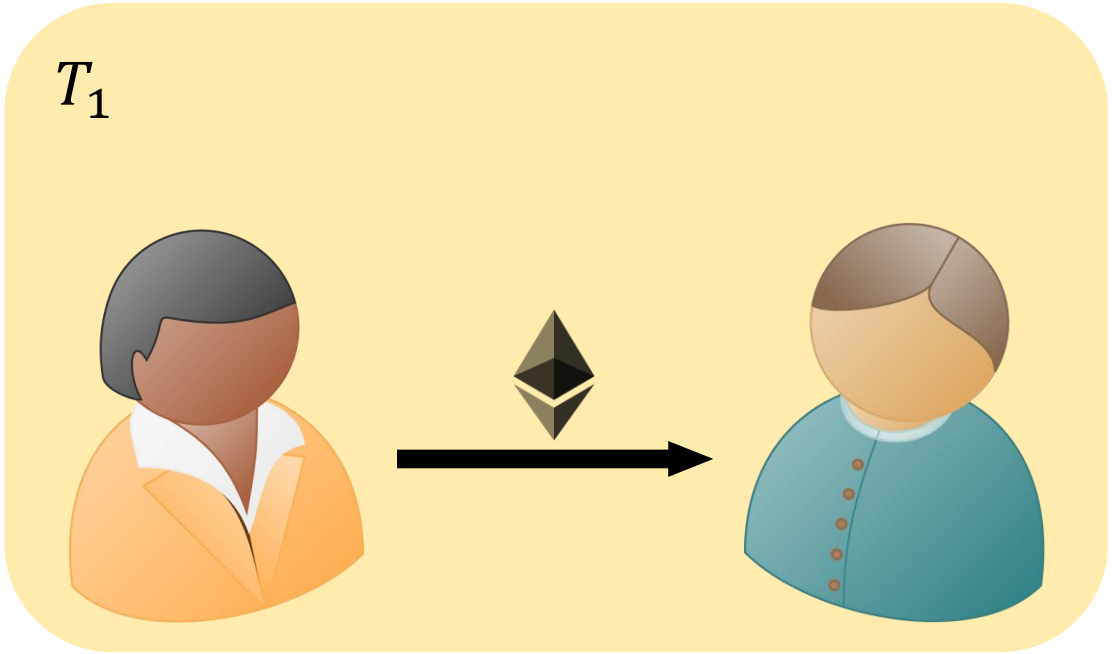
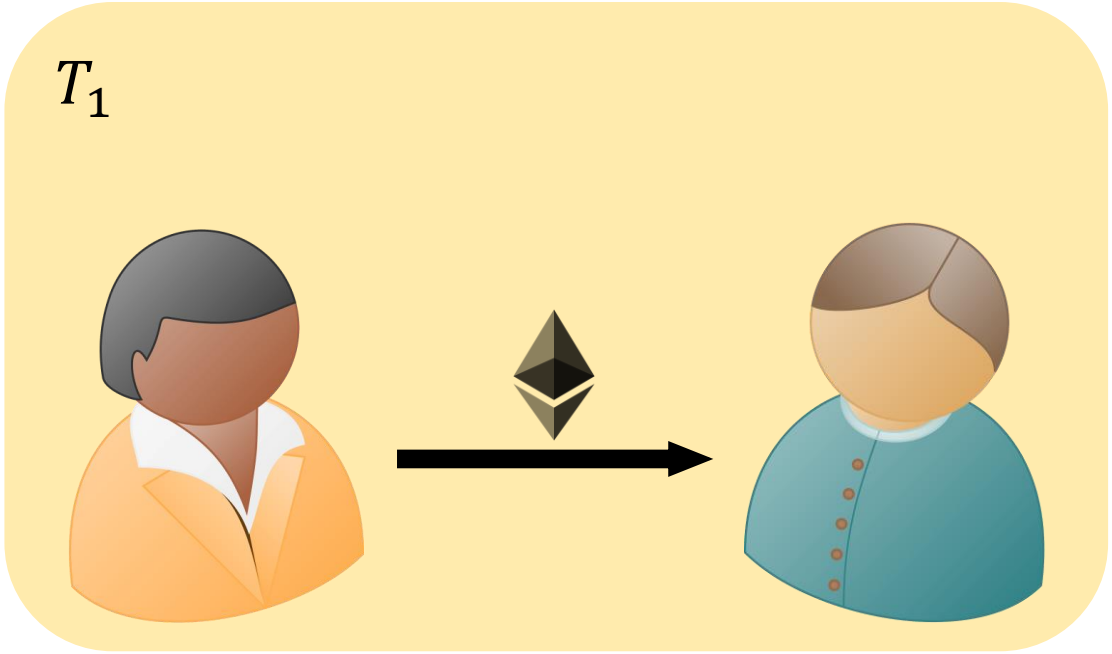
SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance

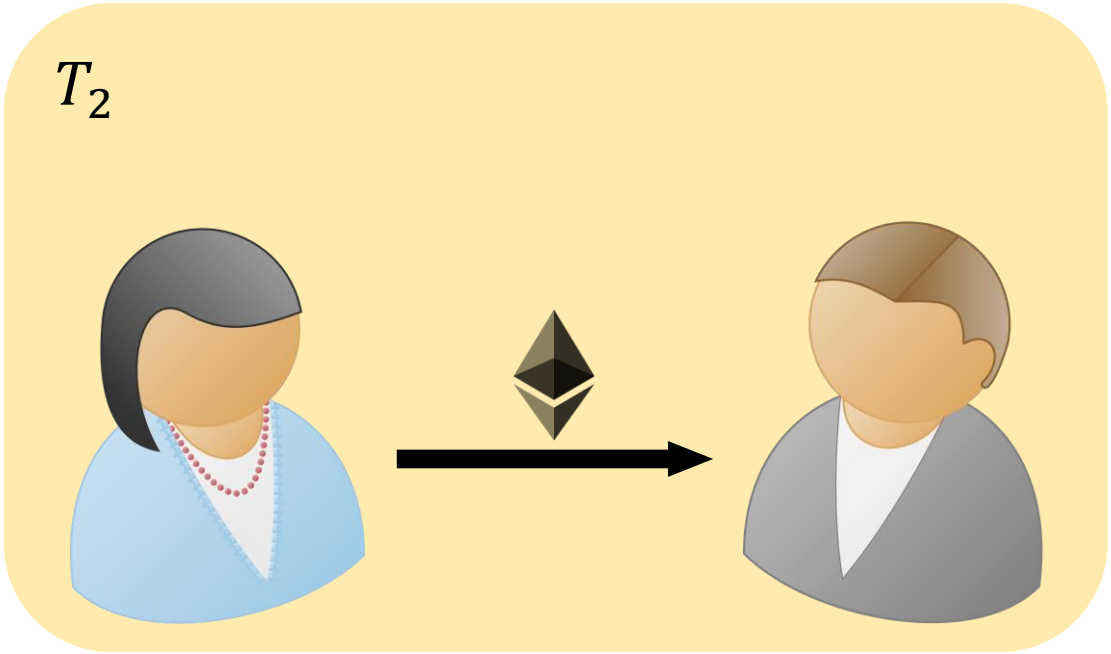
Advances in Financial Technologies (AFT'22)
Lioba Heimbach, Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

Transaction Ordering

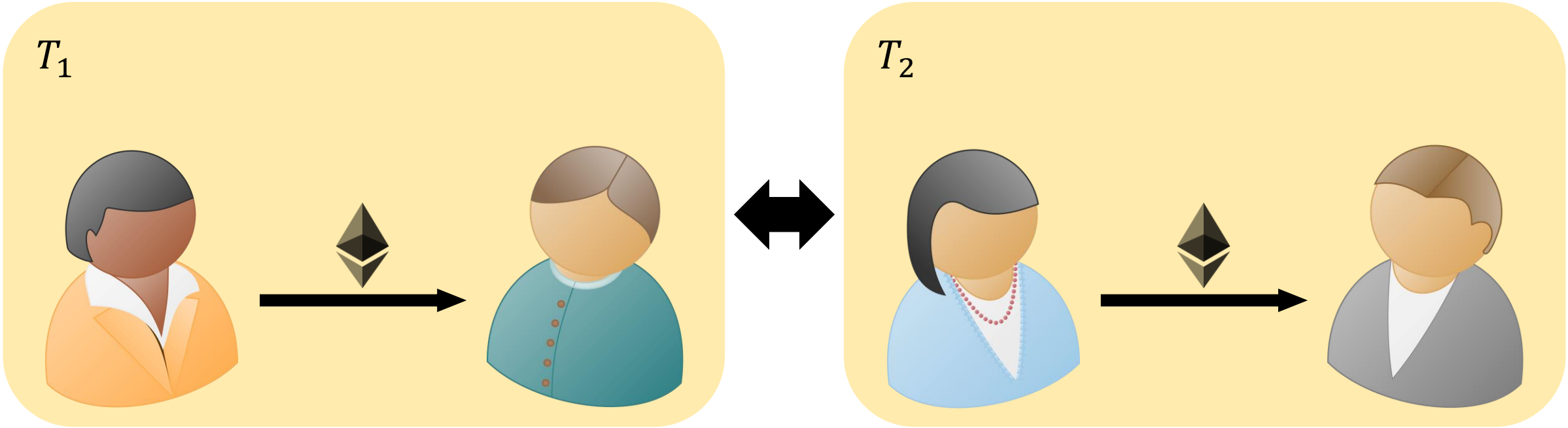


Transaction Ordering





Transaction Ordering



Transaction Ordering

T_E

T_A

T_B

T_C

T_D

Transaction Ordering

T_A T_B T_C T_D T_E

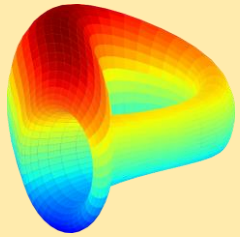
Decentralized Finance (DeFi)

Decentralized Exchanges

Lending Protocols

Decentralized Finance (DeFi)

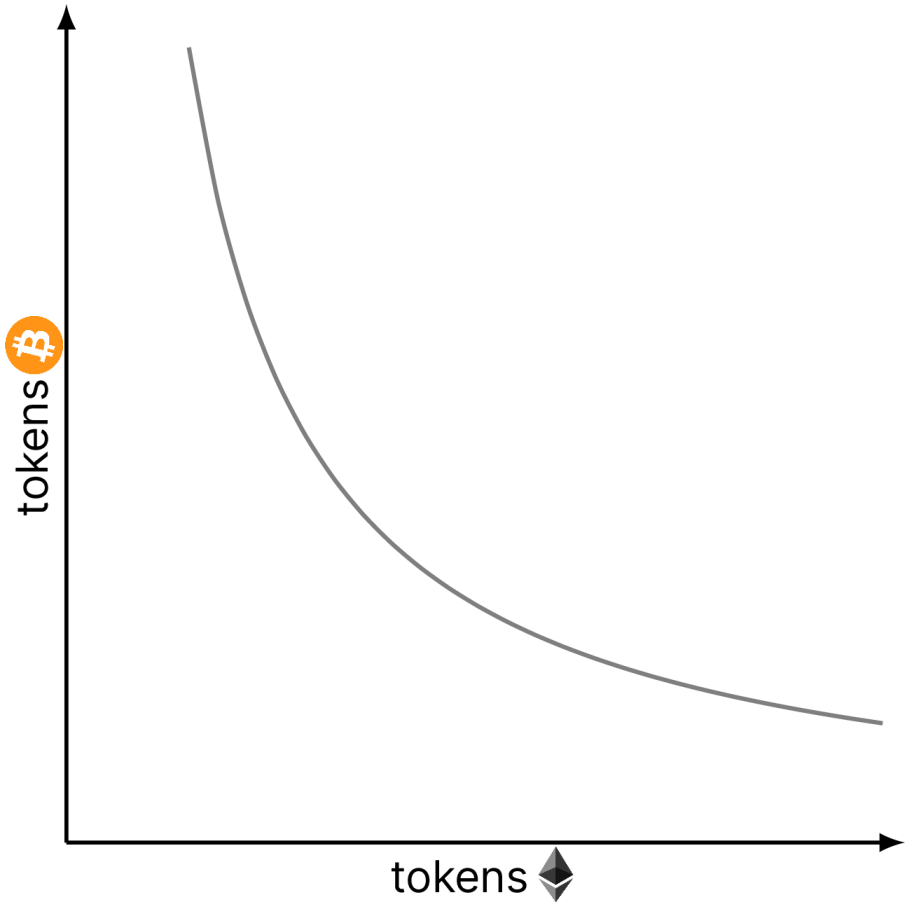
Decentralized Exchanges



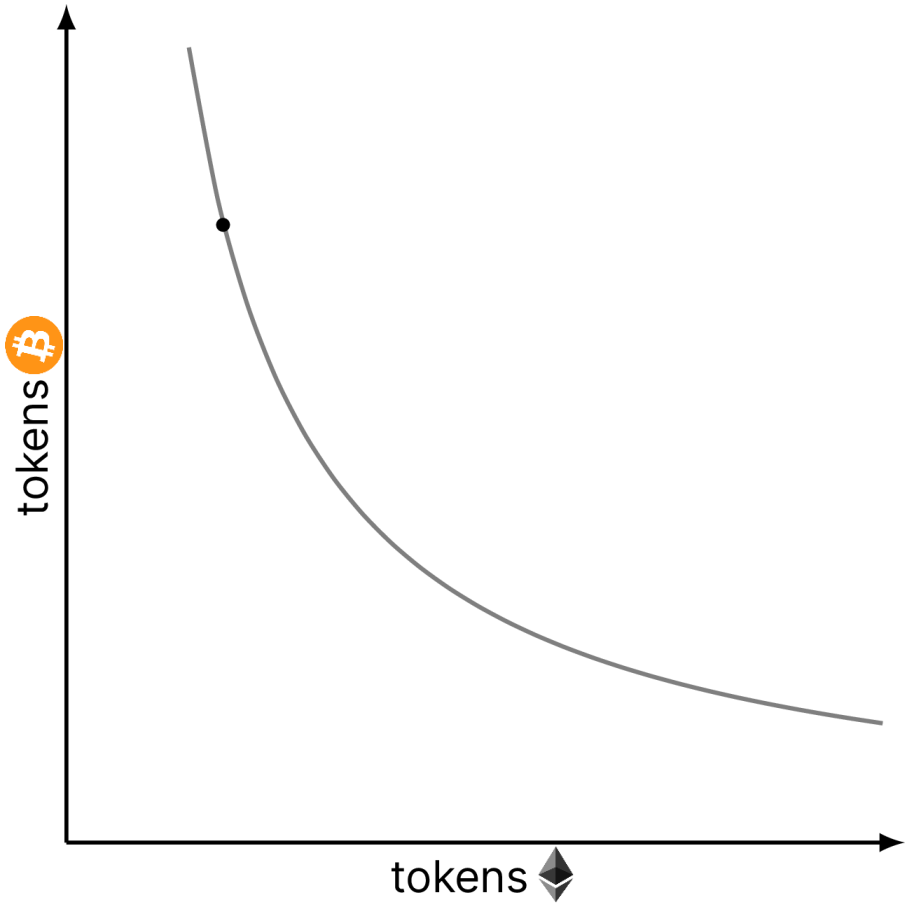
δY/δX

Lending Protocols

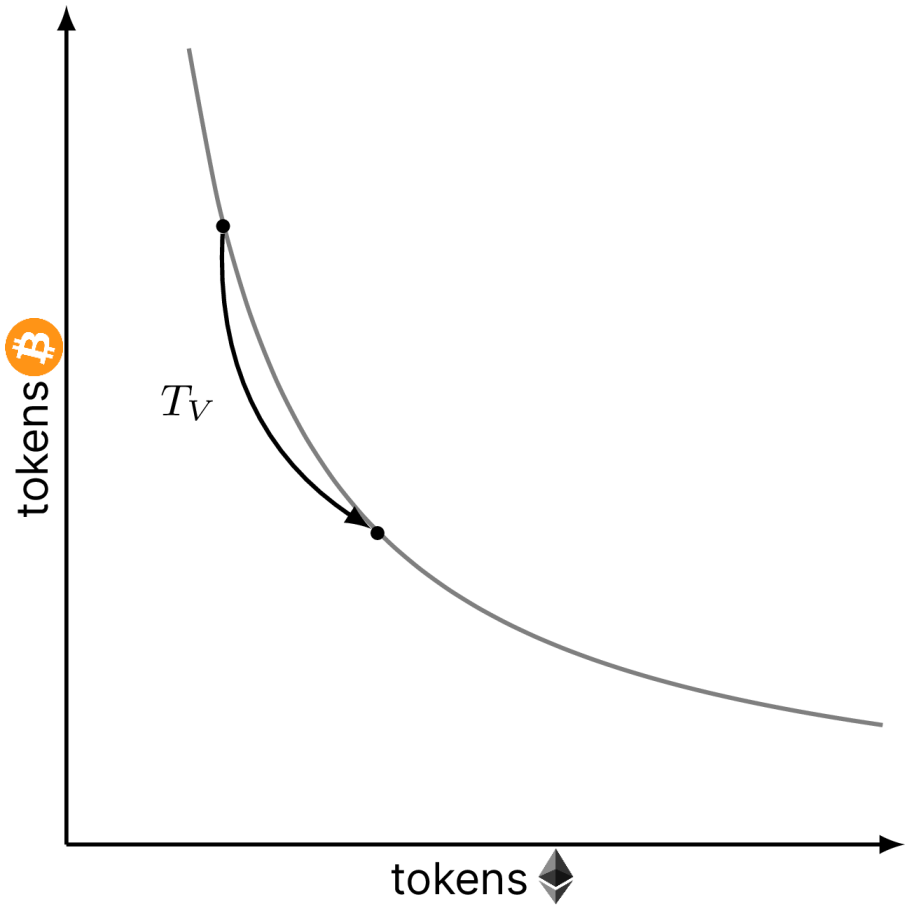
Sandwich Attack

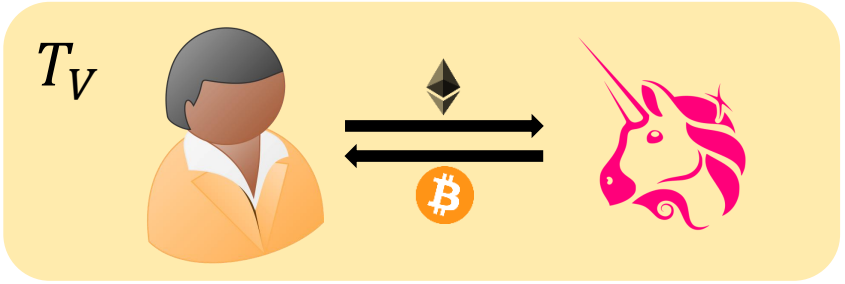


Sandwich Attack

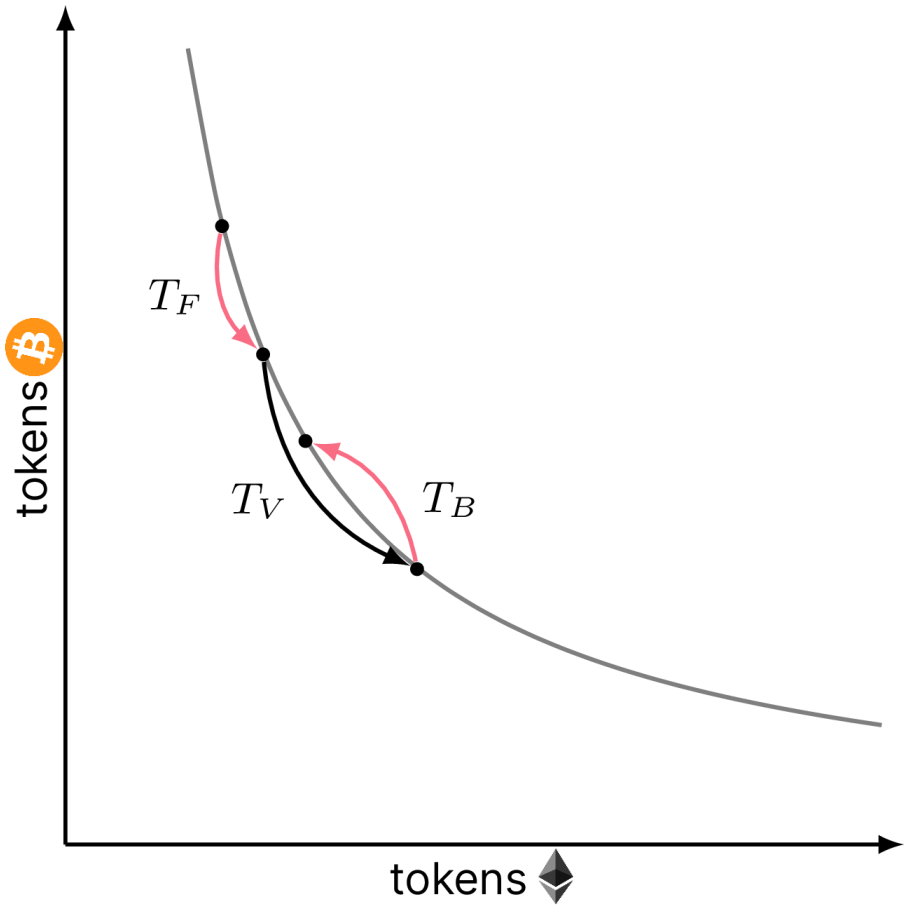


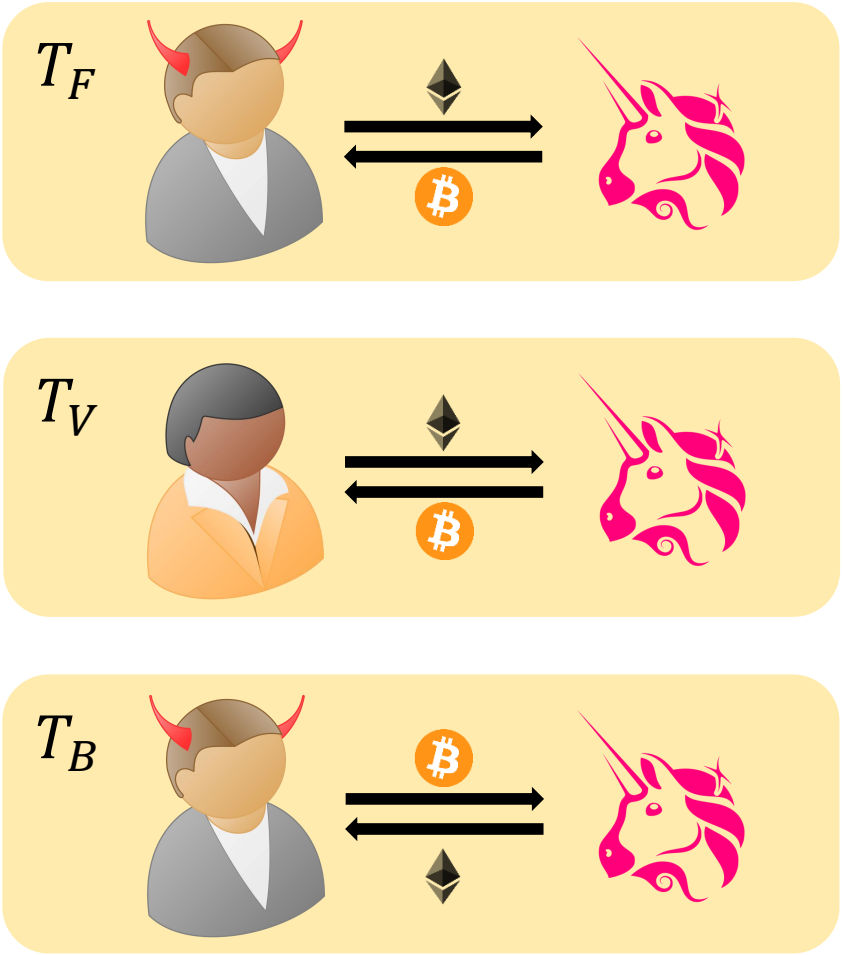
Sandwich Attack





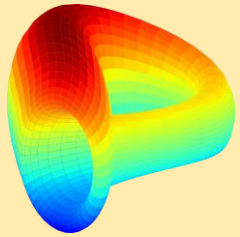
Sandwich Attack





Decentralized Finance (DeFi)

Decentralized Exchanges



δY/δX

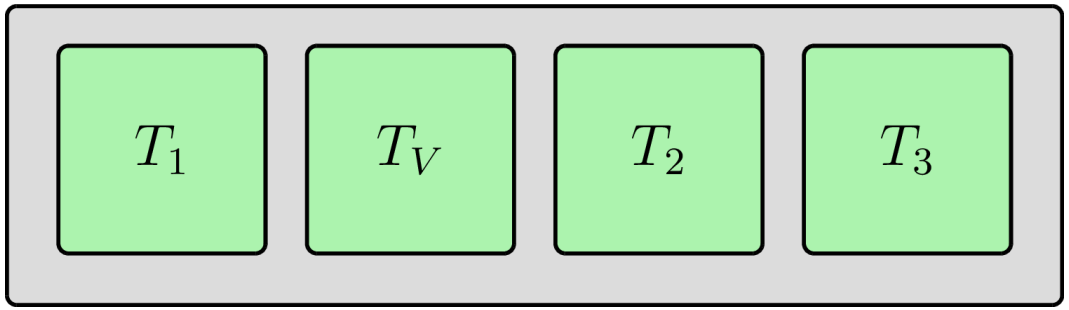
Lending Protocols

MAKER

Blockchain Extractable Value (BEV)

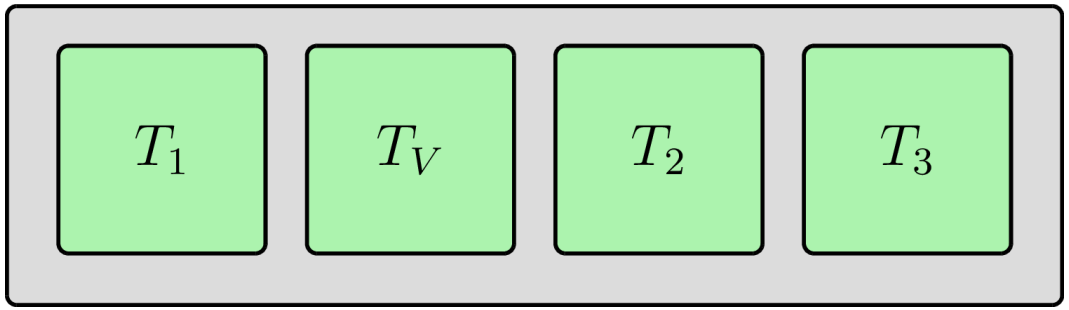
BEV is a measure of the profit that can be made through including, excluding, or re-ordering transactions within block.

