Payment Channels

Designing Secure Watchtowers

Zeta Avarikioti

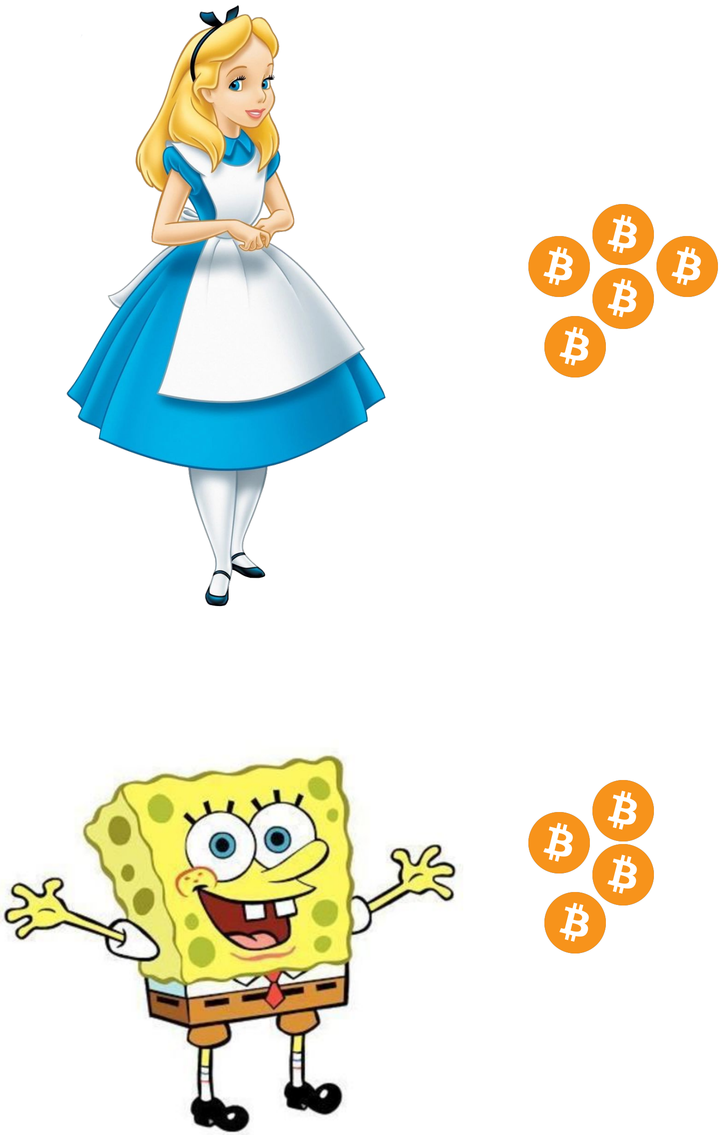
Can cryptocurrencies scale?

