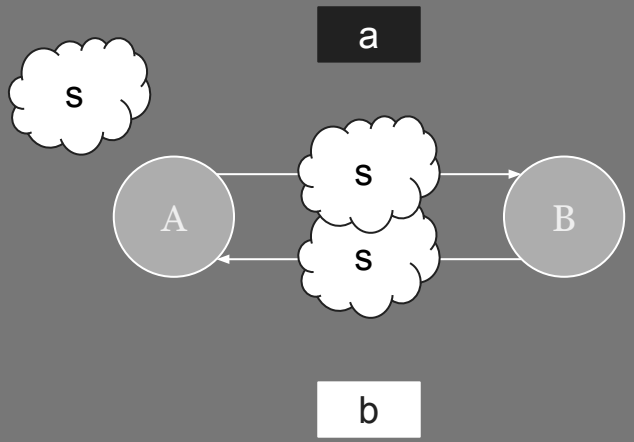
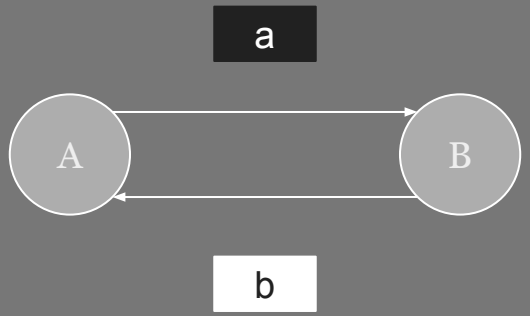
# Limitations of Hashlocks in Cross-Chain Commerce

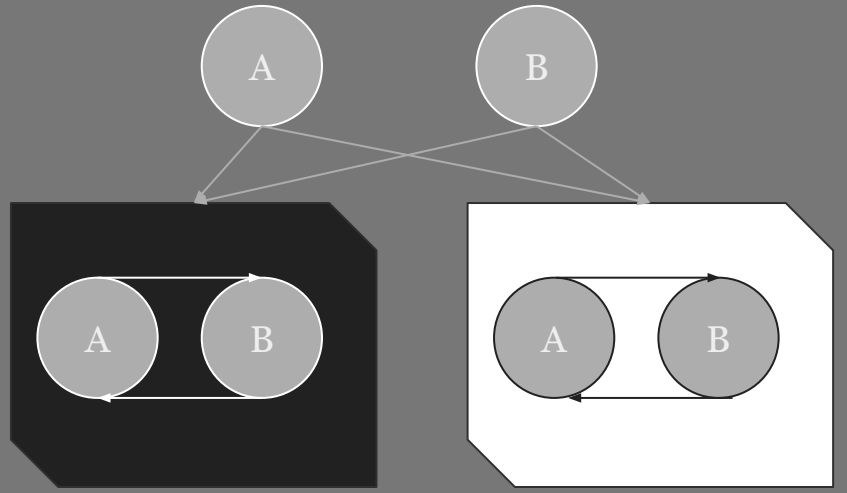
Speaker: Daniel Engel (Brown University)
Advised By: Maurice Herlihy (Brown University)

