

Cerberus Channels

Incentivizing Watchtowers for Bitcoin

Zeta Avarikioti

Orfeas Thyfronitis-Litos

Roger Wattenhofer



Payment Channels



Payment Channels



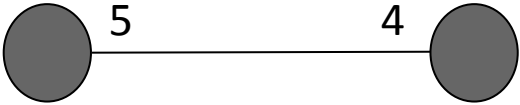
Funding transaction



Payment Channels



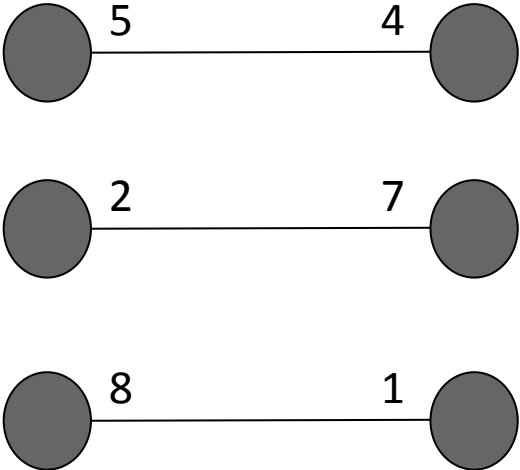
Commitment transaction 



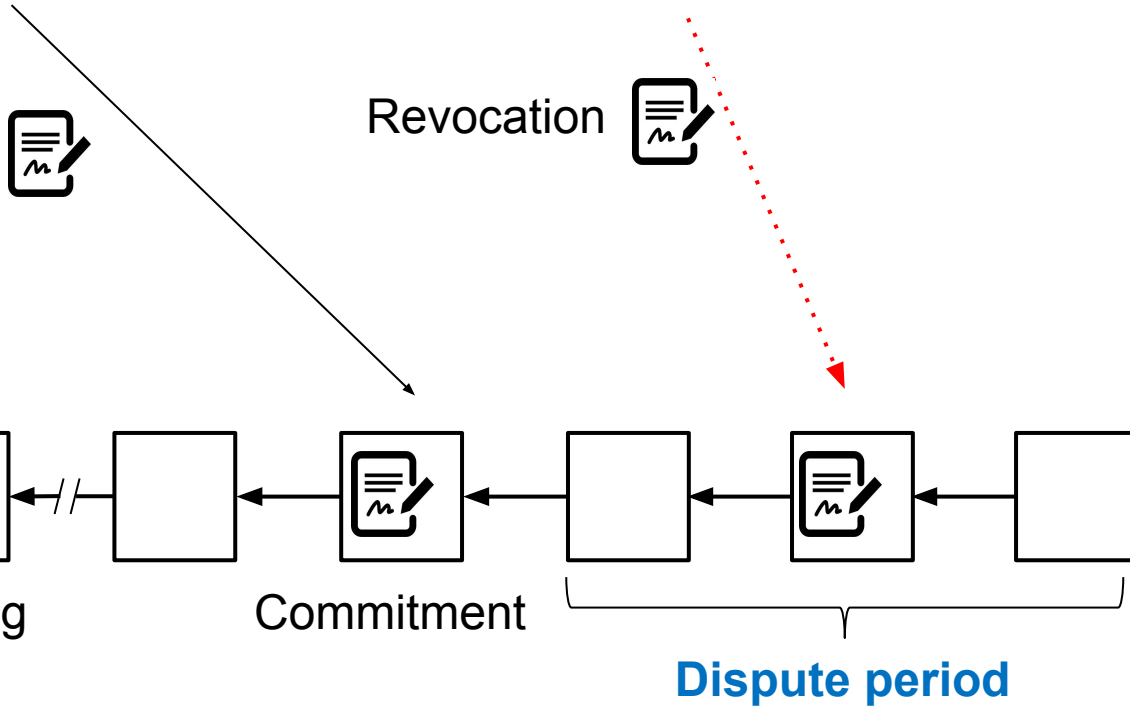
Payment Channels



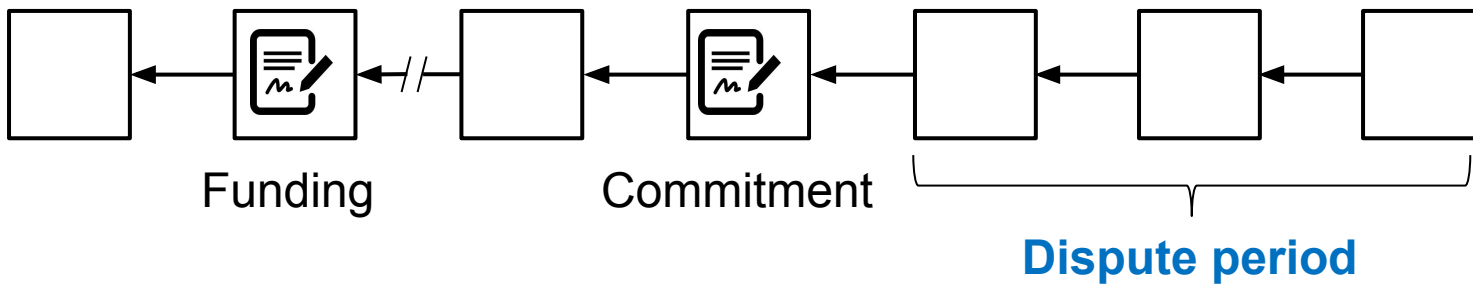
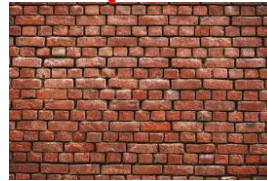
Commitment transaction 



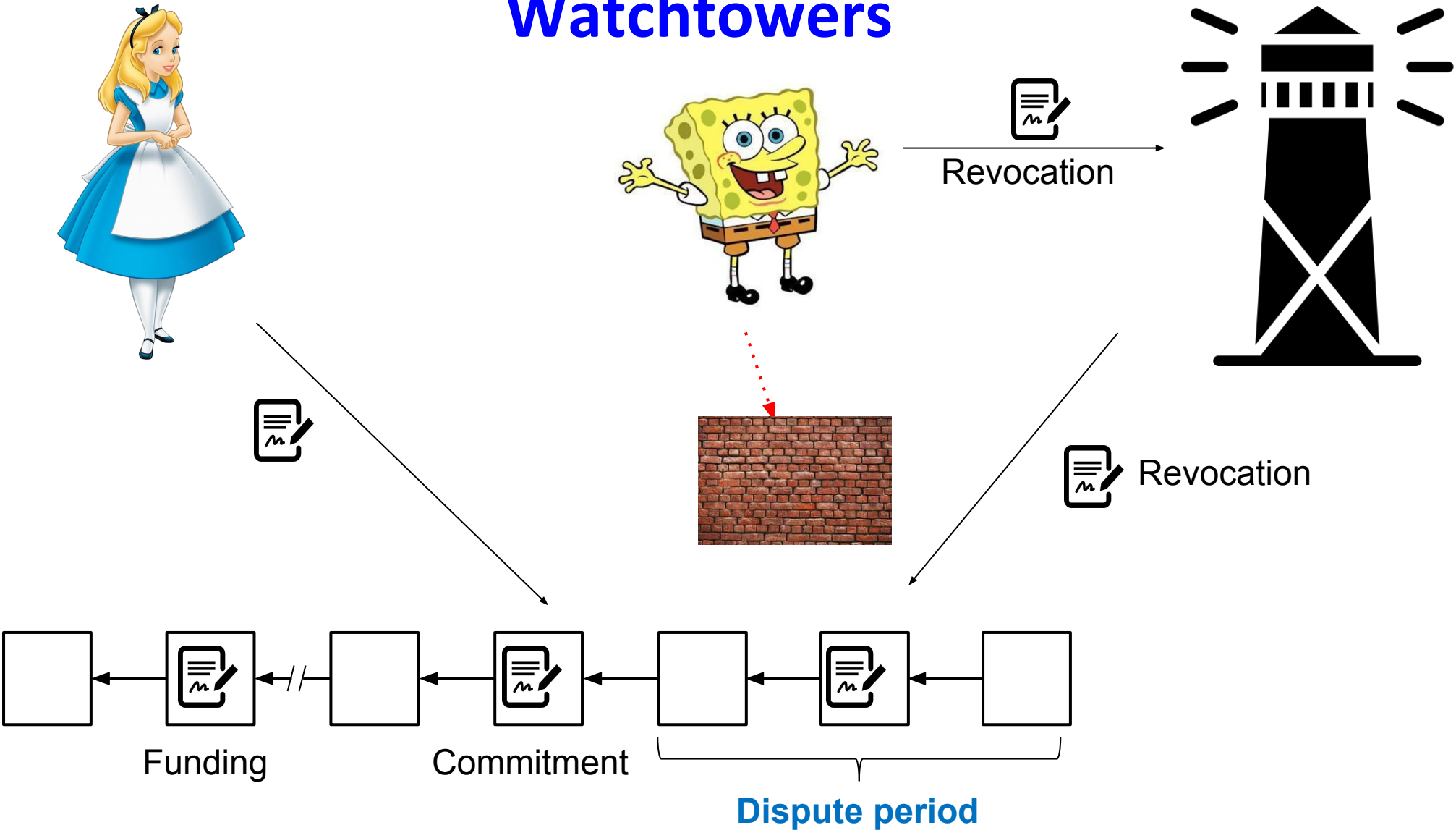
Lightning Channels



Attack



Watchtowers










Why be a Watchtower?

