Payment Channels

Designing Secure Watchtowers

Why be a Watchtower?

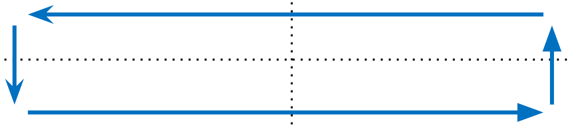
Why be a Watchtower?

Assuming rational parties and watchtowers…

- Will a party commit fraud? ✗
- Will a watchtower get paid? ✗
- Will a party commit fraud? ✓
- Will a watchtower get paid? ✓
- Will a party commit fraud? ... ✗

Why be a Watchtower?

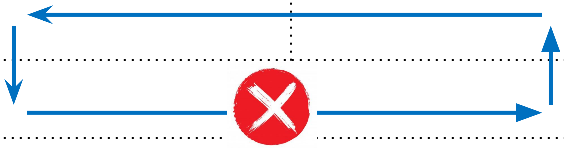
Watchtowers → Parties ↓	Active	Inactive
Fraud		
No Fraud		



Why be a Watchtower?

Premiums

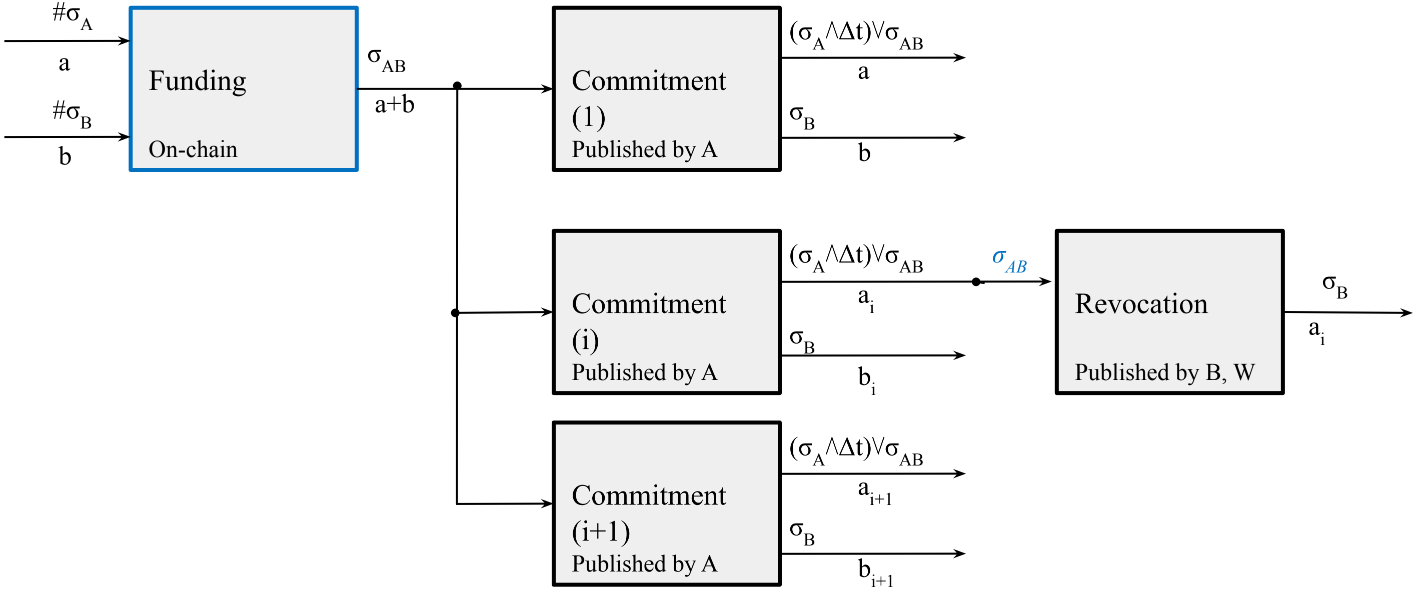
Watchtowers → Parties ↓	Active	Inactive
Fraud		
No Fraud		



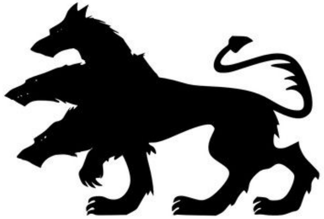
Why be an active Watchtower?