Transaction Reordering

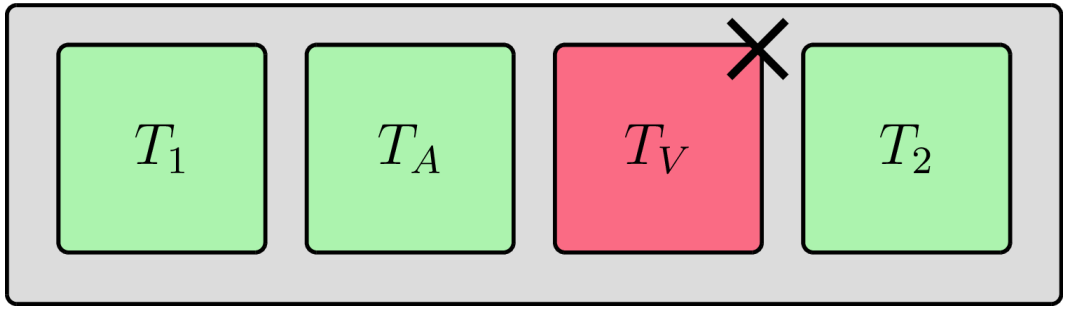


no attack

Transaction Reordering

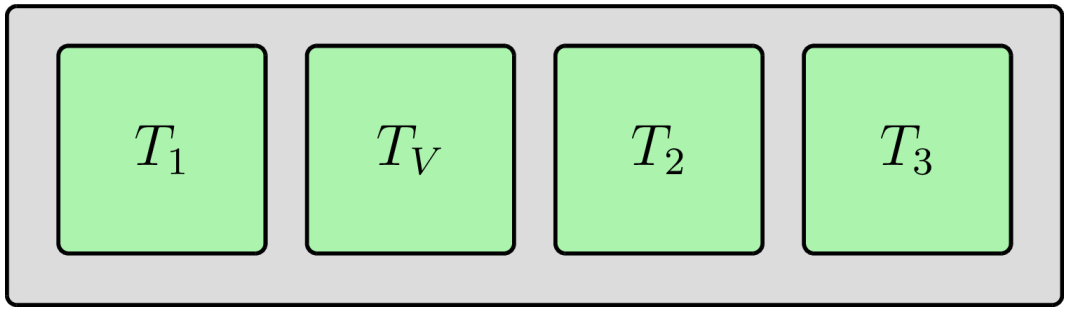


no attack

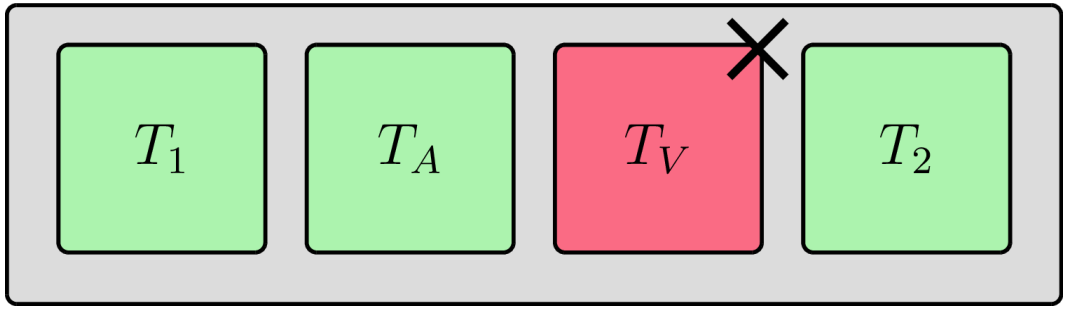


fatal front-running

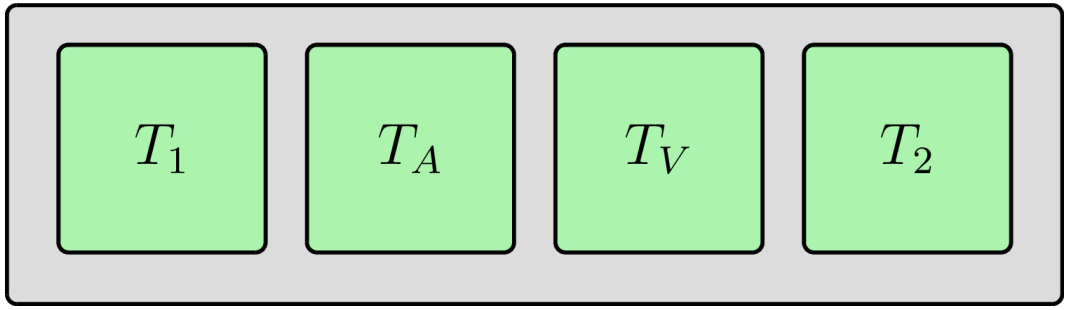
Transaction Reordering



no attack

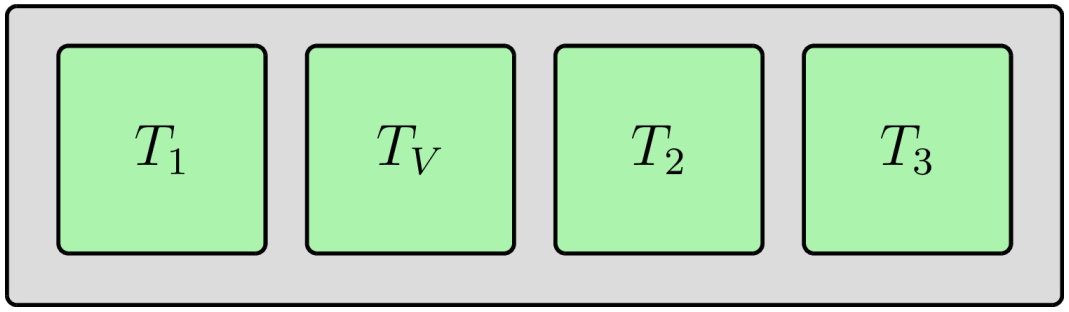


fatal front-running

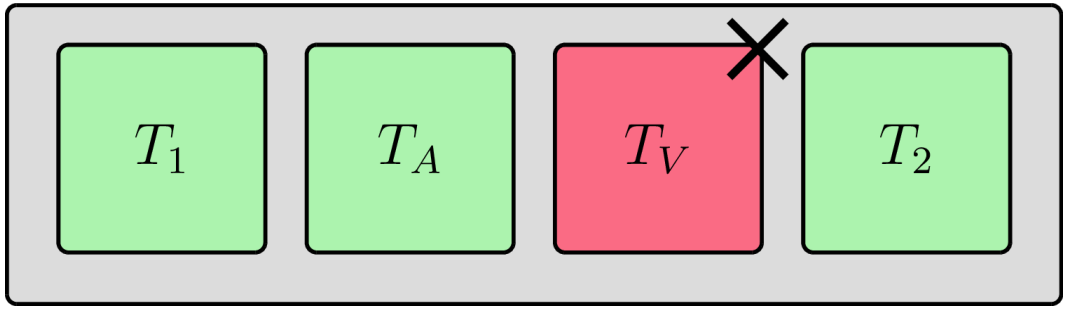


front-running

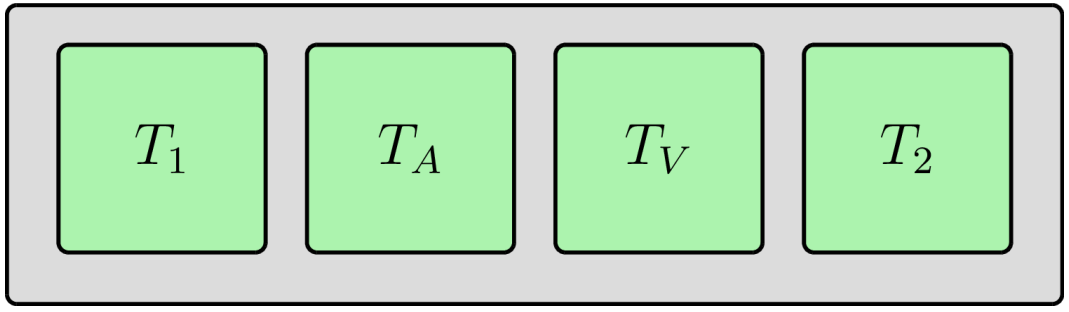
Transaction Reordering



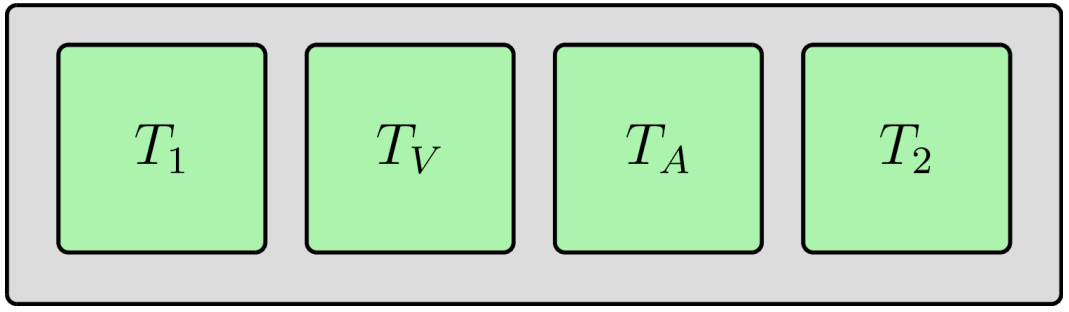
no attack



fatal front-running

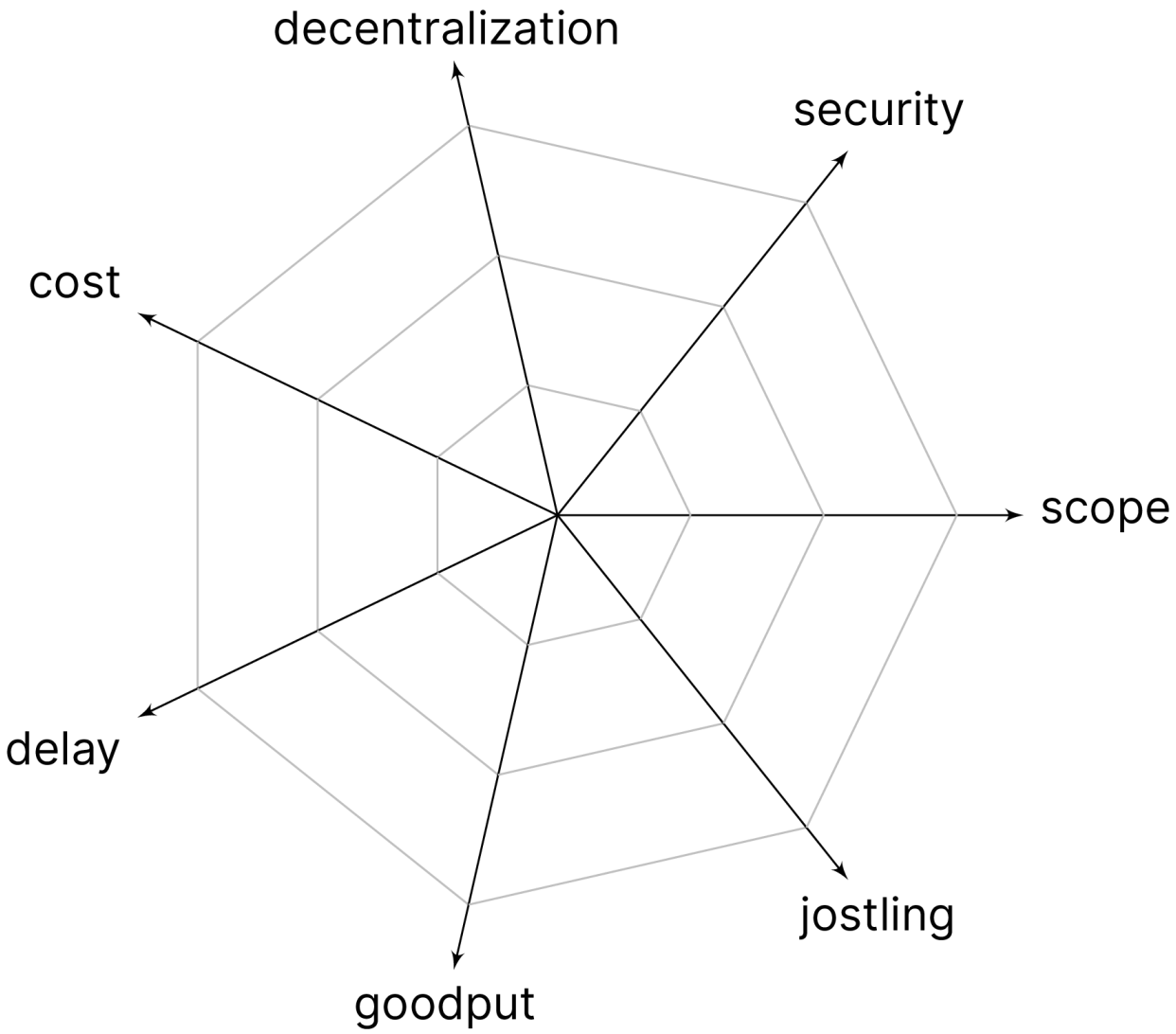


front-running

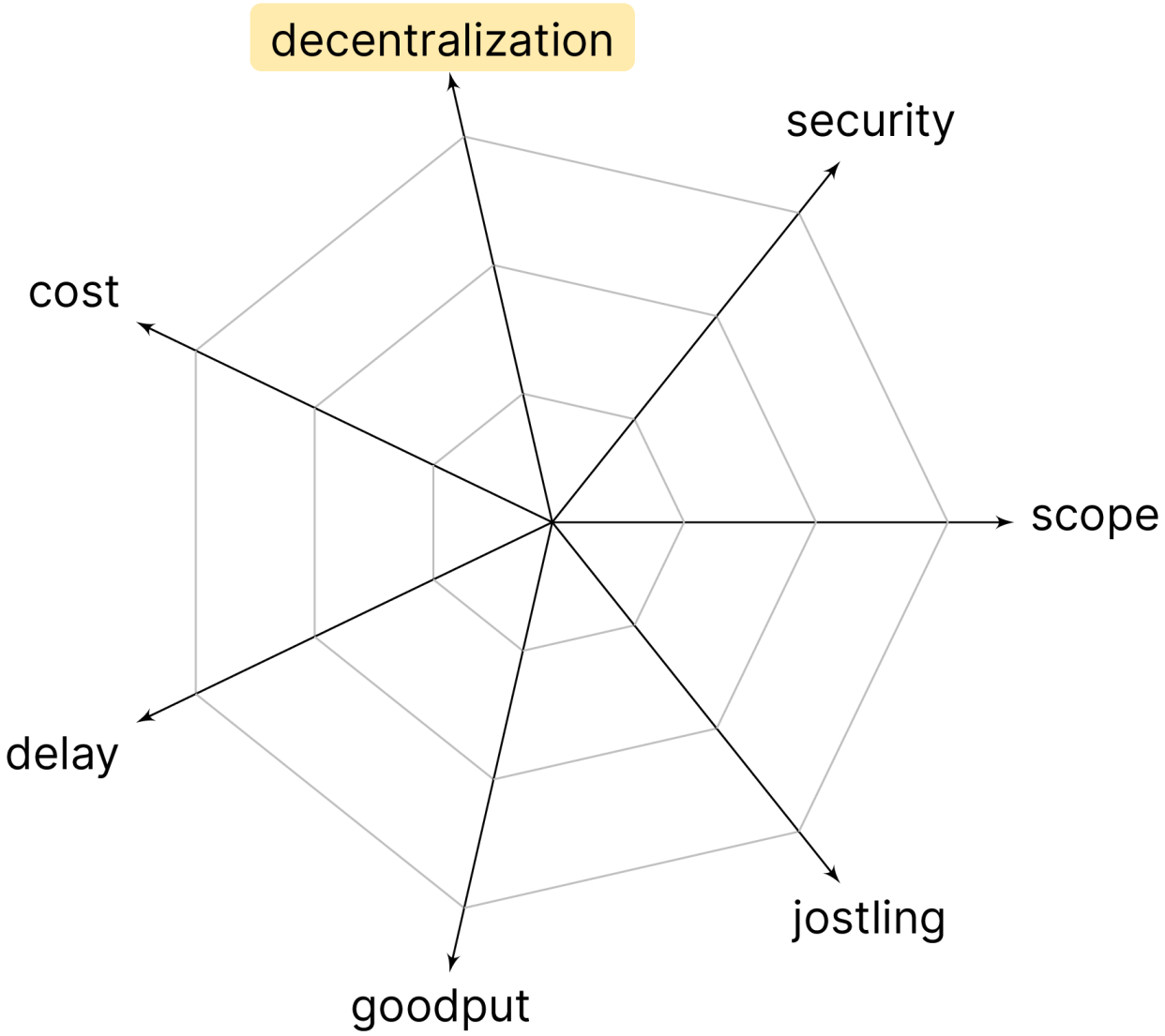


back-running

Measures

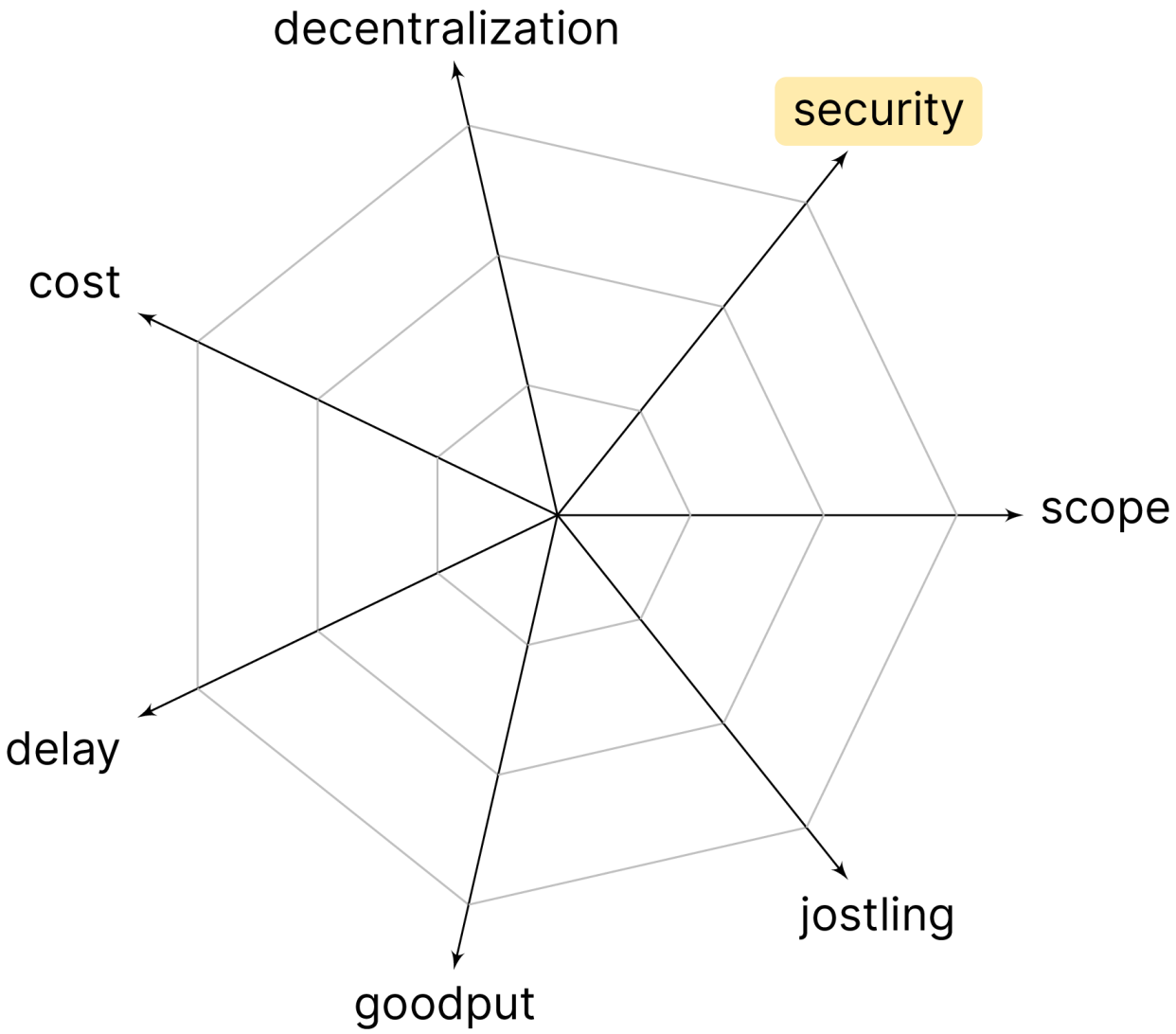

decentralization
security
cost
scope
delay
jostling
goodput

Measures



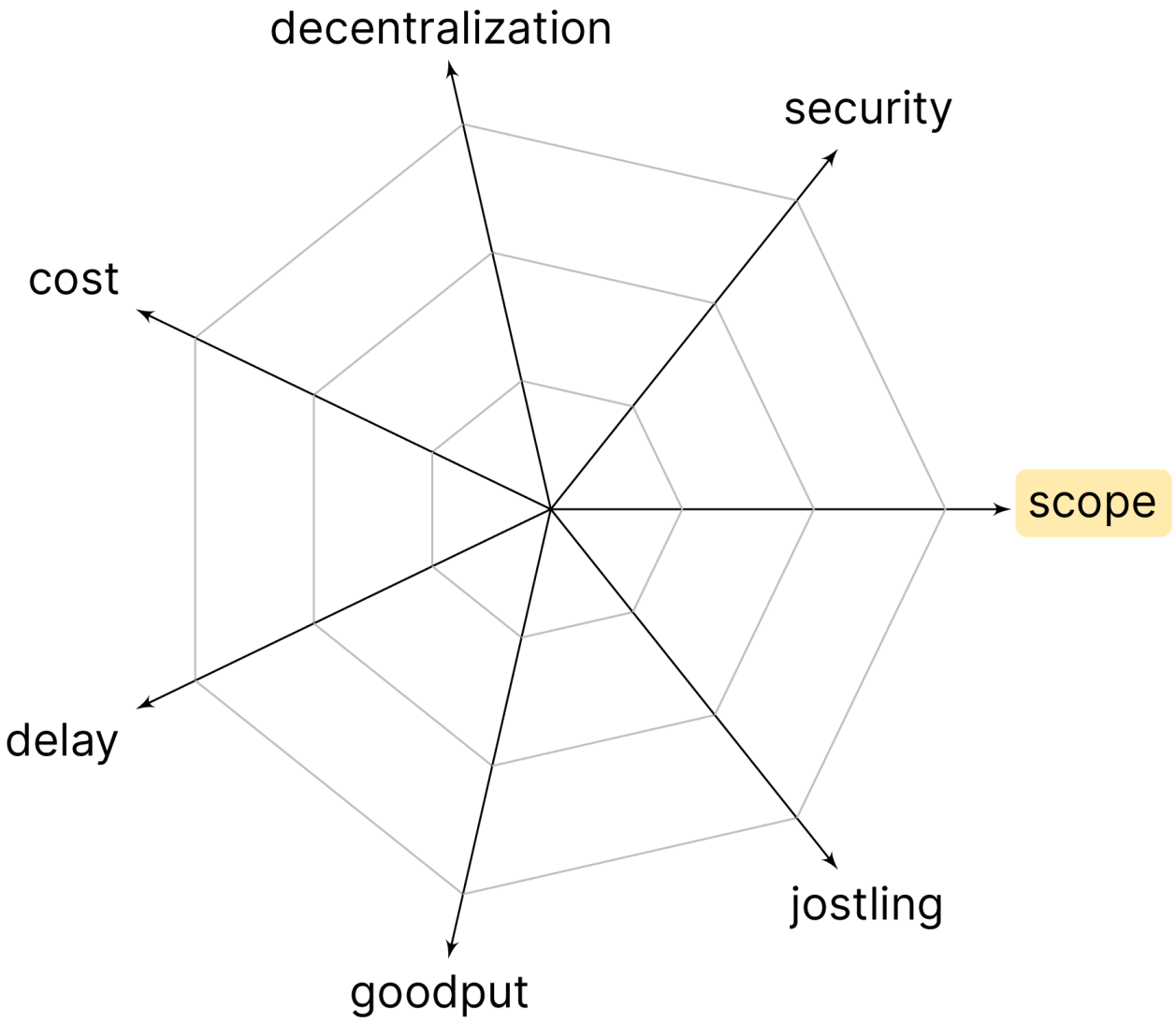
Does the approach decreases the level of decentralization?

Measures



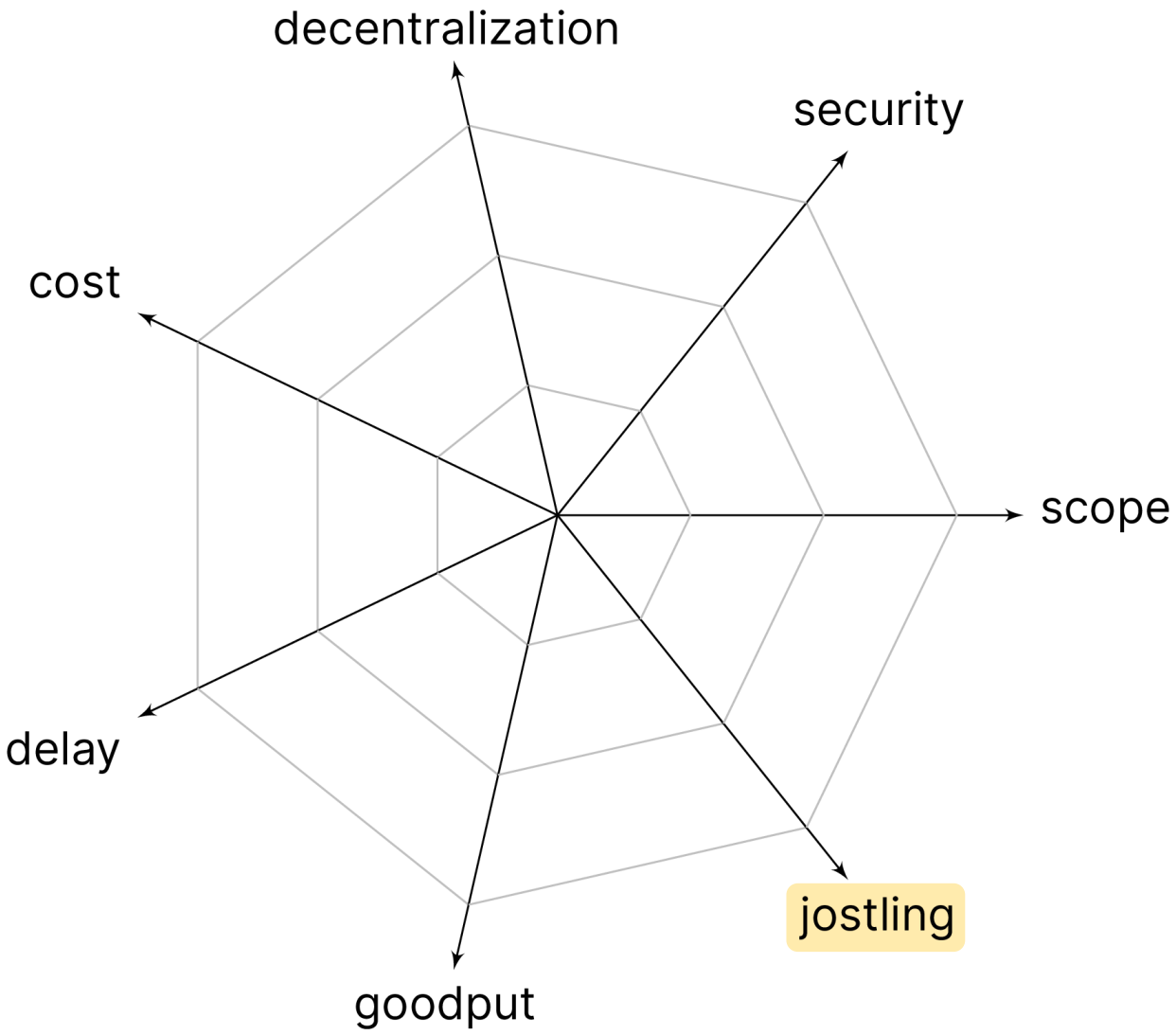
Is the approach susceptible to attacks?