7 tx/s

20 tx/s

65.000 tx/s

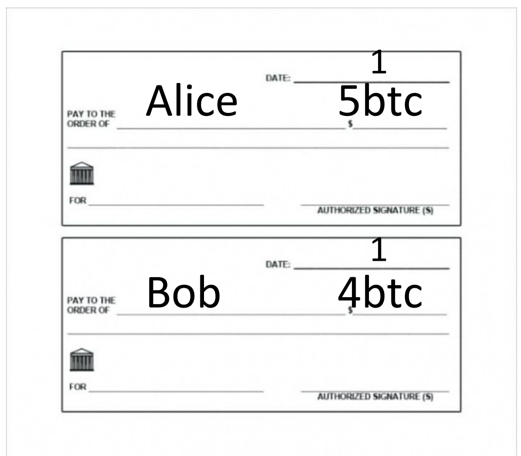
Payment Channels



Payment Channels

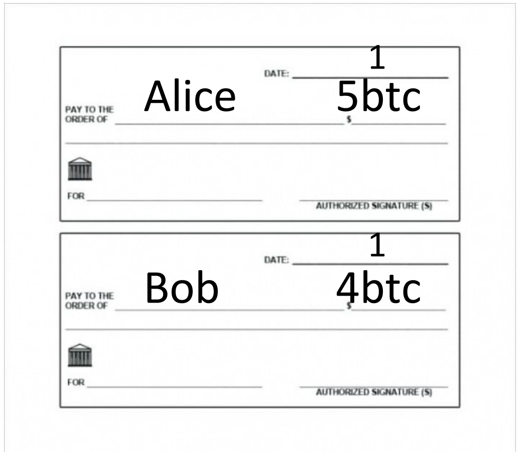
Payment Channels

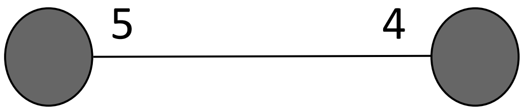
Funding transaction



Payment Channels

Funding transaction

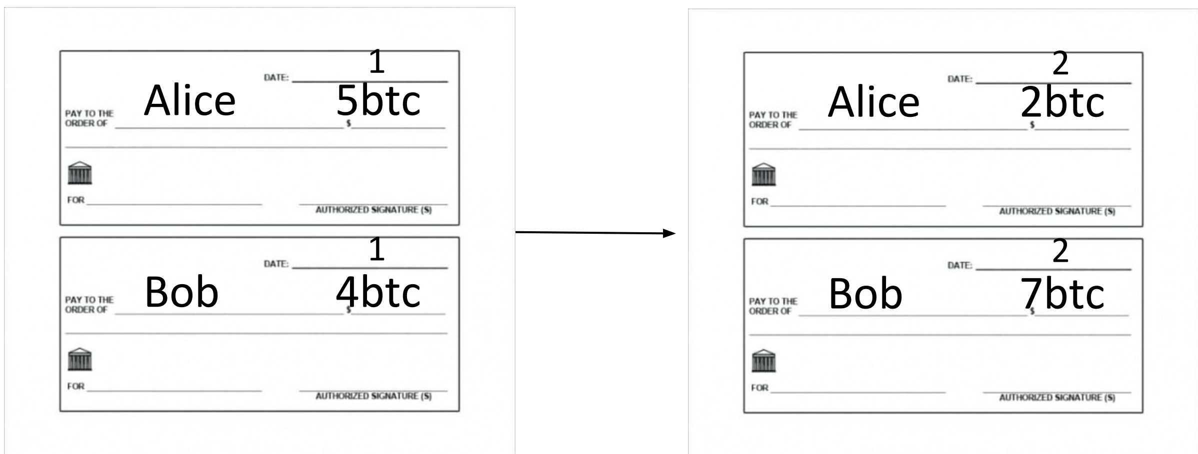




Payment Channels