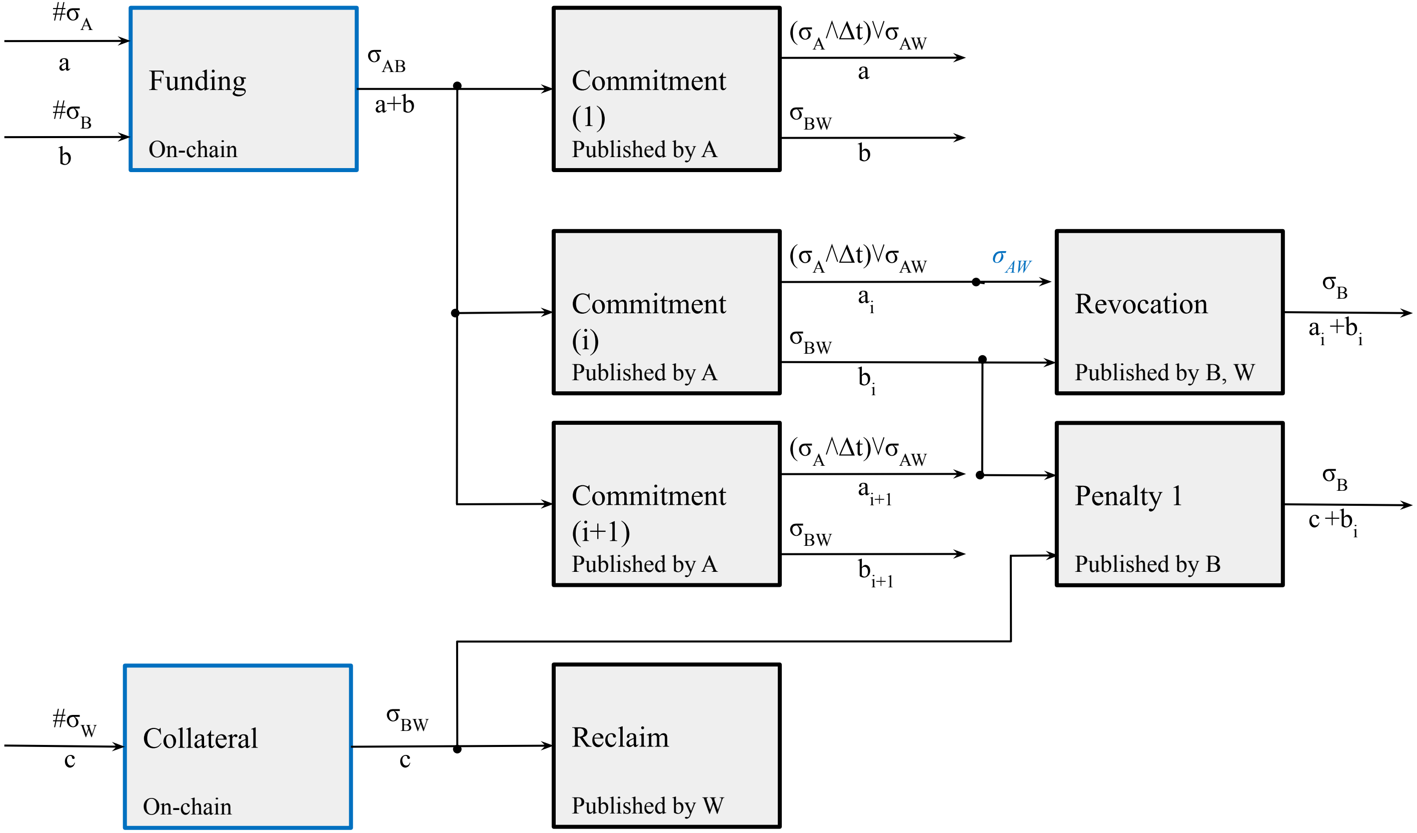
Collateral

Lightning Channels

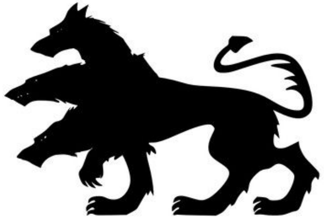


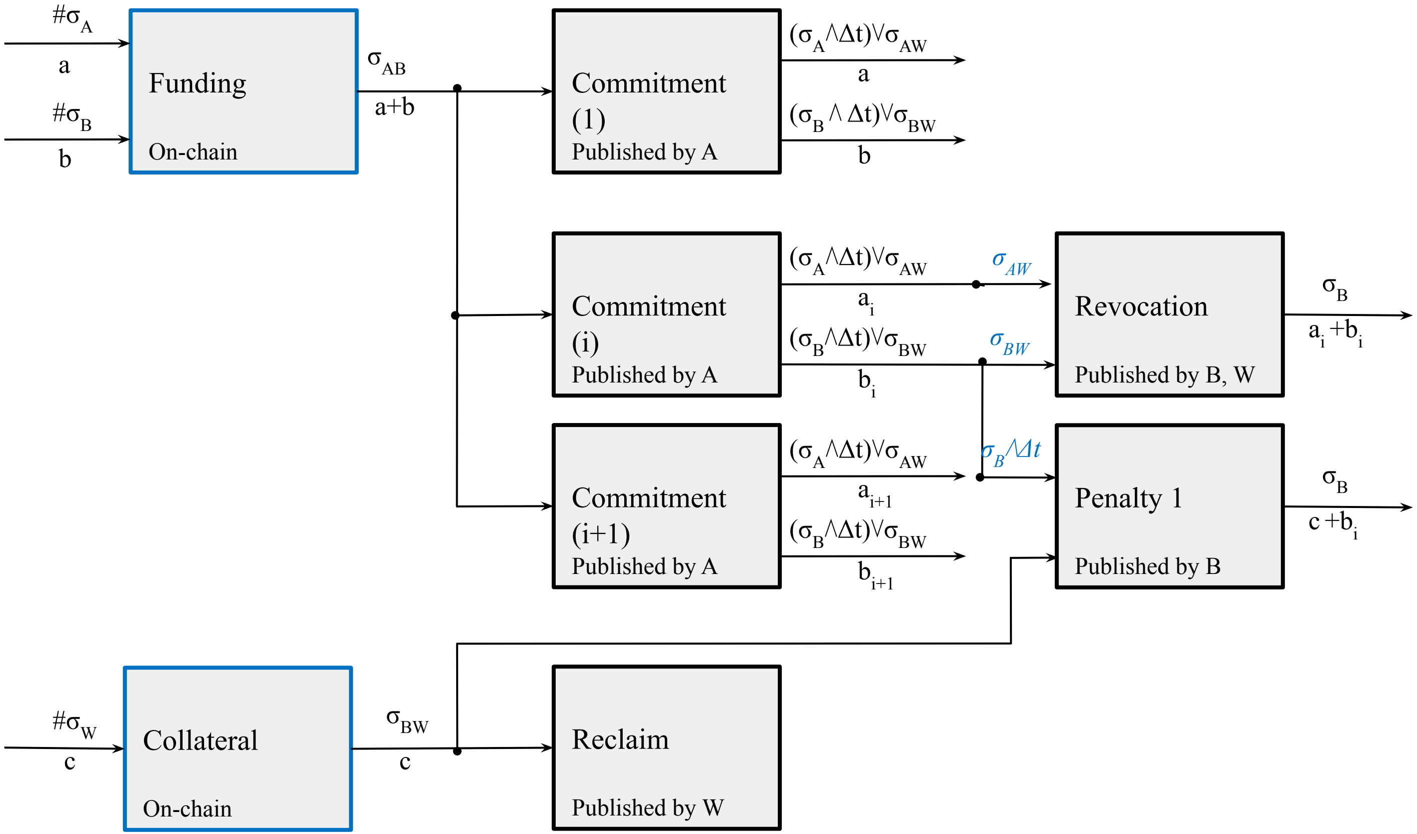
Cerberus Channels





Cerberus Channels





$\#\sigma_A$

a

$\#\sigma_B$

b

Funding

On-chain

σ_{AB}

a+b

Commitment (1)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b

Commitment (i)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a_i