Measures



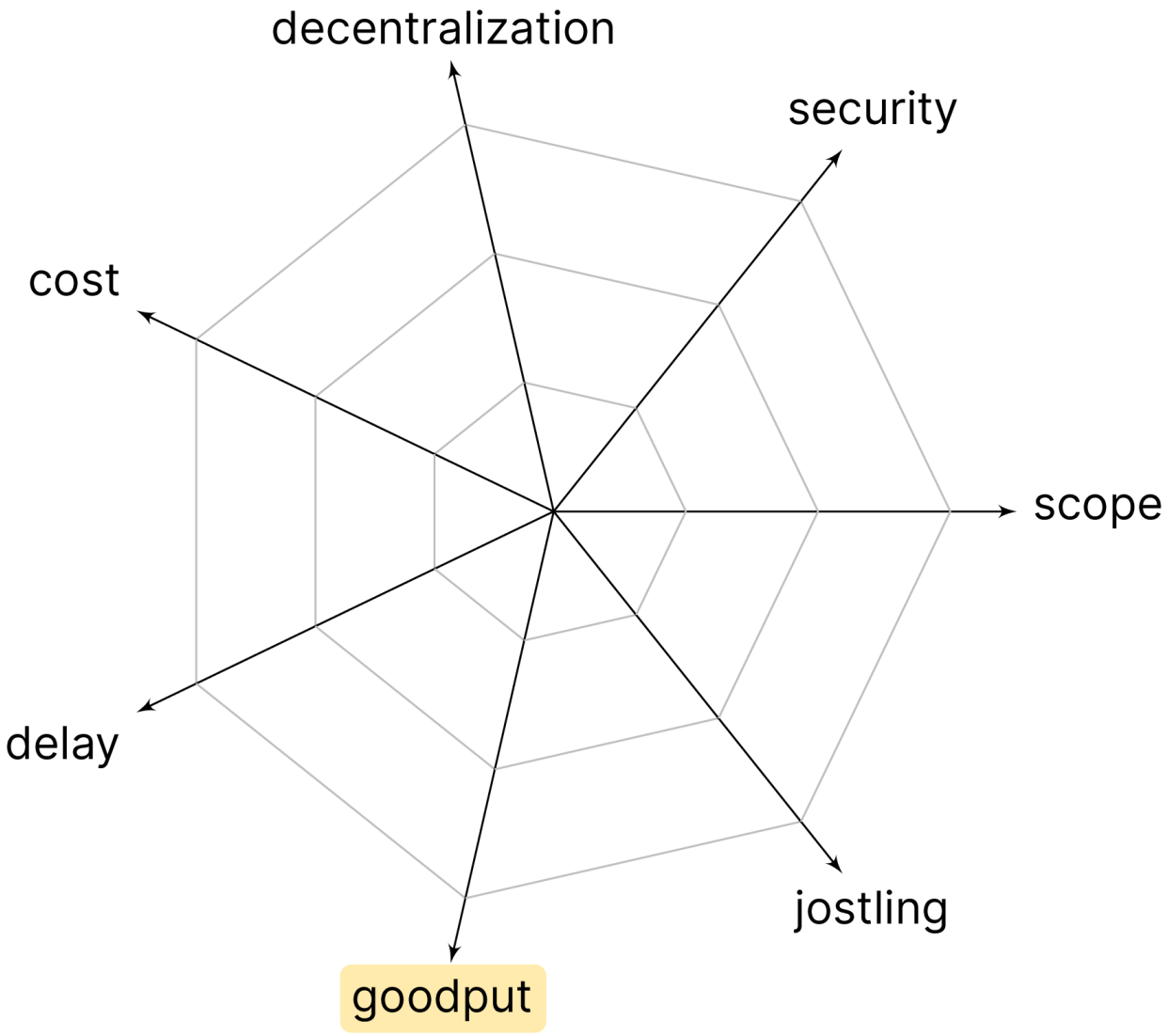
Is the approach wide-reaching?

Measures



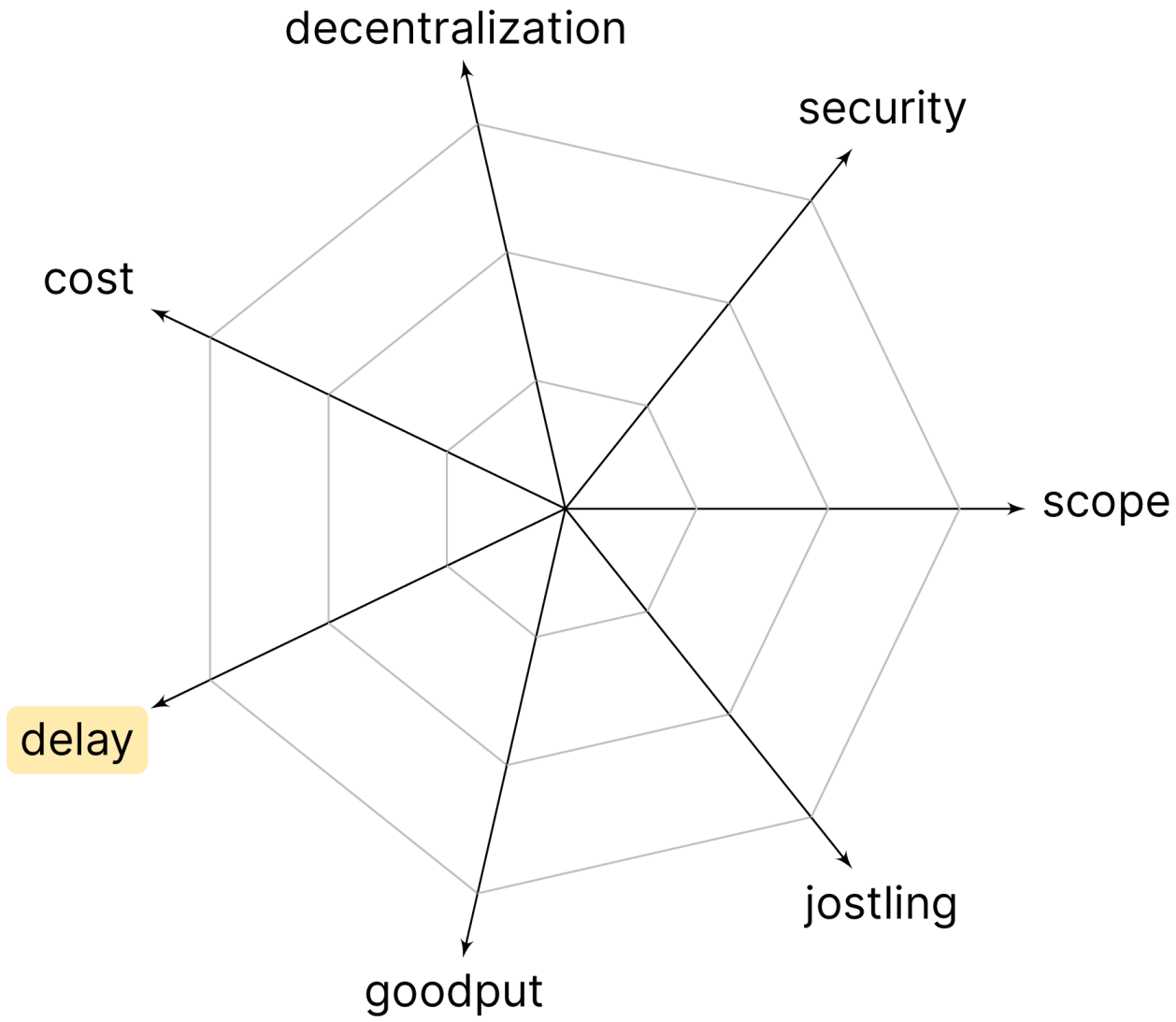
Does the approach create competition between traders for block inclusion?

Measures



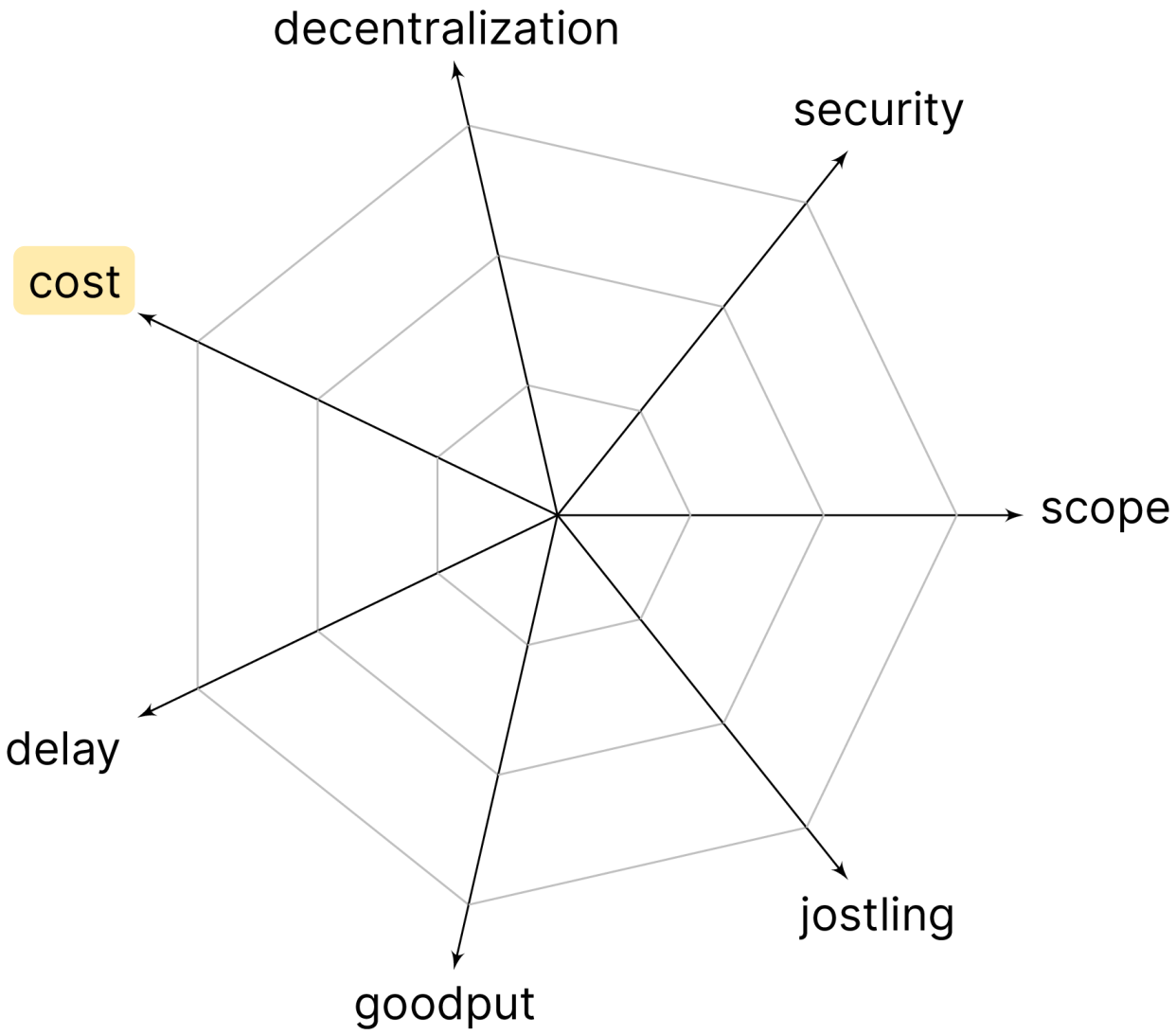
Does the approach impact the number of genuine transactions processed?

Measures



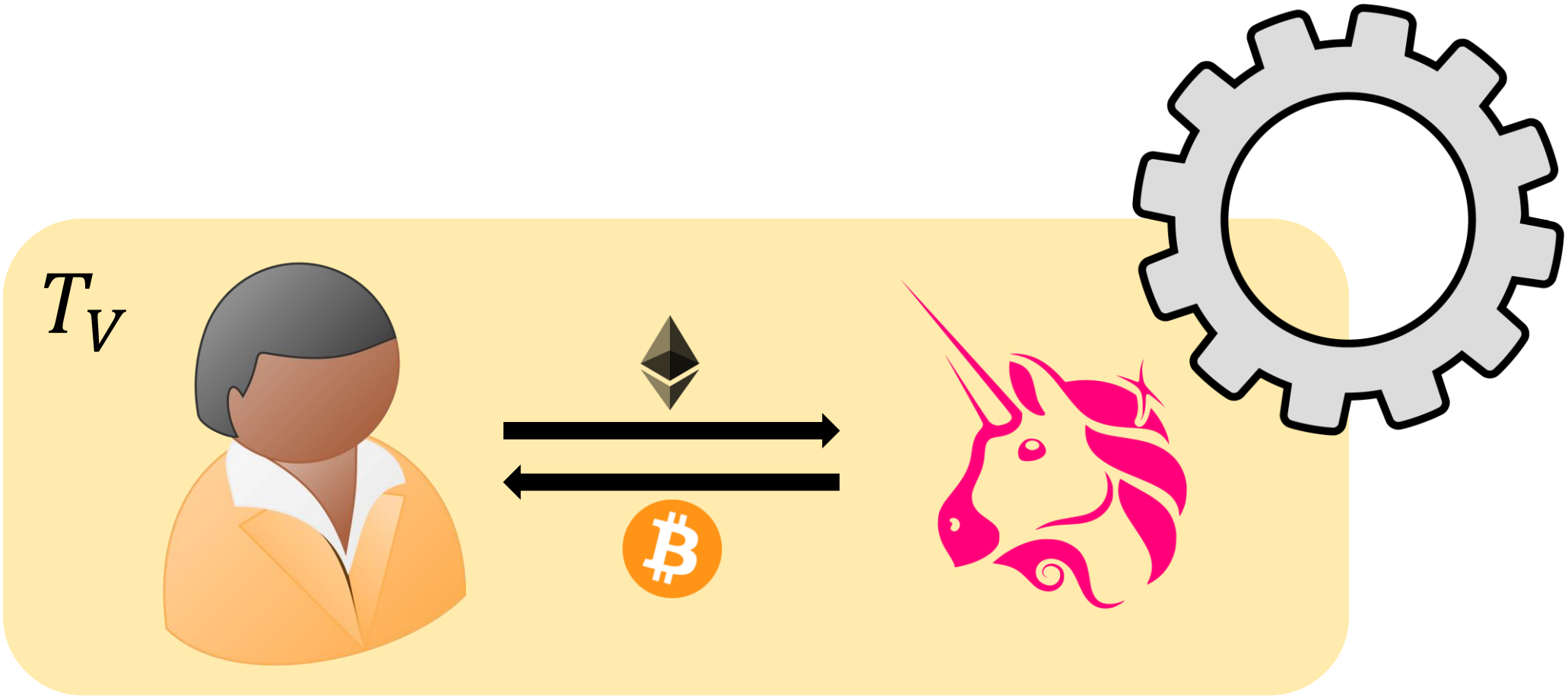
Does the approach delay transaction execution?

Measures

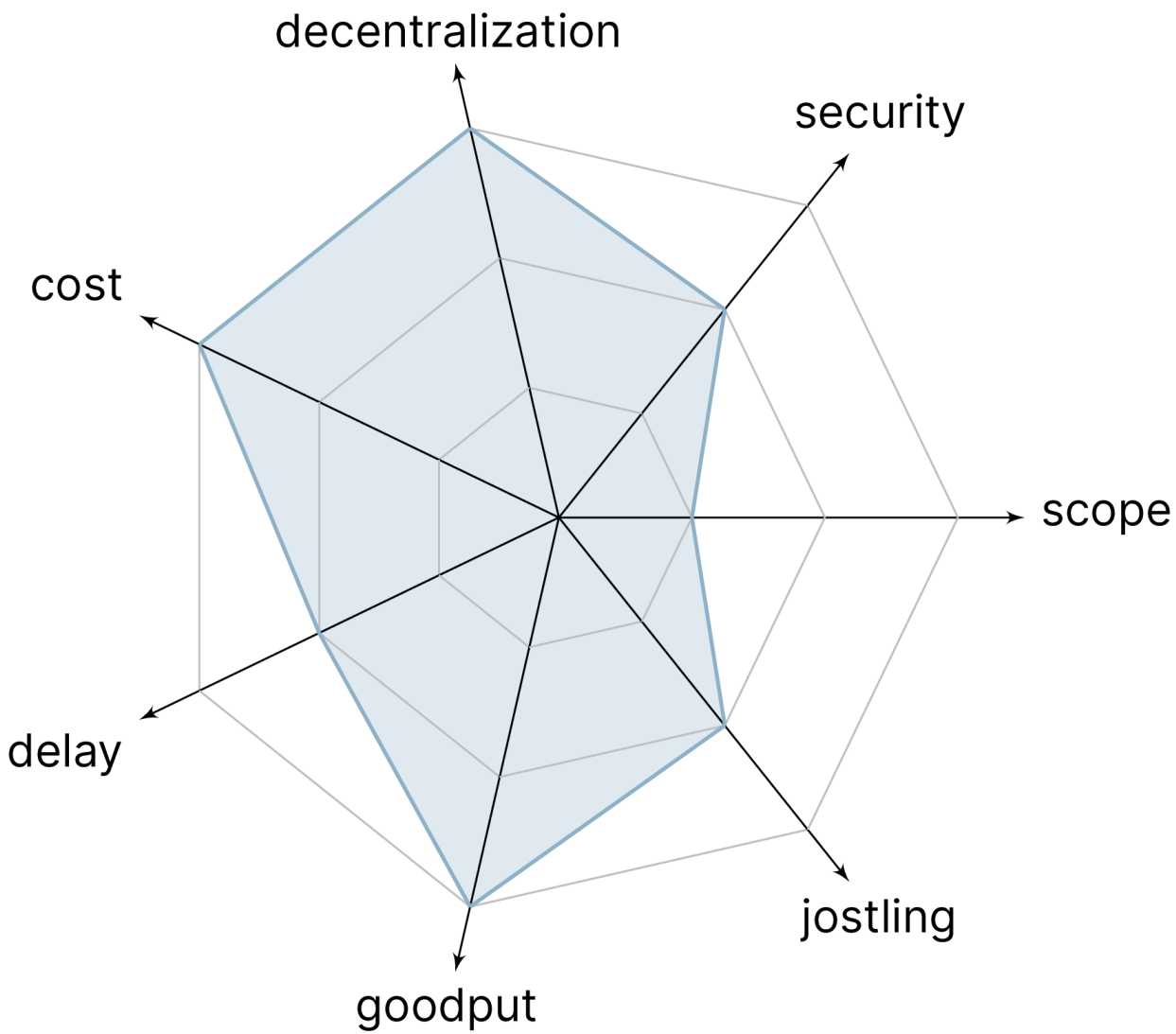


Does the approach create additional costs for transaction execution?