Funding transaction

Alice sends 3btc

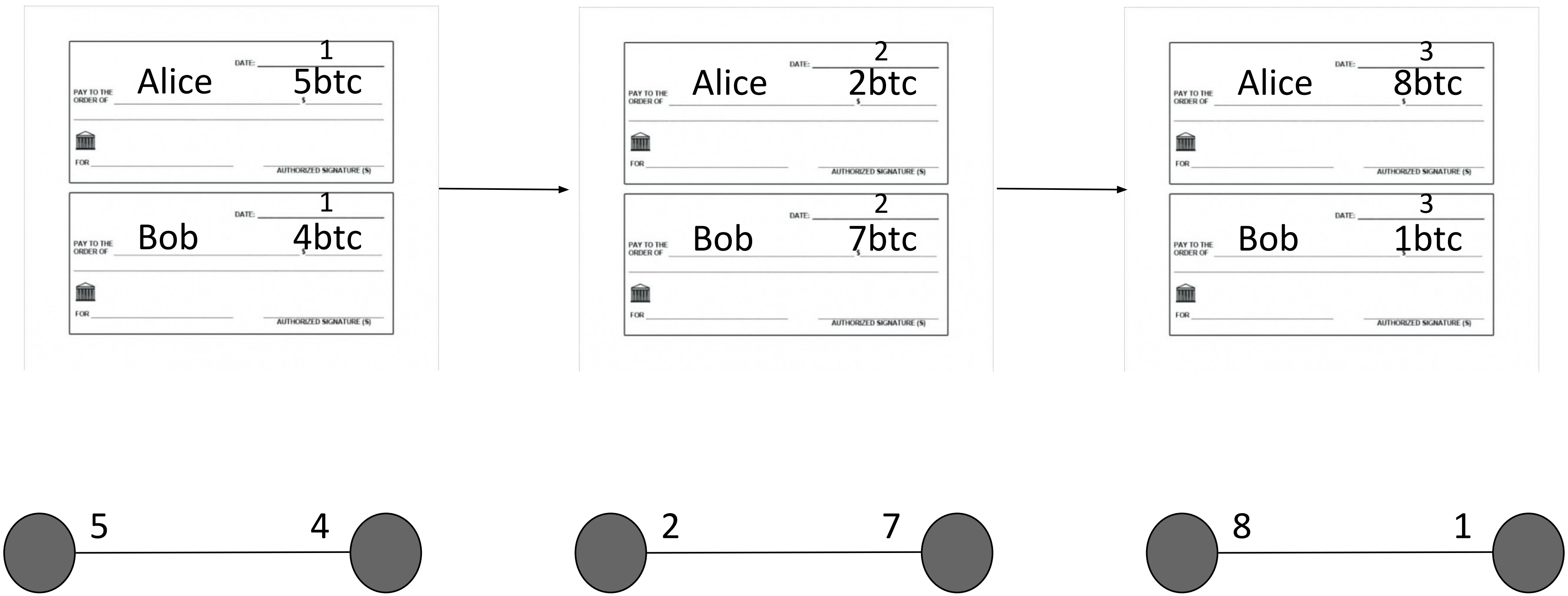


Payment Channels

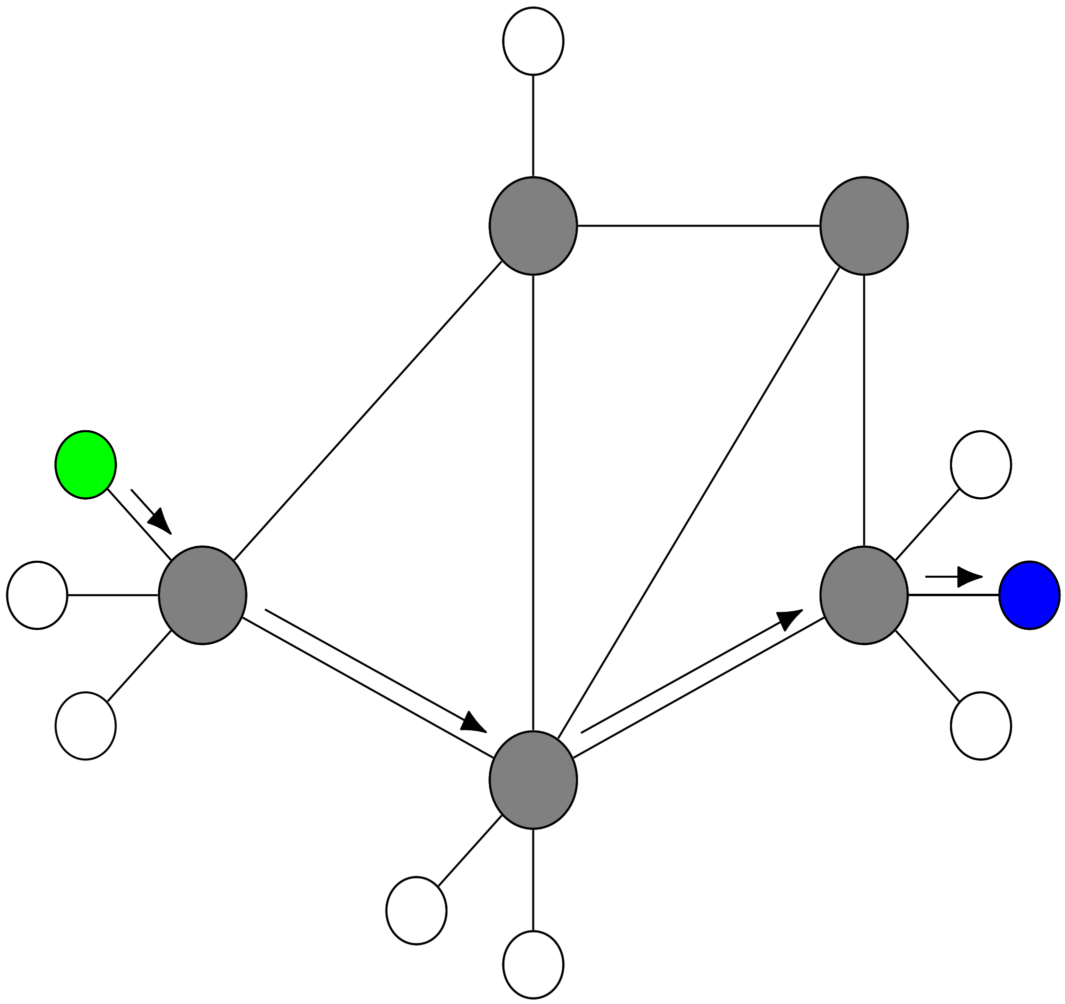
Funding transaction

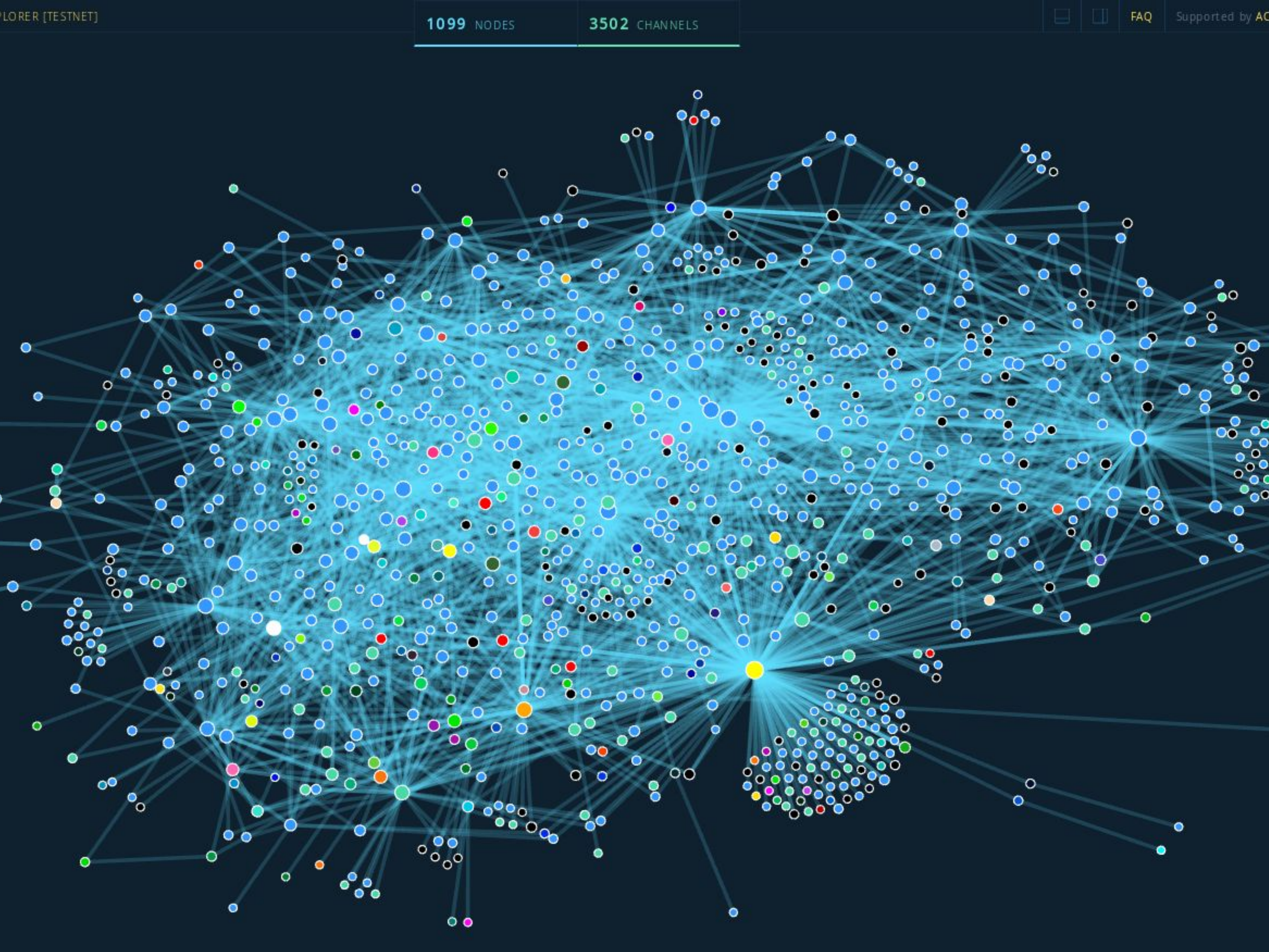
Alice sends 3btc

Bob sends 6btc

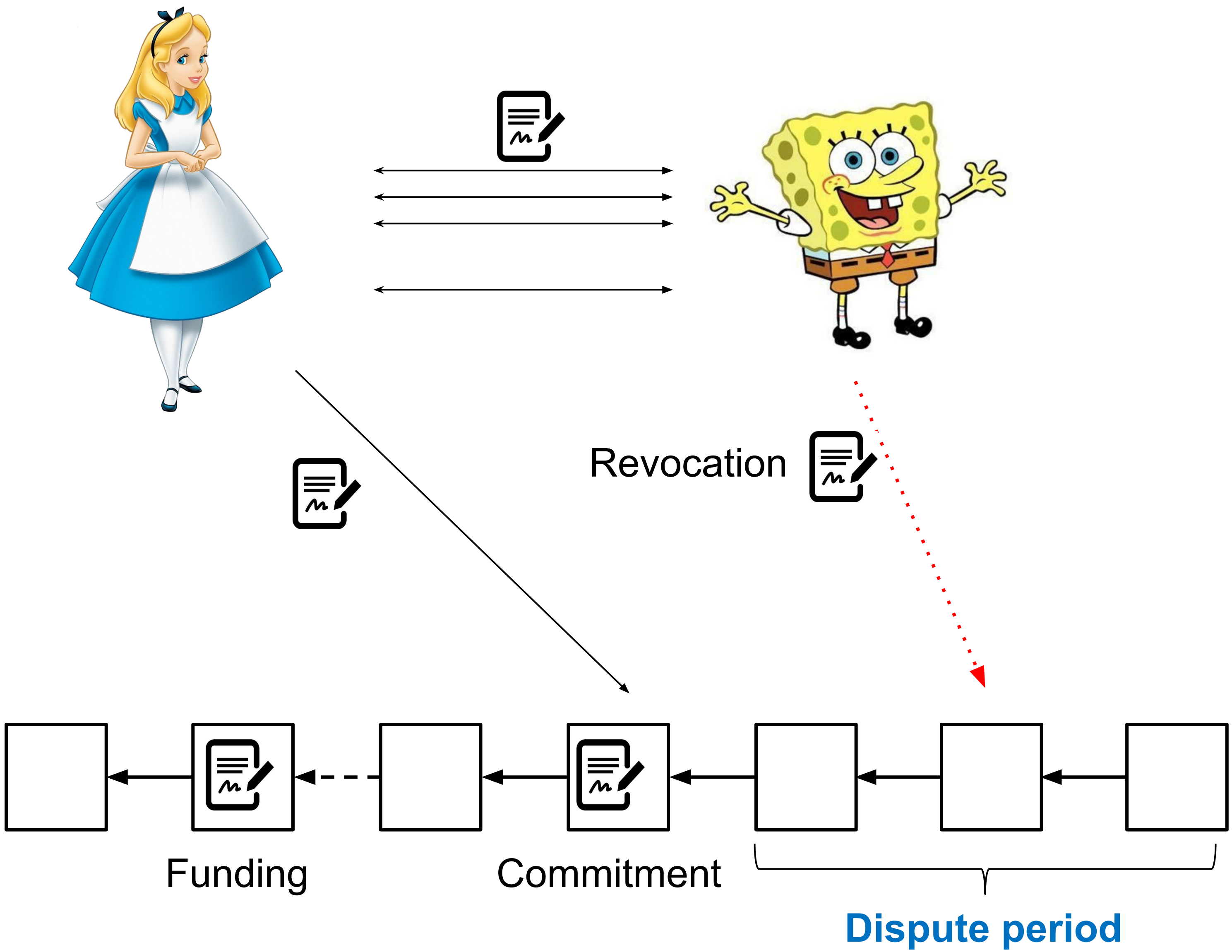


Payment Network

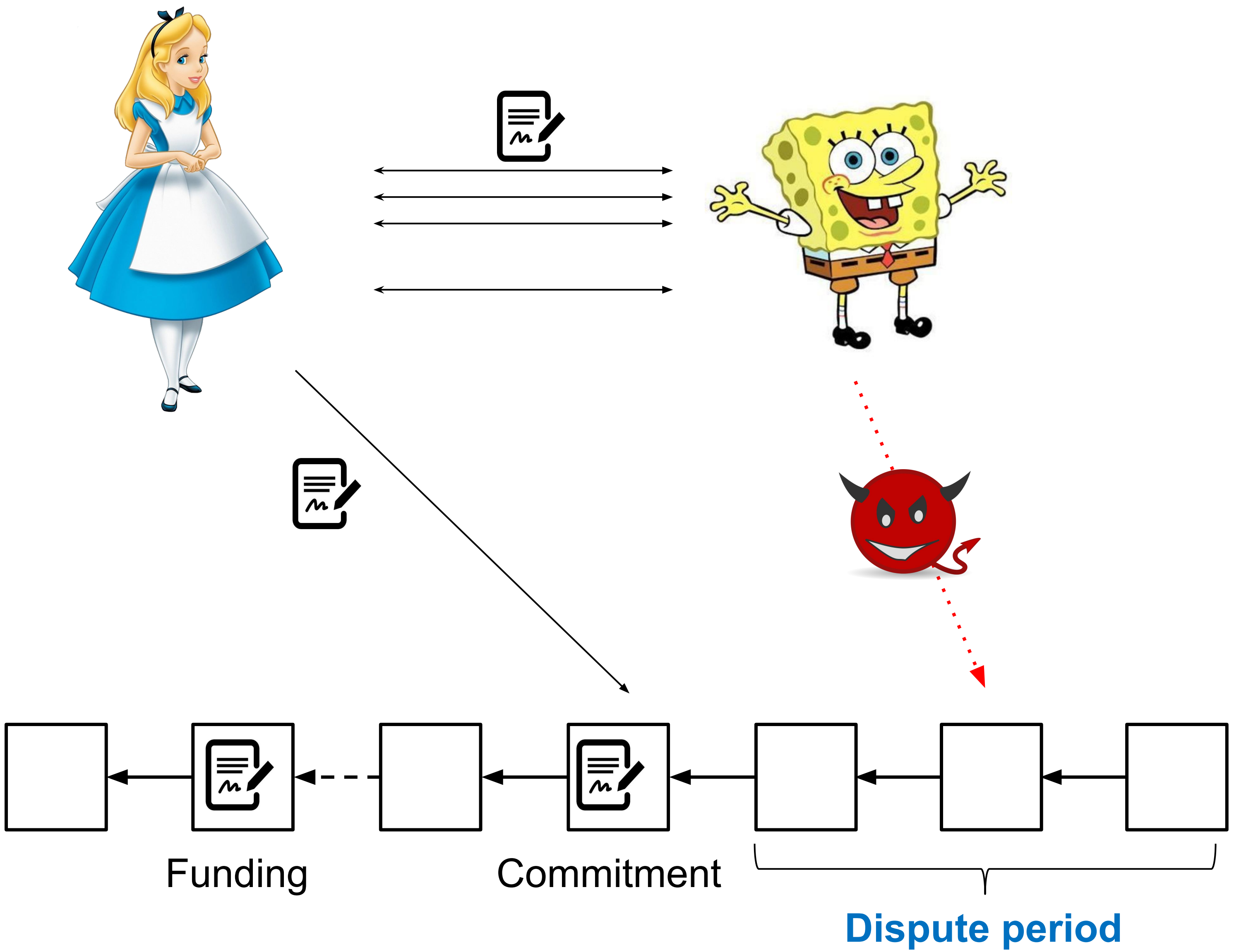