# Motivation

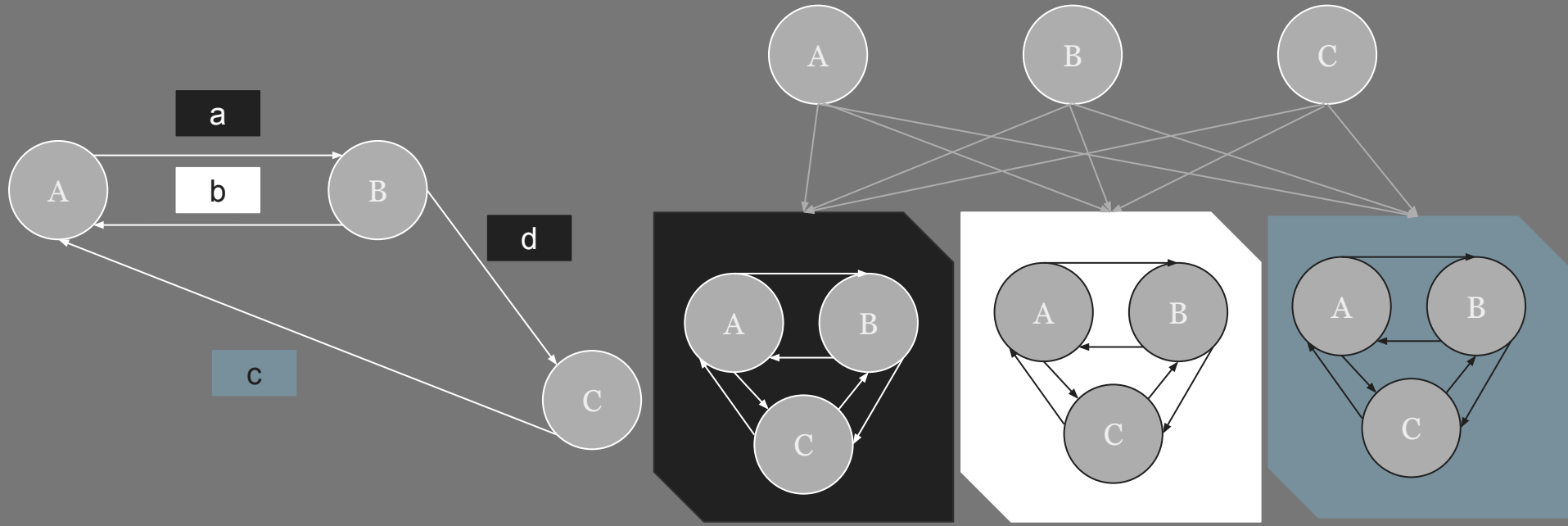


# Motivation

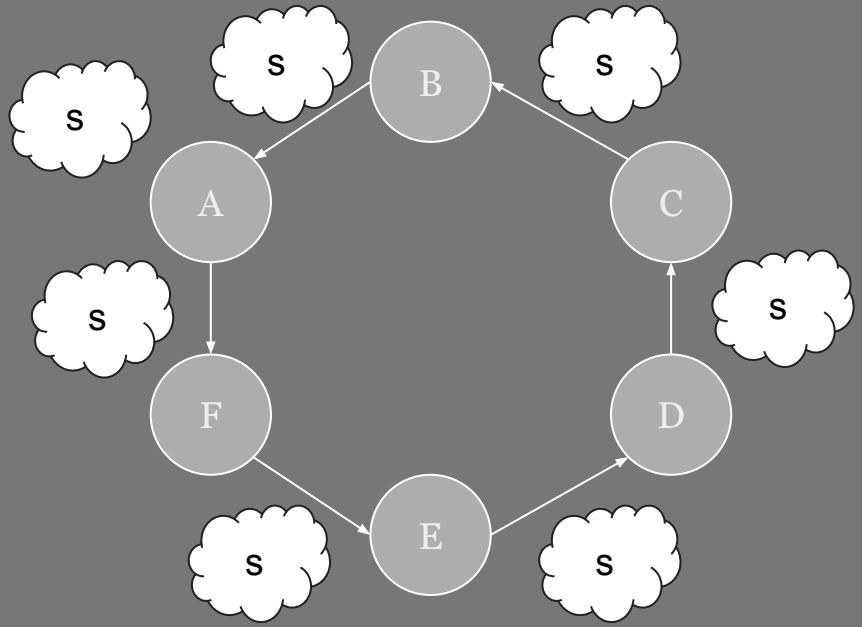


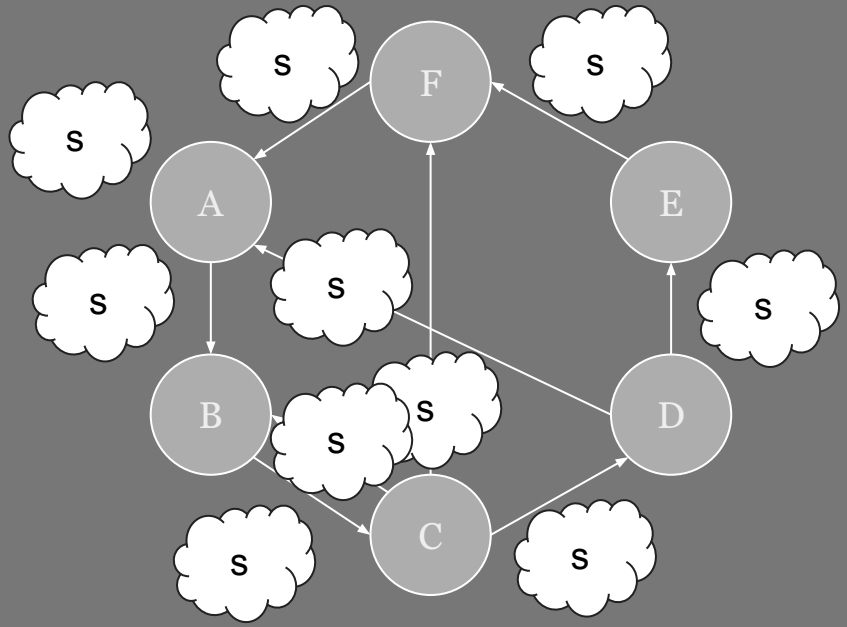
# Motivation



# Motivation



# Motivation



# Motivation

- A general synchronous model
- Captures network attacks
- When are simple hash locks not enough?
- Task complexity and number of locks