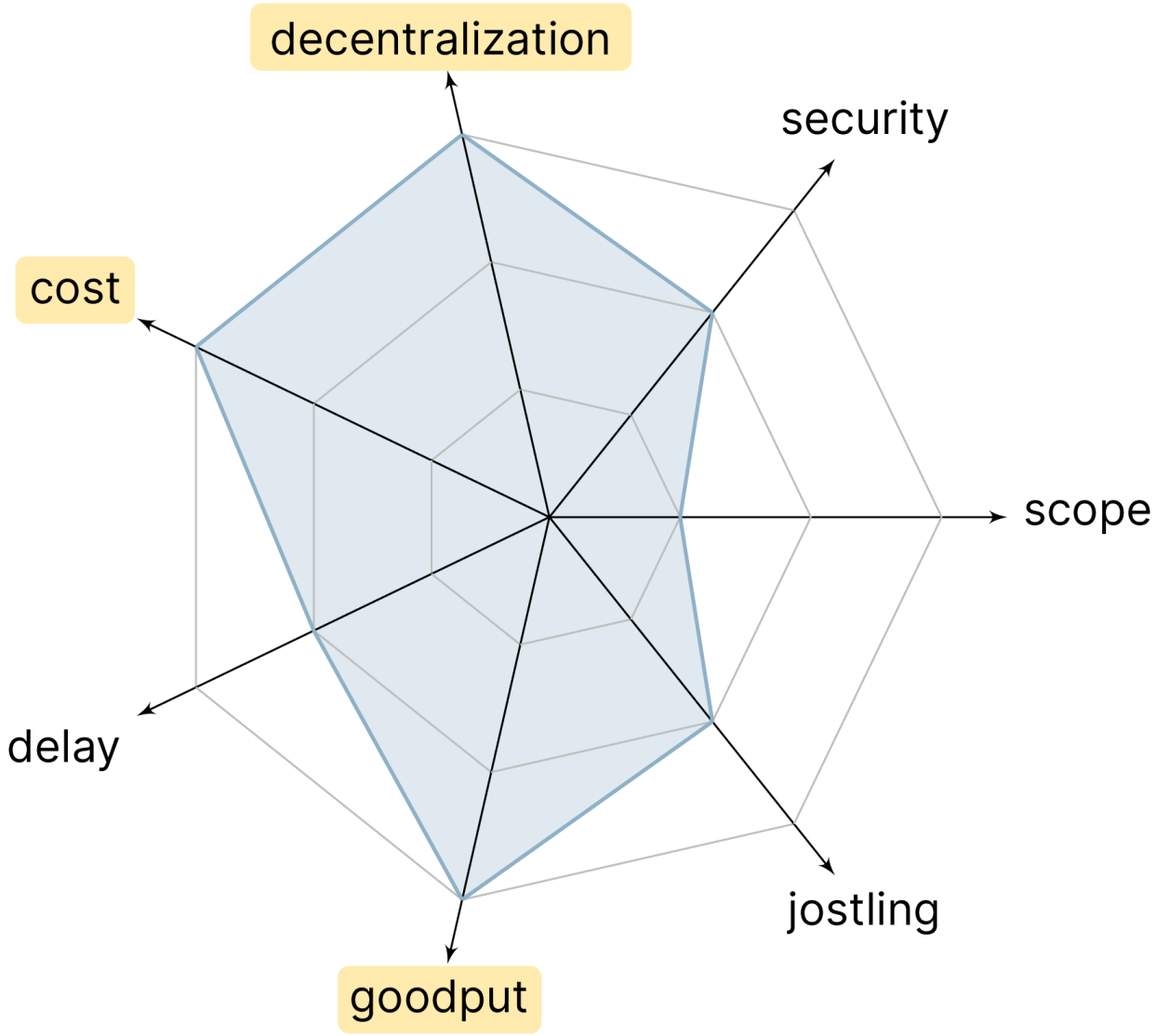
Optimized Trade Execution



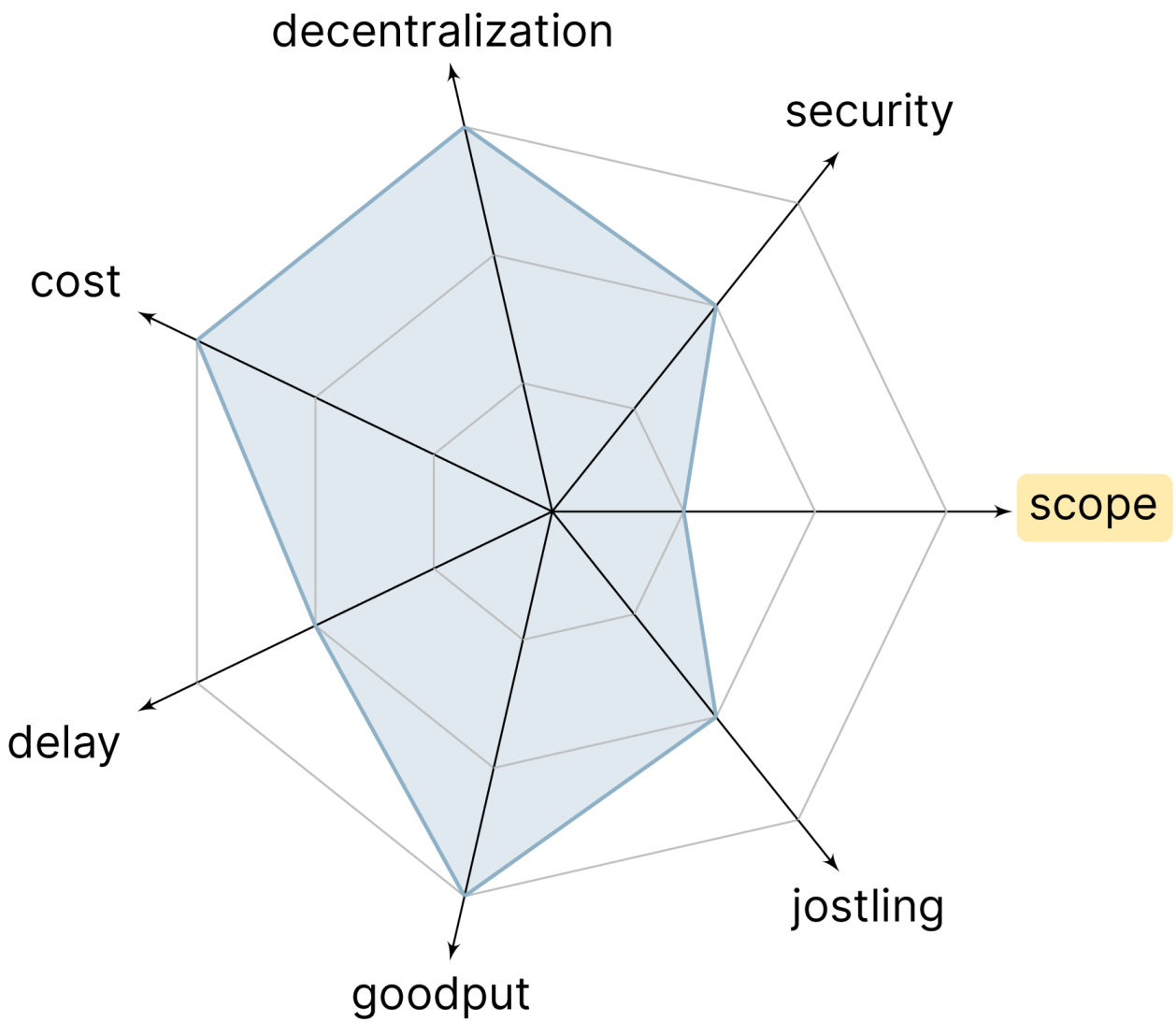
Optimized Trade Execution



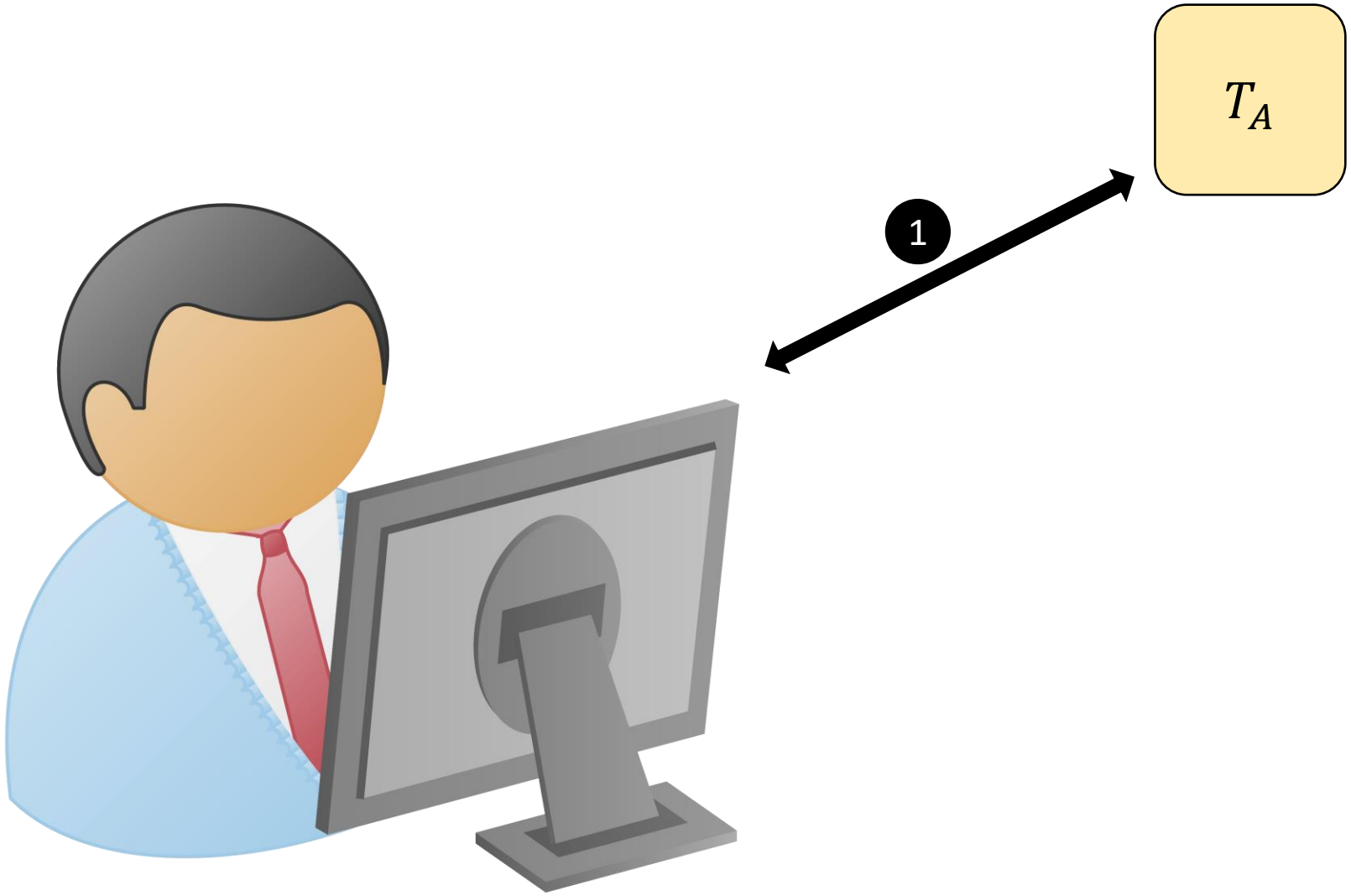
Optimized Trade Execution



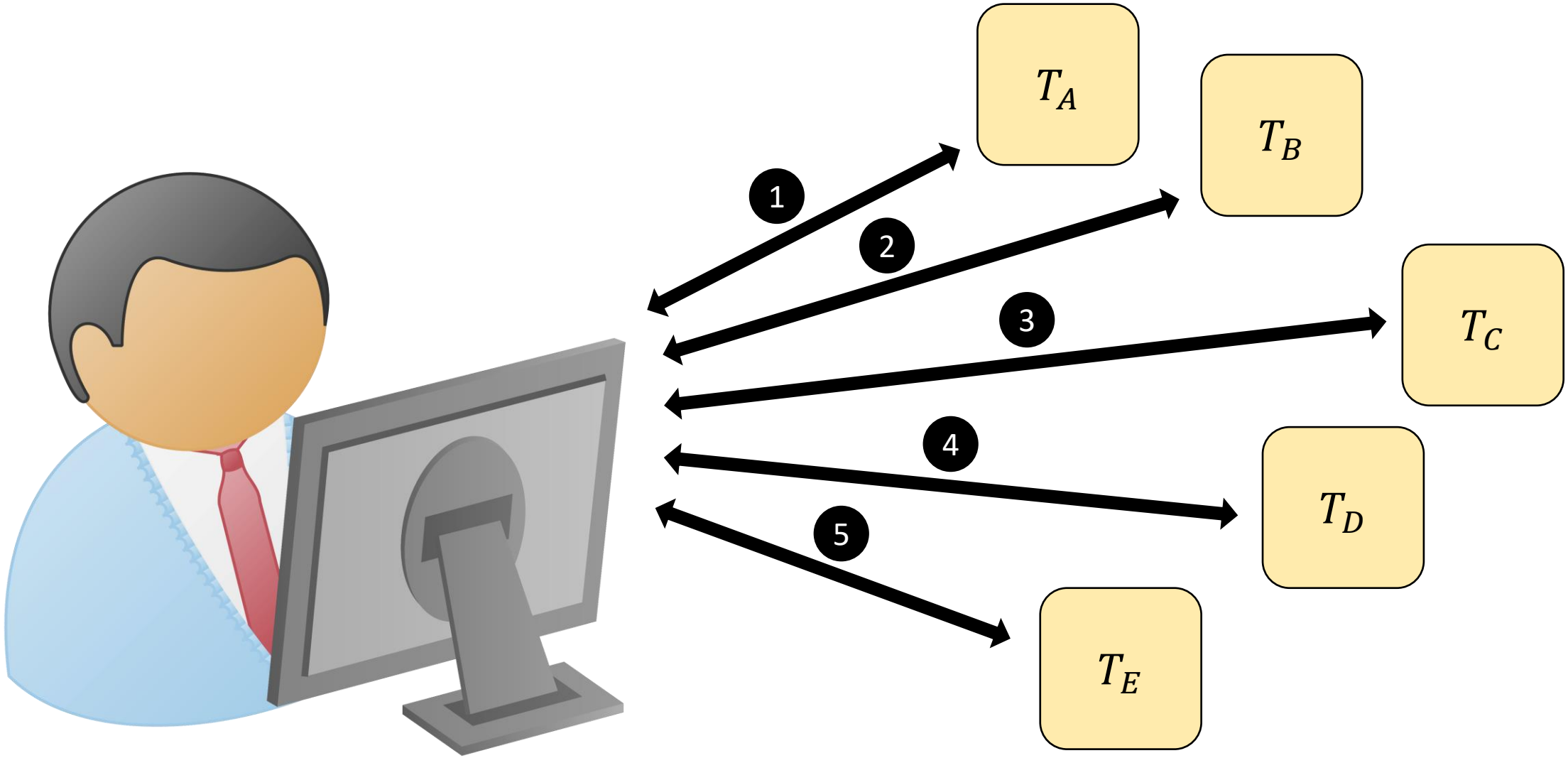
Optimized Trade Execution



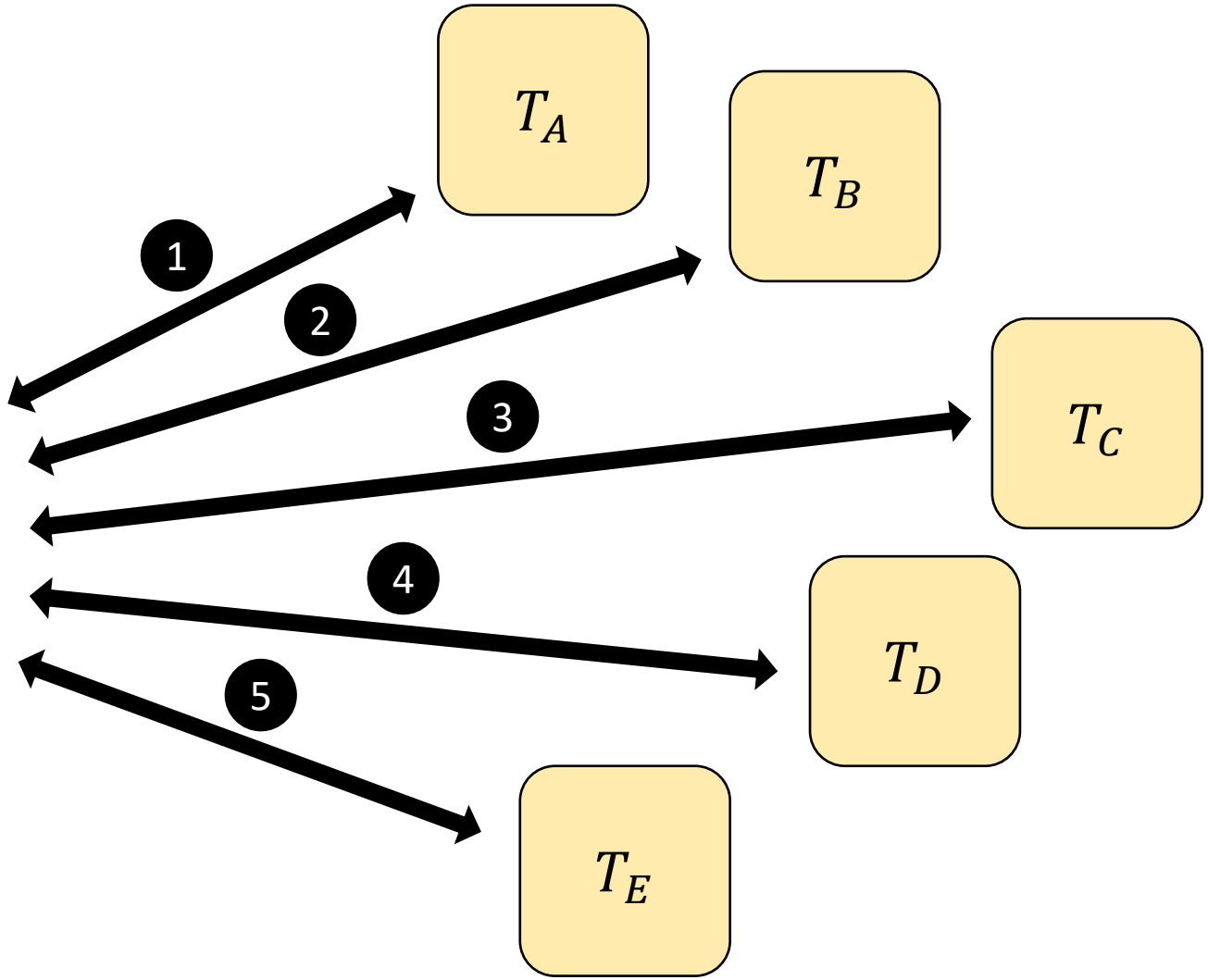
Professional Market Makers



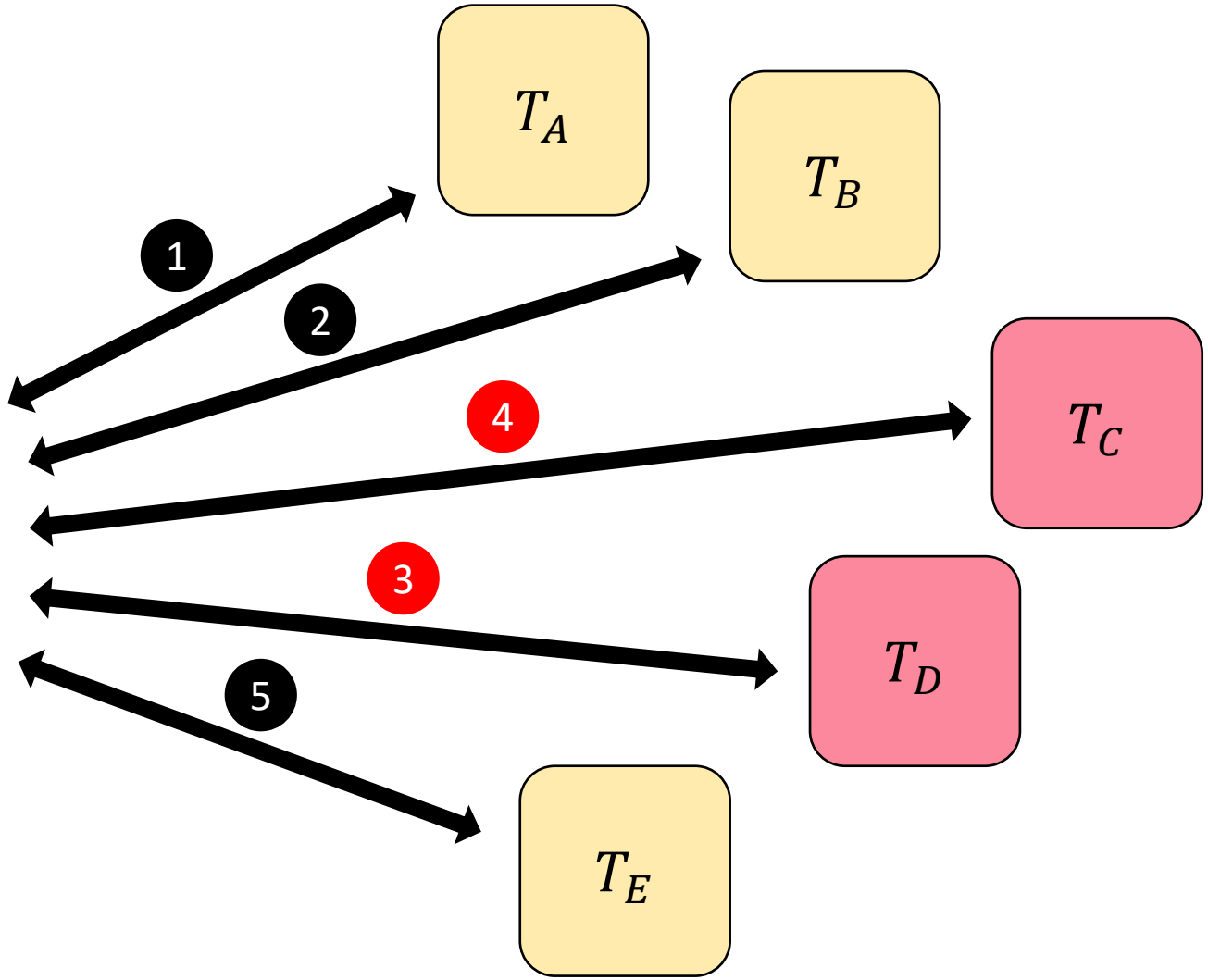
Professional Market Makers



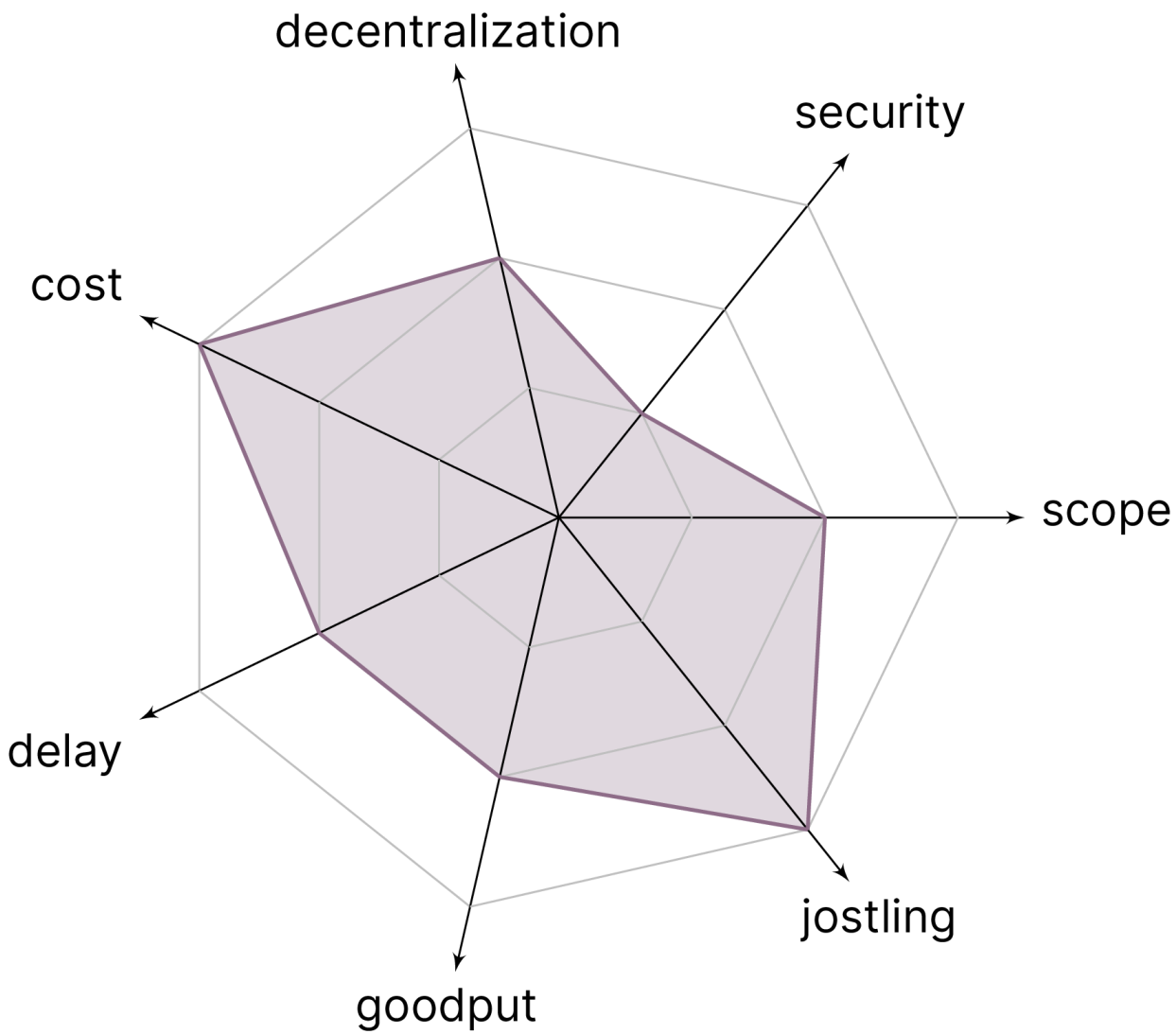
Professional Market Makers



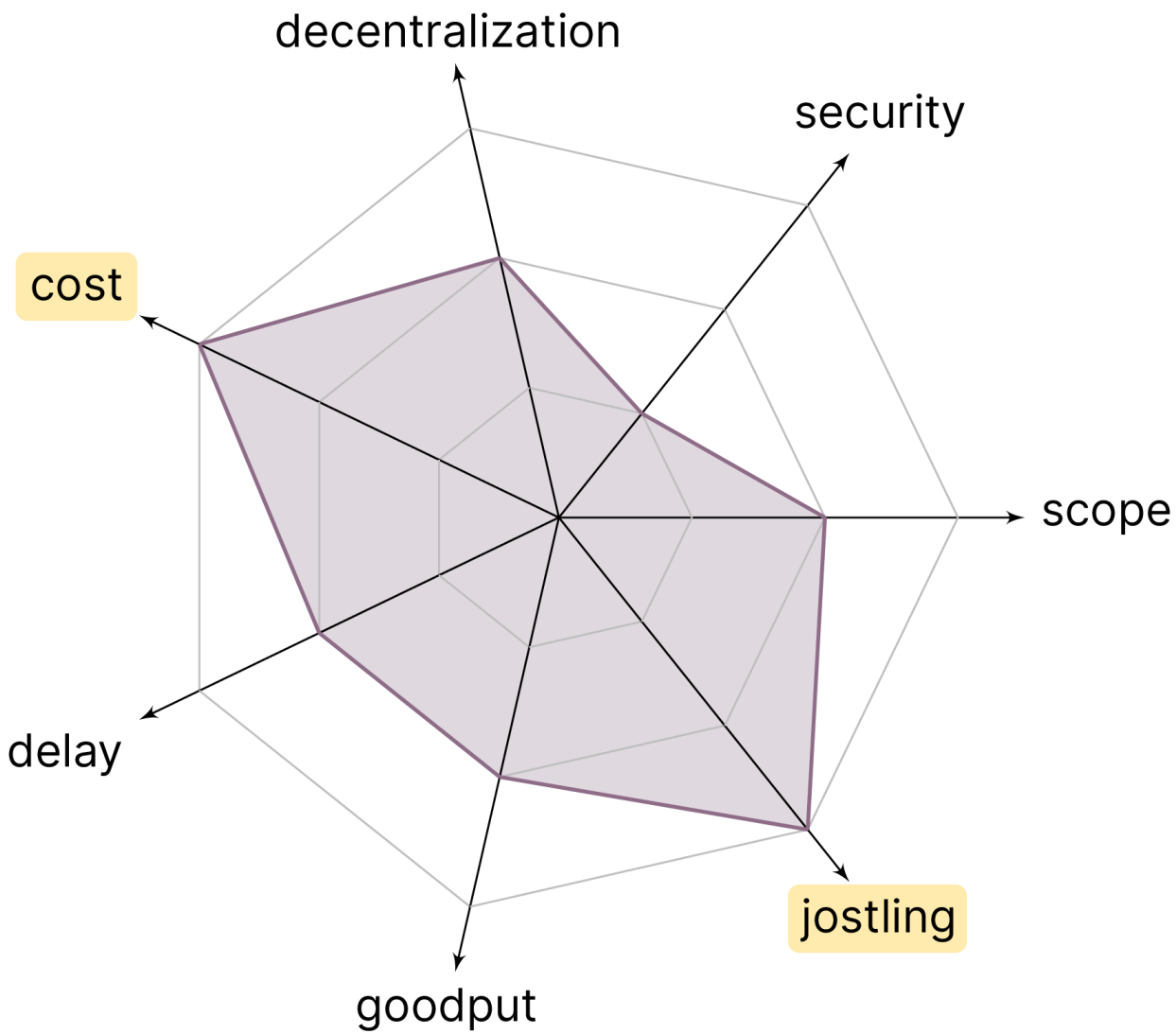
Professional Market Makers



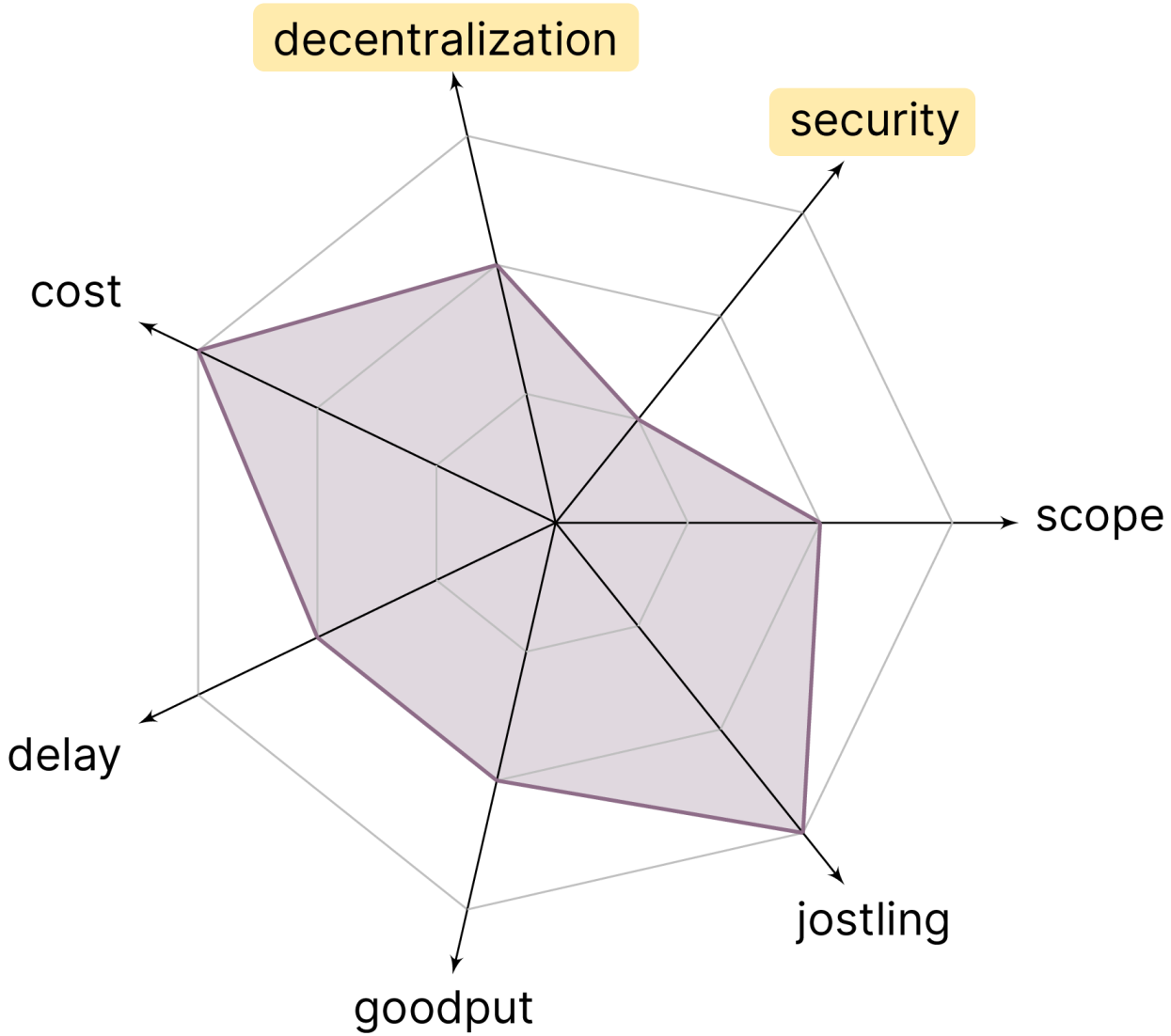
Professional Market Makers



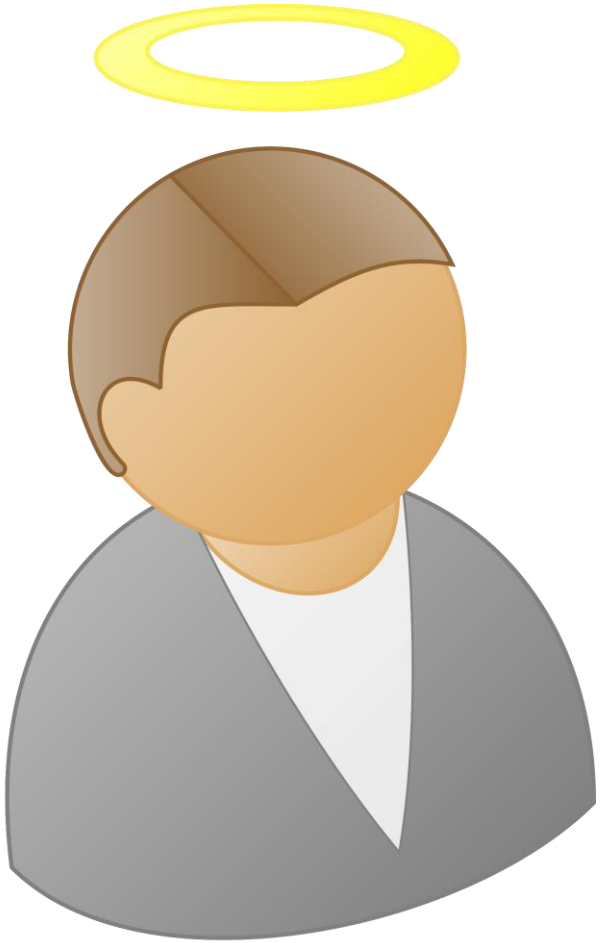
Professional Market Makers



Professional Market Makers



Trusted Third Party Ordering



T_E

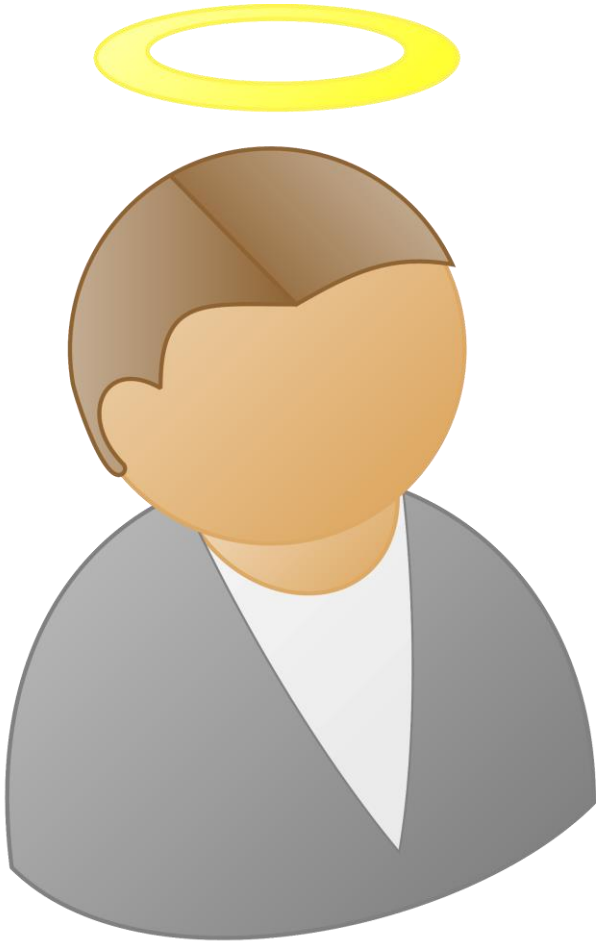
T_A

T_B

T_C

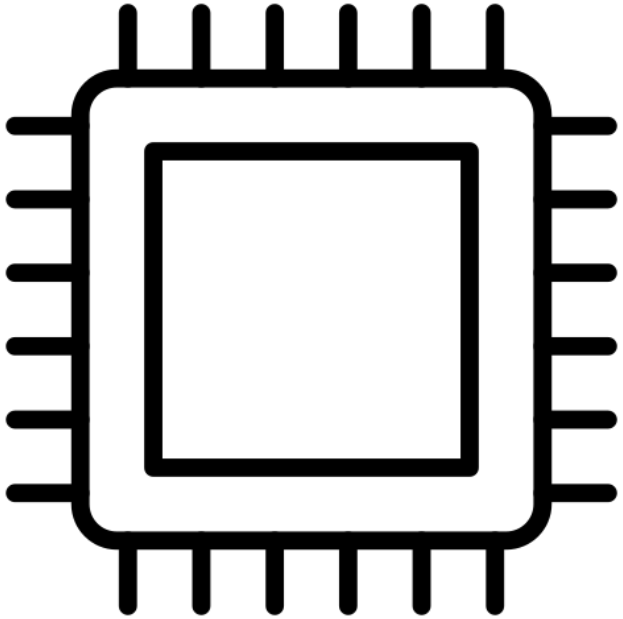
T_D

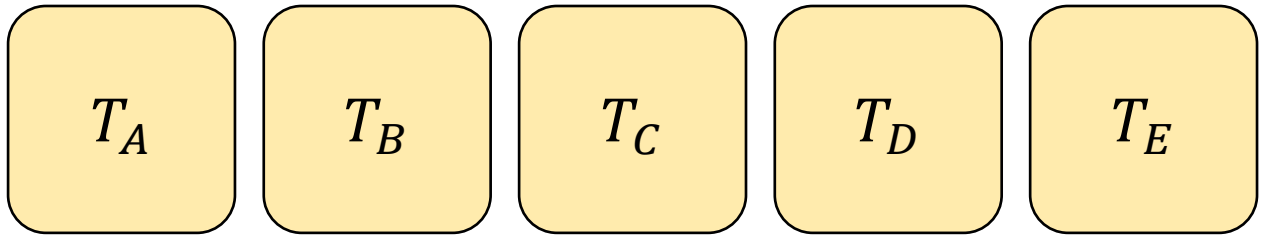