LORER [TESTNET]
1099 NODES
3502 CHANNELS
FAQ
Supported by AC

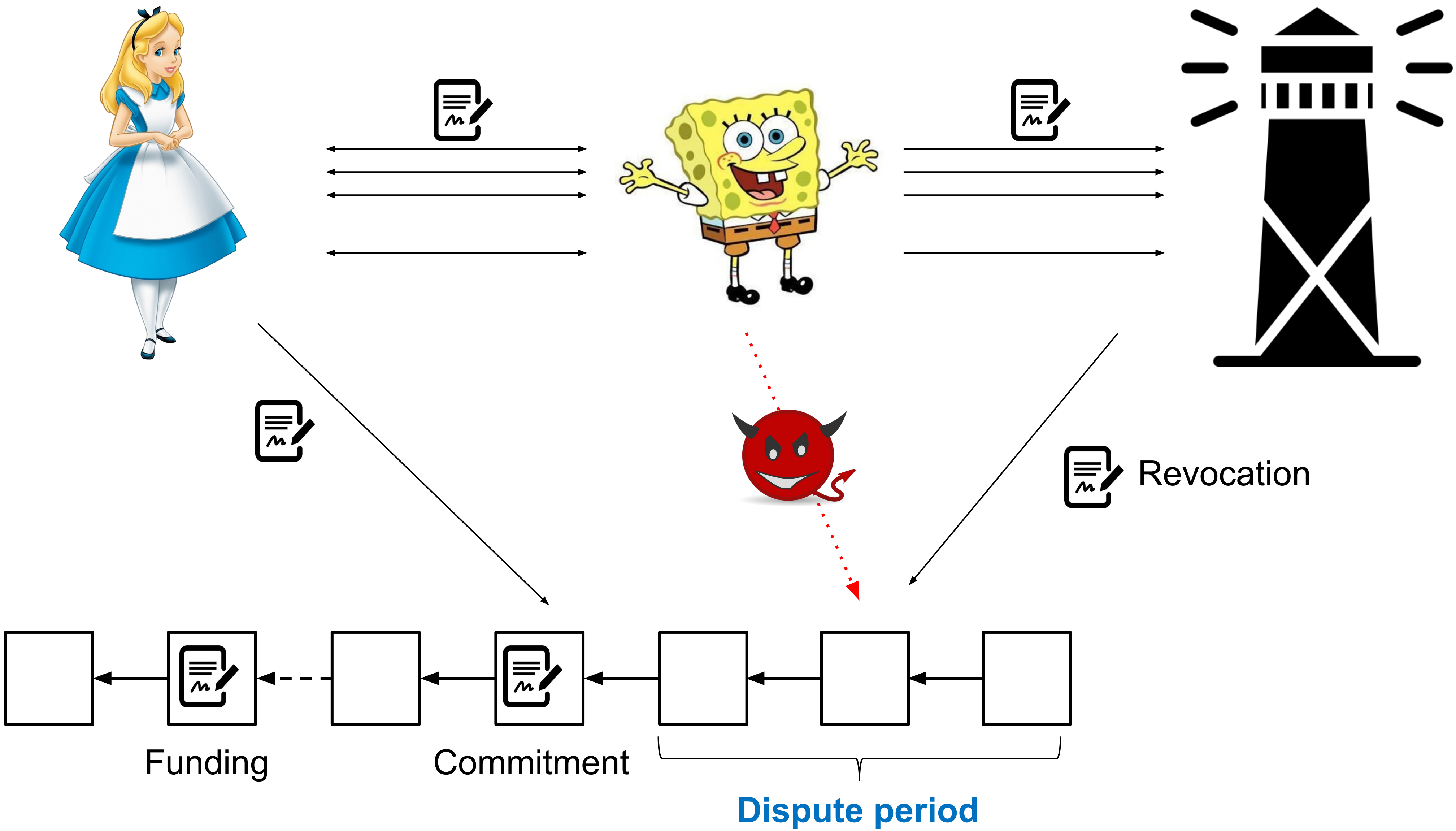
Lightning Channels



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 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		

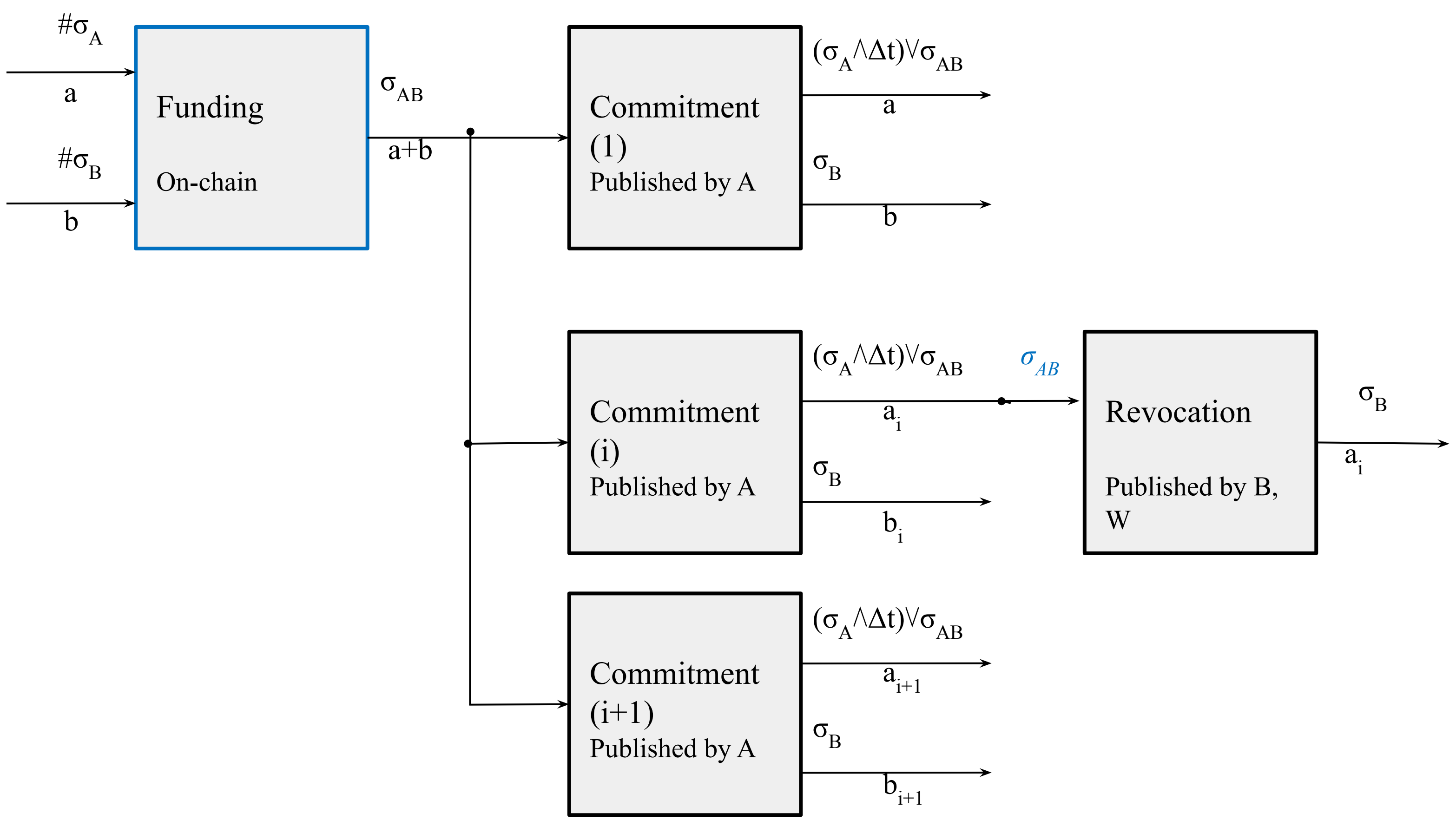
Why be an active Watchtower?