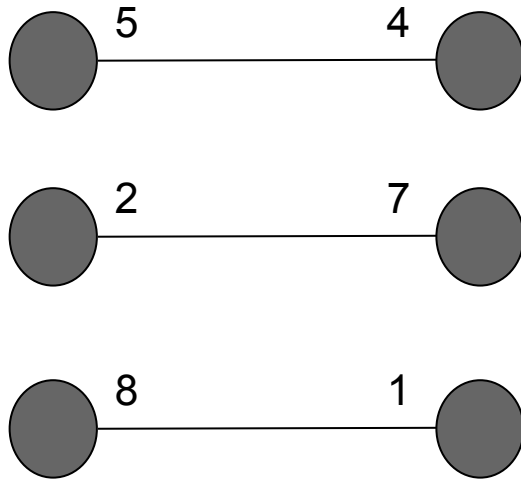


Why be a Watchtower?

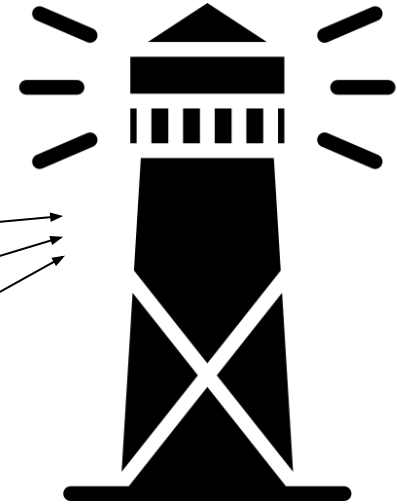
Assuming rational parties and watchtowers...

- Will a party commit fraud? 
- Will a watchtower get paid? 
- Will there be a watchtower? 
- Will a party commit fraud? 
- Will a watchtower get paid? 
- Will there be a watchtower? 
- Will a party commit fraud? ... 

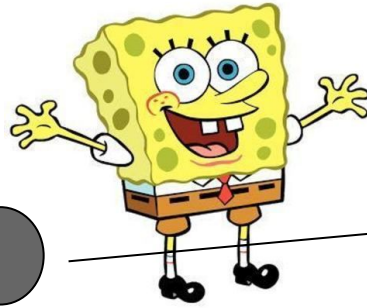
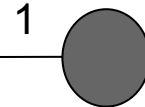
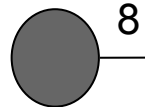
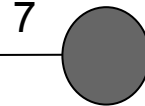
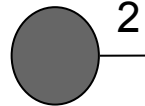
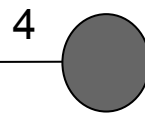
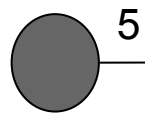
Per-update premiums?



0.01
0.01
0.01



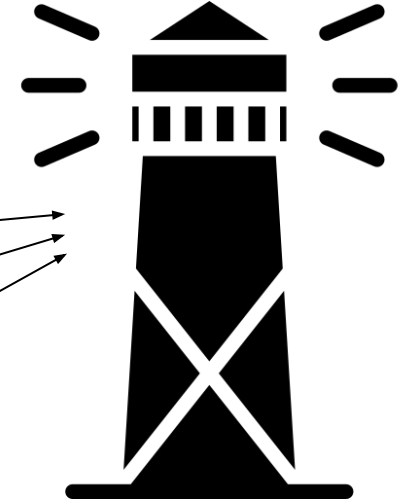
Per-update premiums?



0.01

0.01

0.01



Watchtower paid even if **inactive!**
No incentive to watch chain

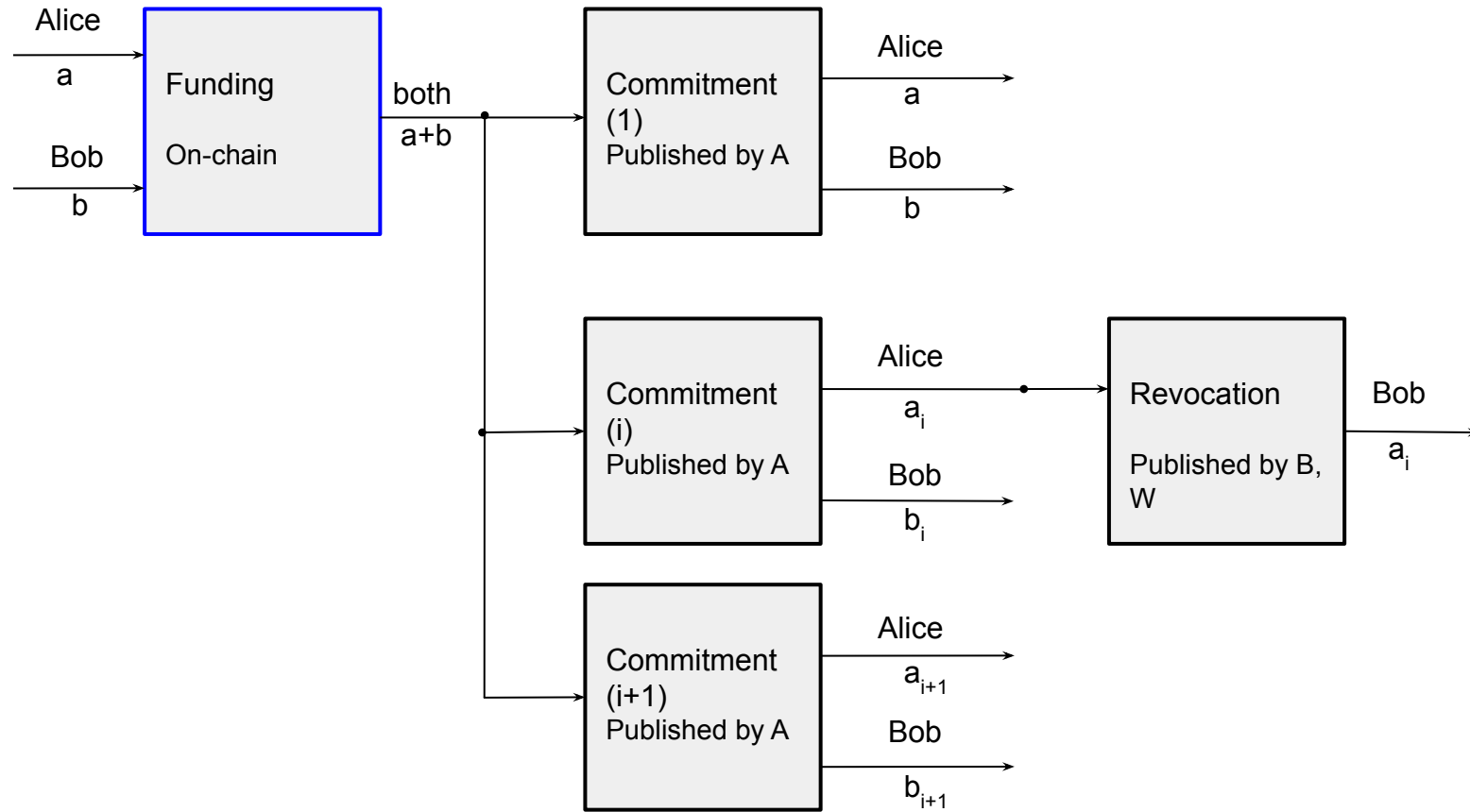
Why be an **active** Watchtower?