Trusted Third Party Ordering



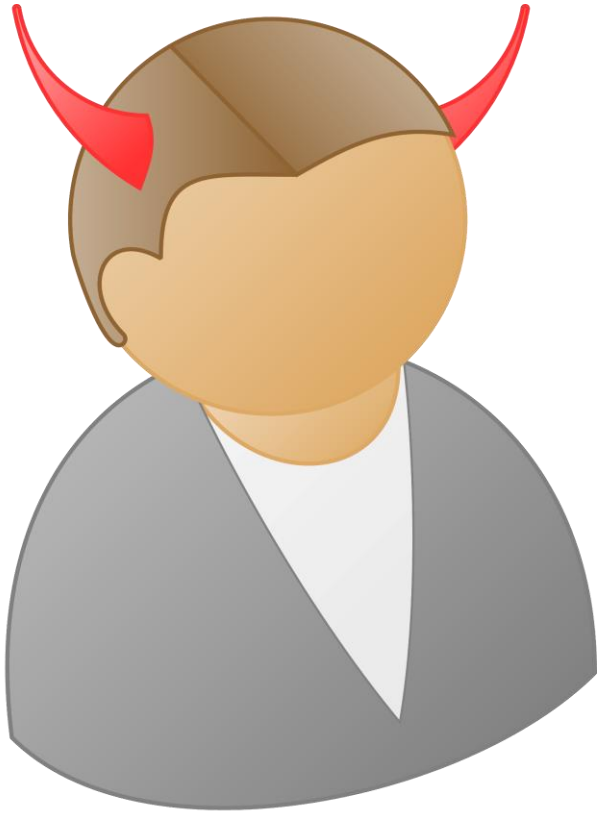
T_A T_B T_C T_D T_E

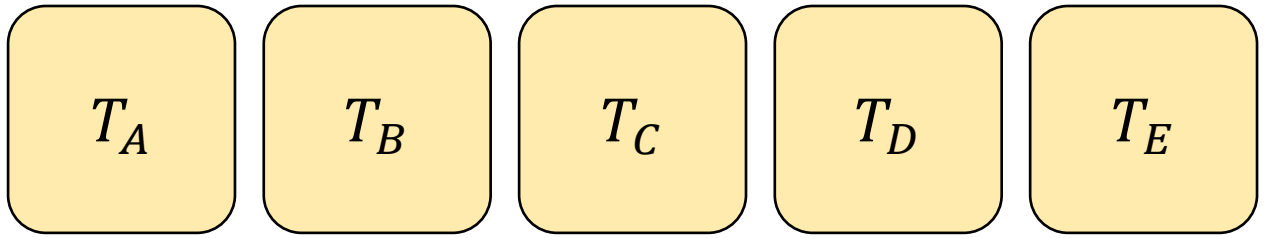
Trusted Third Party Ordering



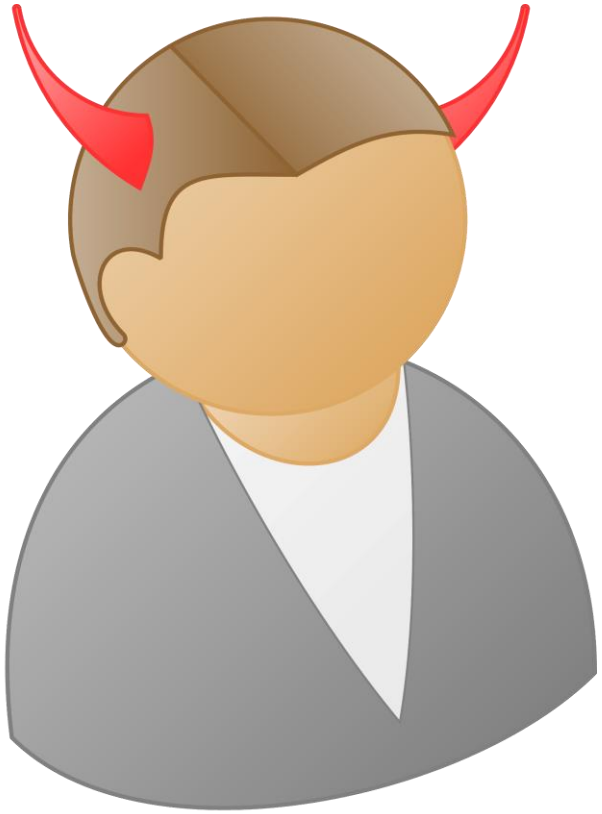


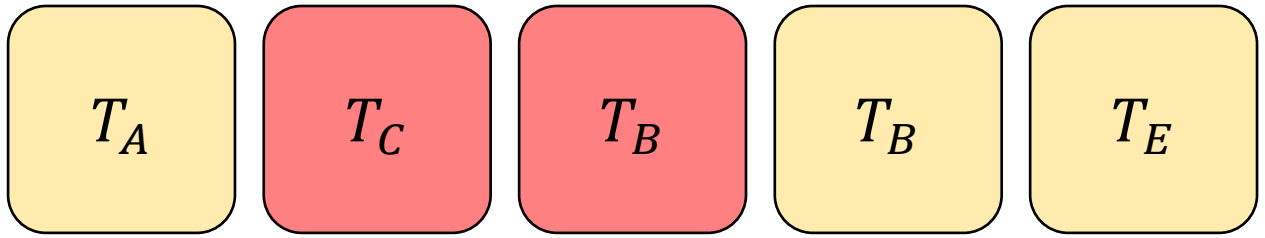
Trusted Third Party Ordering



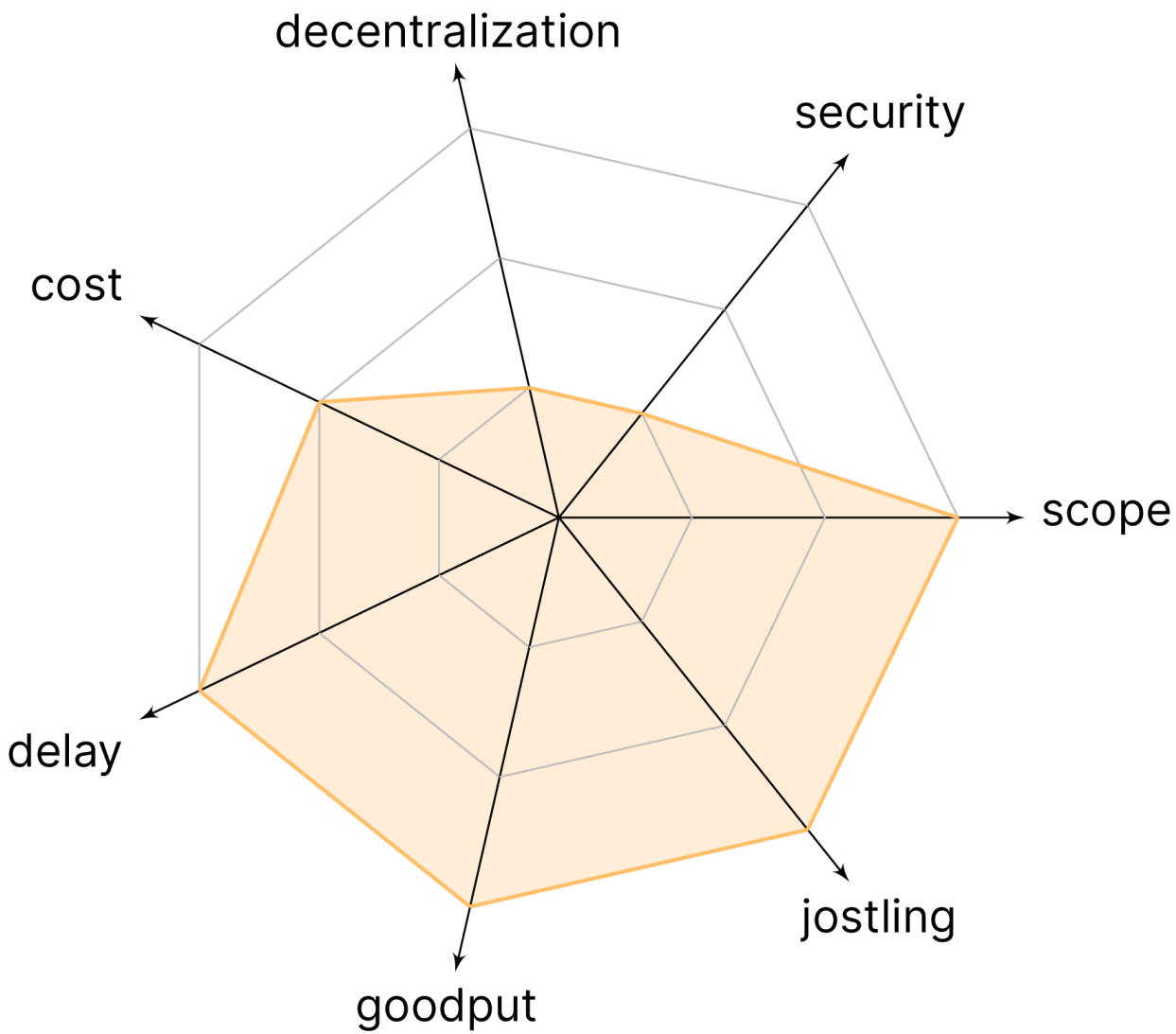


Trusted Third Party Ordering

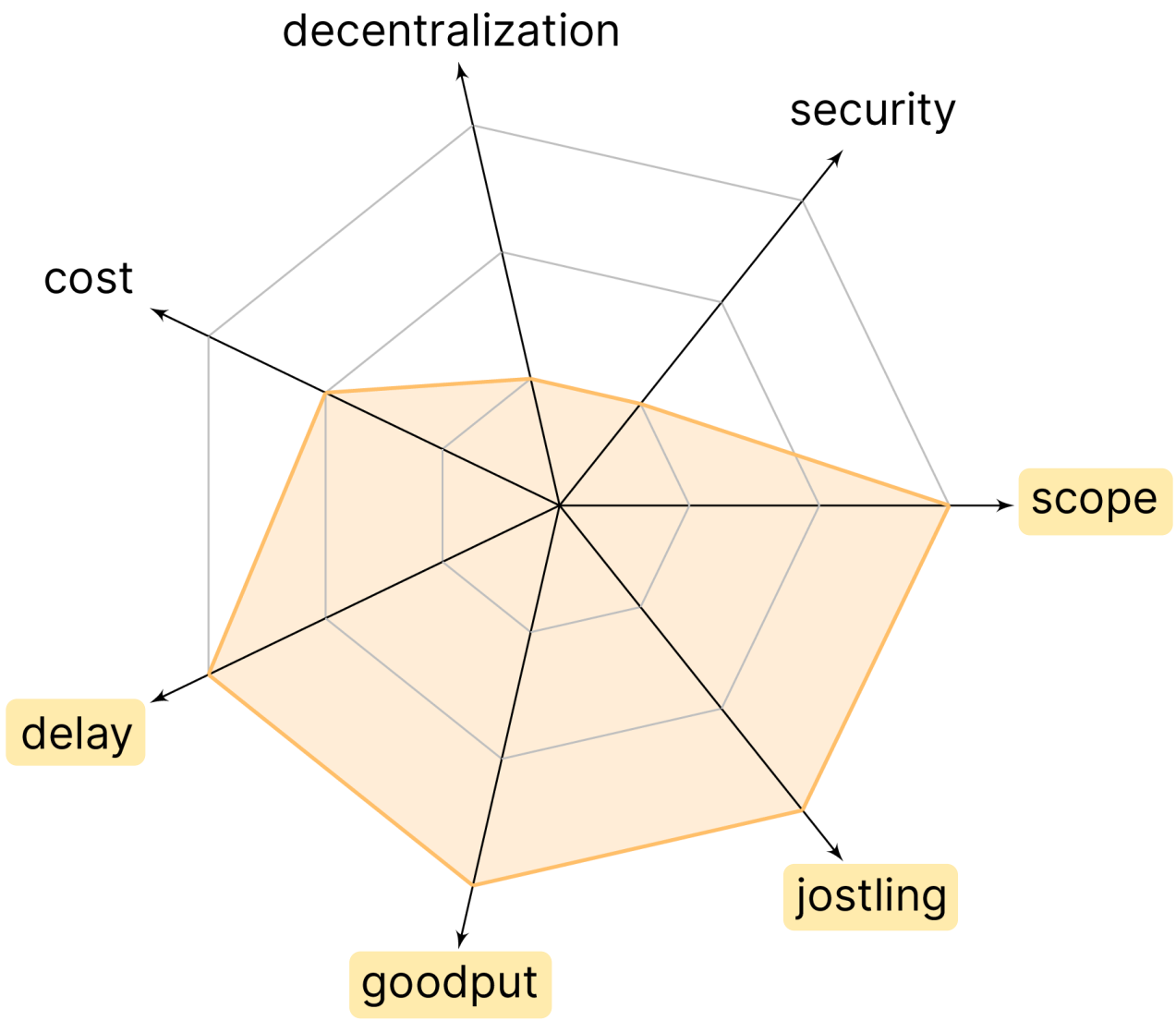




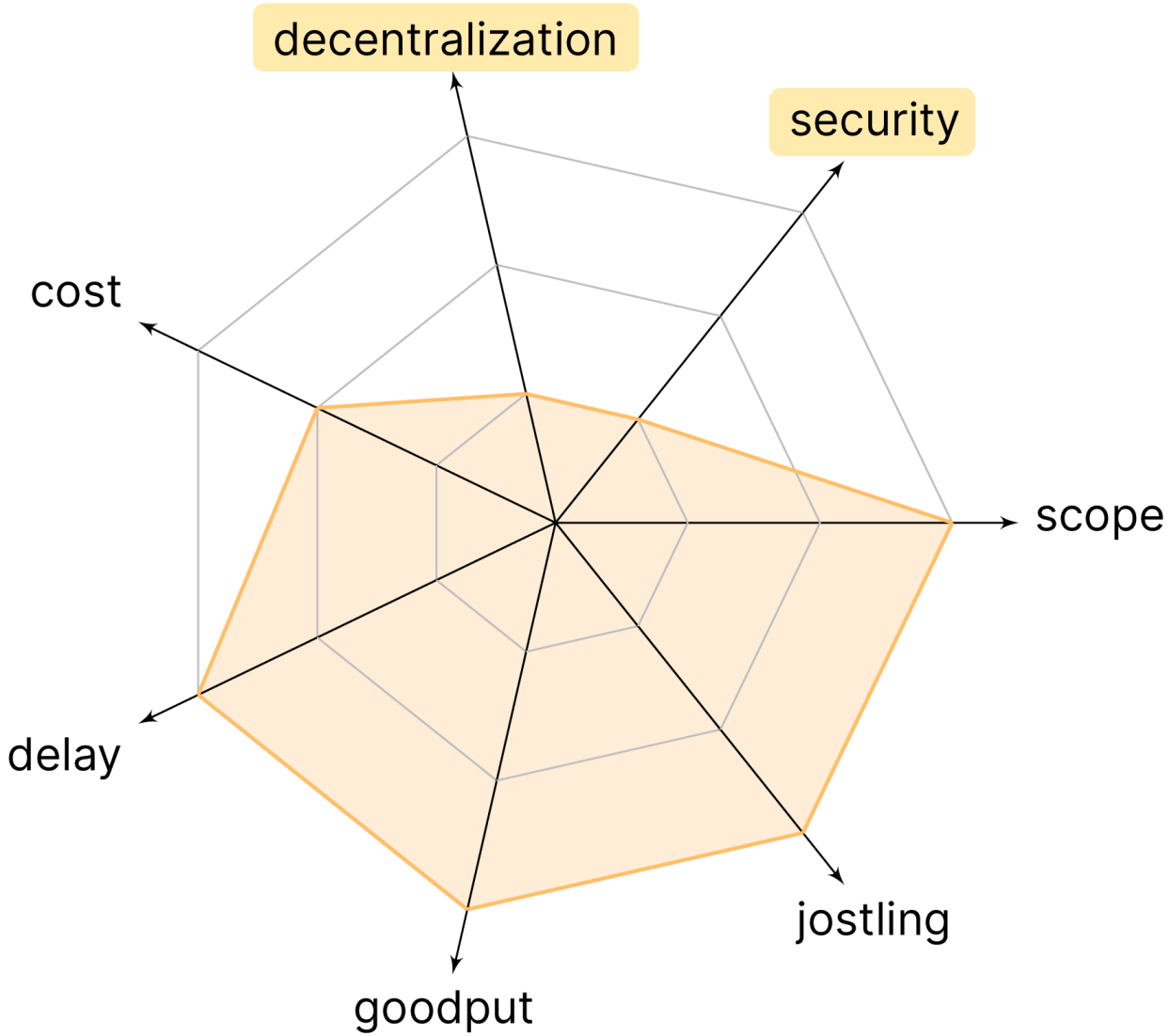
Trusted Third Party Ordering



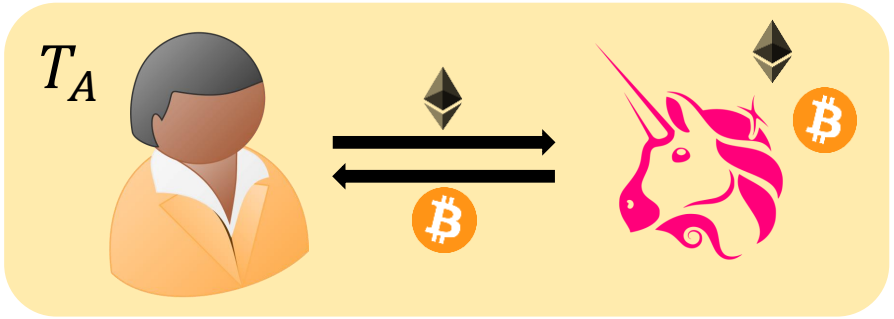
Trusted Third Party Ordering



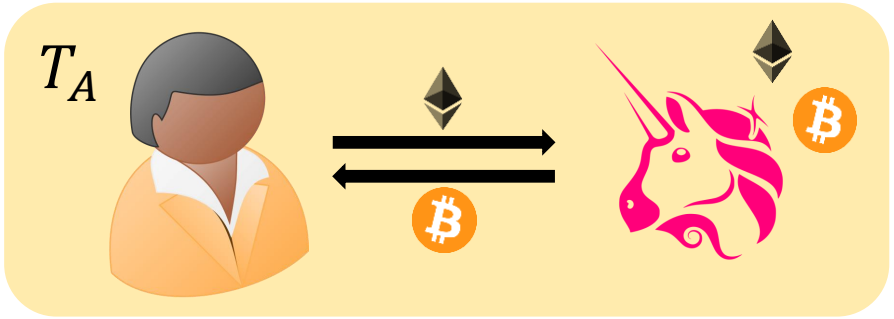
Trusted Third Party Ordering

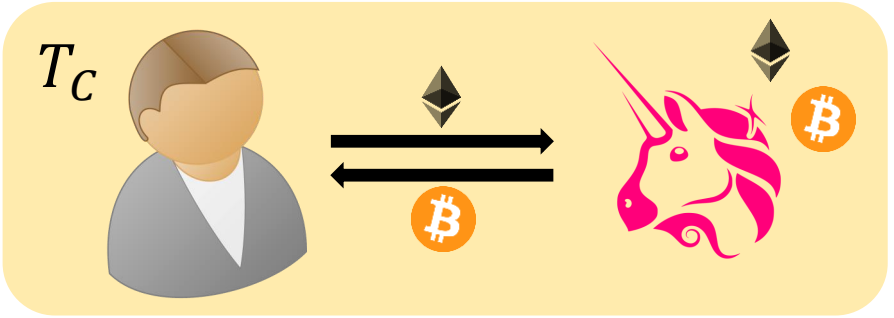


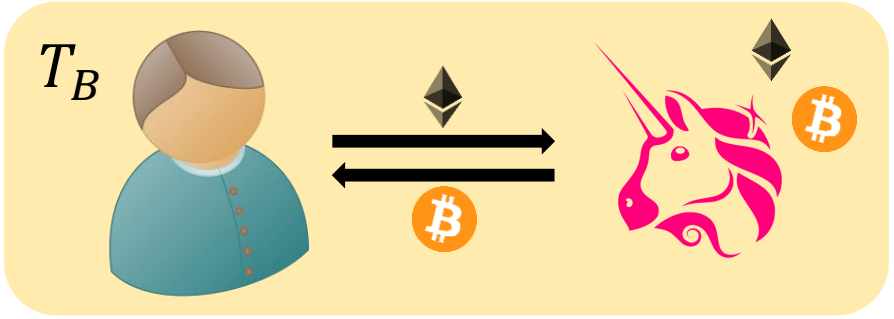
eUTXO

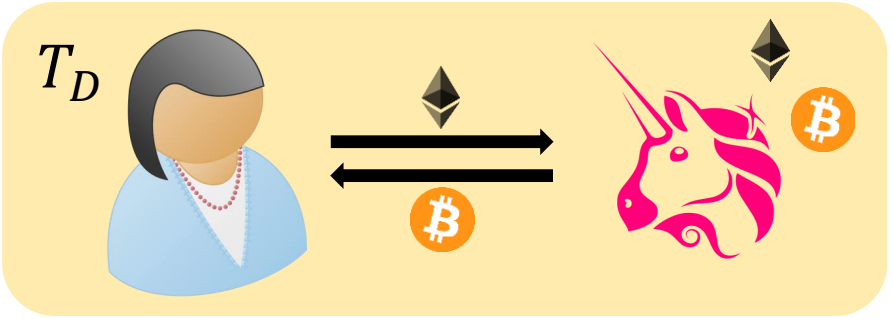


eUTXO

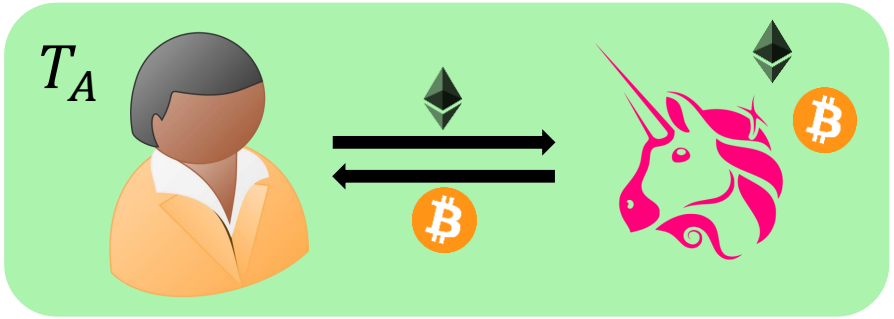


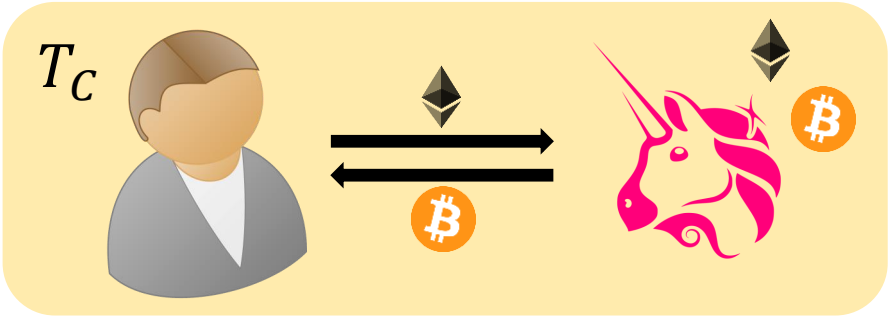


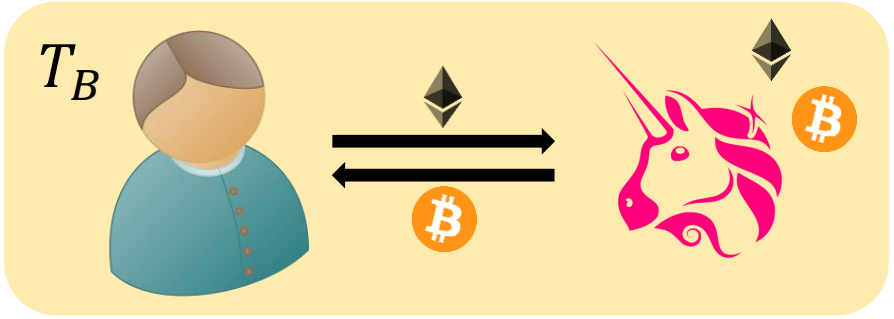