Collateral

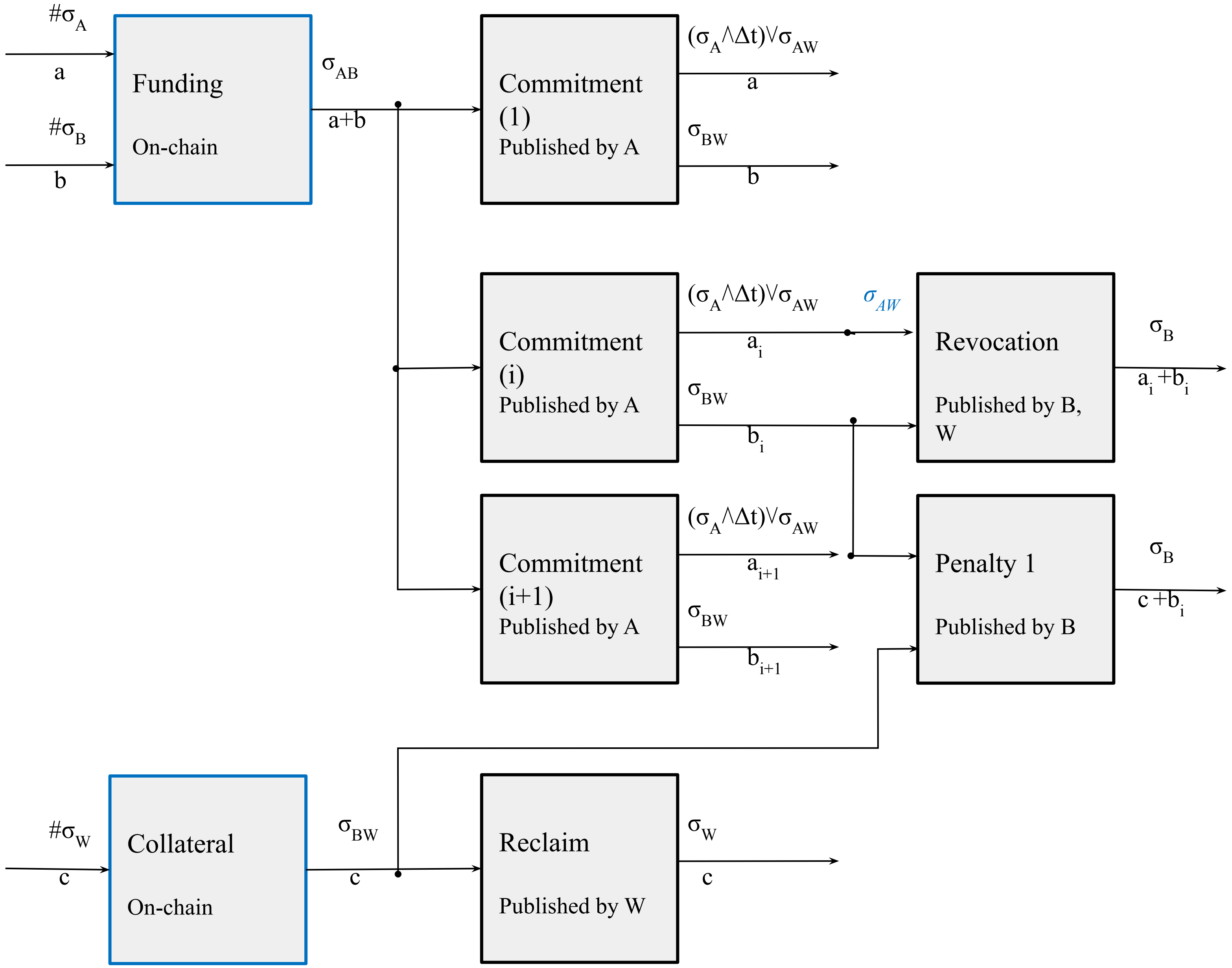
Bitcoin

- ➔ UTXO-based (Unspent Transaction Output)
- ➔ Transaction: consumes & produces UTXOs
- ➔ Multi-signatures: σ_{AB}
- ➔ Timelocks: Δt