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b_i

σ_{AW}

σ_{BW}

Revocation

Published by B, W

σ_B

$a_i + b_i$

Commitment (i+1)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a_{i+1}

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b_{i+1}

$\sigma_B \wedge \Delta t$

Penalty 1

Published by B

σ_B

$c + b_i$

$\#\sigma_W$

c

Collateral

On-chain

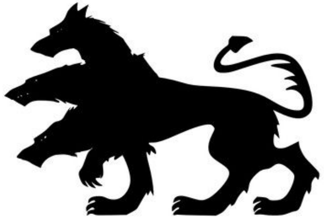
σ_{BW}

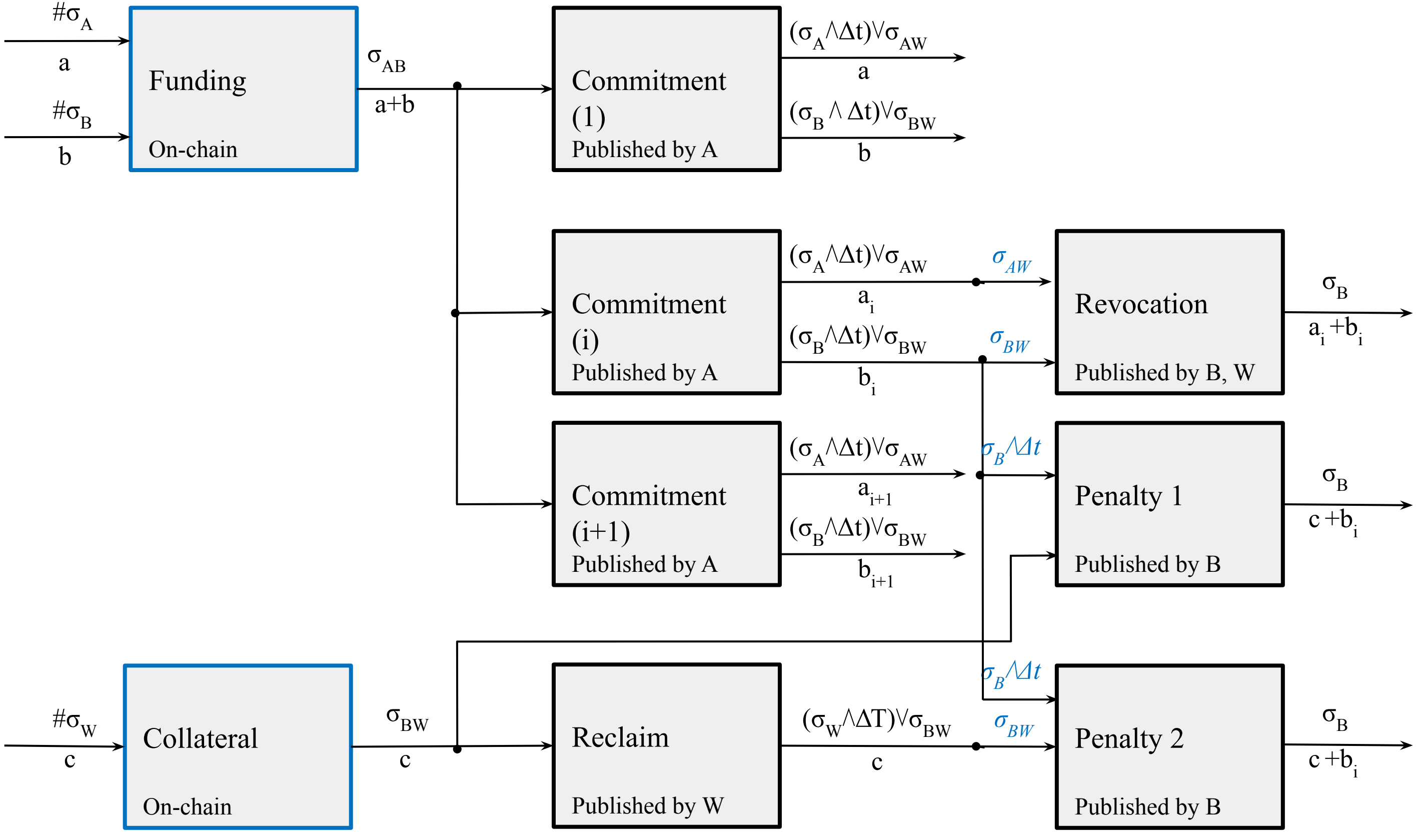
c

Reclaim

Published by W

Cerberus Channels





$\#\sigma_A$

a

$\#\sigma_B$

b

Funding

On-chain

σ_{AB}

a+b

Commitment (1)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b

Commitment (i)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a_i

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b_i

σ_{AW}

σ_{BW}

Revocation

Published by B, W

σ_B

$a_i + b_i$

Commitment (i+1)

