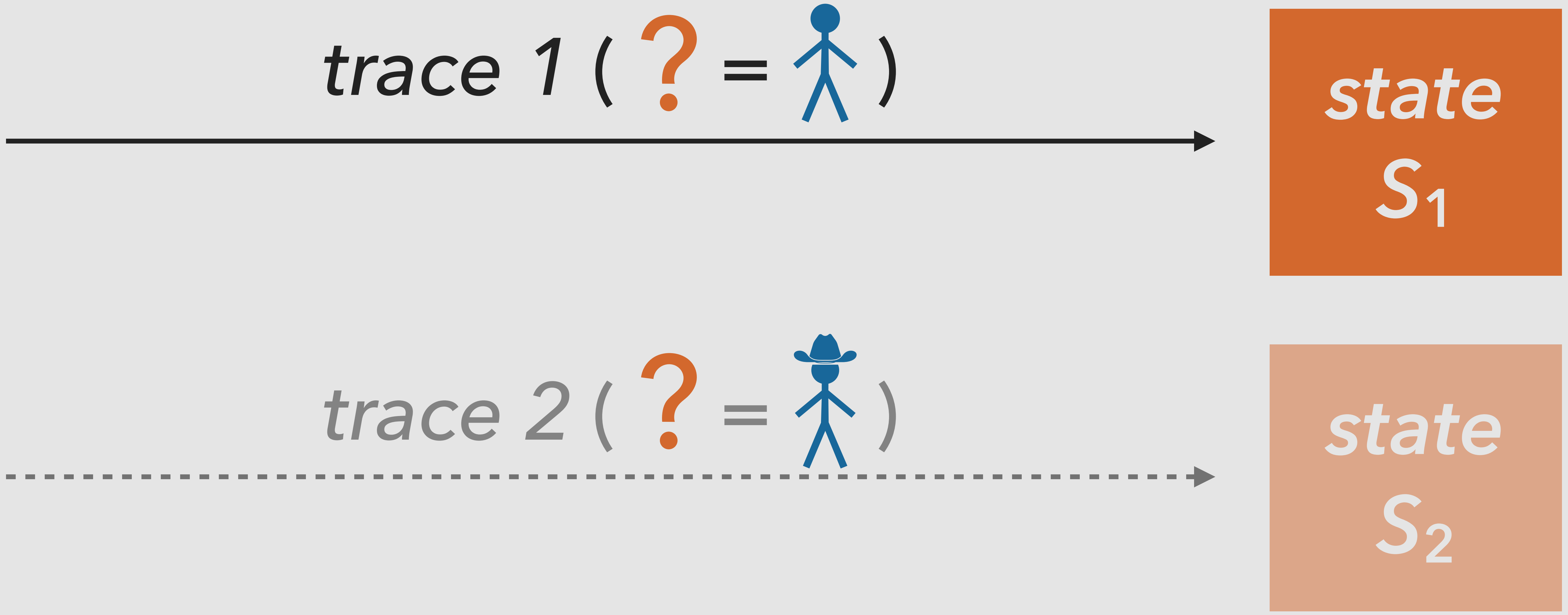
Property

For all traces *T*, the final state *S* of *T* is "**fine**"

chosen local property on the final state

Indistinguishability





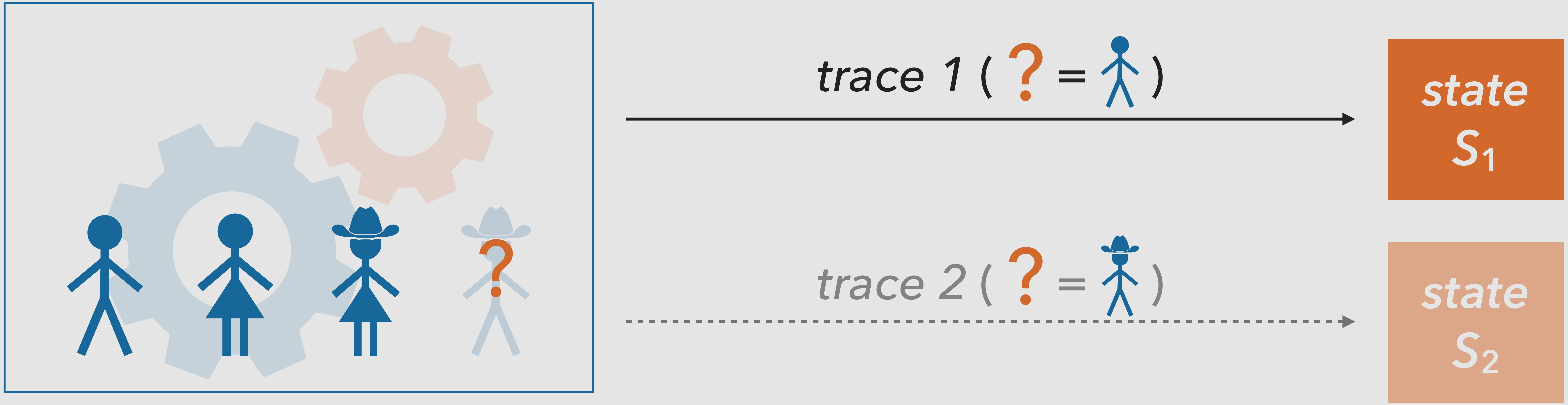
trace 1 (? =)