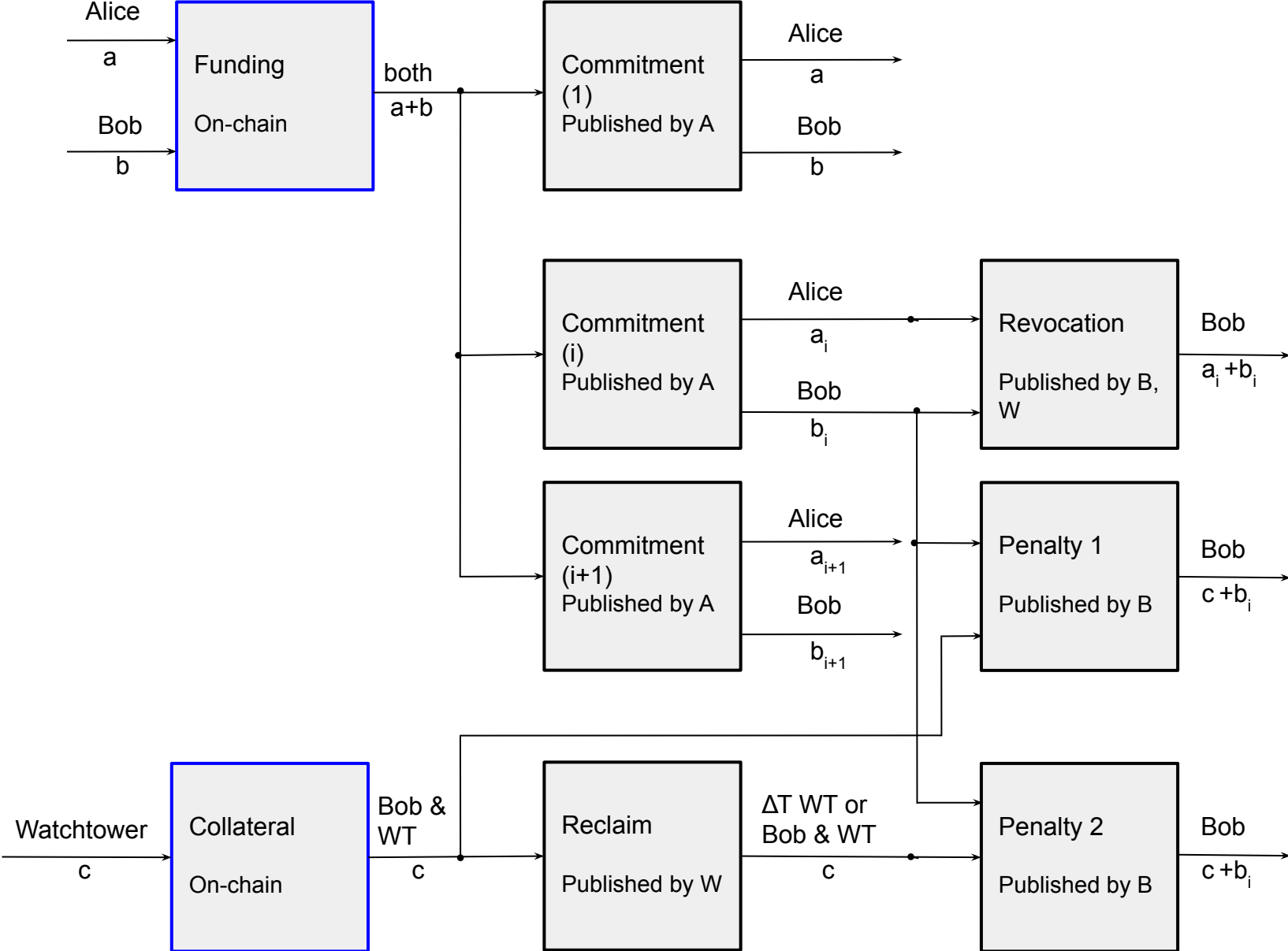
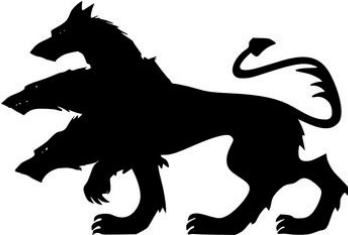
Collateral!