Published by A

$(\sigma_A \wedge \Delta t) \vee \sigma_{AW}$

a_{i+1}

$(\sigma_B \wedge \Delta t) \vee \sigma_{BW}$

b_{i+1}

$\sigma_B \wedge \Delta t$

Penalty 1

Published by B

σ_B

$c + b_i$

$\#\sigma_W$

c

Collateral

On-chain

σ_{BW}

c

Reclaim

Published by W

$(\sigma_W \wedge \Delta T) \vee \sigma_{BW}$

c

$\sigma_B \wedge \Delta t$

σ_{BW}

Penalty 2

Published by B

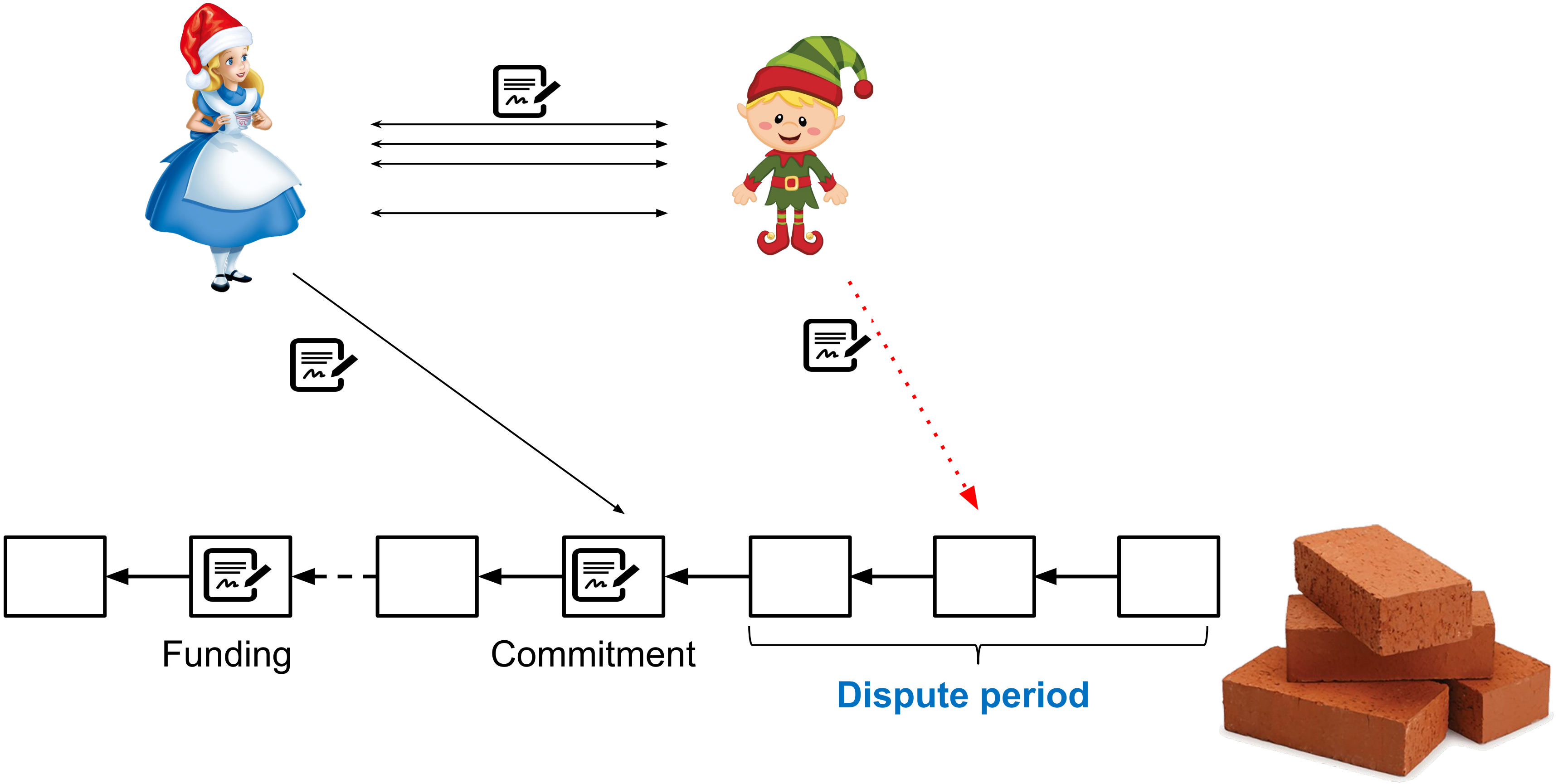
σ_B

$c + b_i$

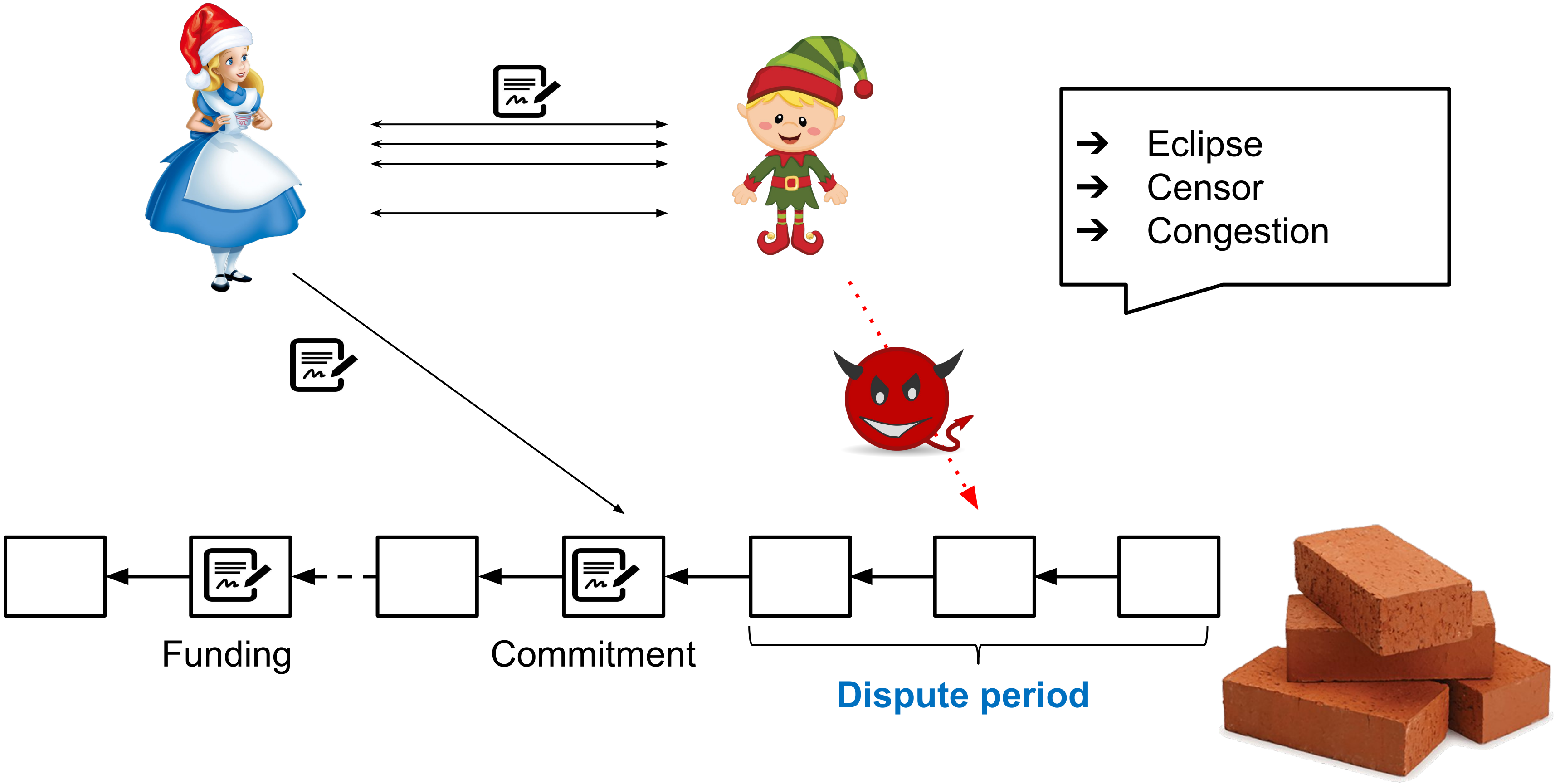
Fundamentals of Channels

⏪

Fundamentals of Channels



Attacks



→ Eclipse
→ Censor
→ Congestion

Funding

Commitment

Dispute period

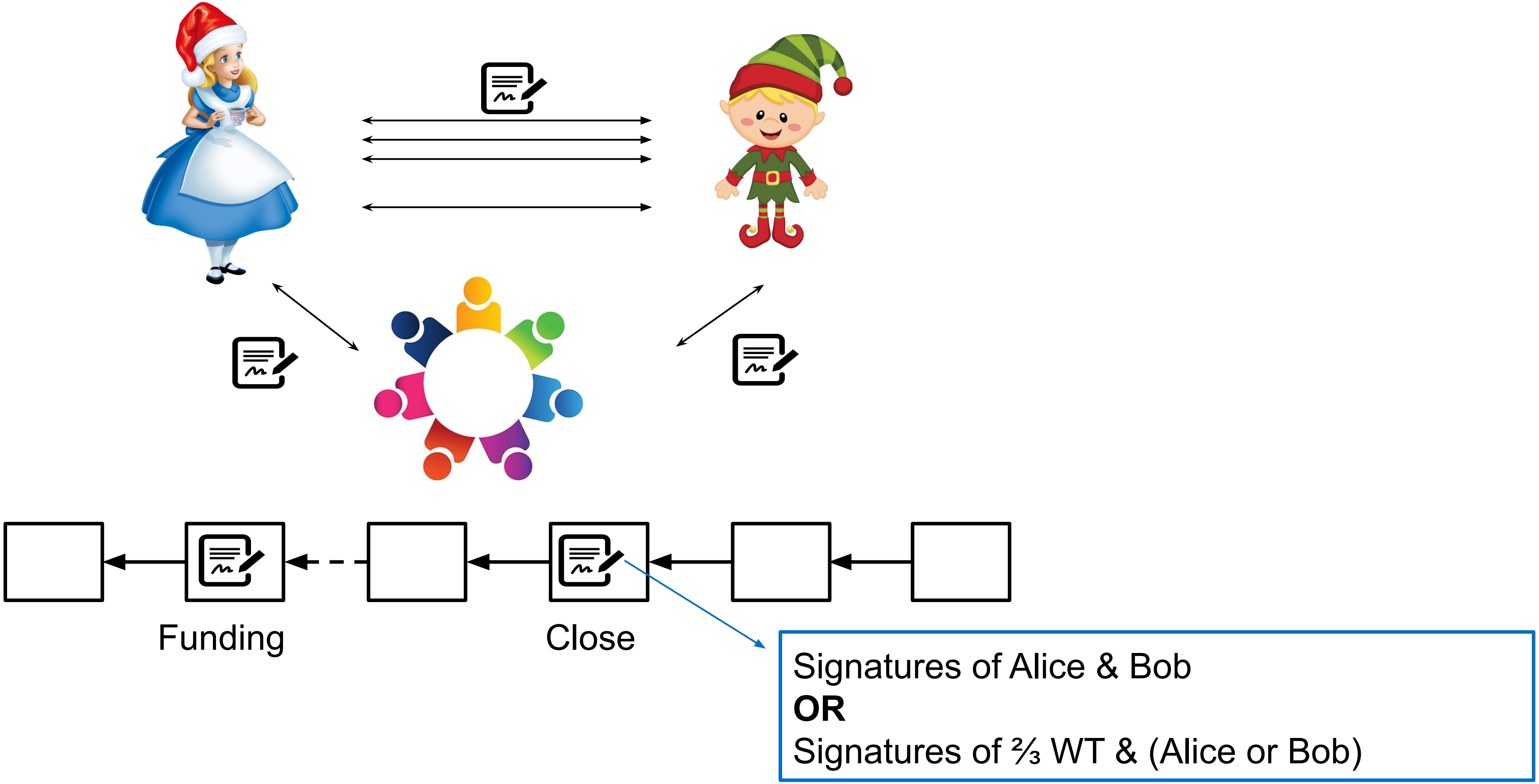
Time = CryptoMoney!