state S_1

trace 2 (? =)

state S_2

Indistinguishability



trace 1 (? =)

state S_1

trace 2 (? =)

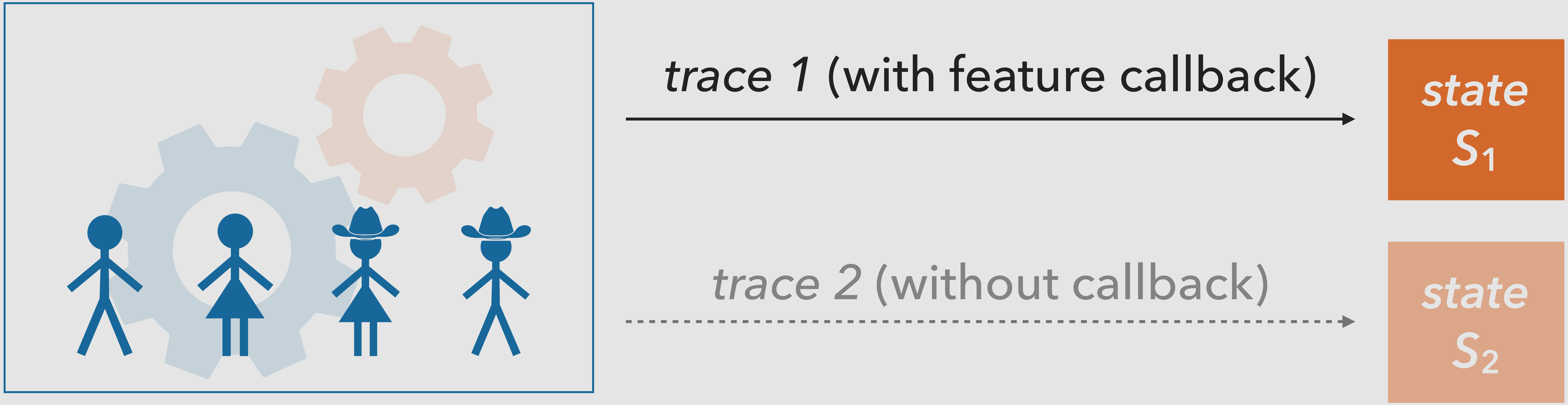
state S_2

Property

For all traces T_1, there exists a trace T_2, “$\boldsymbol{T_1 \sim T_2}$”