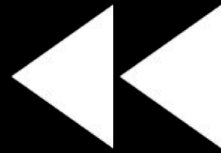
Lightning Channels



Cerberus Channels

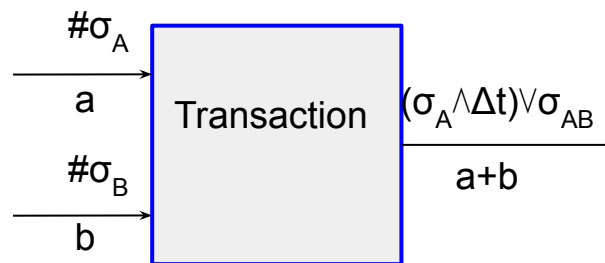


Lightning Channels

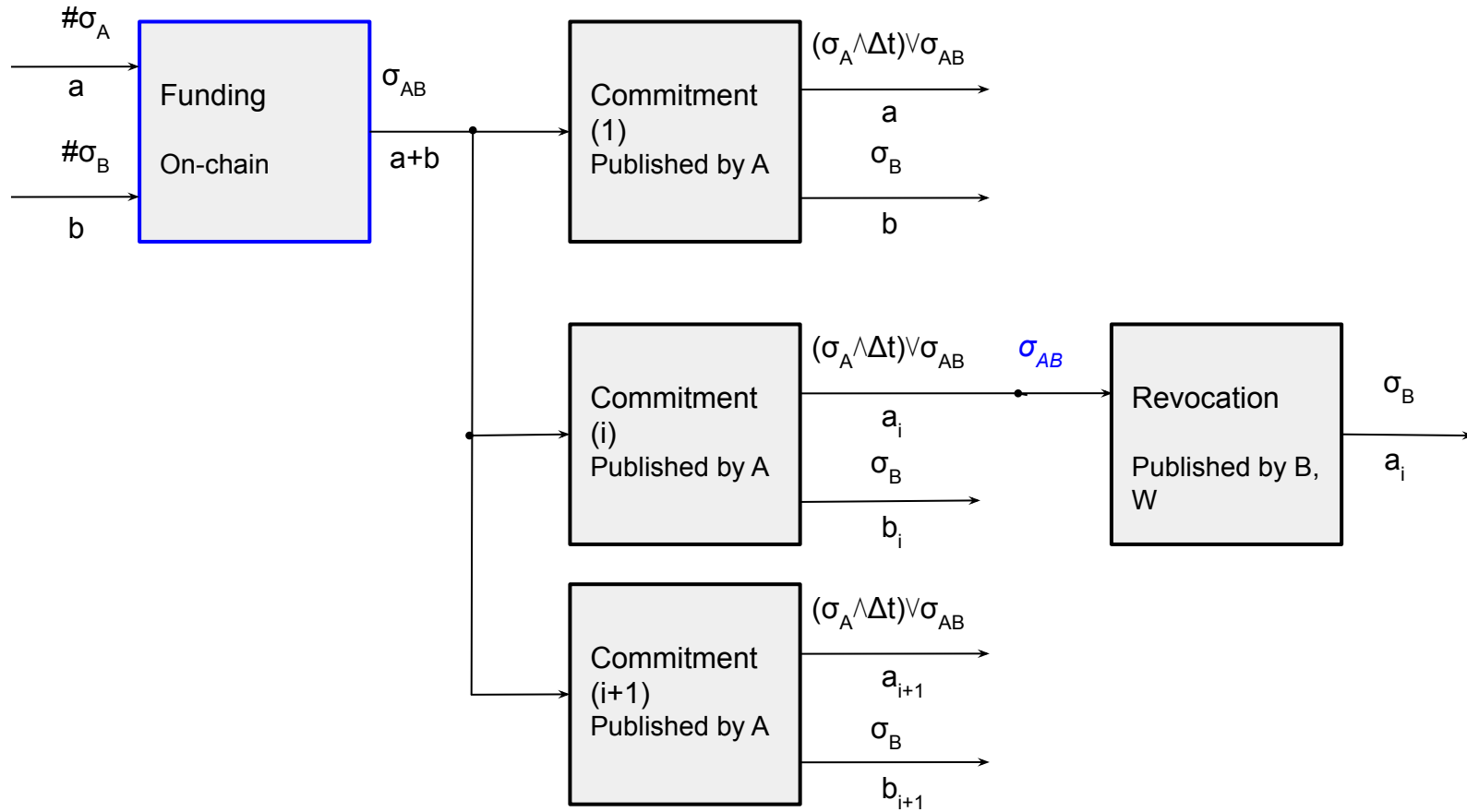


Notation

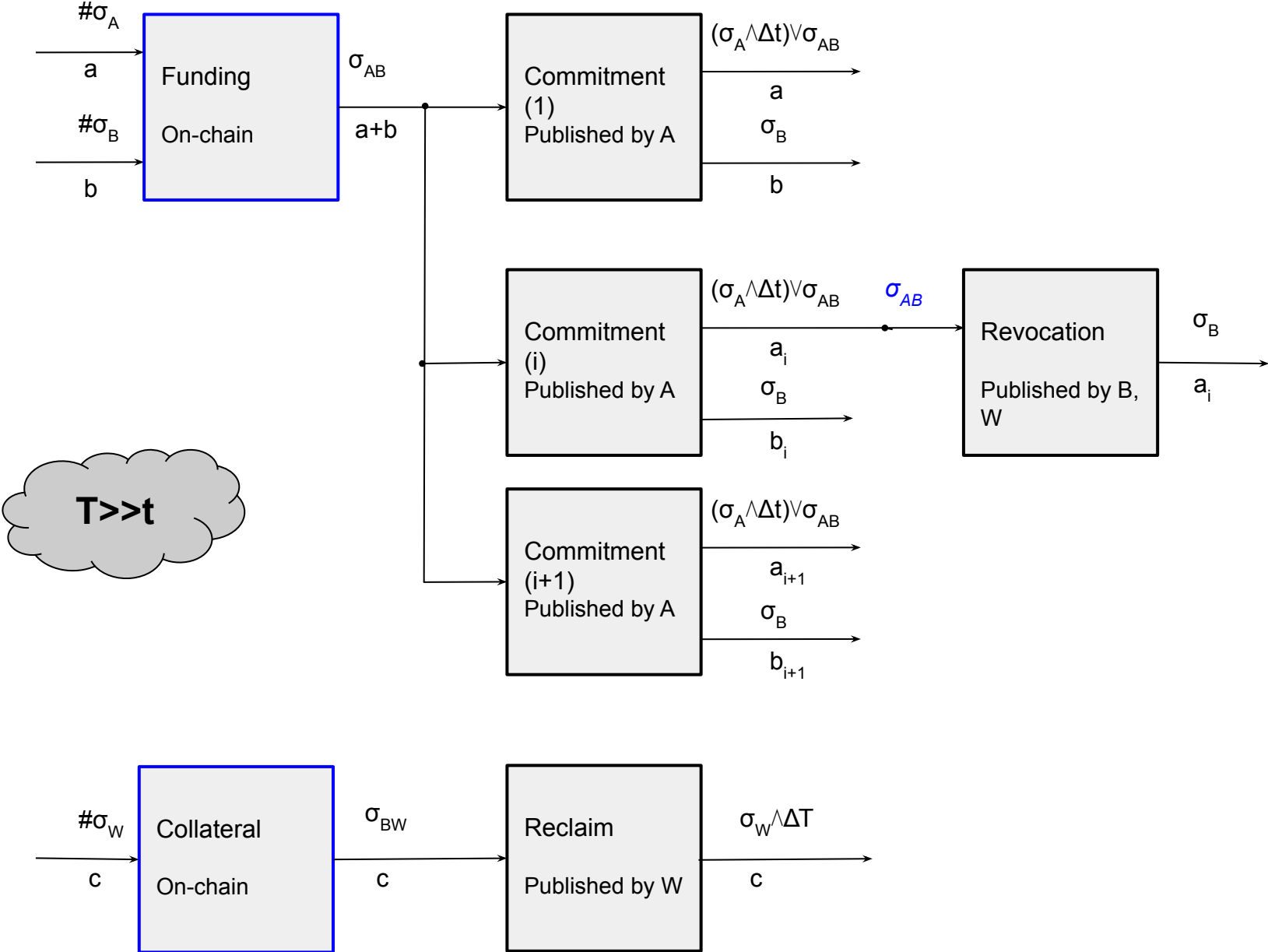
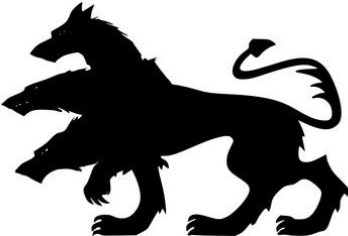
- Multi-signatures: σ_{AB}
- Timelocks: Δt
- AND \wedge , OR \vee



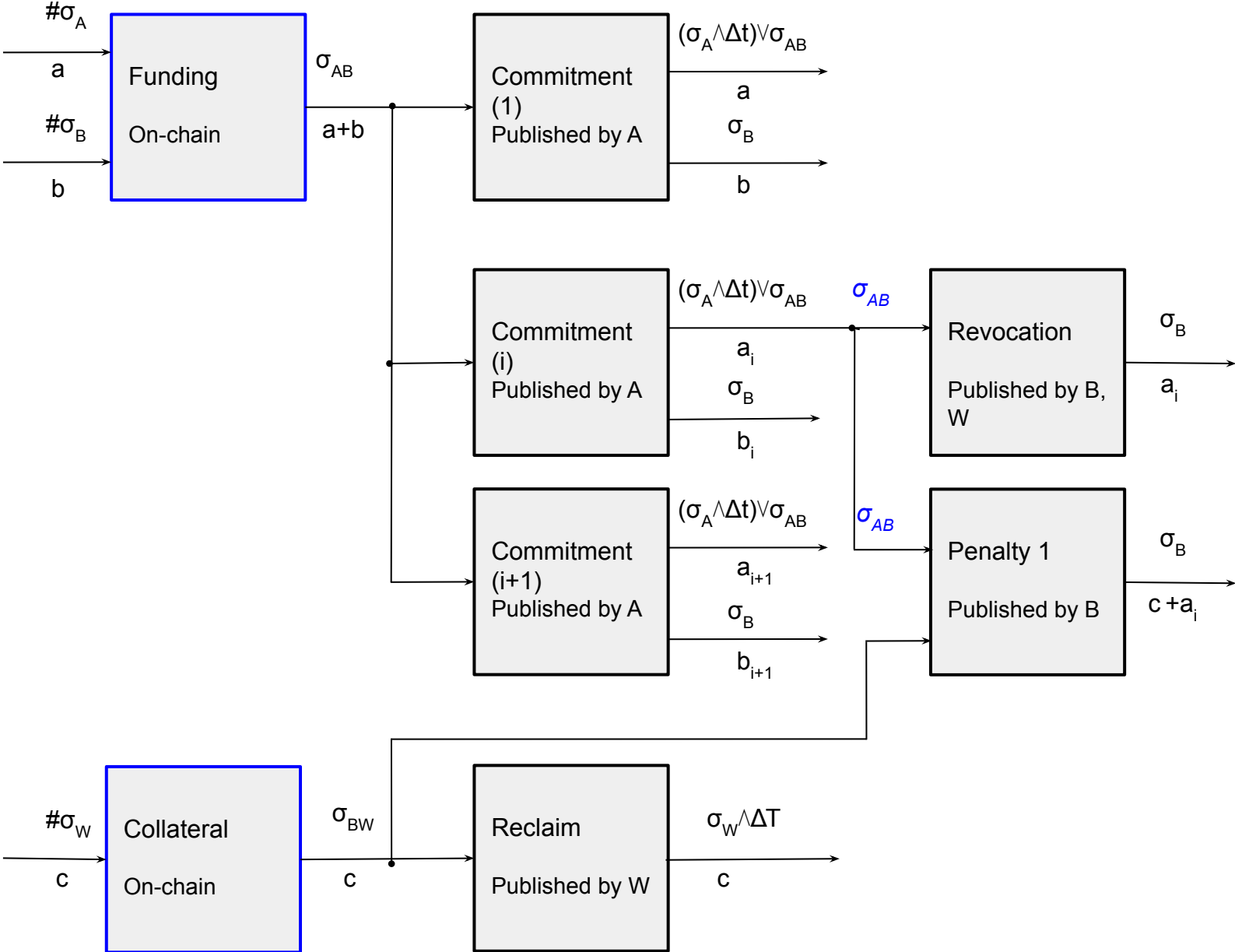
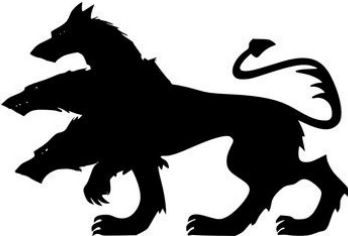
Lightning Channels