Time = CryptoMoney!

Asynchronous channels?

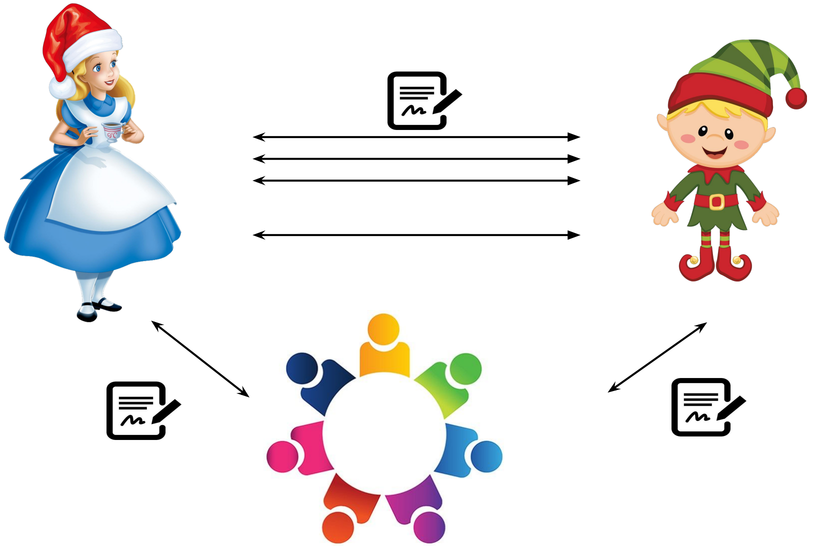
Be proactive, not reactive

Be proactive, not reactive



Signatures of Alice & Bob
OR
Signatures of ⅔ WT & (Alice or Bob)