indistinguishable by adversarial tests

⚠️ *Effective callback freedom*



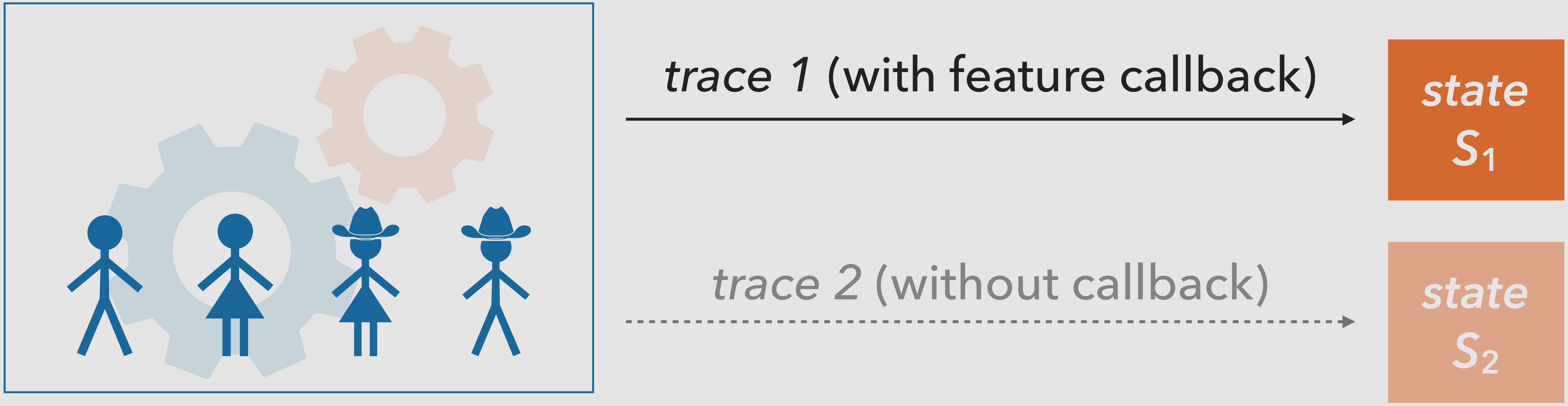
trace 1 (with feature callback)

state S_1

trace 2 (without callback)

state S_2

⚠️ *Effective callback freedom*



trace 1 (with feature callback)

trace 2 (without callback)