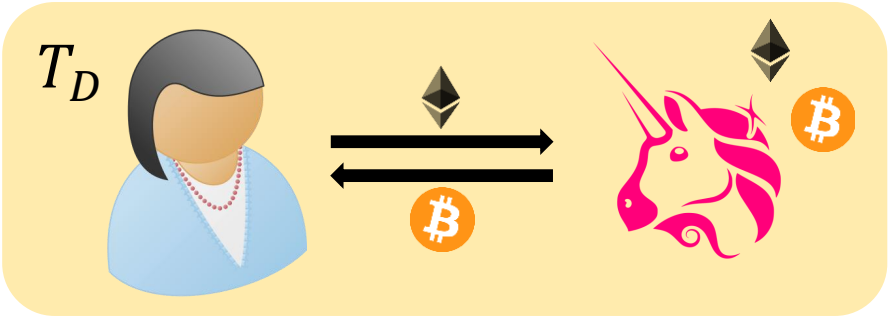


eUTXO

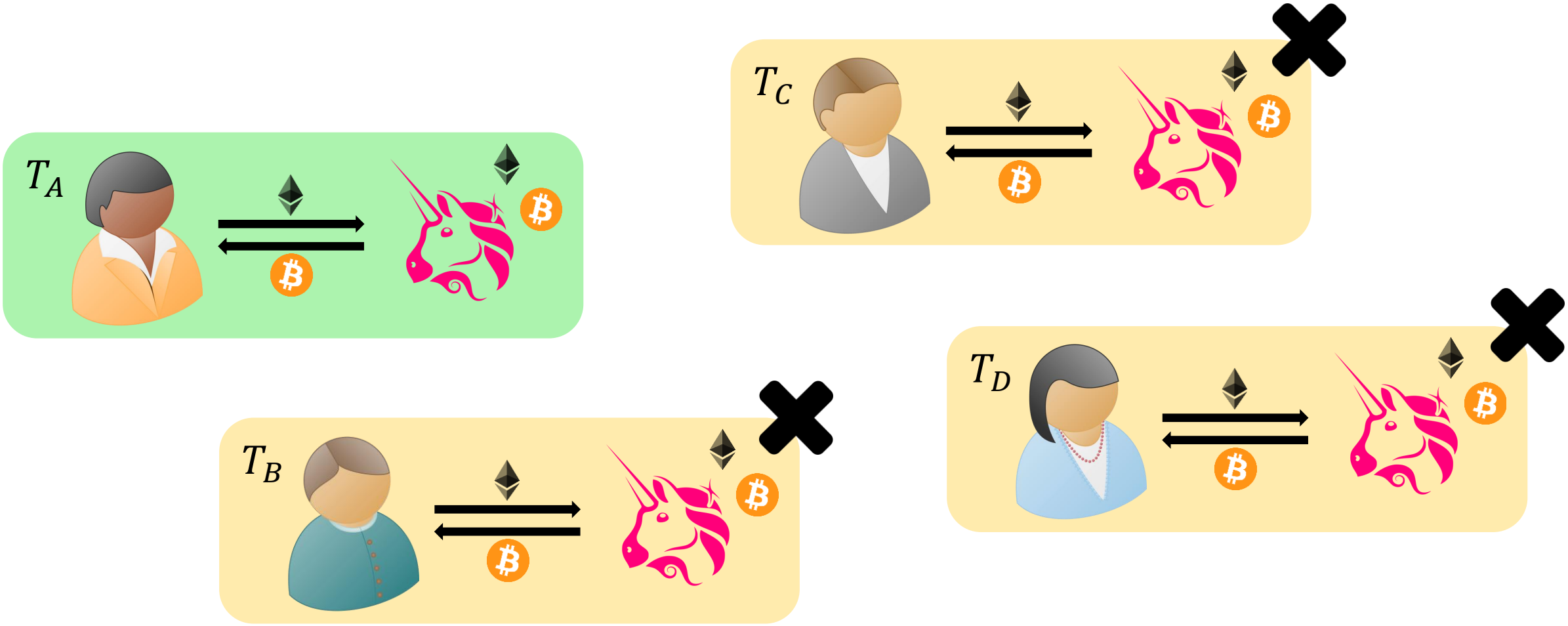




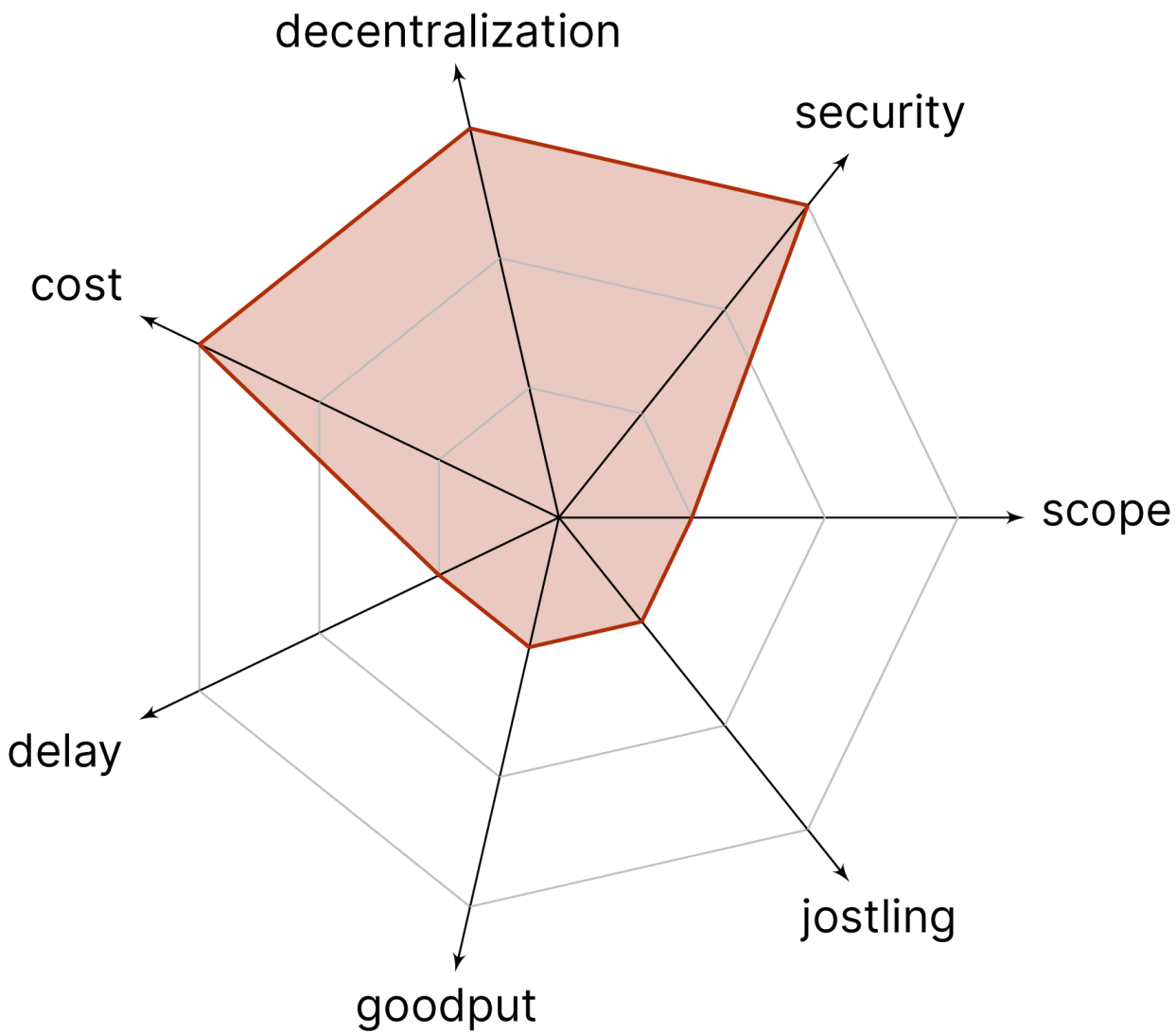




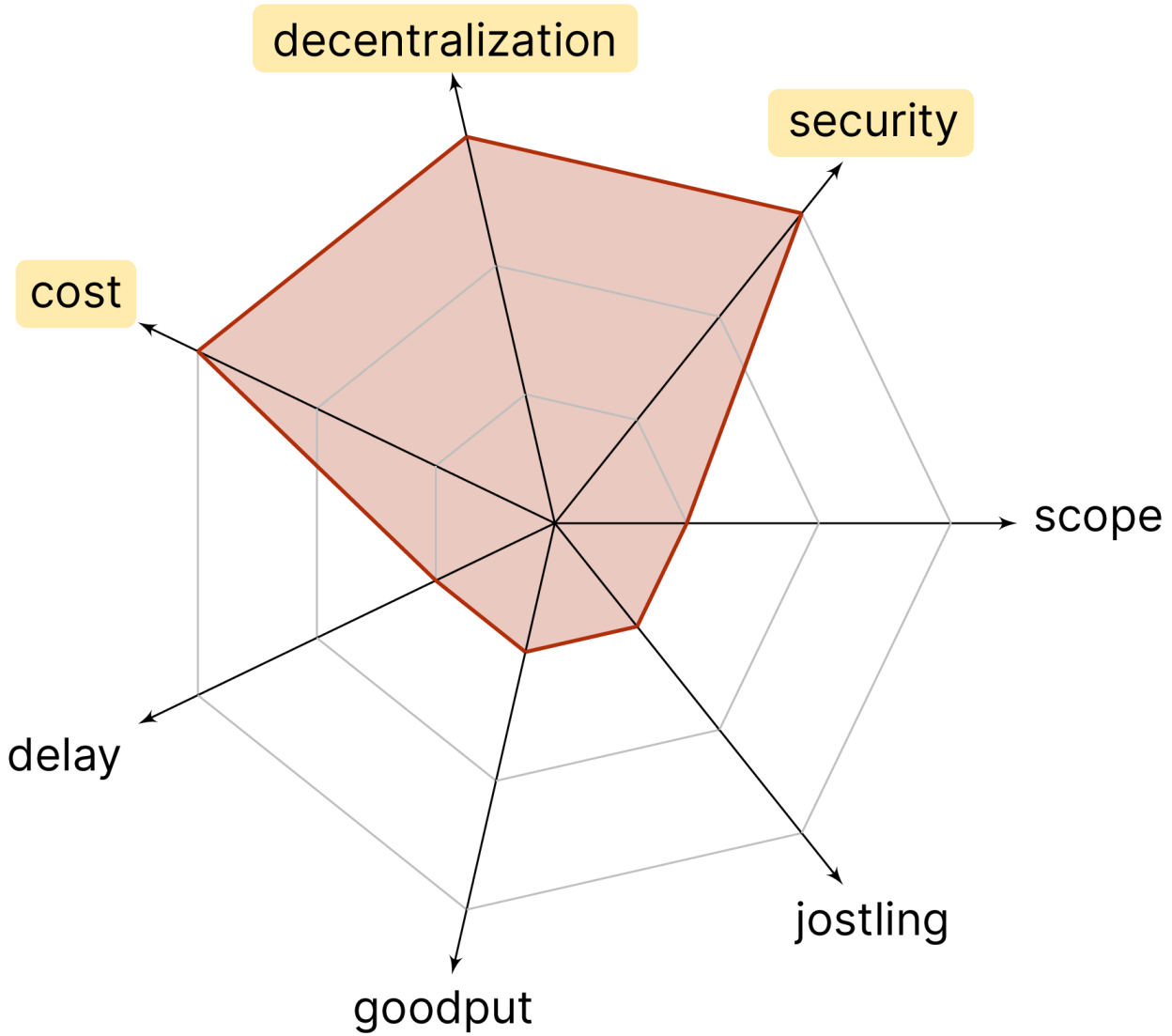
eUTXO



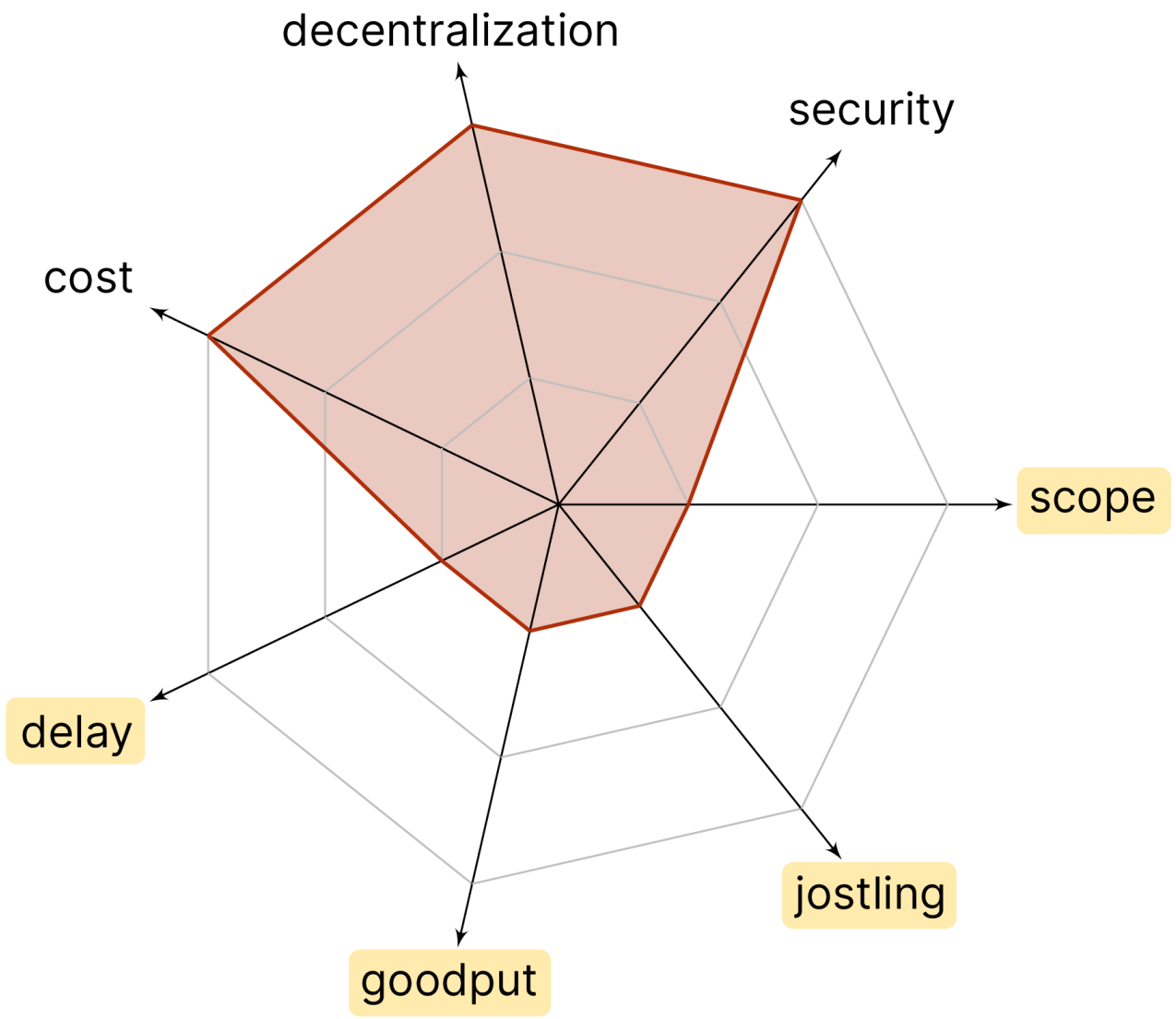
eUTXO


decentralization
security
cost
scope
delay
jostling
goodput

eUTXO


decentralization
security
cost
scope
delay
jostling
goodput

eUTXO


decentralization
security
cost
scope
delay
jostling
goodput

Algorithmic Committee Ordering

T_E

T_A

T_B

T_C

T_D

Algorithmic Committee Ordering

T_A T_B T_C T_D T_E

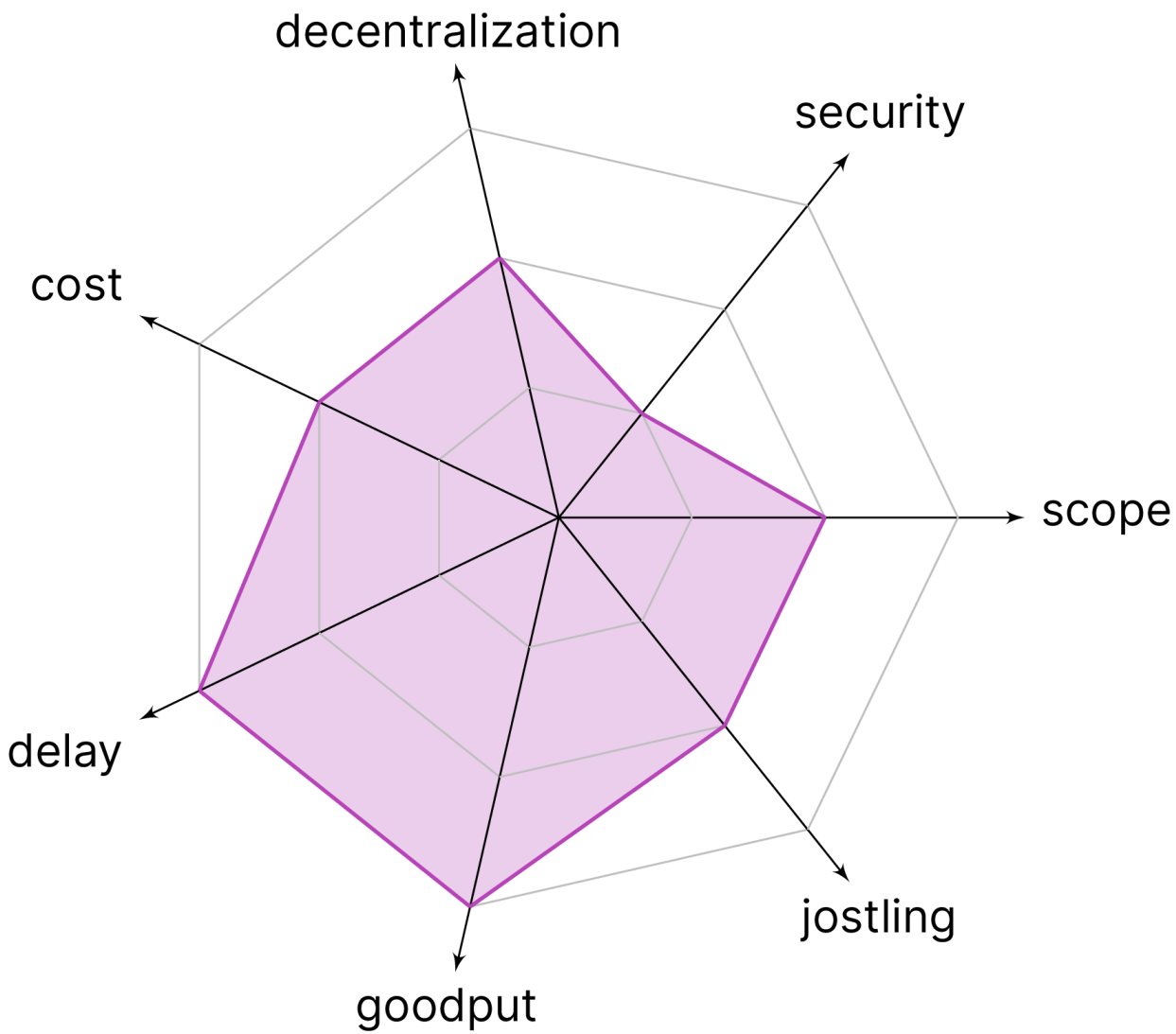
Algorithmic Committee Ordering

T_A T_B T_C T_D T_E

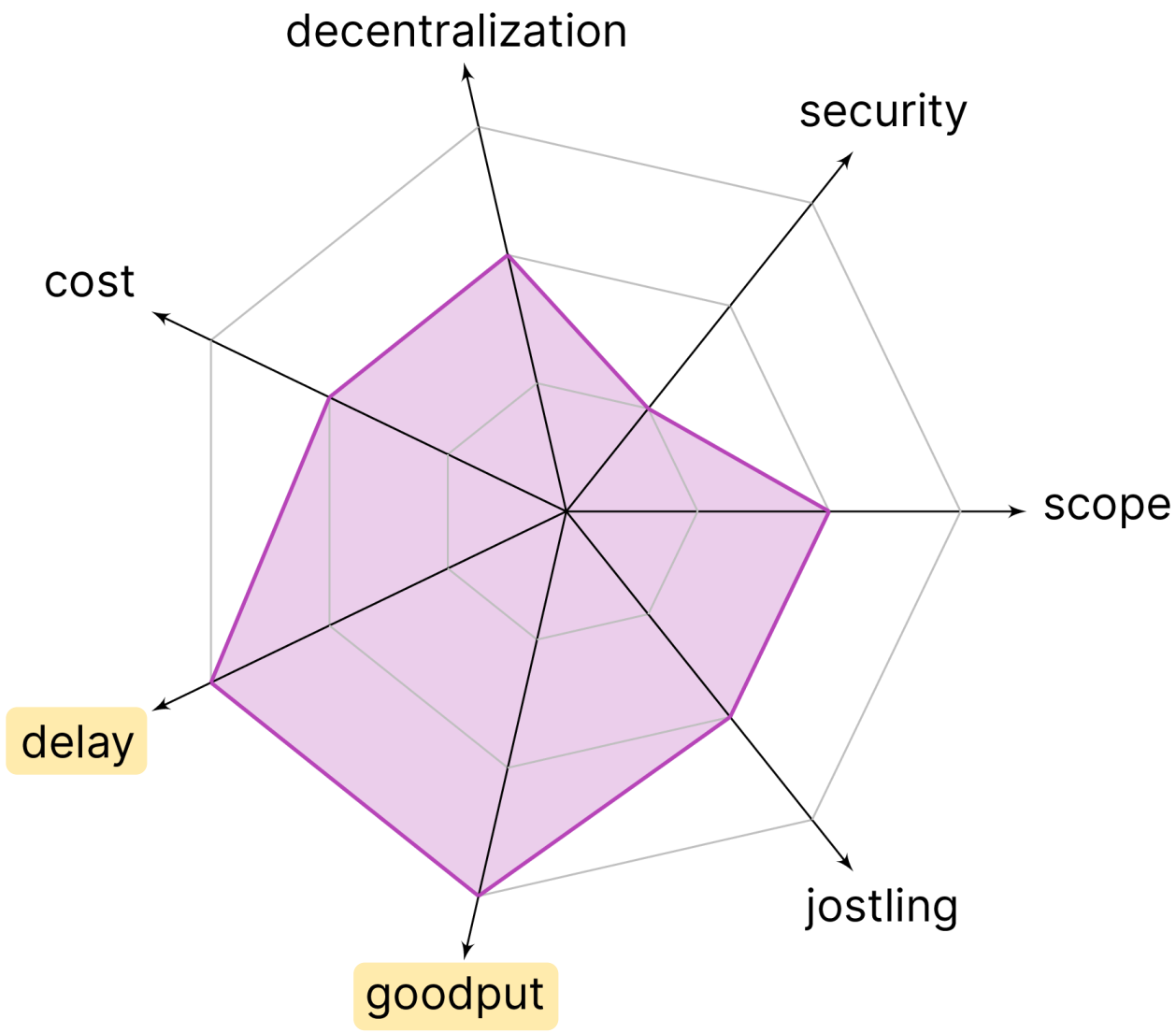
Algorithmic Committee Ordering

T_A T_C T_B T_B T_E

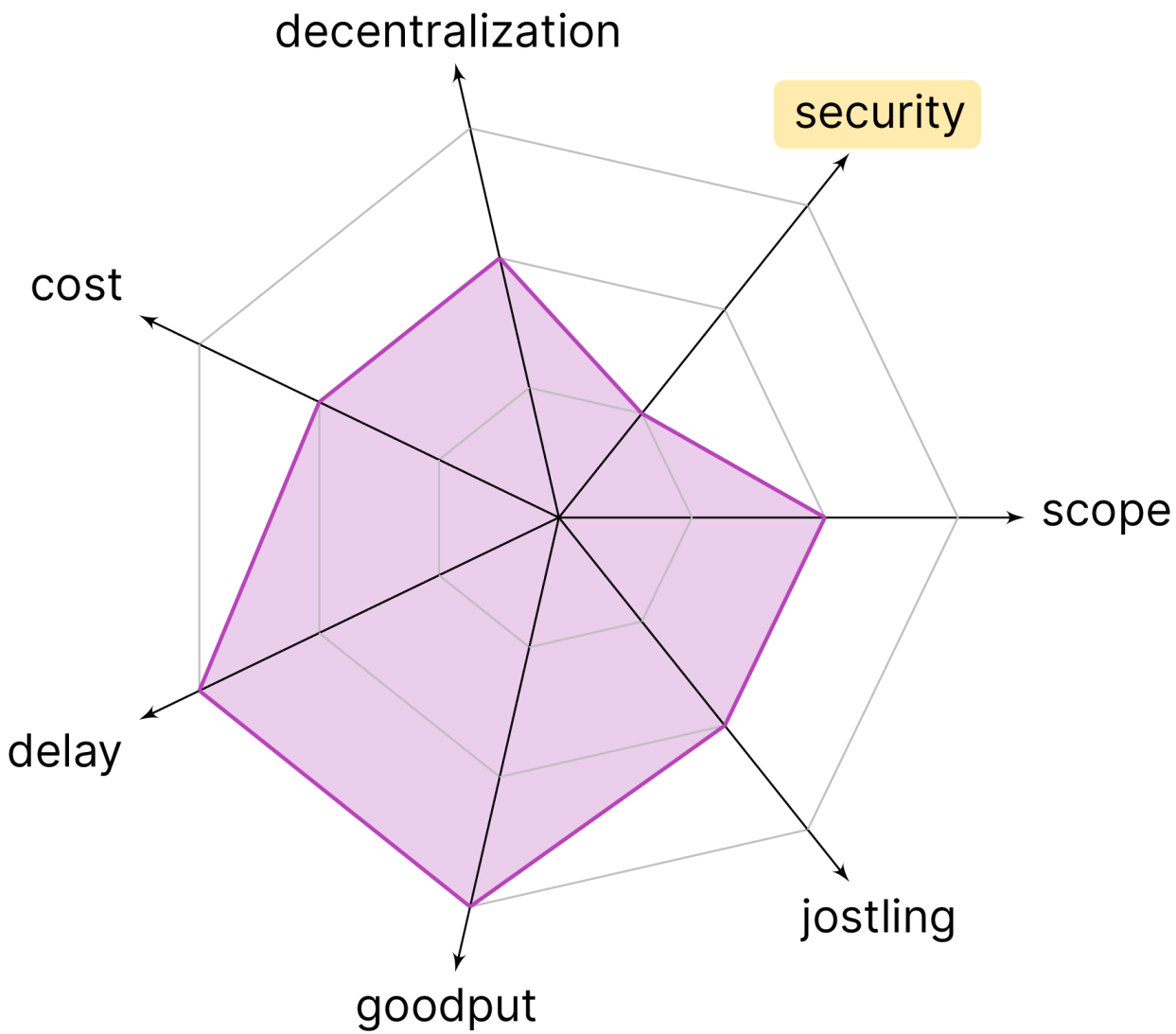
Algorithmic Committee Ordering



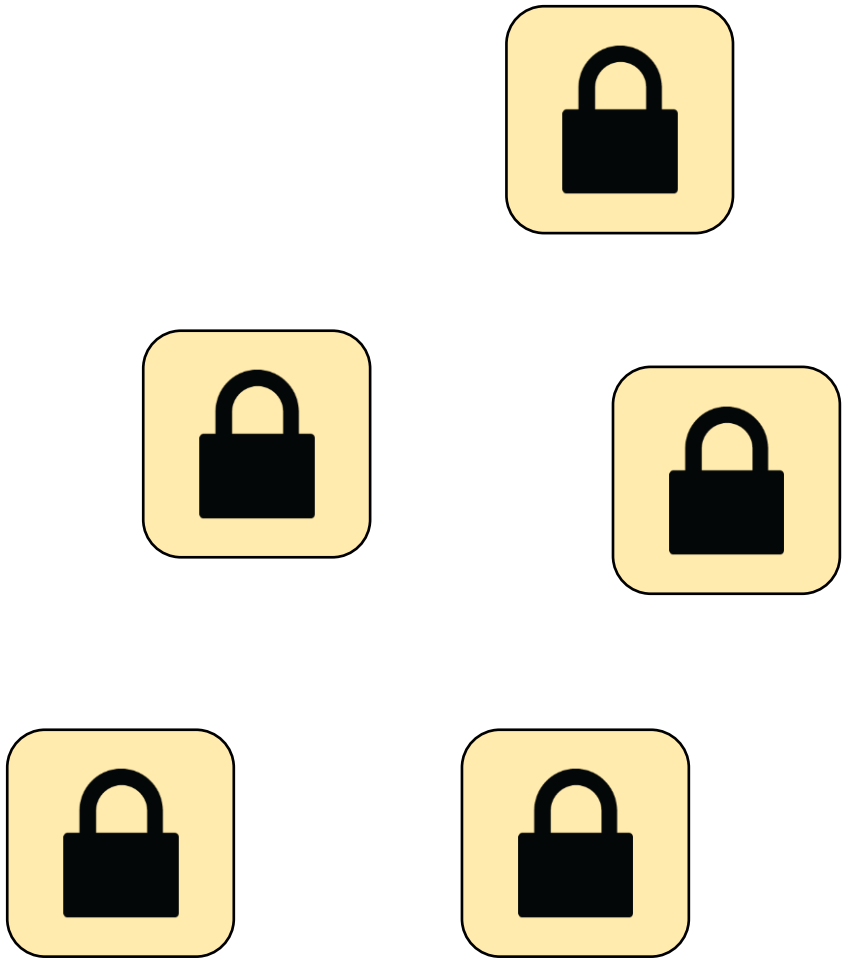
Algorithmic Committee Ordering