Challenges

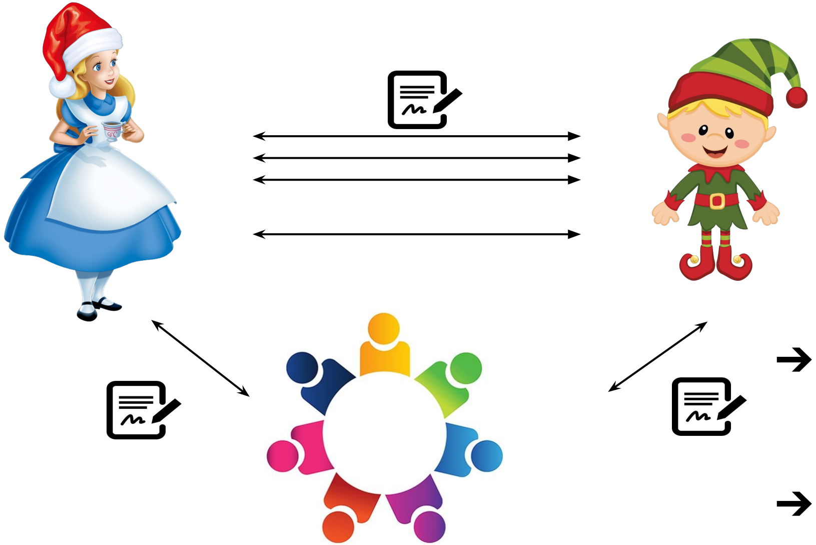


1) Consensus is costly

2) Privacy is important

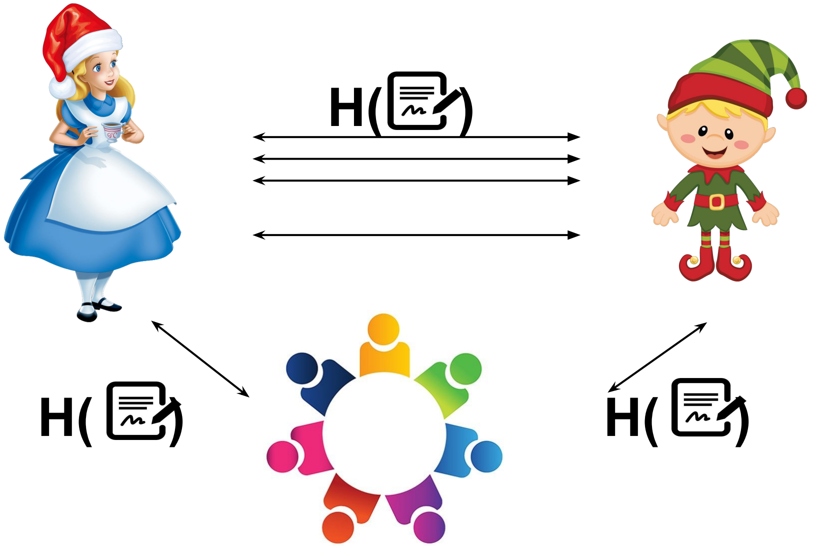
3) Incentives are critical

Consistent Broadcast



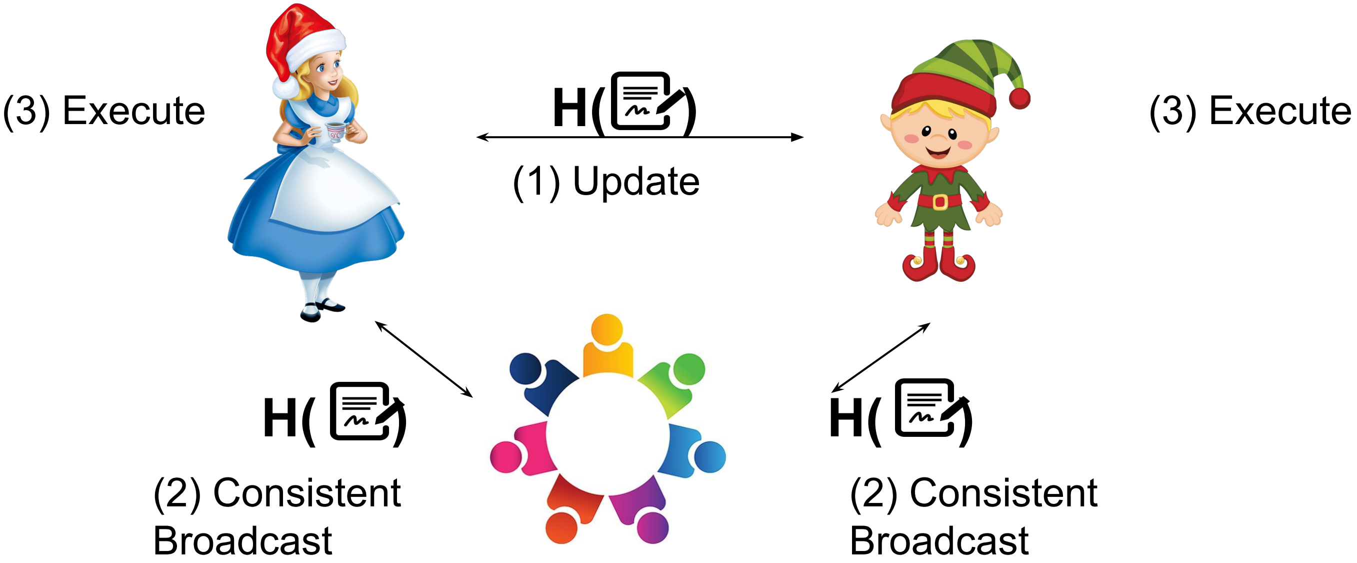
- ➔ O(n) communication complexity for state updates
- ➔ Verification of consensus between Alice & Bob
- ➔ No liveness guarantees, if Alice & Bob both misbehave
- ➔ Consensus needed only for closing, if there is a dispute

Encrypted State



- ➔ Privacy preserving
- ➔ Alice/Bob cannot publish a previous transaction

Brick Architecture



(3) Execute

H(📝)

(1) Update

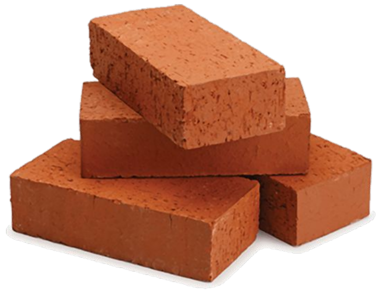
(3) Execute

H(📝)

(2) Consistent Broadcast

H(📝)

(2) Consistent Broadcast



Incentives

- Unilateral channel for fees:
  Repeated game lifts fair exchange impossibility

- Fees for closing the channels:
  Only payable in dispute → Incentive to agree

- Collateral for anti-bribing:
  Reduction to fair-exchange
  WT Committee size ↑ → per WT collateral ↓

Brick Advantages

- **Asynchronous channels**
- **Security even under L1 failure**
- **Privacy**
- **Incentive-compatible**
- **Embarrassingly parallel**
- **Linear communication**

[Avarikioti et al. *Brick: Asynchronous State Channels*.]