state S_1

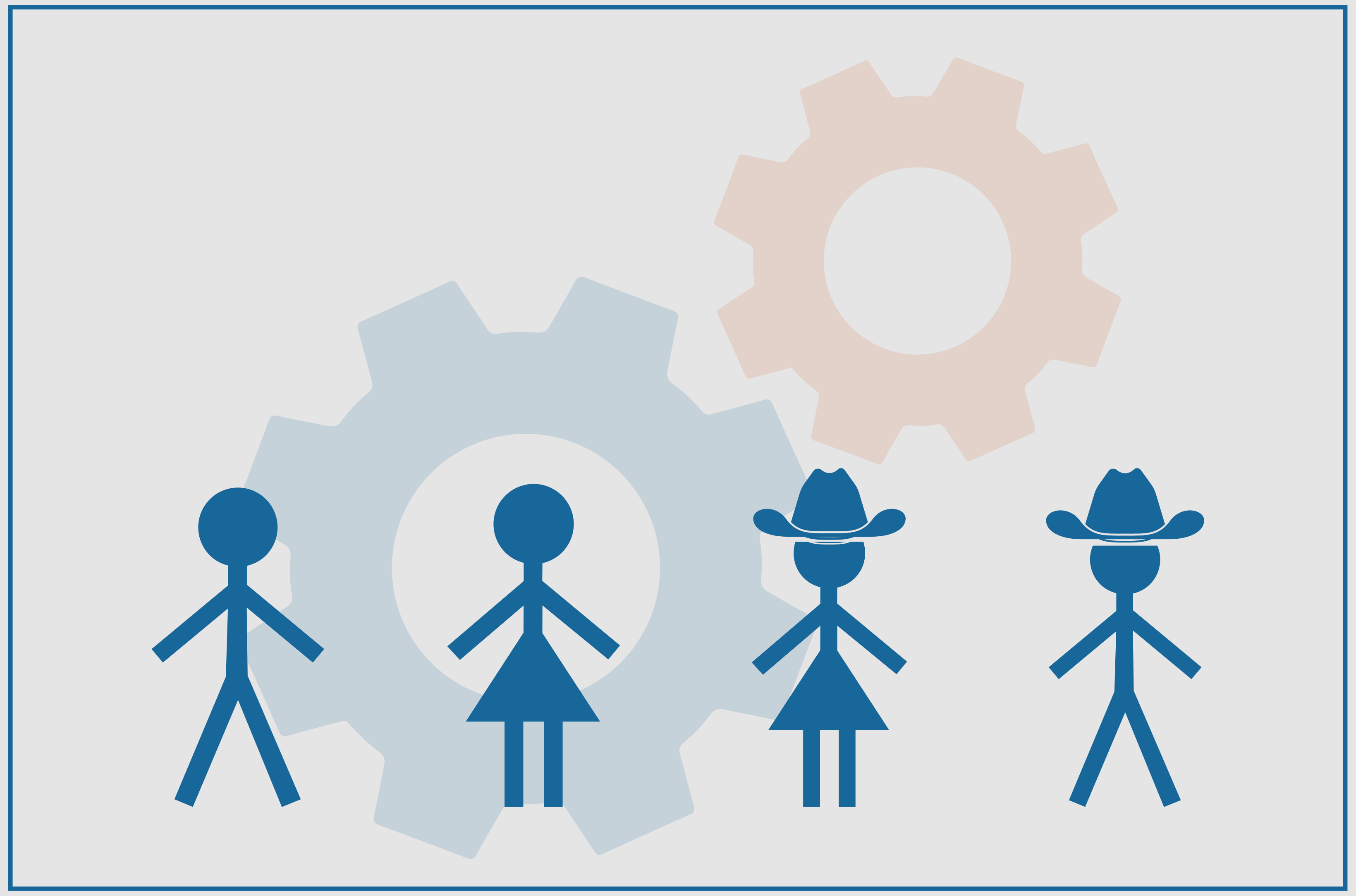
state S_2

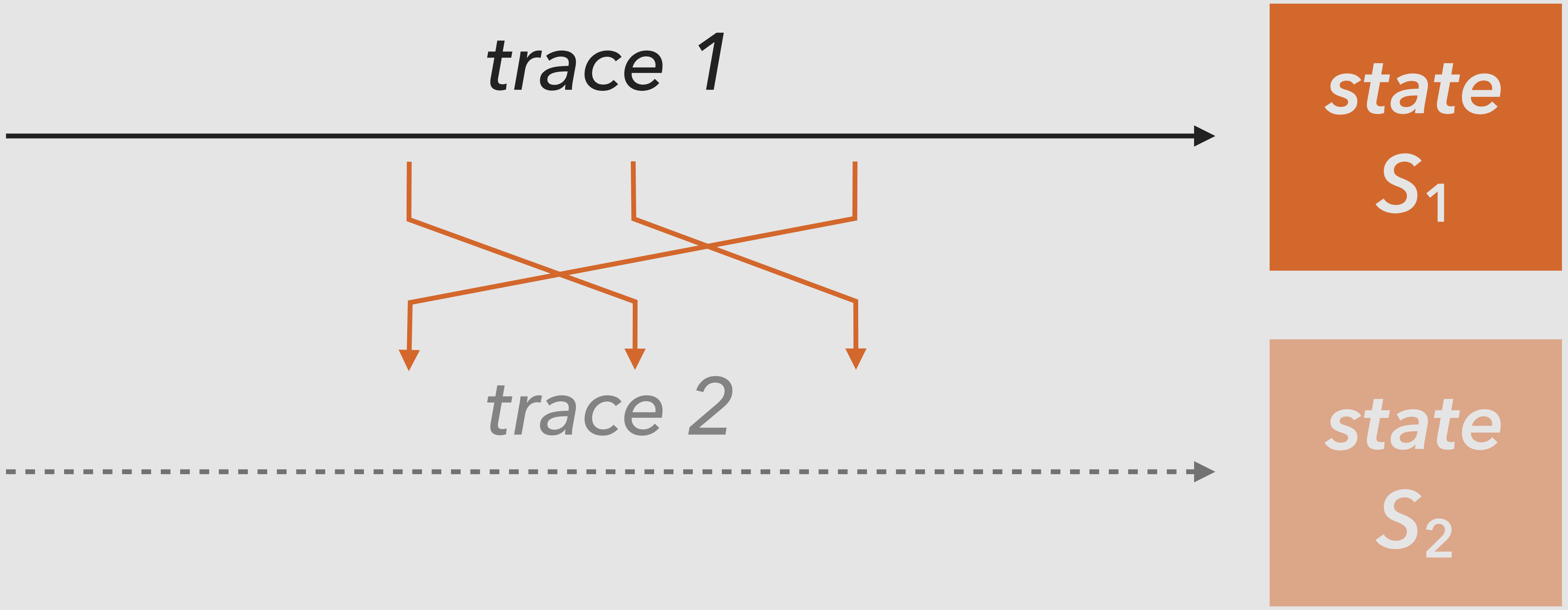
Property

For all traces T_1, there exists a trace T_2 (without callback), "$\boldsymbol{S_1 \approx S_2}$"