Algorithmic Committee Ordering

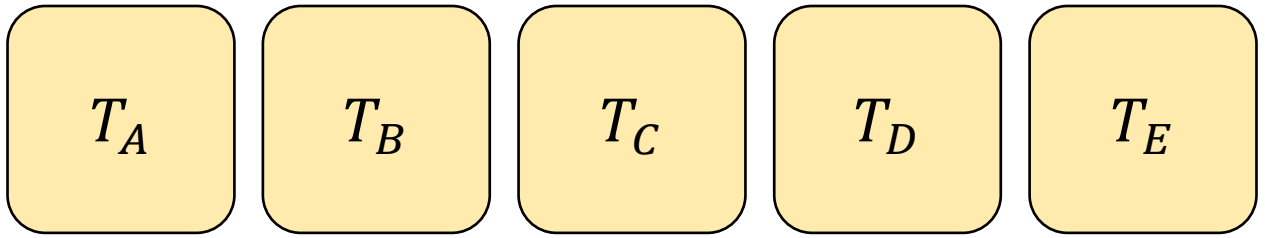


On-chain Commit & Reveal

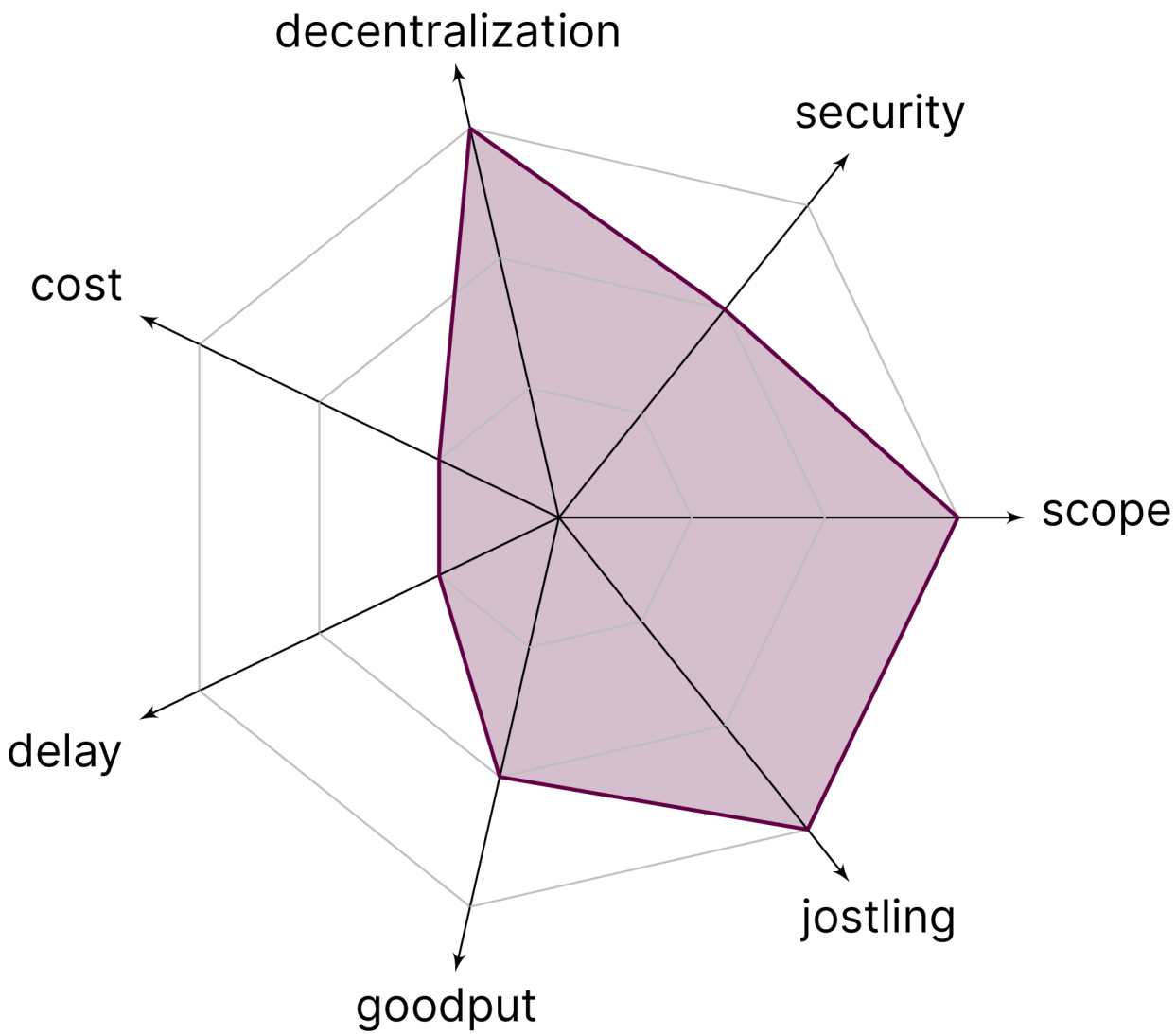


On-chain Commit & Reveal

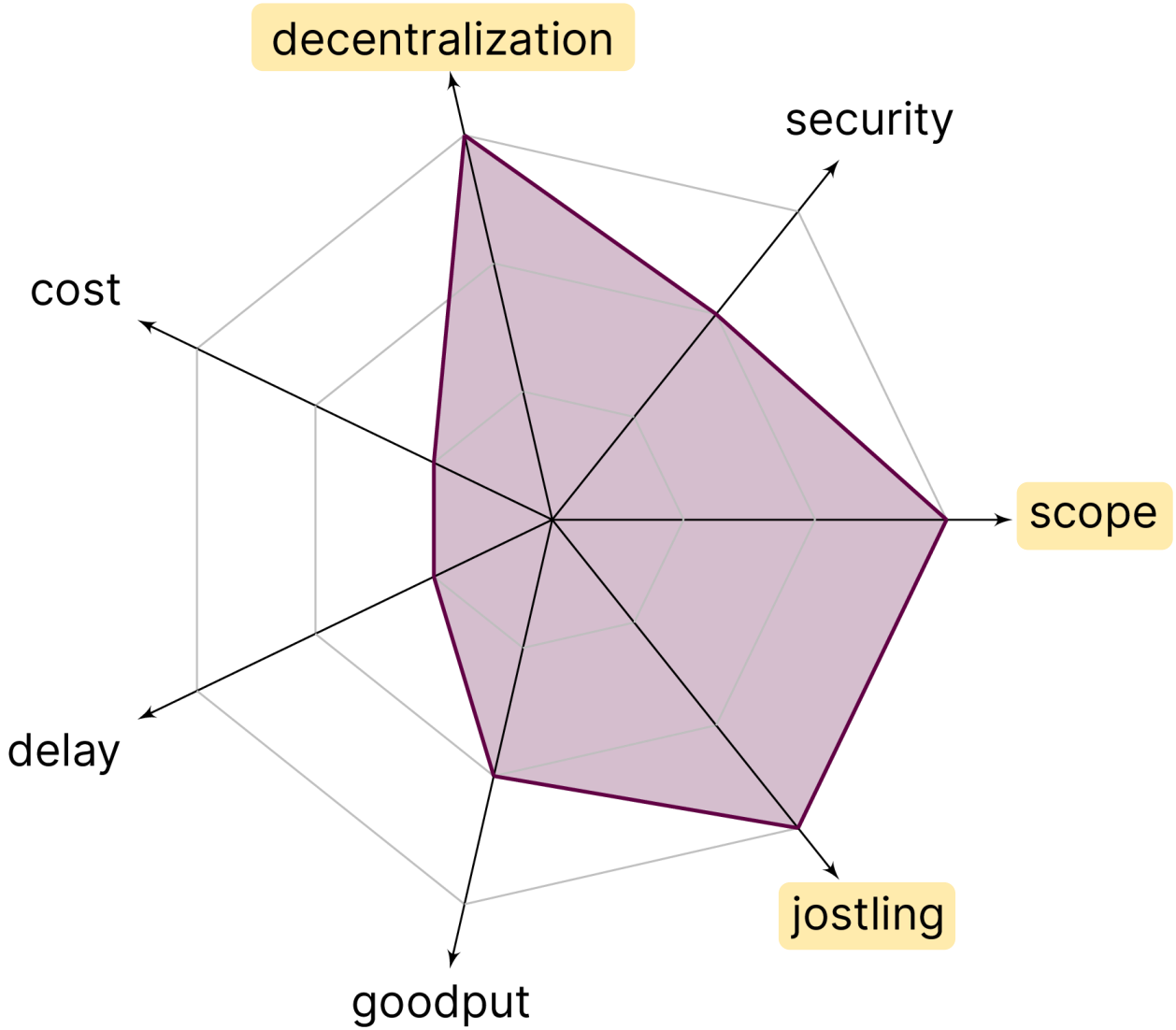
On-chain Commit & Reveal



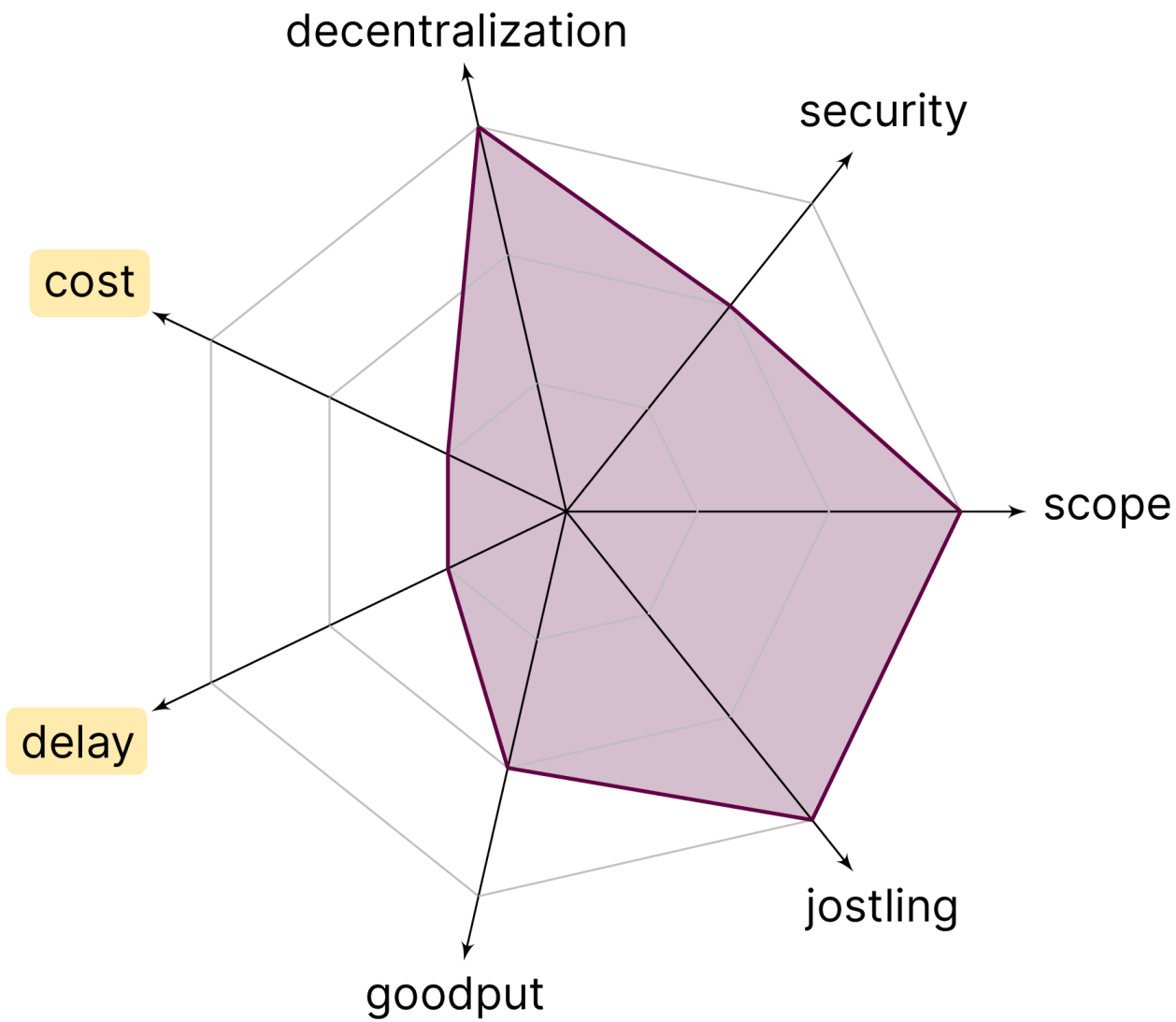
On-chain Commit & Reveal



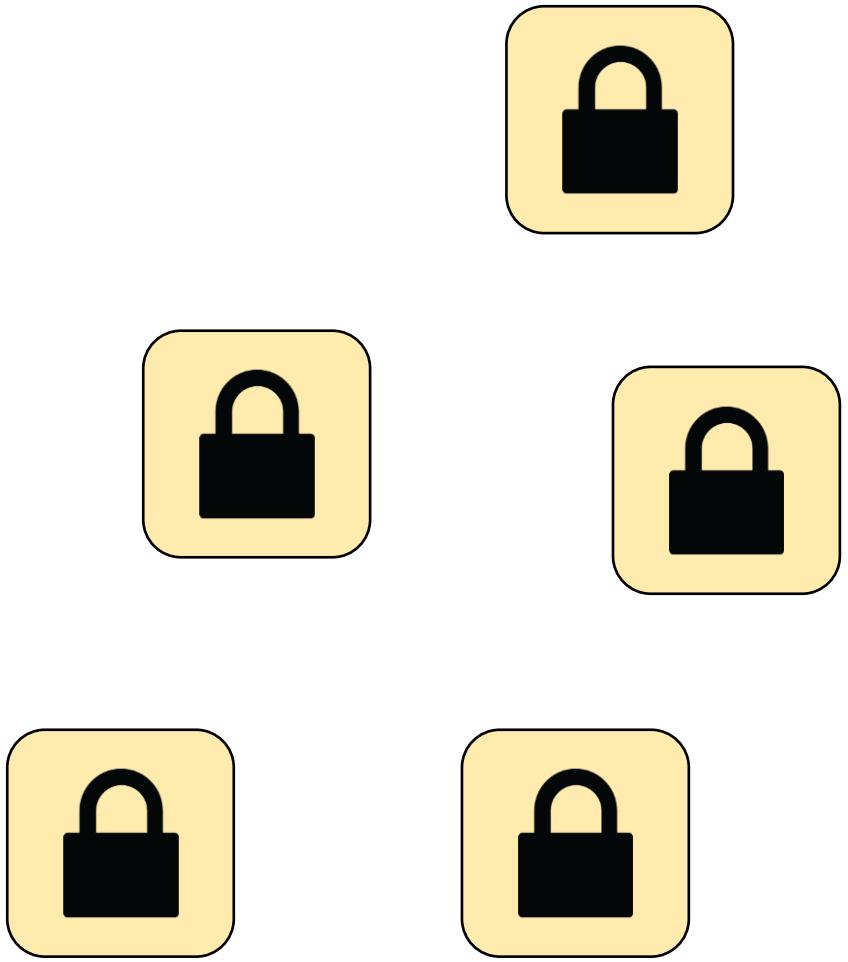
On-chain Commit & Reveal



On-chain Commit & Reveal



Off-chain Commit & Reveal



Off-chain Commit & Reveal

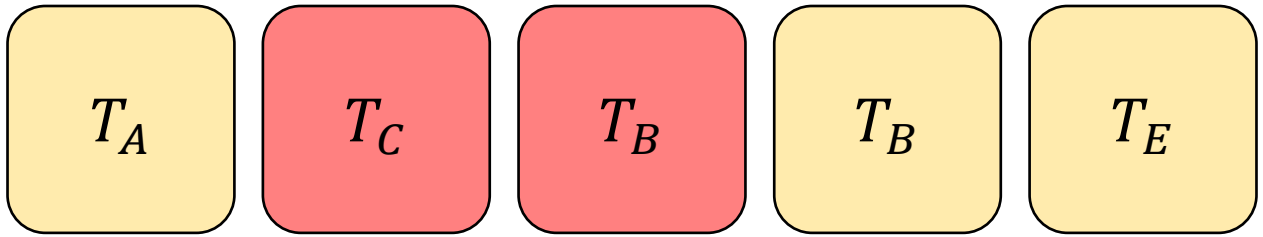
Off-chain Commit & Reveal

T_A T_B T_C T_D T_E

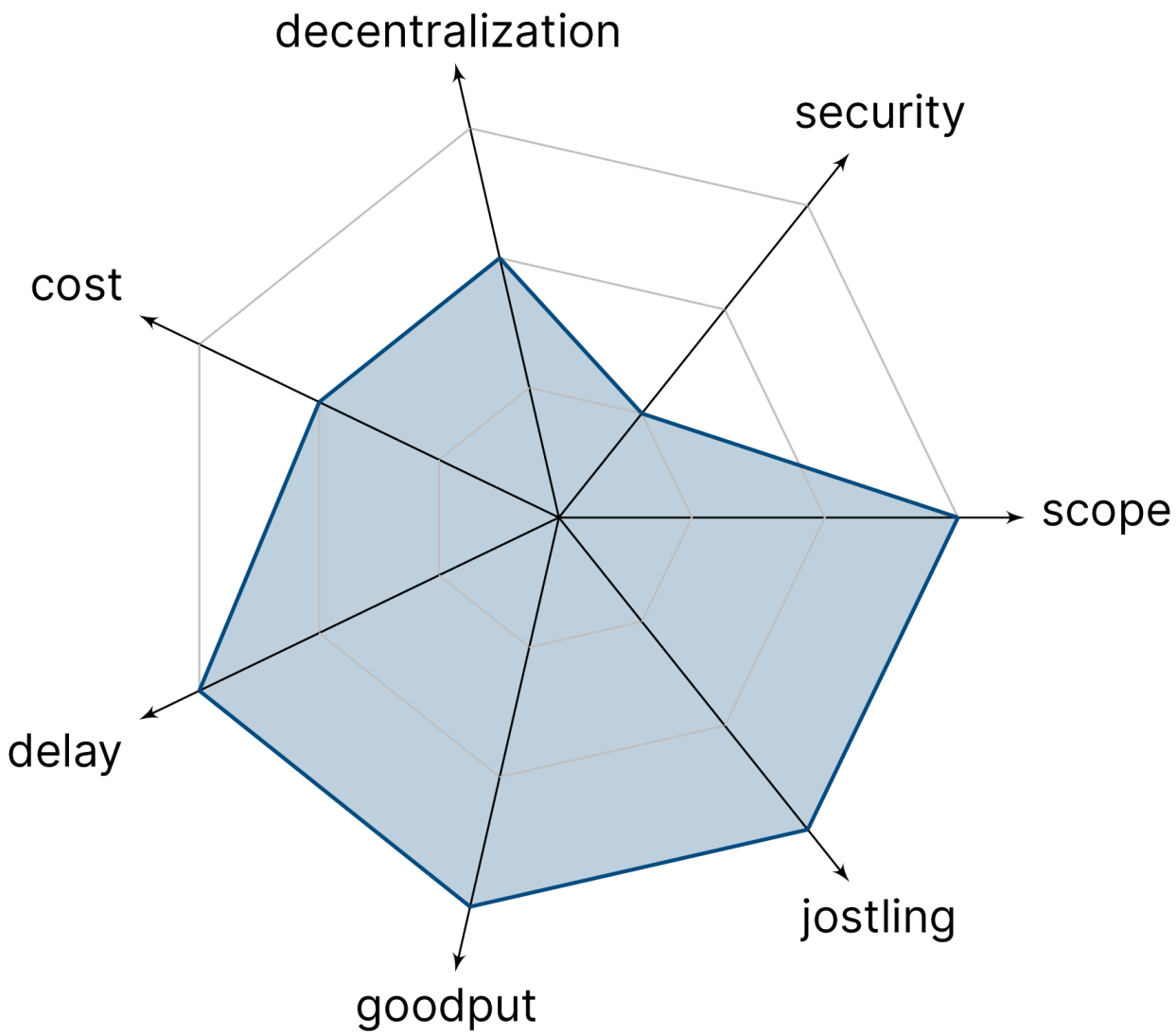
Off-chain Commit & Reveal

T_A T_B T_C T_D T_E

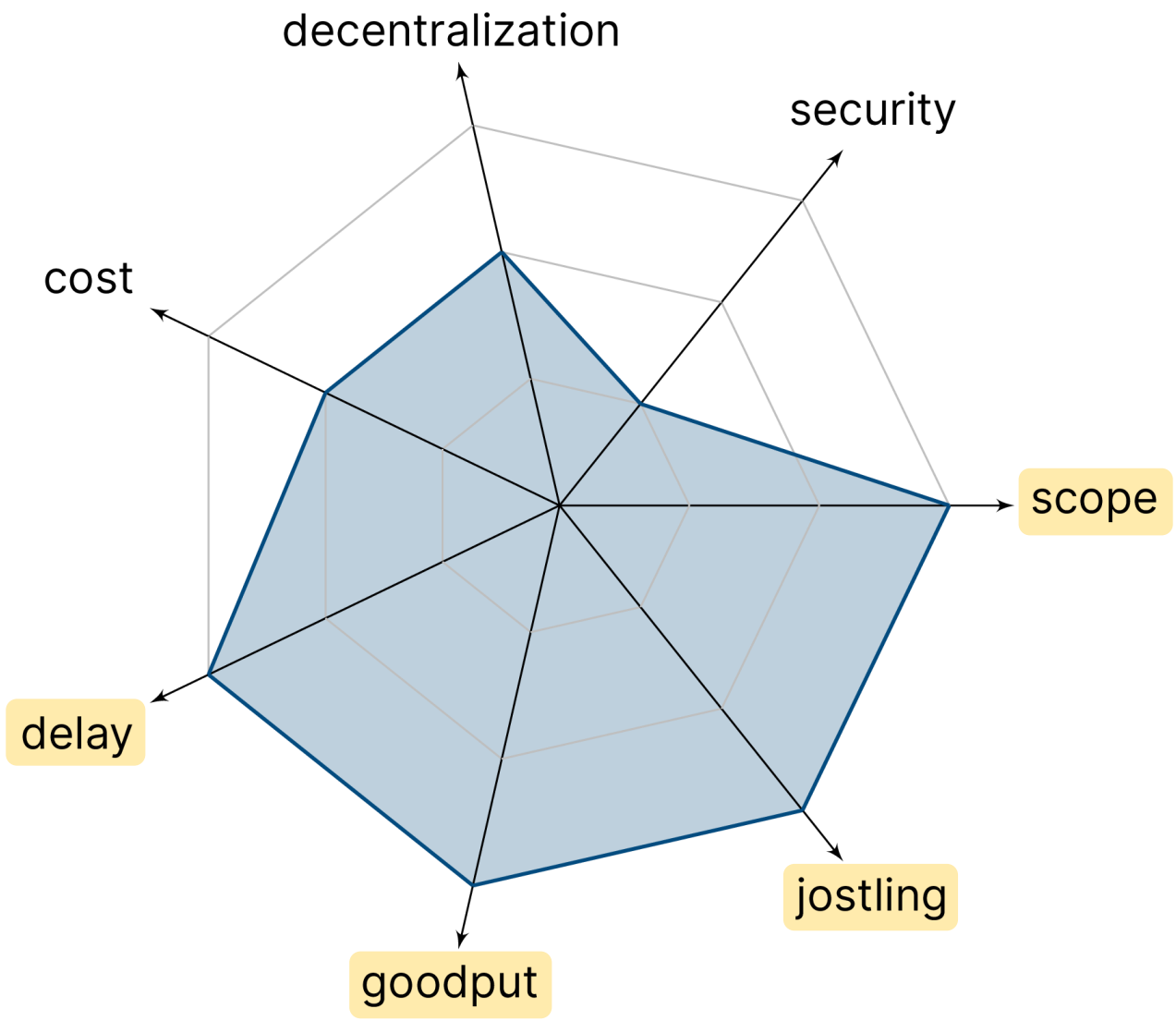
Off-chain Commit & Reveal



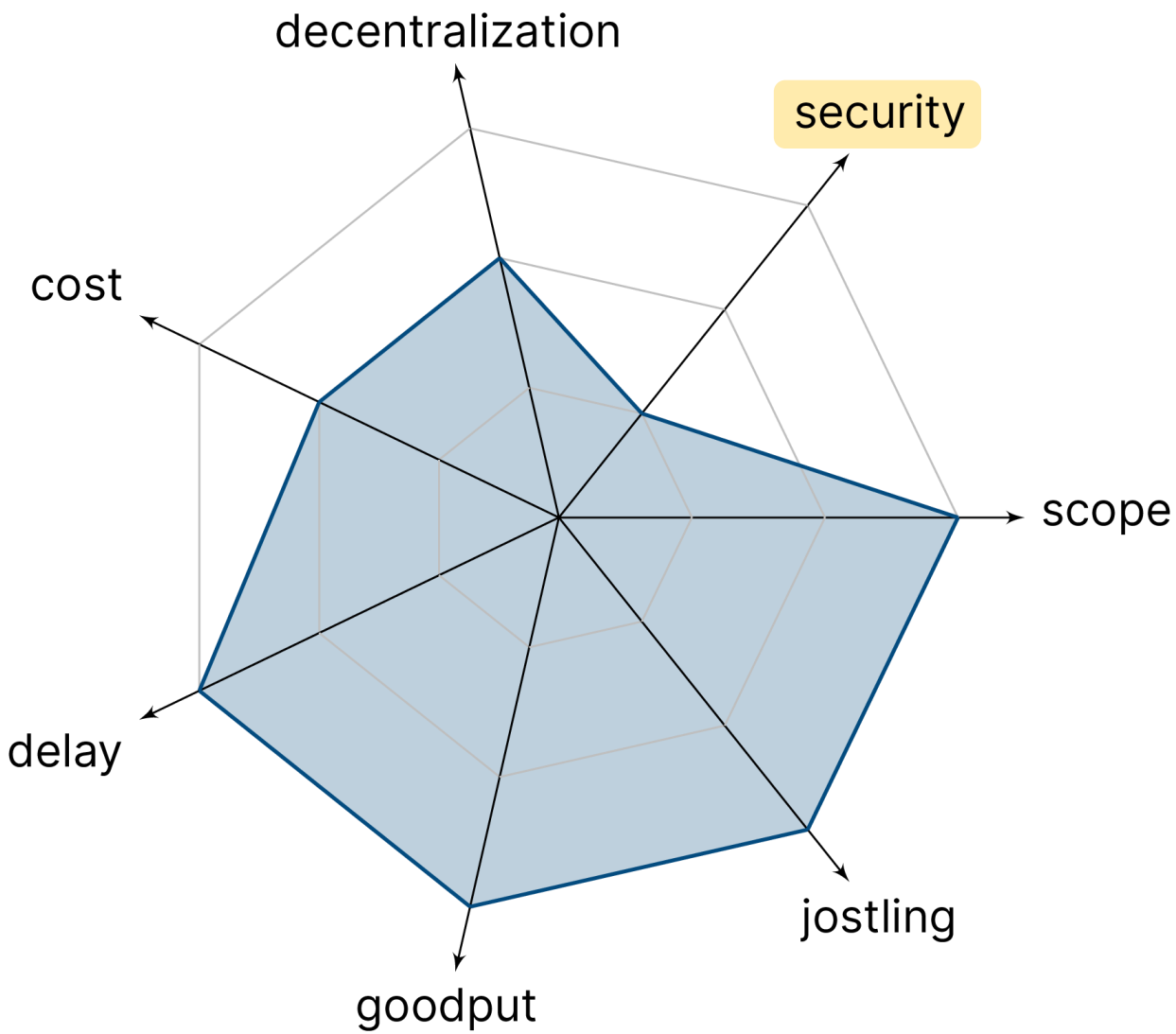
Off-chain Commit & Reveal



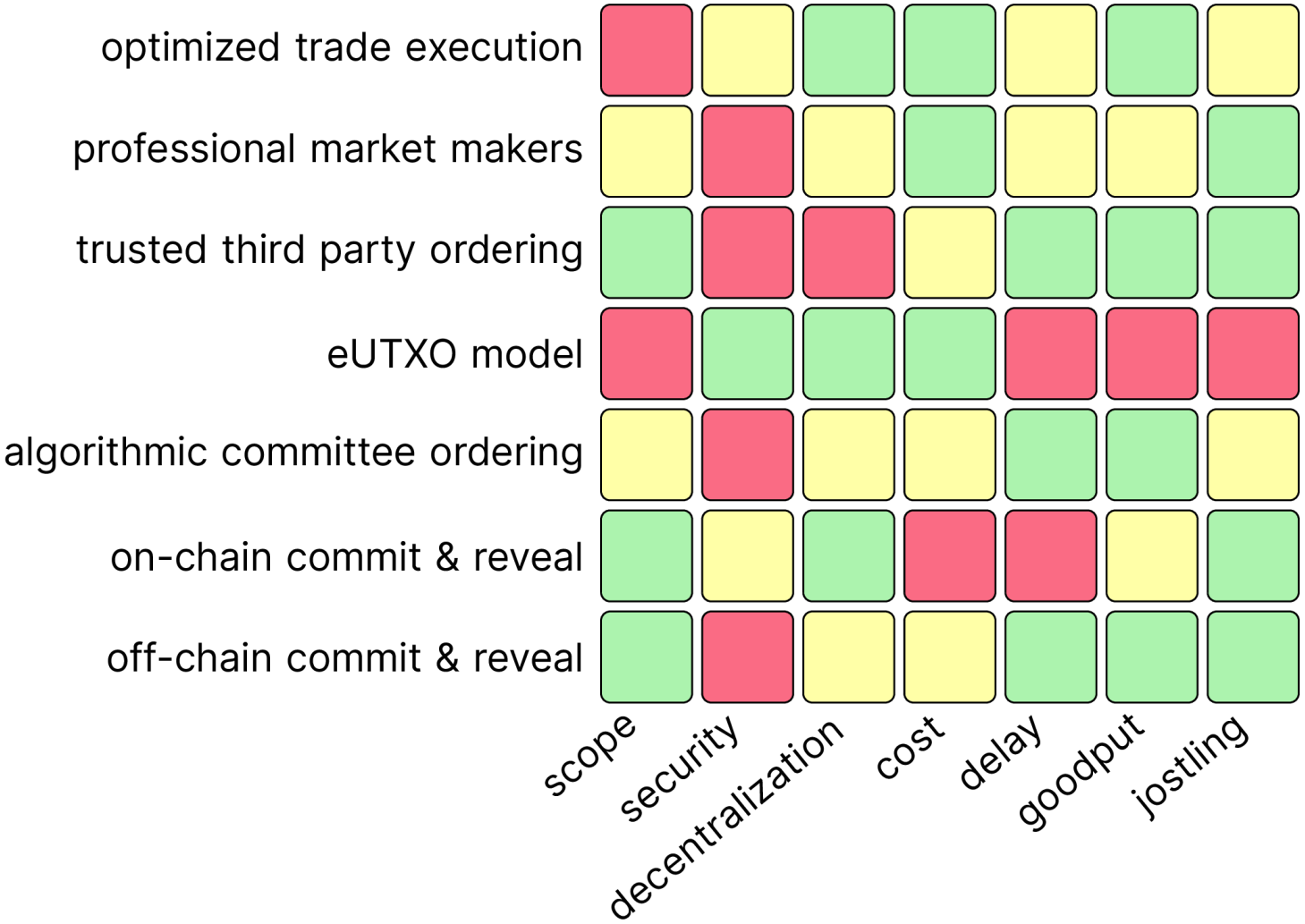
Off-chain Commit & Reveal



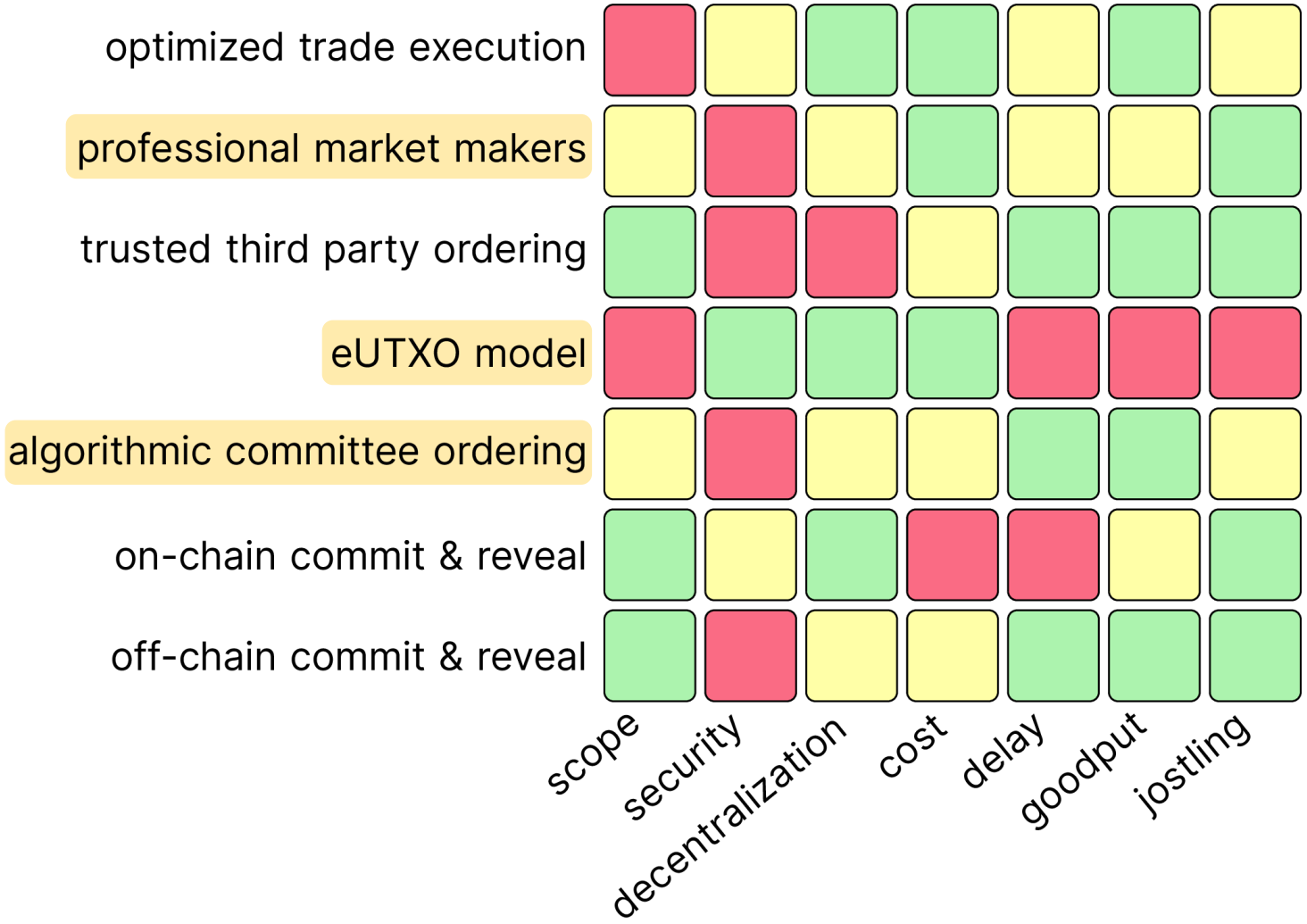
Off-chain Commit & Reveal