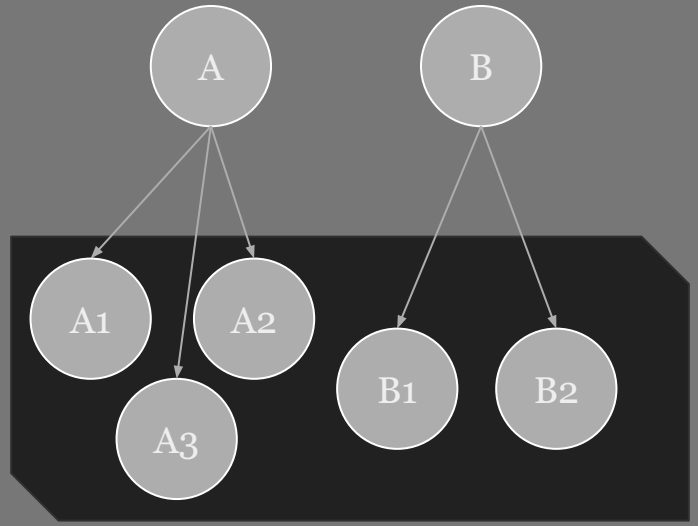
# Talk Overview

- Operational model
- Combinatorial model
- Applications of model
- Beyond simple hashlocks

# Operational Model

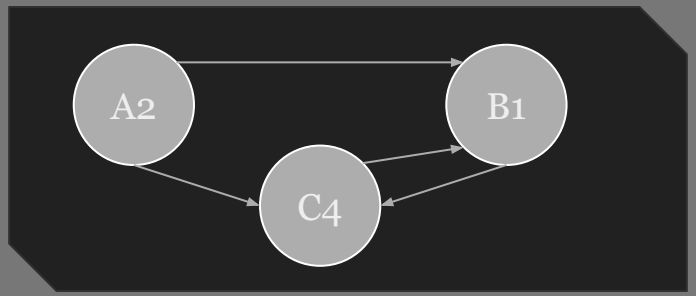
# Basic model (Parties)

- Parties own accounts



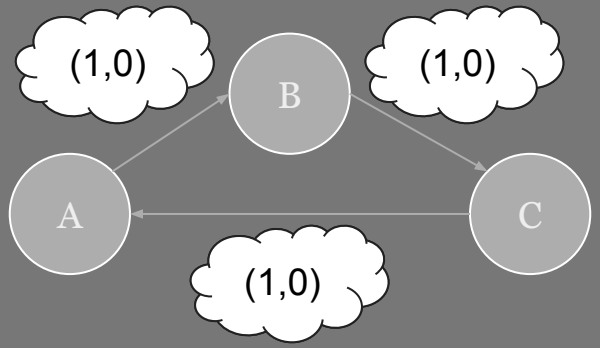
# Basic model (Contracts)