equivalence relation on final states

⚠️ *Front-Running Resistance*





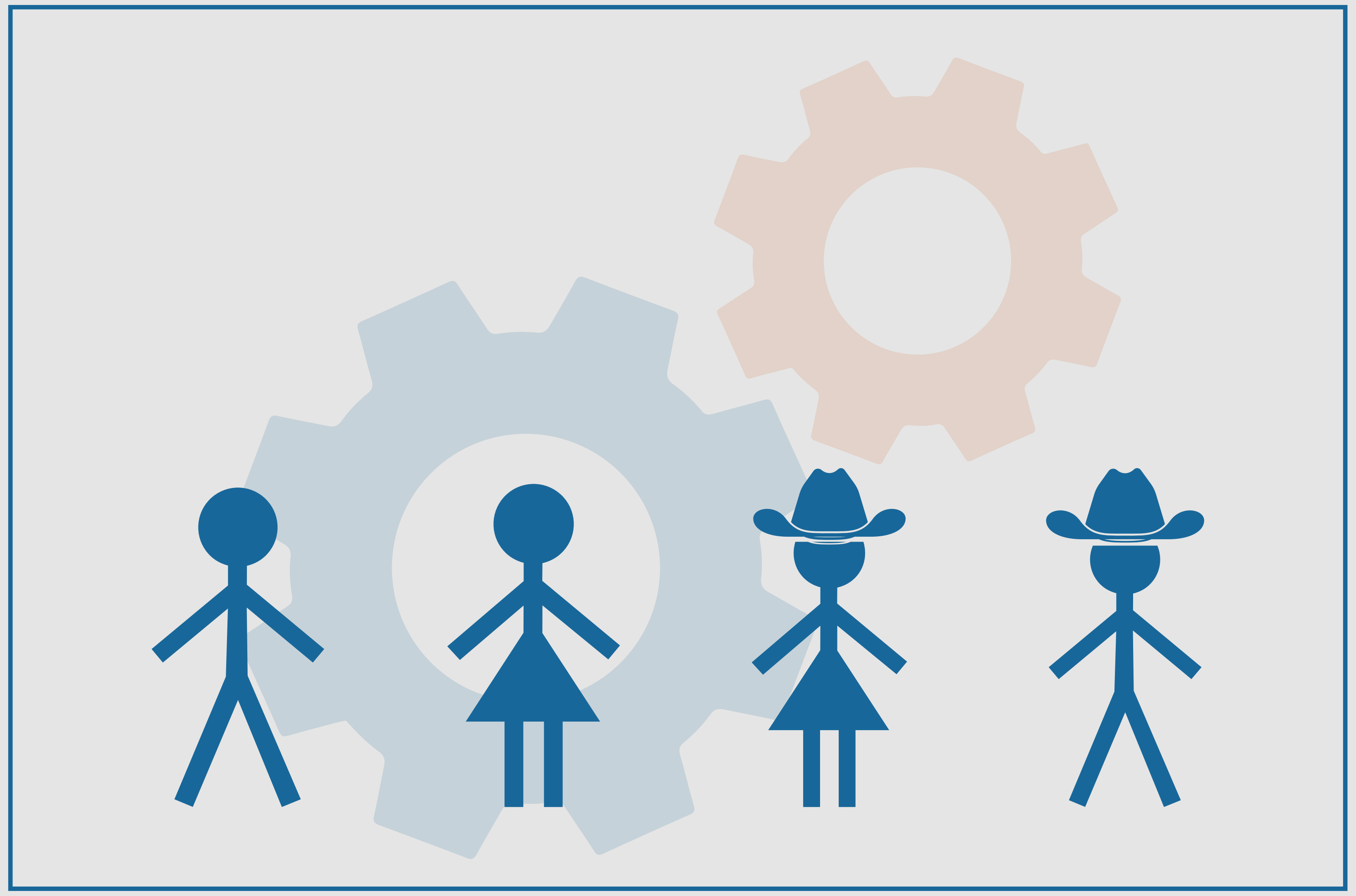
trace 1

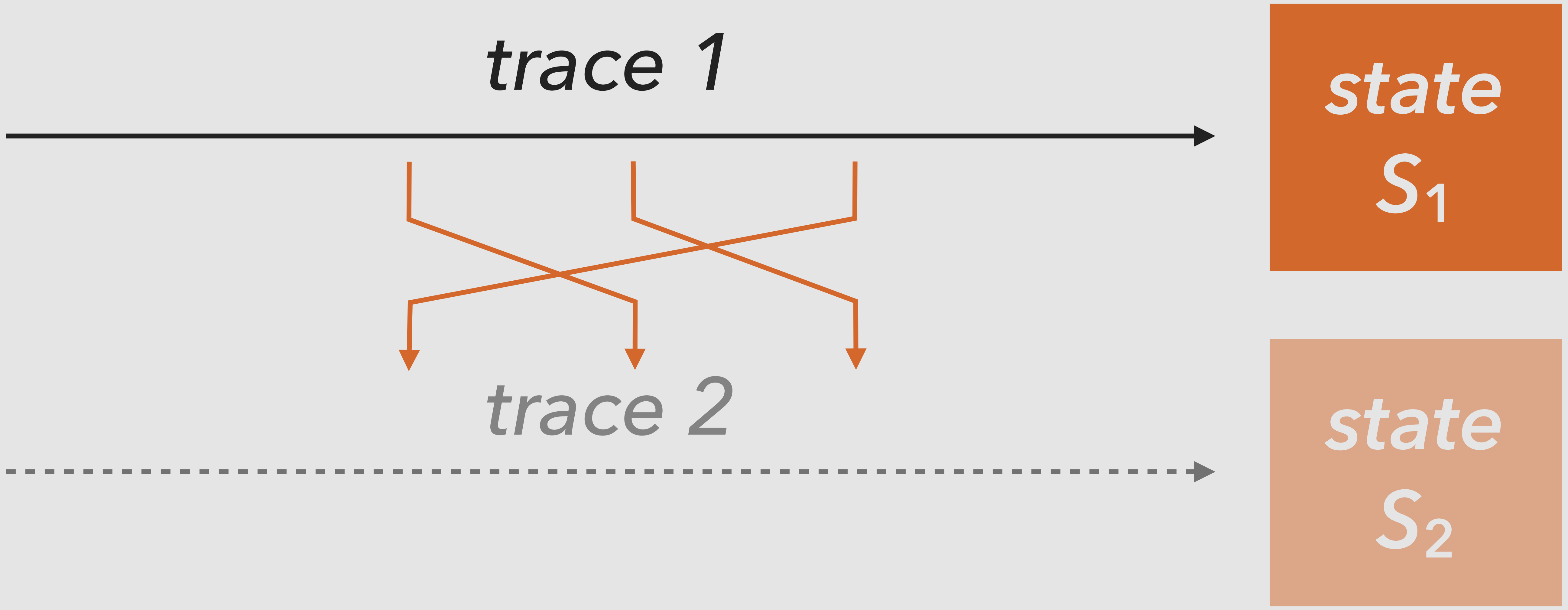
state S_1

trace 2