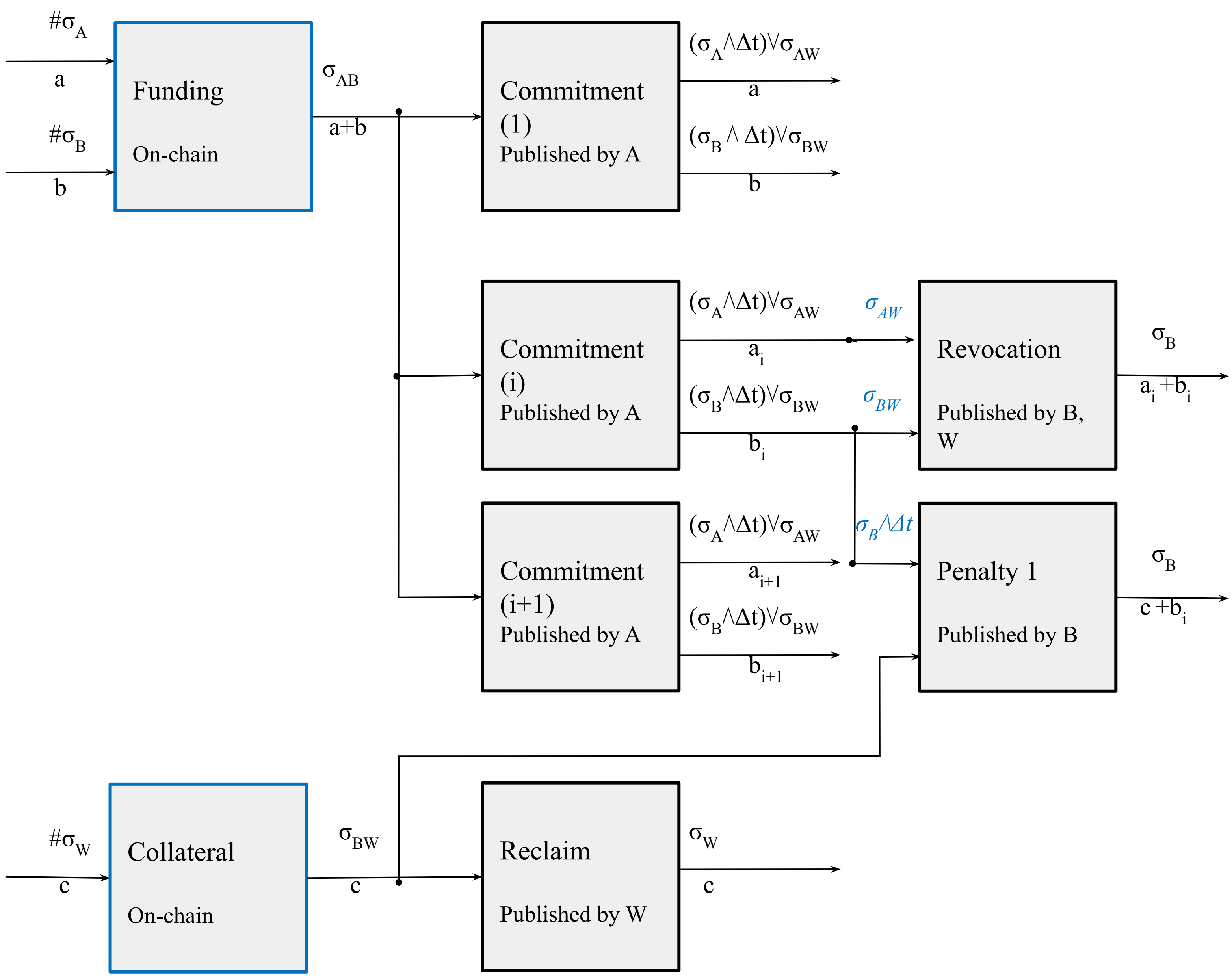
Lightning Channels



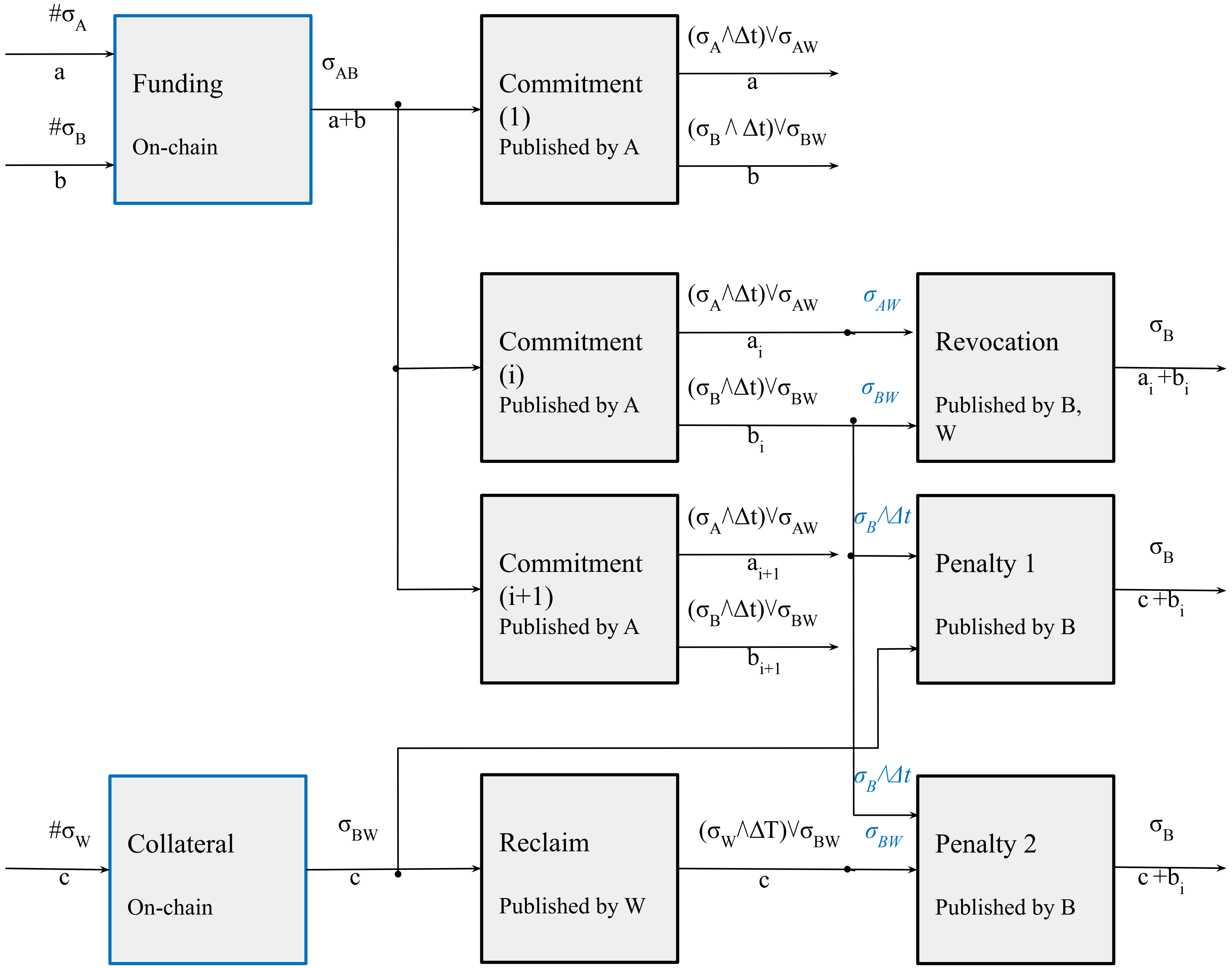
Cerberus Channels



Cerberus Channels



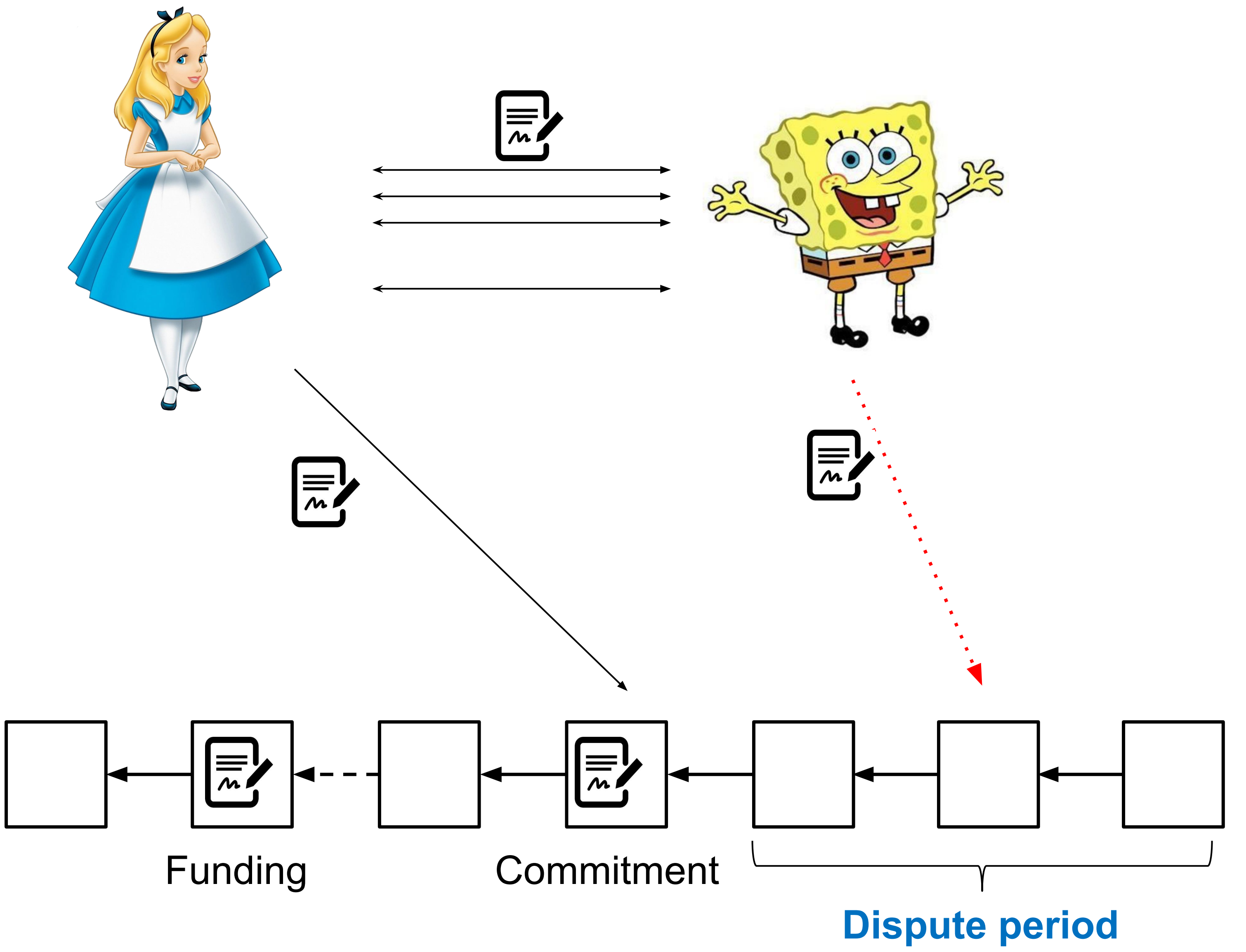