- Contracts manage assets



# Hashlock Representation

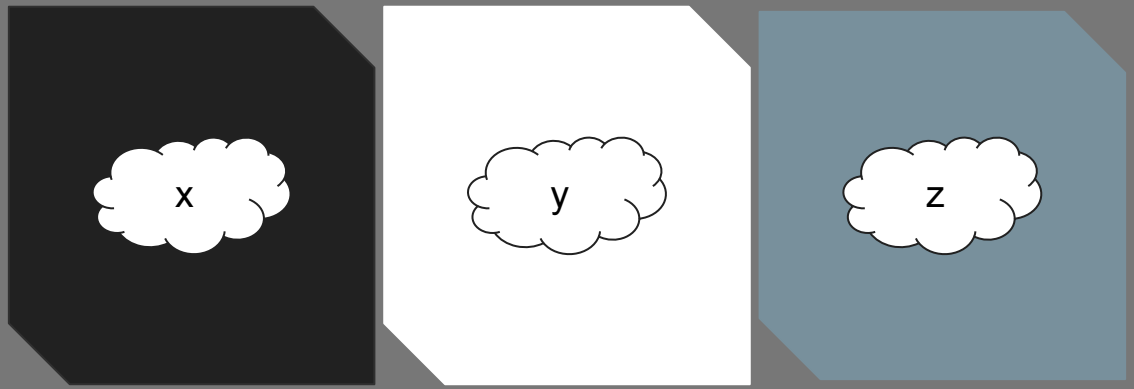
- Lock vectors



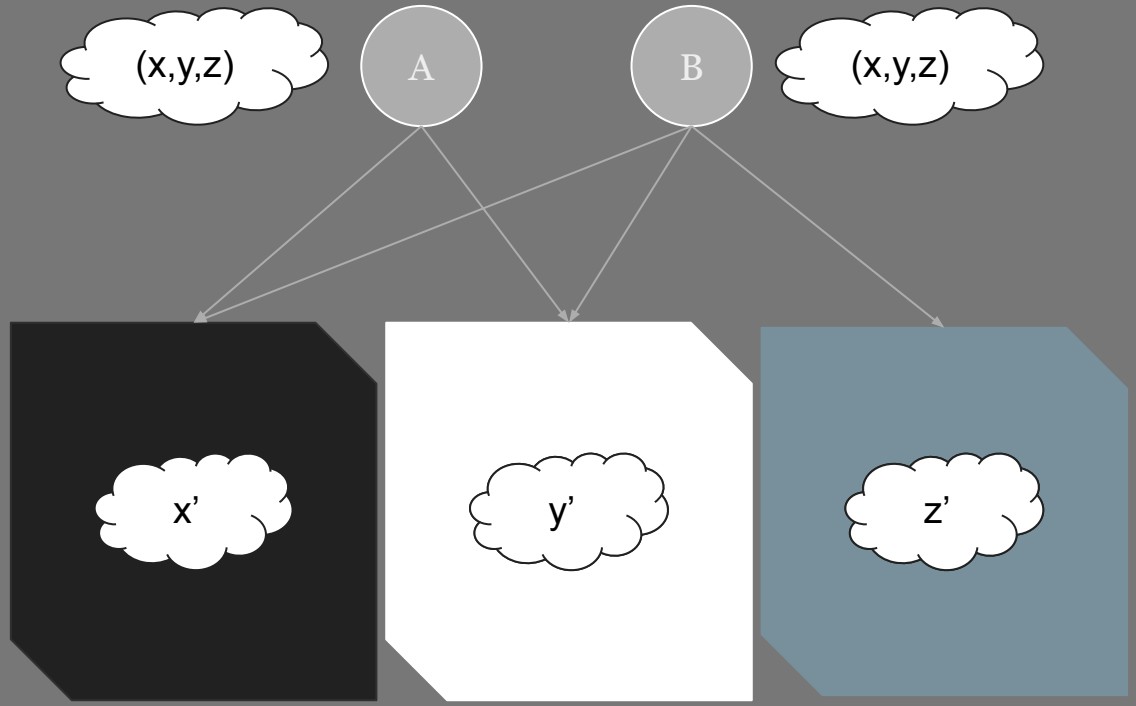
# Model of Computation

- Consists of rounds
- Each round has two phases
- Global snapshot (Phase 1)
- Arbitrary enabled calls (Phase 2)
- Special timeout call

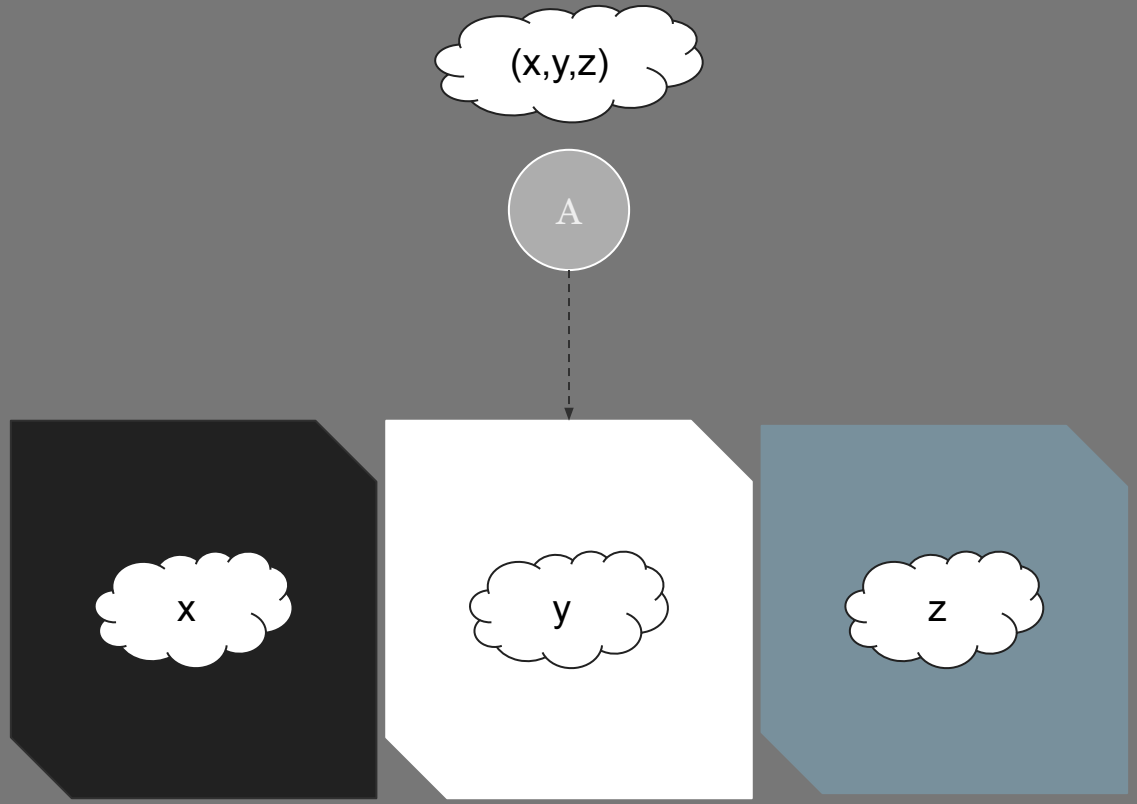
# Model of Computation (Snapshot)