state S_2

⚠️ *Front-Running Resistance*





trace 1

state S_1

trace 2

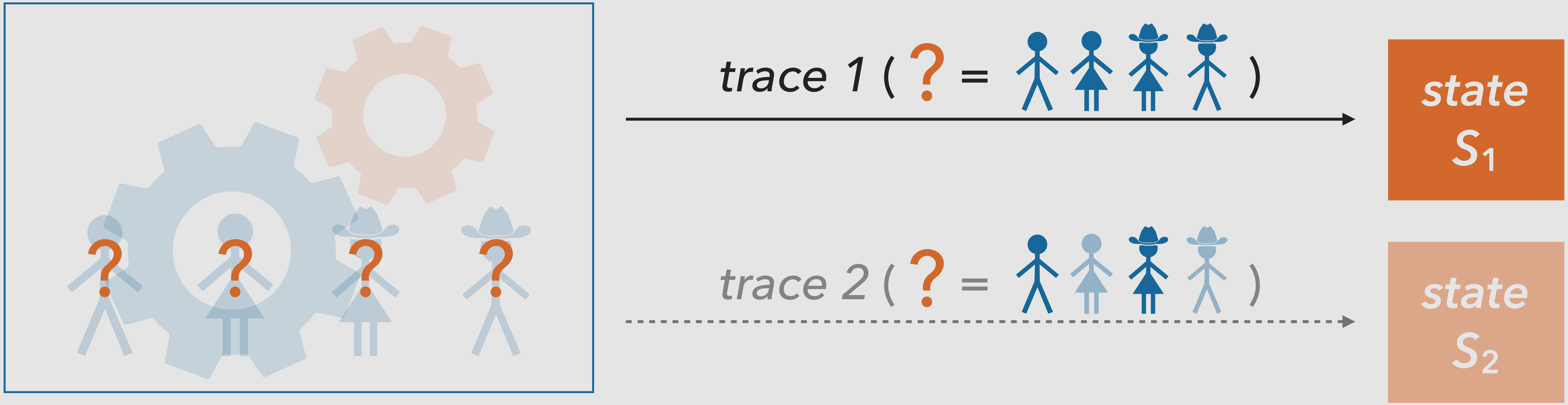
state S_2

Property

For all traces T_1, for all traces T_2 that