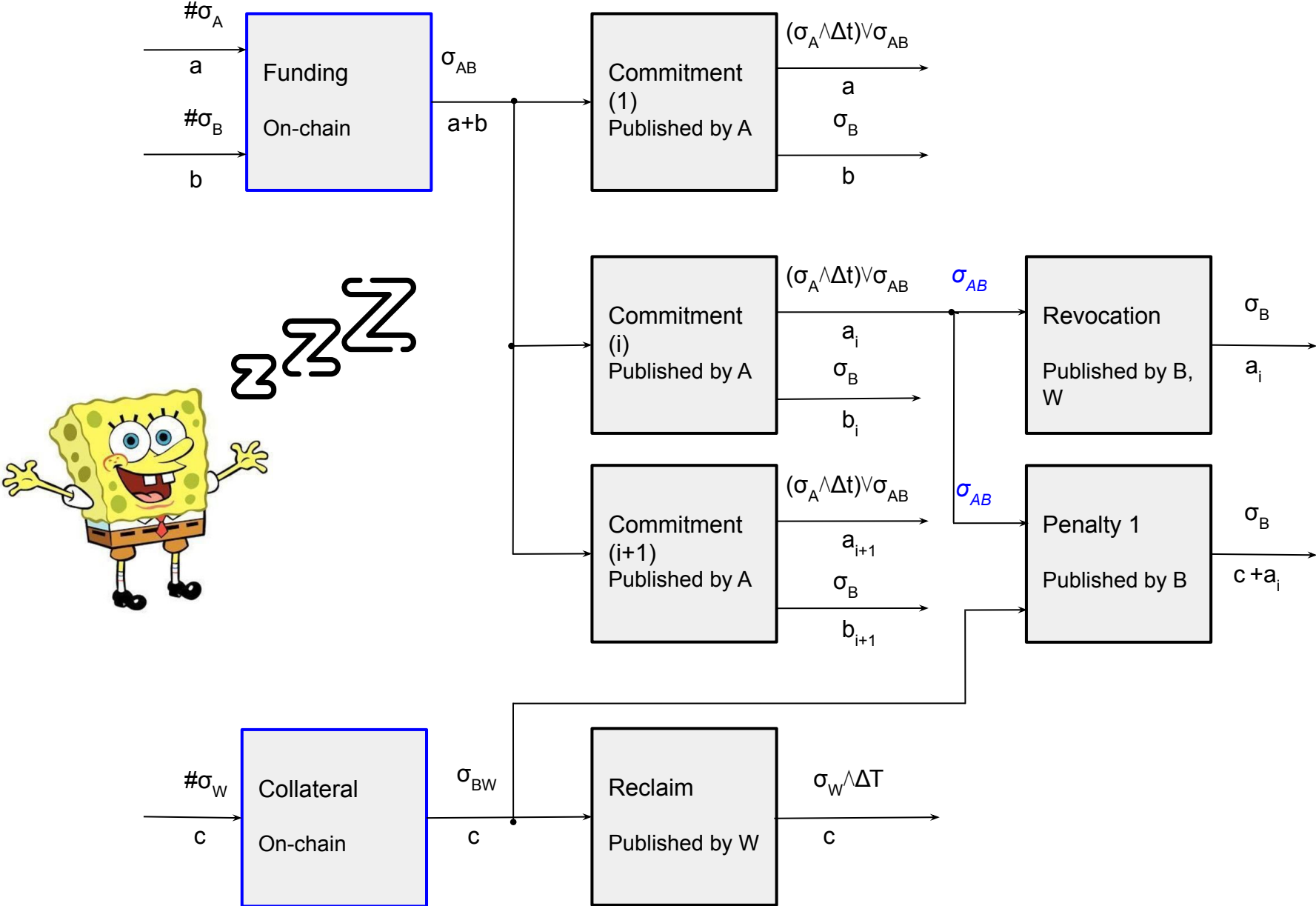
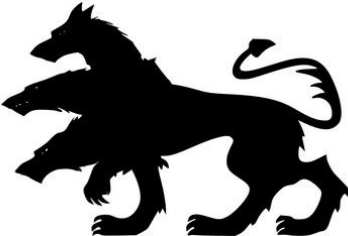
Cerberus Channels



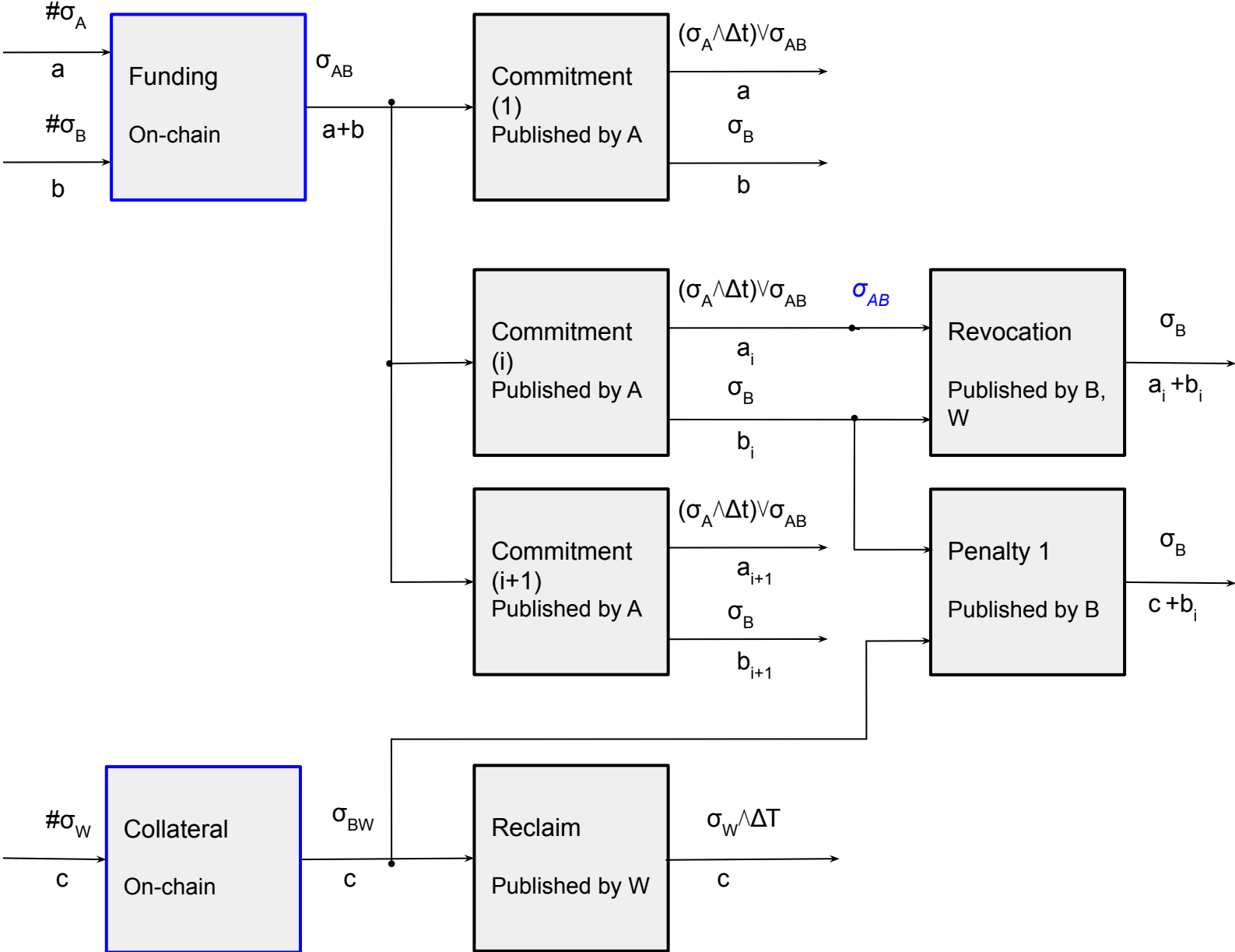
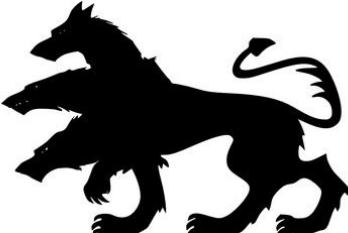
Cerberus Channels