Cerberus Channels



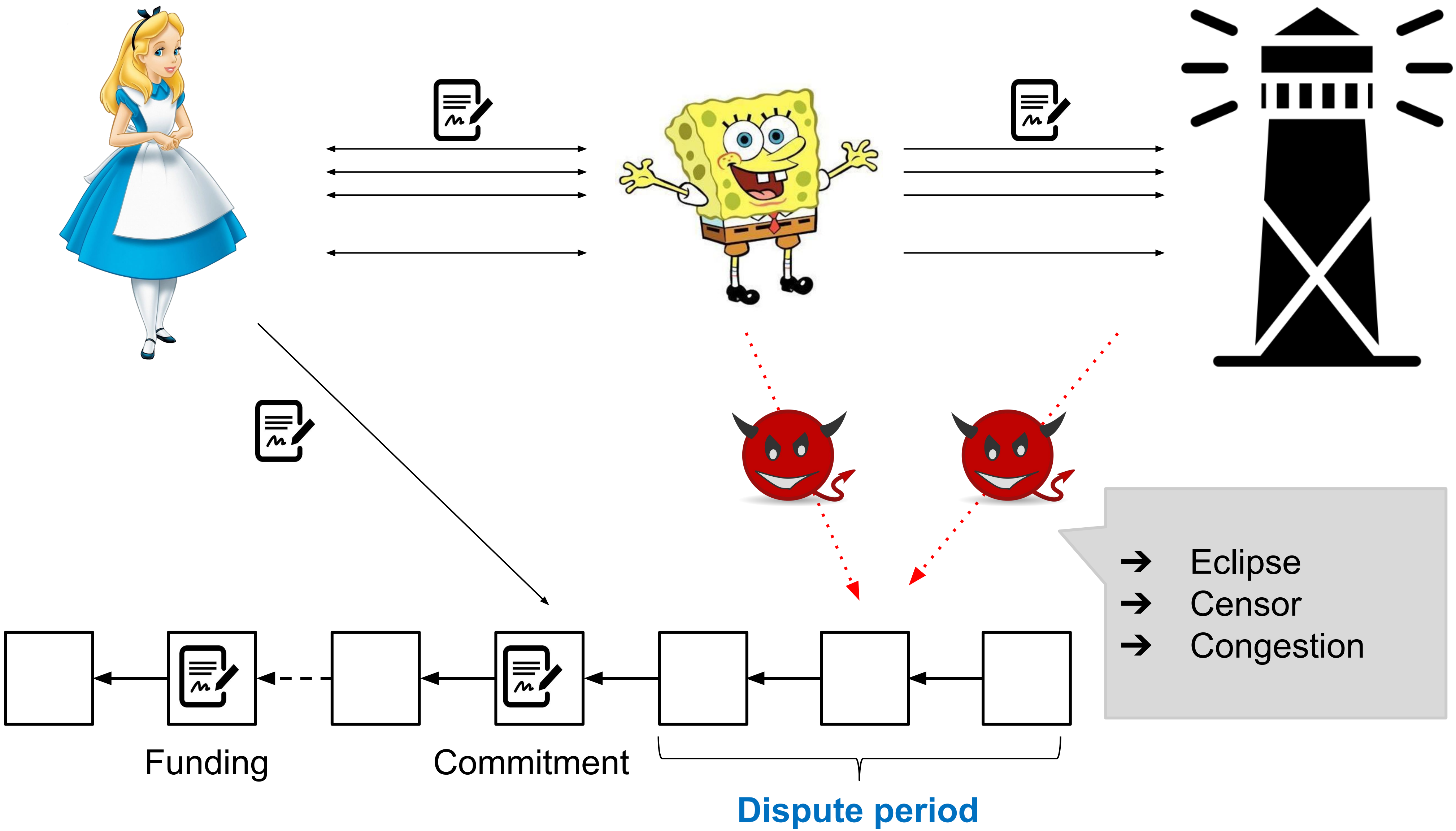
[Avarikioti, Tyfronitis-Litos, Wattenhofer. *Cerberus Channels: Incentivizing Watchtowers for Bitcoin*.]