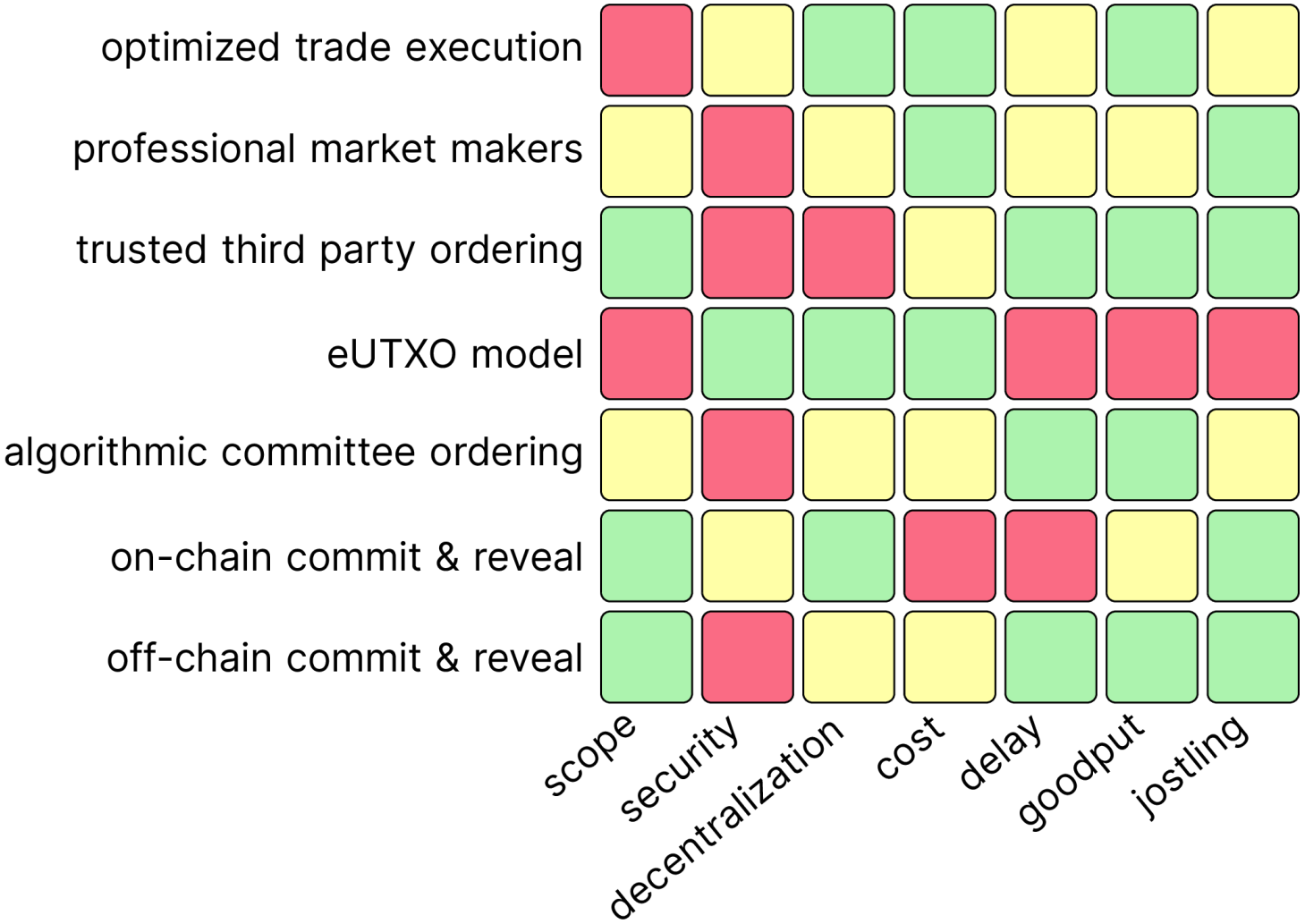
Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

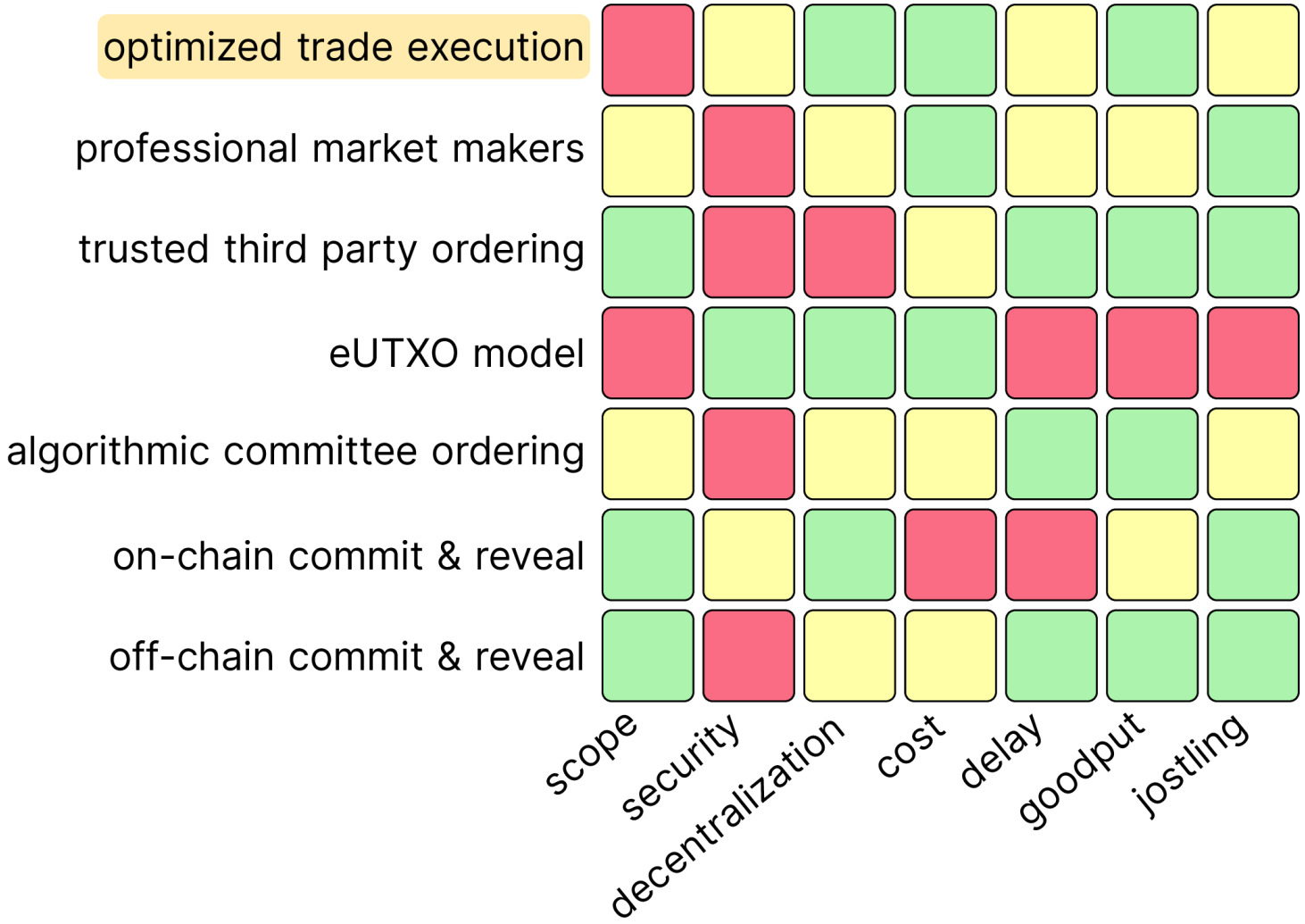
Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

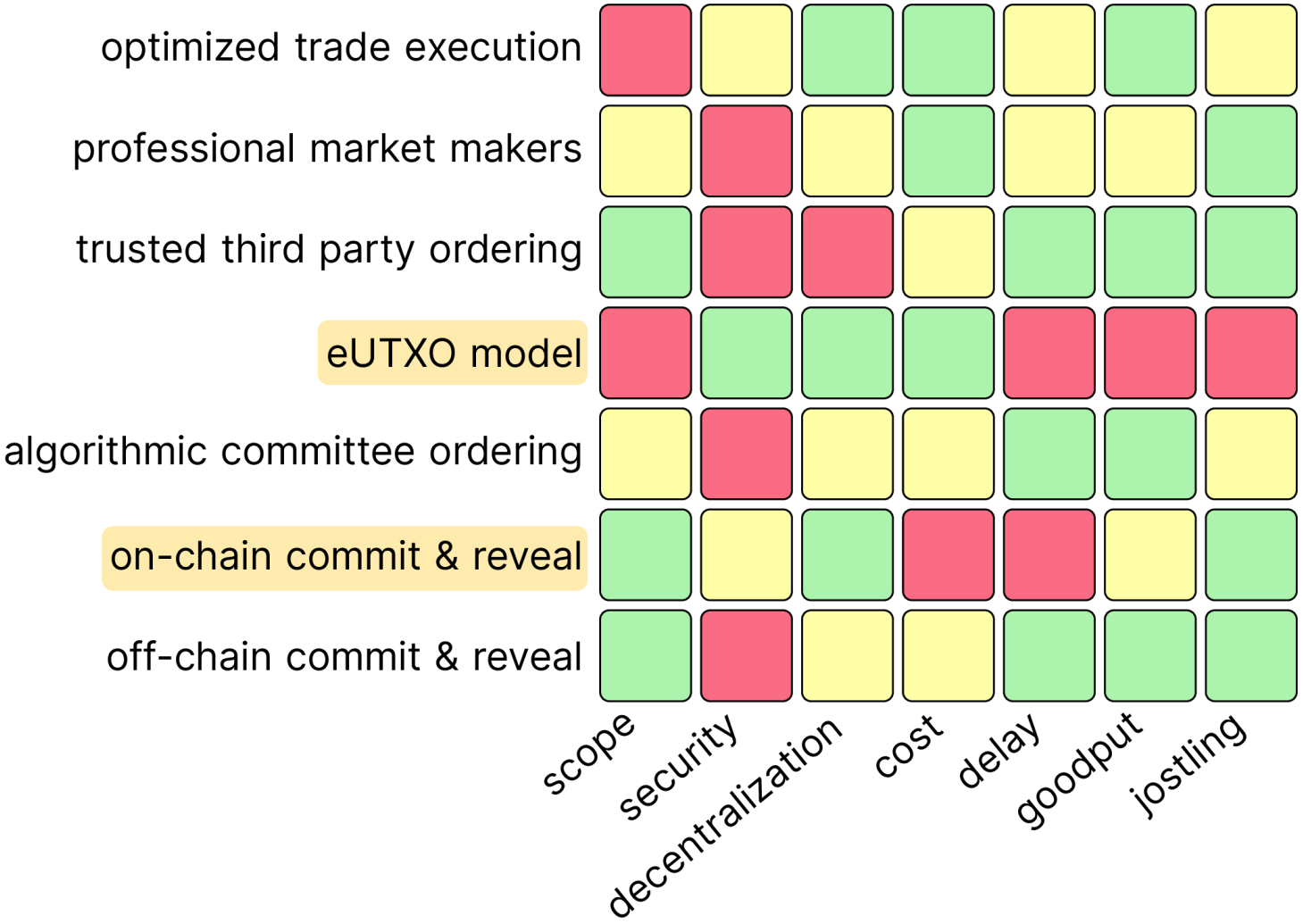
Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

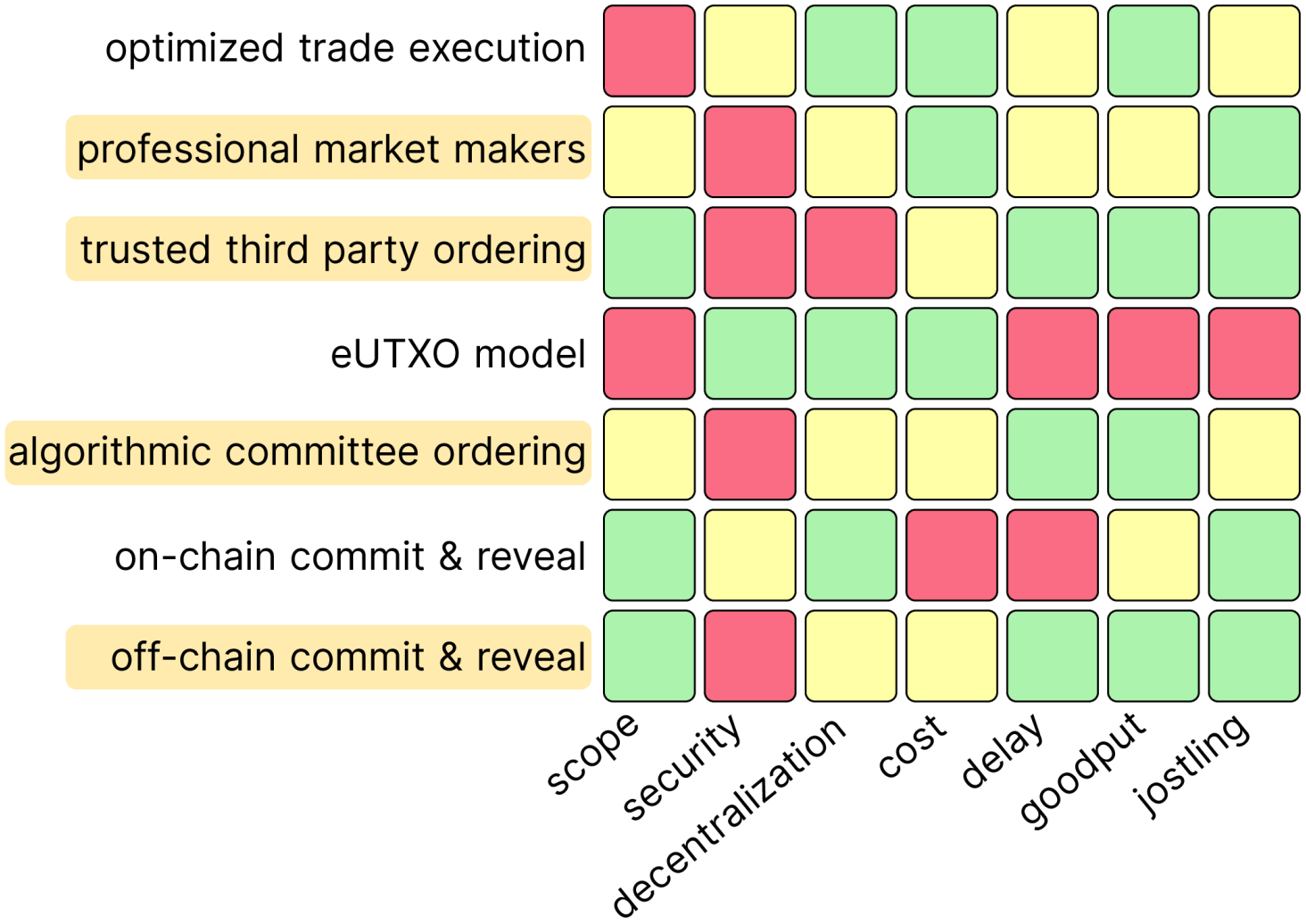
Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

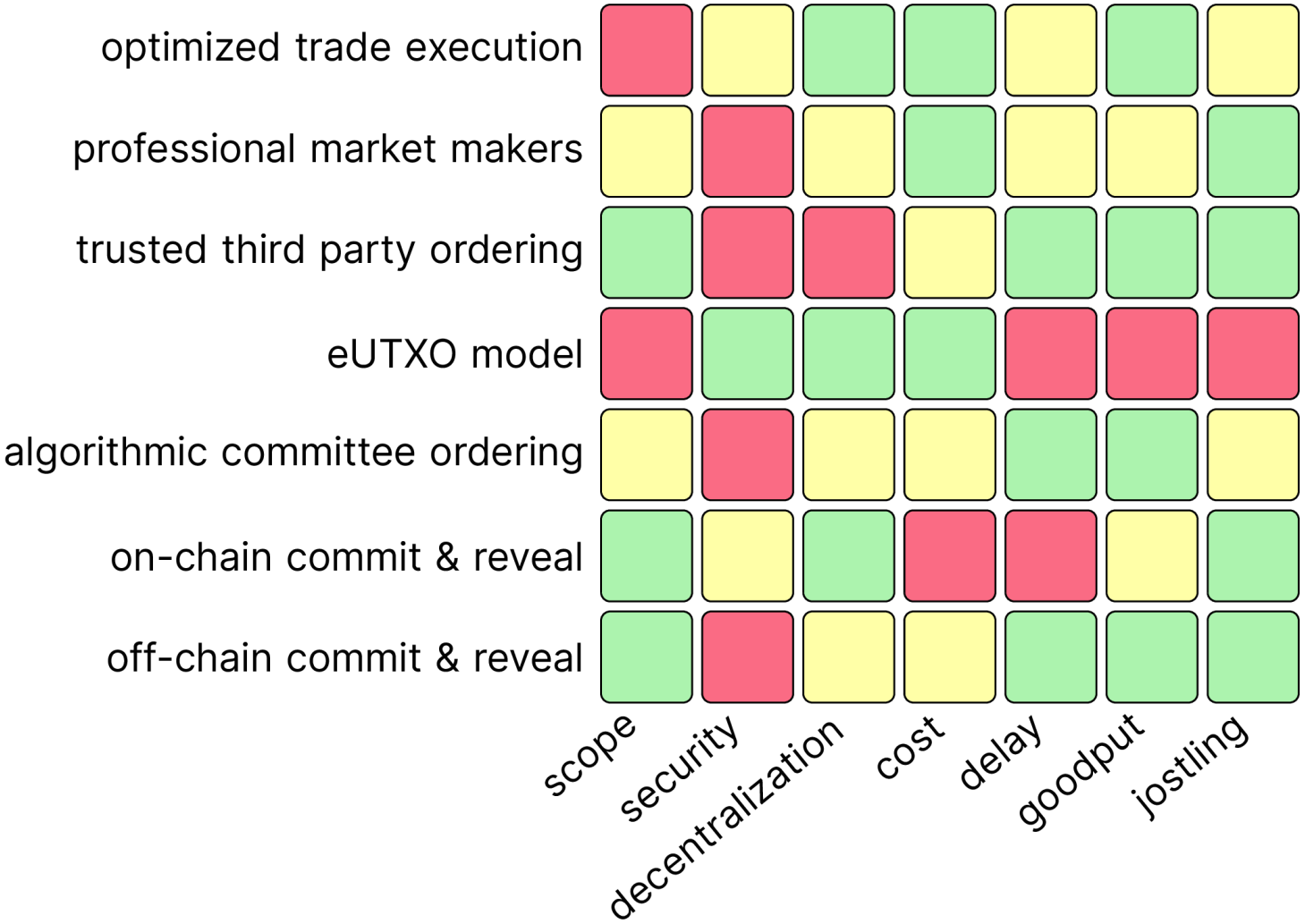
Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

Summary


optimized trade execution
professional market makers
trusted third party ordering
eUTXO model
algorithmic committee ordering
on-chain commit & reveal
off-chain commit & reveal
scope
security
decentralization
cost
delay
goodput
jostling

Thank You!

Questions & Comments?

Advances in Financial Technologies (AFT'22)
Lioba Heimbach, Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

Cyclic Arbitrage