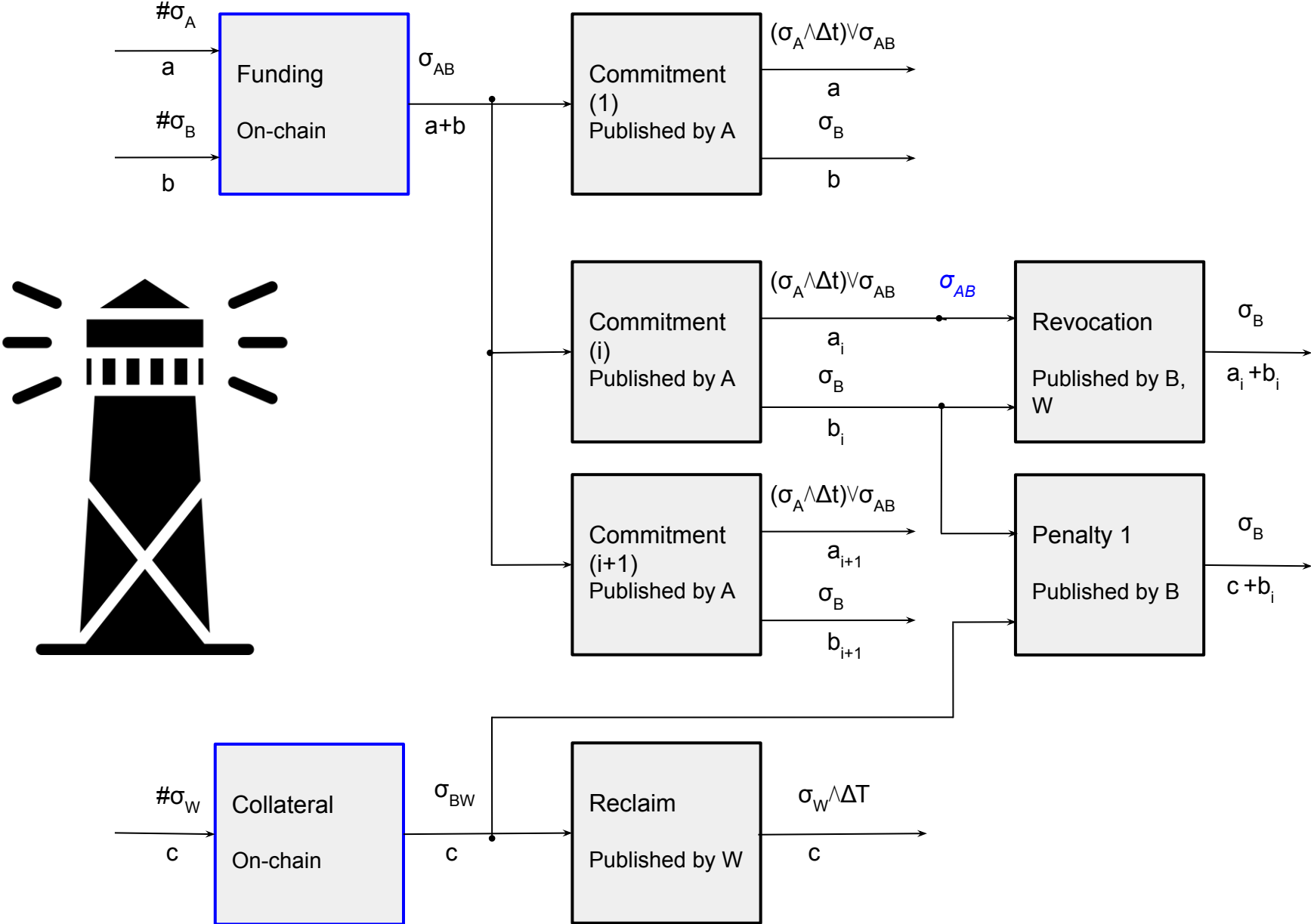
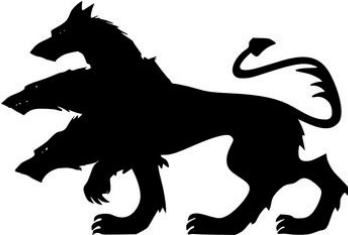
Cerberus Channels



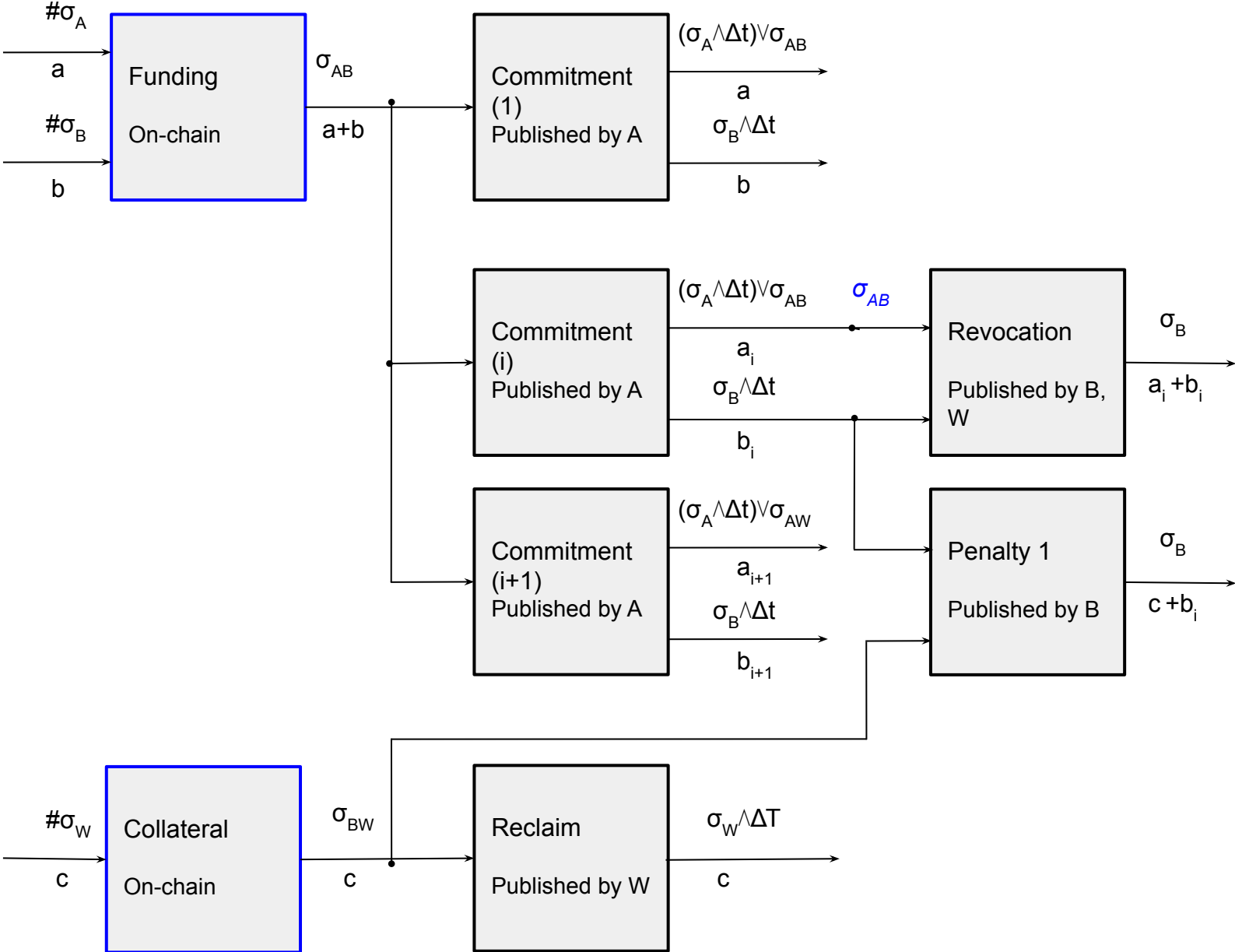
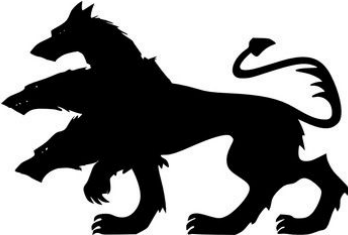
Cerberus Channels