is a permutation of T_1, "$\boldsymbol{S_2 \approx S_1}$"

equivalence relation on final states

⚠️ Coalition Resistance



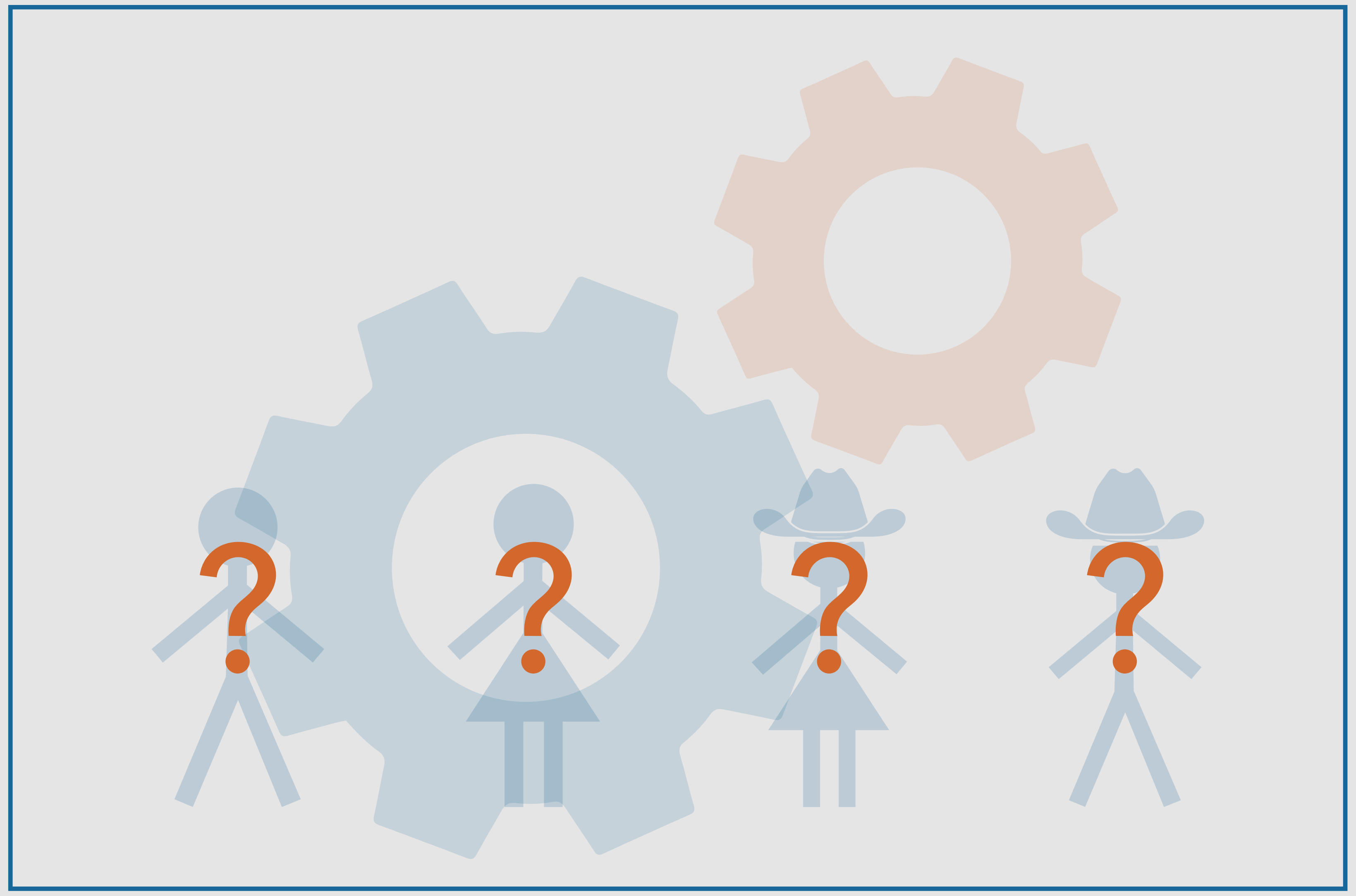
trace 1 (? =)