# Model of Computation (Enabled calls)



# Model of Computation (Timeouts)



# Protocols

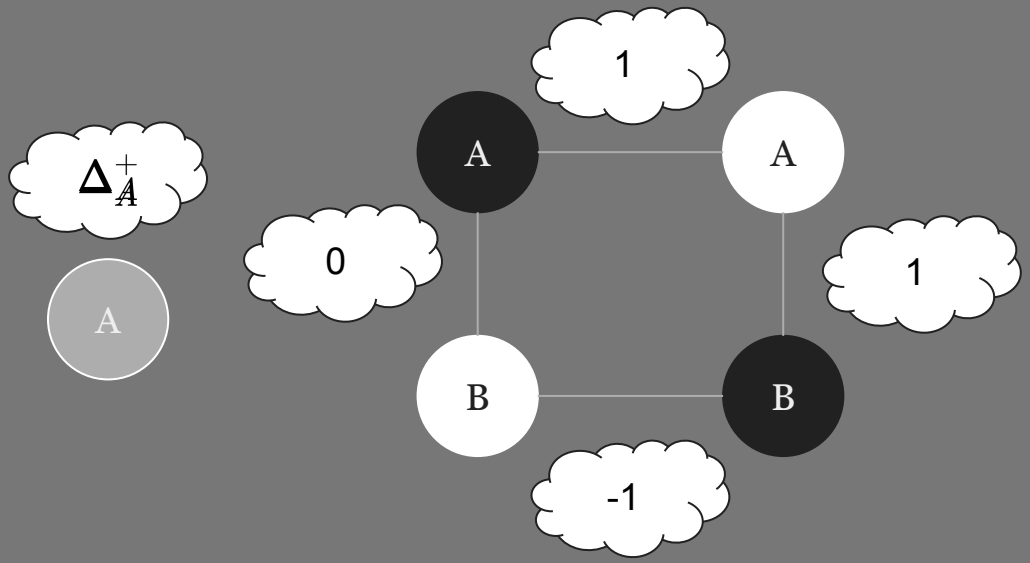
- One enabled call on each contract per round
- Compliant if party follows protocol
- Deviating if not