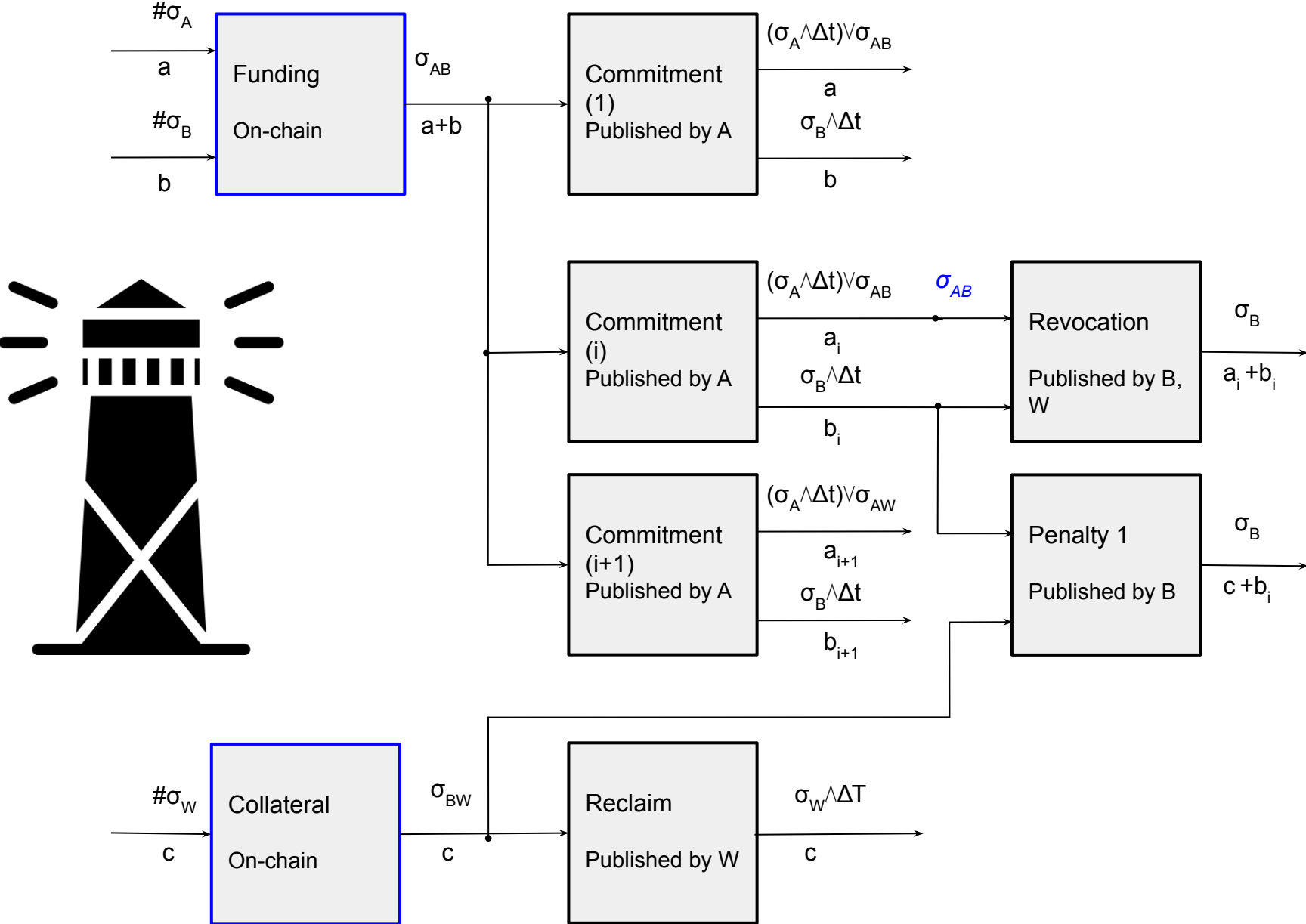
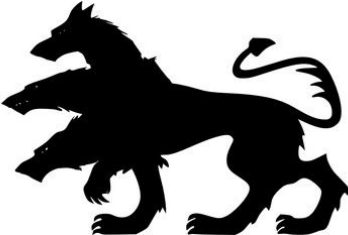
Cerberus Channels



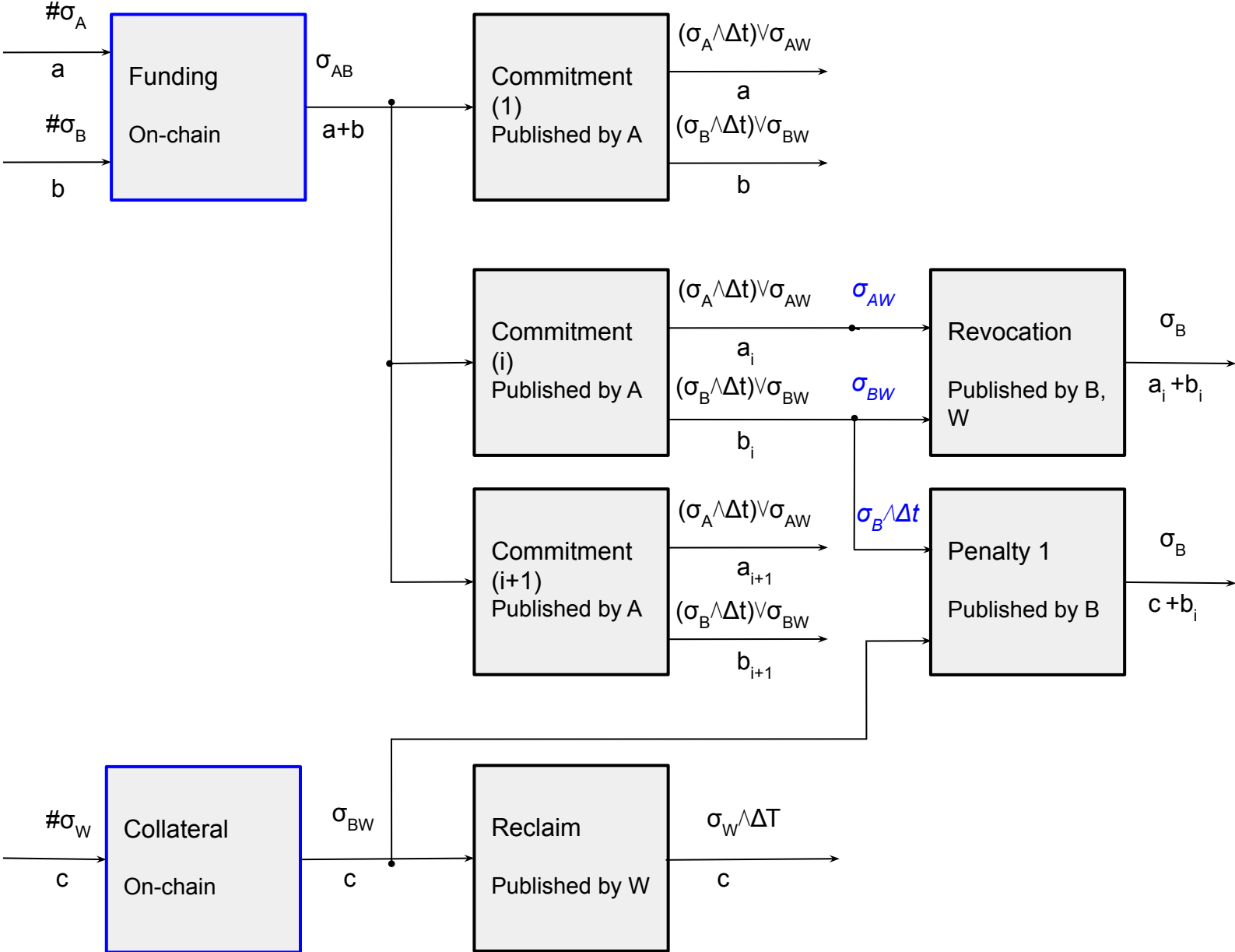
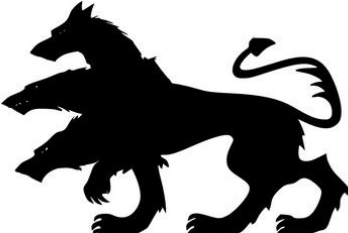
Cerberus Channels