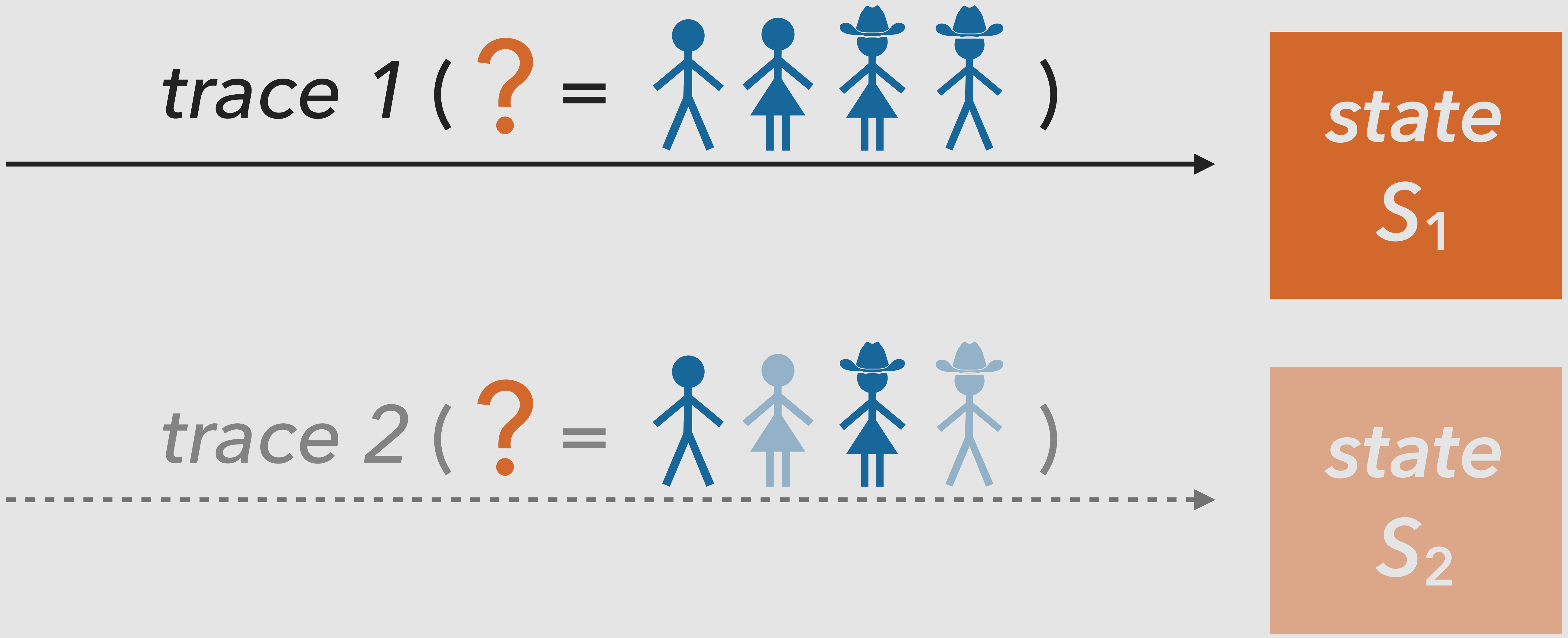
state S_1

trace 2 (? =)

state S_2

⚠️ Coalition Resistance





trace 1 (? =)

state S_1

trace 2 (? =)

state S_2

Property

For all traces T_1, for all traces T_2 involving a subset of T_1's participants, "$\boldsymbol{S_2 \leq S_1}$"

ordering on states (advantage)