# Combinatorial Model

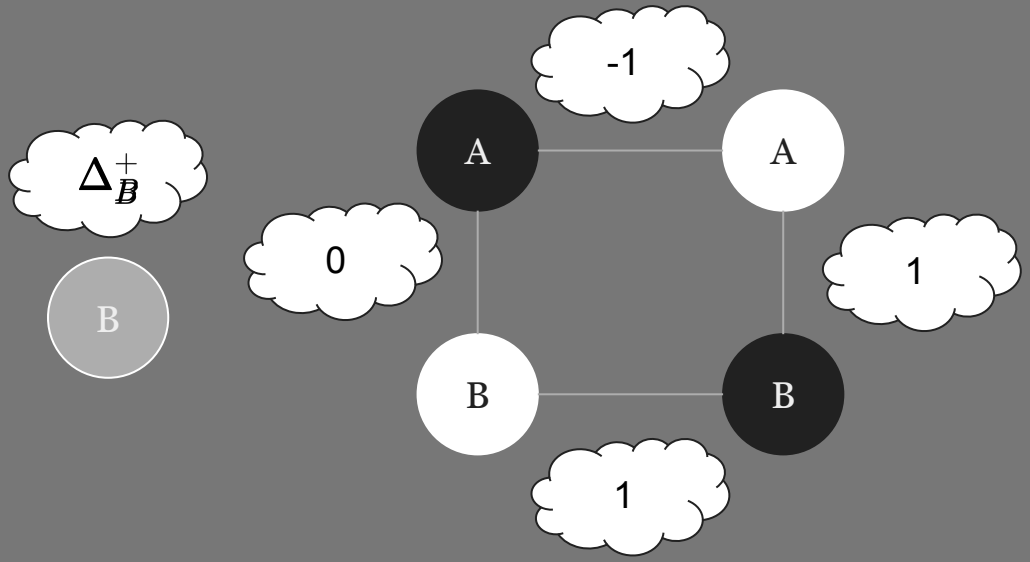
# Combinatorial Model

- Useful in classical distributed computing
- Used for impossibility/lower bounds
- Easy to modify safety notion
- Can compare power of sync primitives

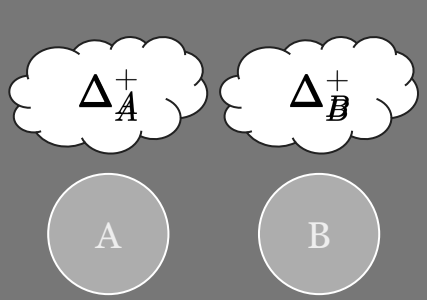
# An Example (Alice)