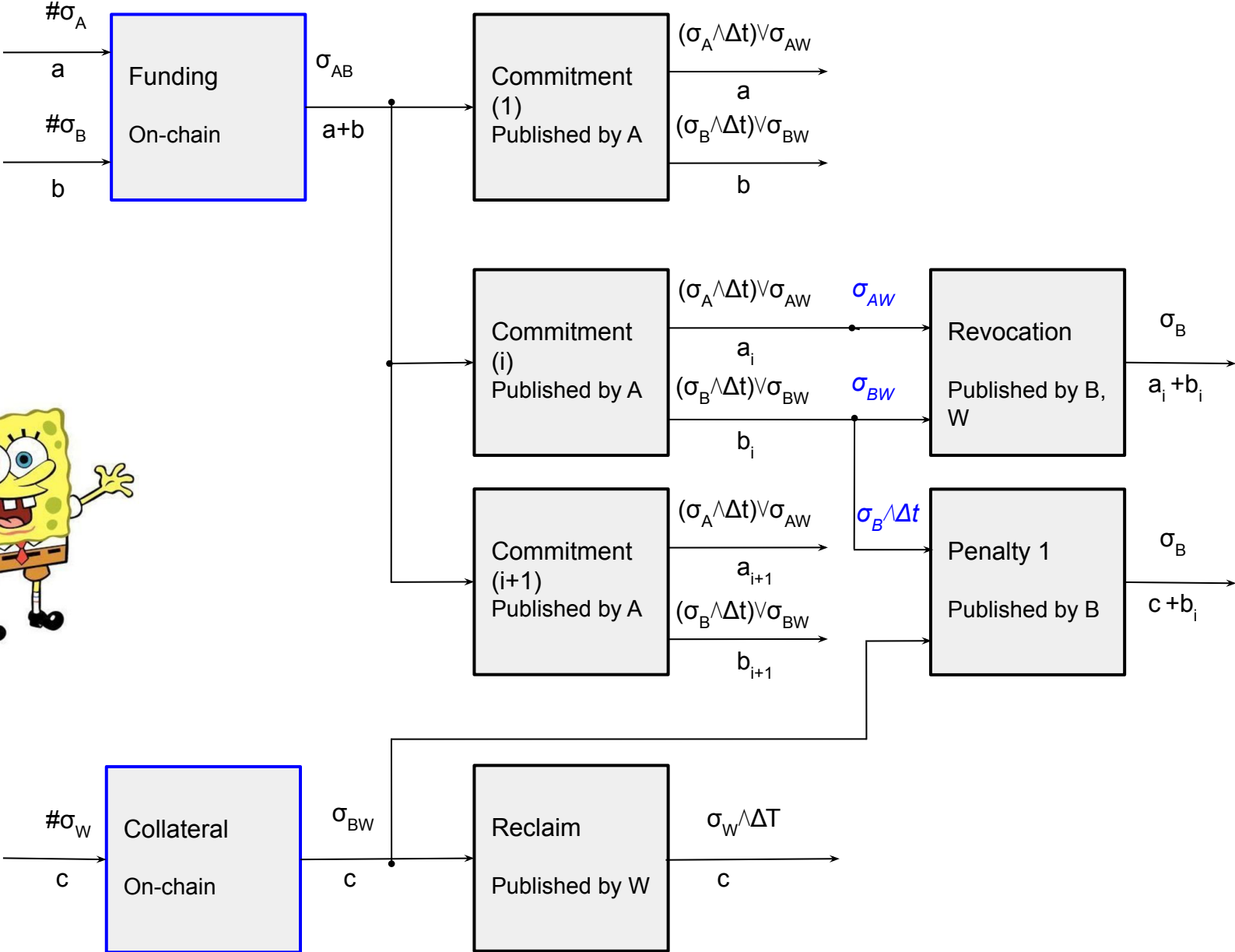
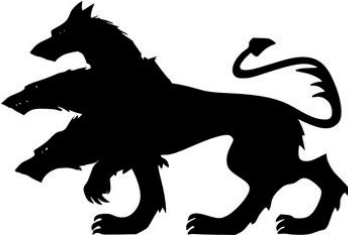
Cerberus Channels



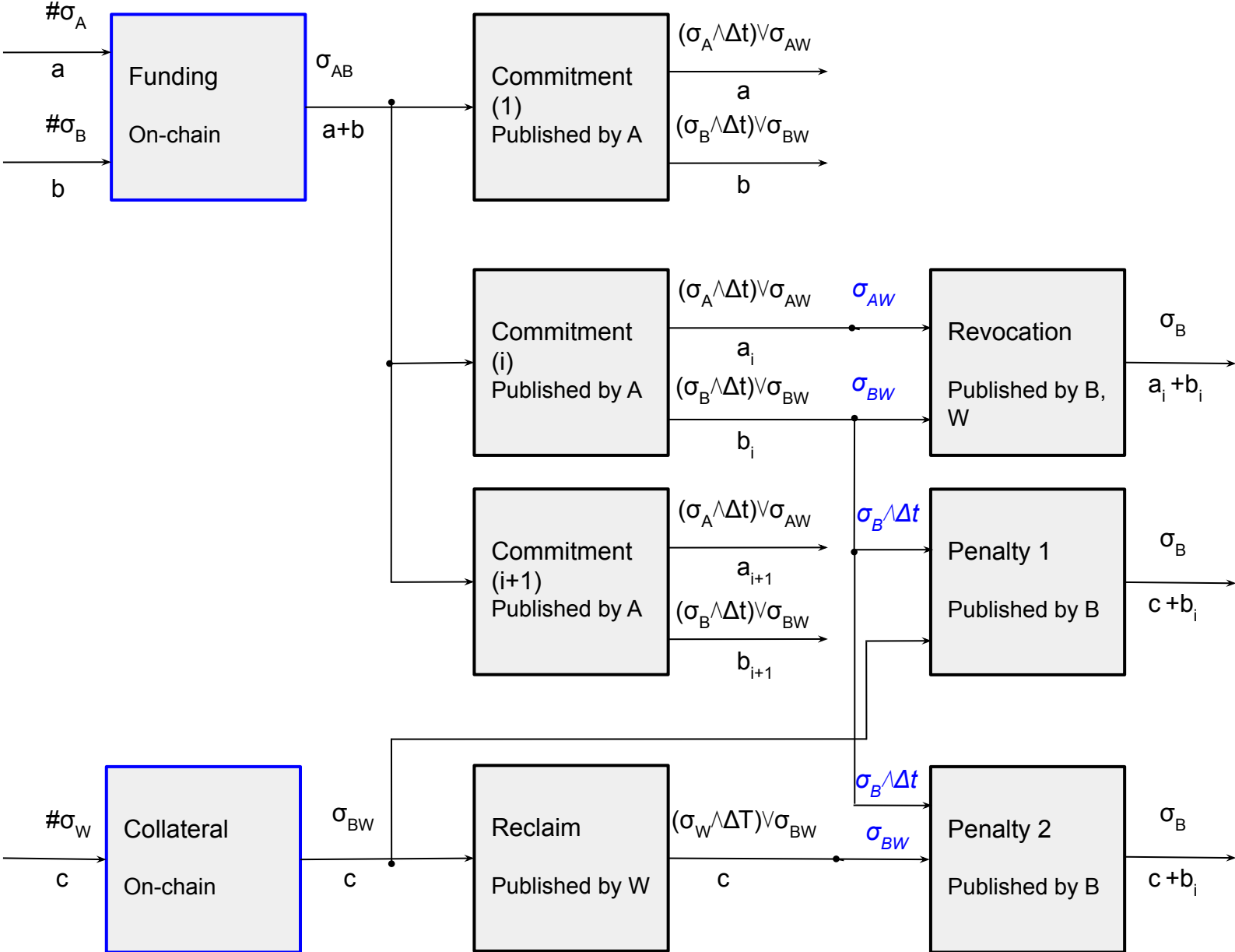
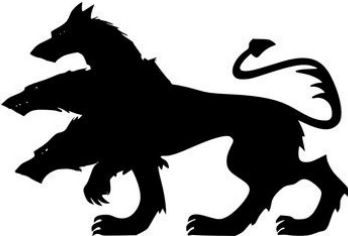
Cerberus Channels



Cerberus Channels



Cerberus Channels



Cerberus Channels

- **Incentive-compatible solution**
- **Extended offline period for channel party**
- **WTs can withdraw the service**
- **Bitcoin PoC implementation**
- **Limitations:**
 - **Privacy**
 - **Synchrony - Timelocks**

Thank you!

Questions?