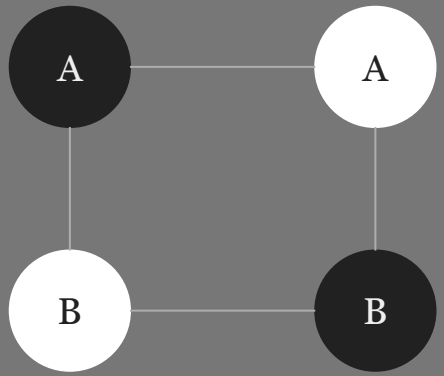


# An Example (Bob)

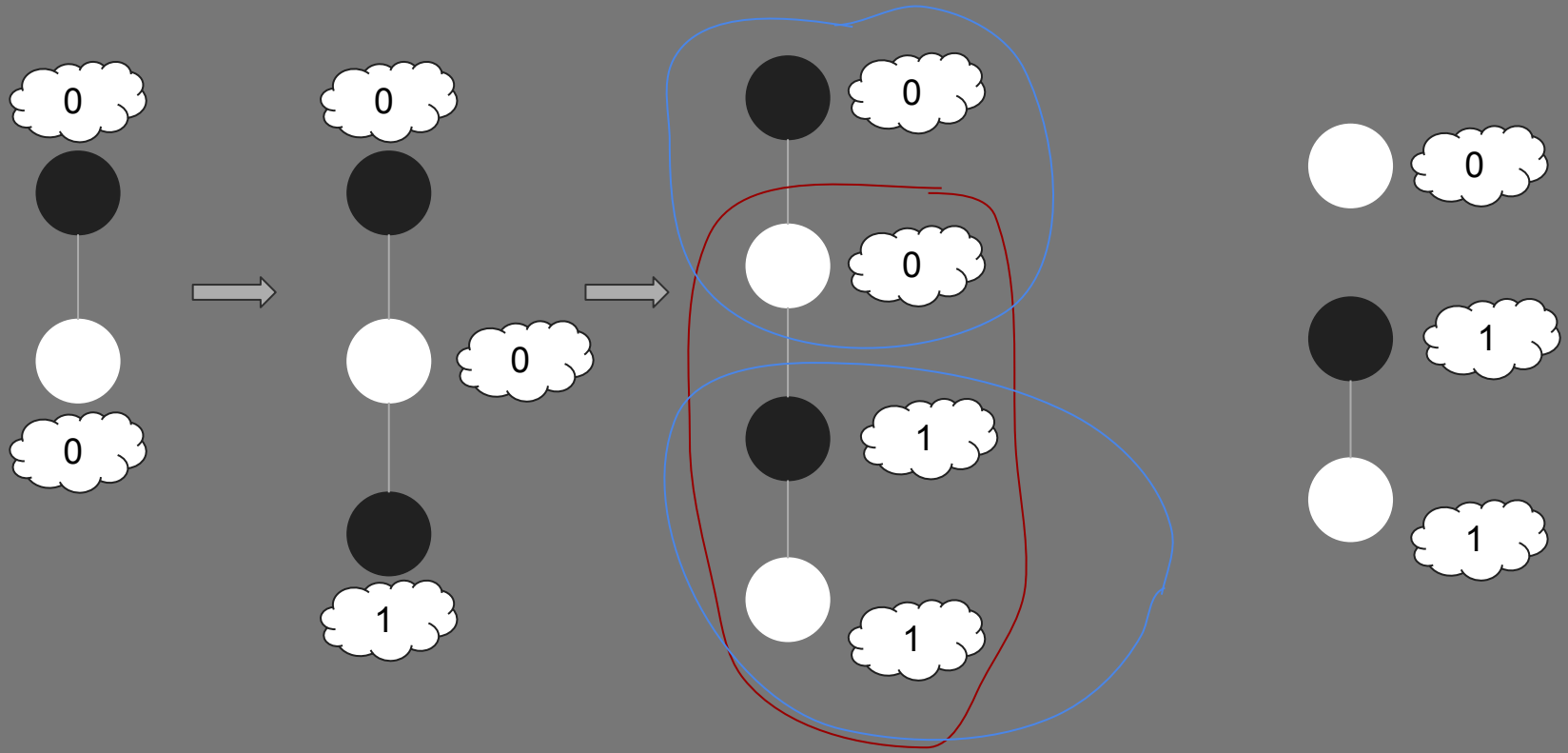


# An Example (Alice & Bob)

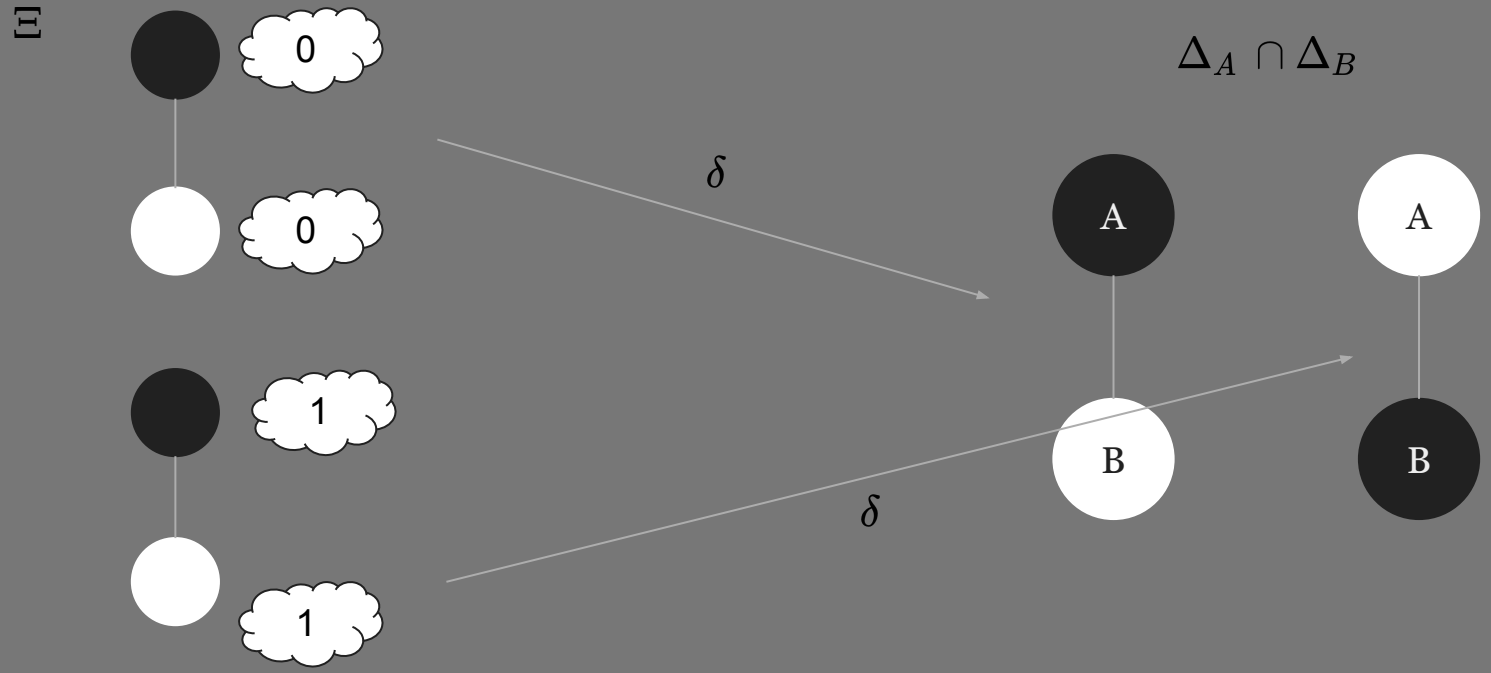


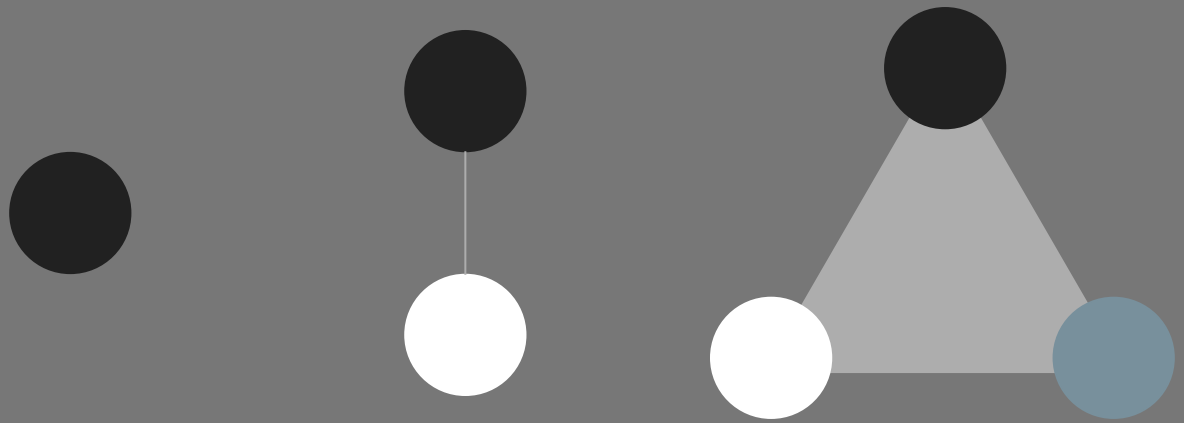
# An Example (Execution Graph)



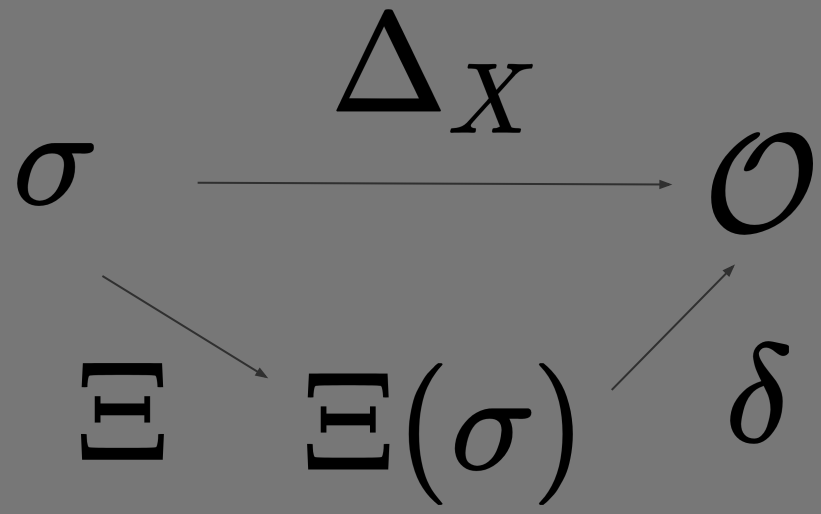
# An Example (Solvability)



# Higher Dimensional Analogs



# Generally



# Safety

$$\delta(\mathcal{P}_{\mathrm{P}}(\sigma)) \subseteq \Delta_{\mathrm{P}}(\sigma)$$

# Liveness

$$\delta\left(\cap_{P \in \mathbb{P}} \mathcal{P}_{\mathrm{P}}(\sigma)\right) \subseteq \Delta^{+}_{\mathrm{P}}(\sigma)$$

# Applications of Model

# Network attacks

- Thm: All hashlock protocols are vulnerable to a denial of service attack
- Argument uses fact that deal is disconnected
- Explains value of watchtowers

# Removing Hash locks

- Without hashlocks, complex is connected
- Can’t solve a disconnected deal

# Summary

- Two equivalent synchronous models
- Hashlock protocols and DOS
- Possibility questions are topological ones

# Ongoing and Future Extensions

- When exactly do simple hash locks fail?
- Partially synchronous setting
- Cross-chain proofs

Thank you

# Questions?

Contact Info:
daniel_engel1@brown.edu