Fundamentals of Channels

Fundamentals of Channels



Fundamentals of Channels

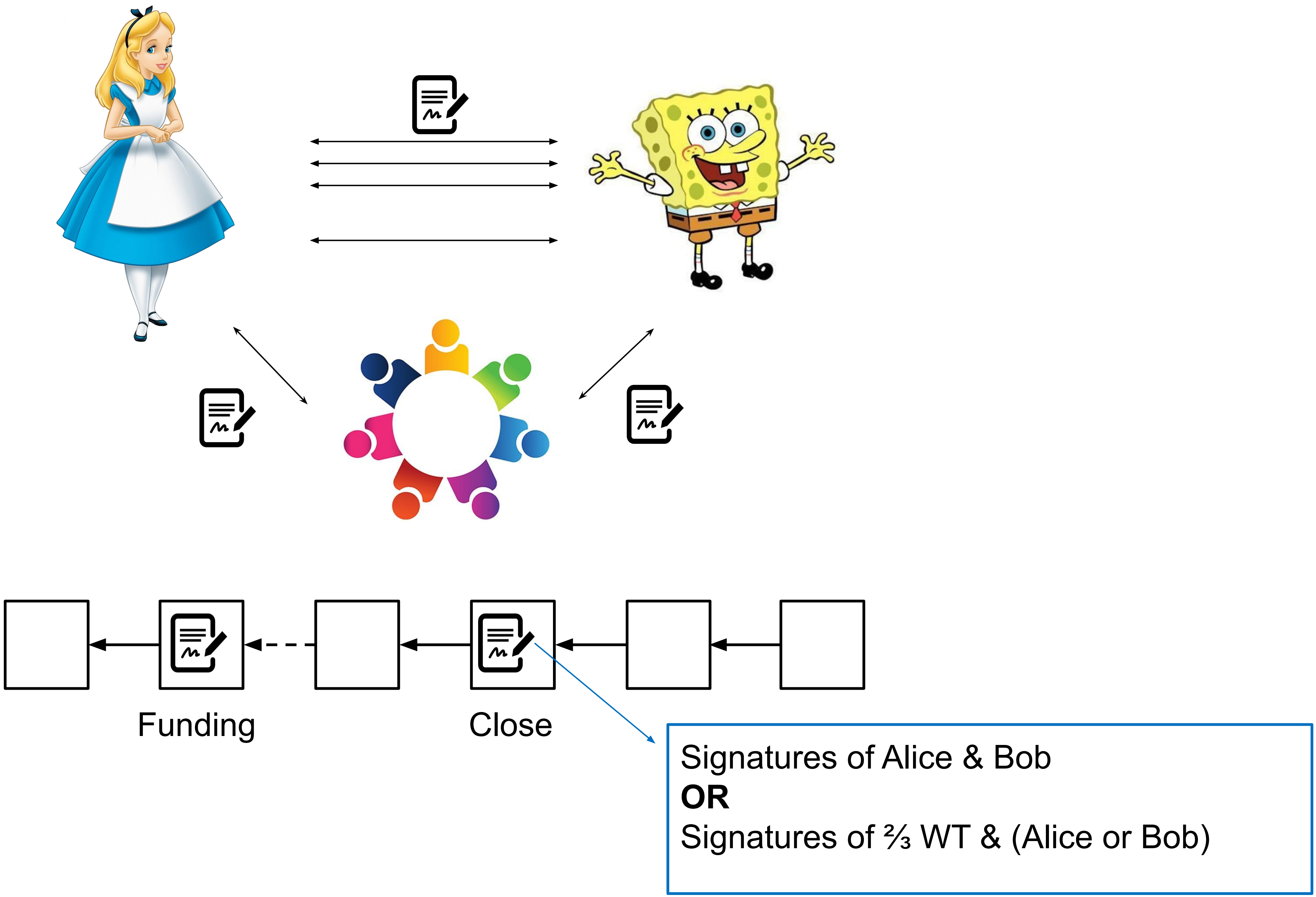


Time = CryptoMoney!

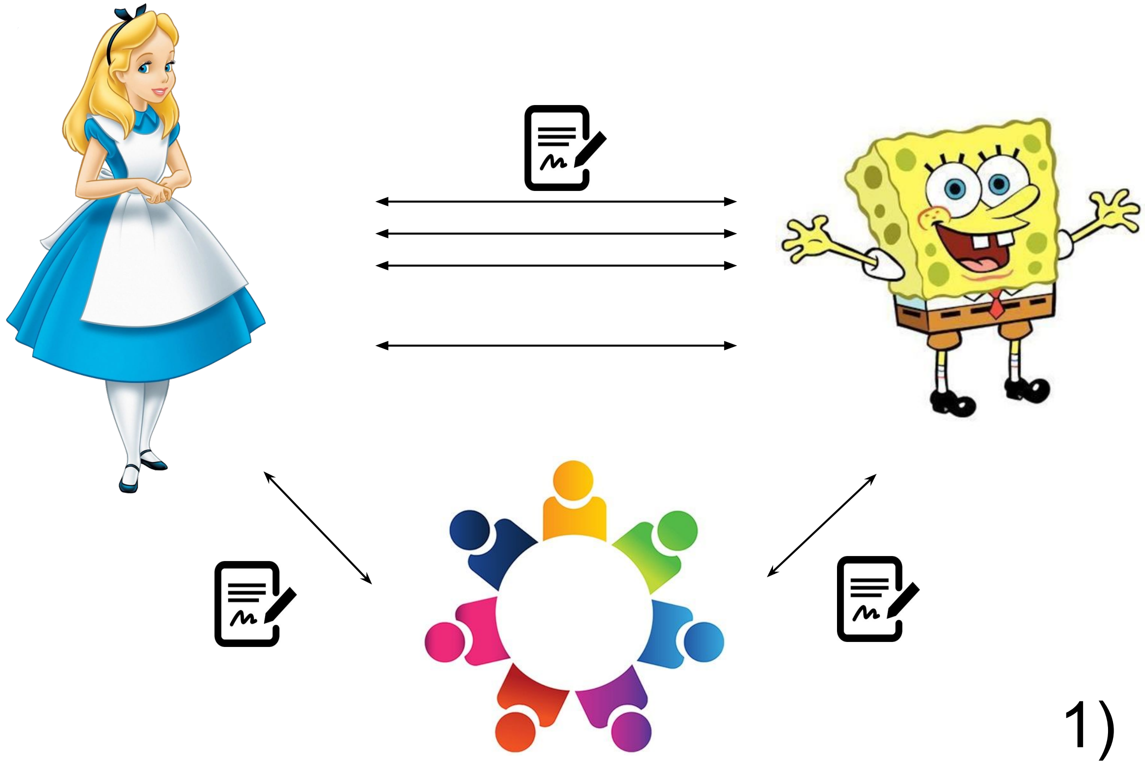
Time = CryptoMoney!

Be proactive, not reactive

Be proactive, not reactive

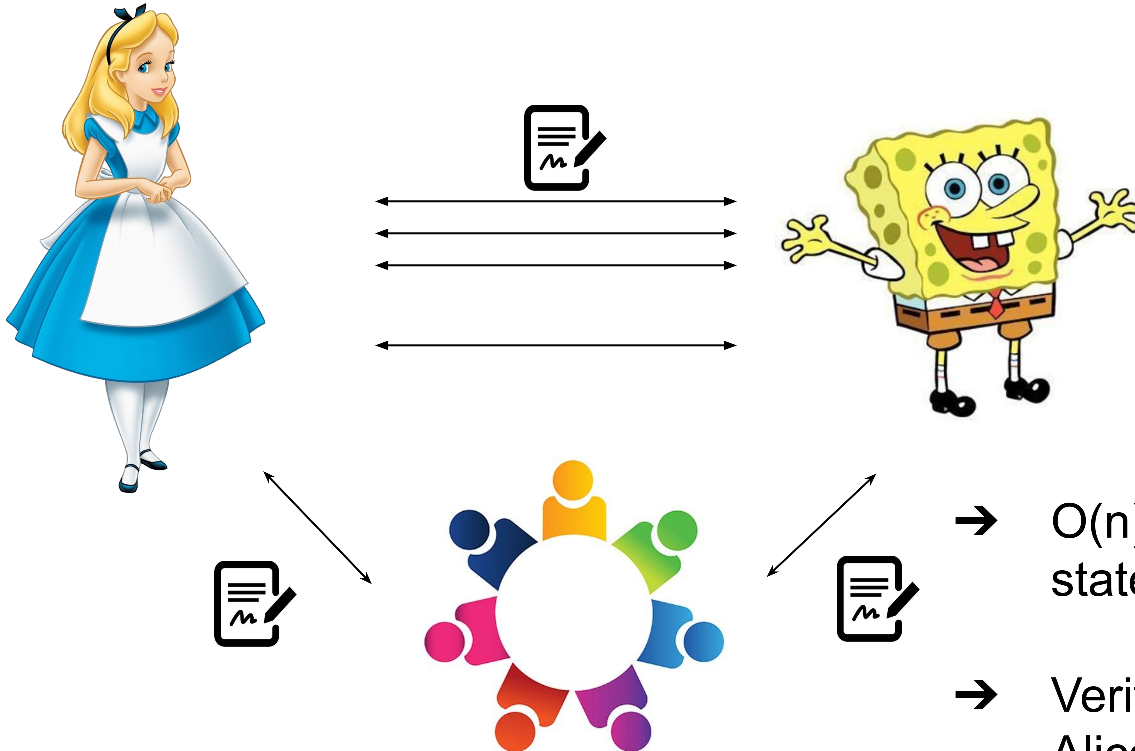


Challenges



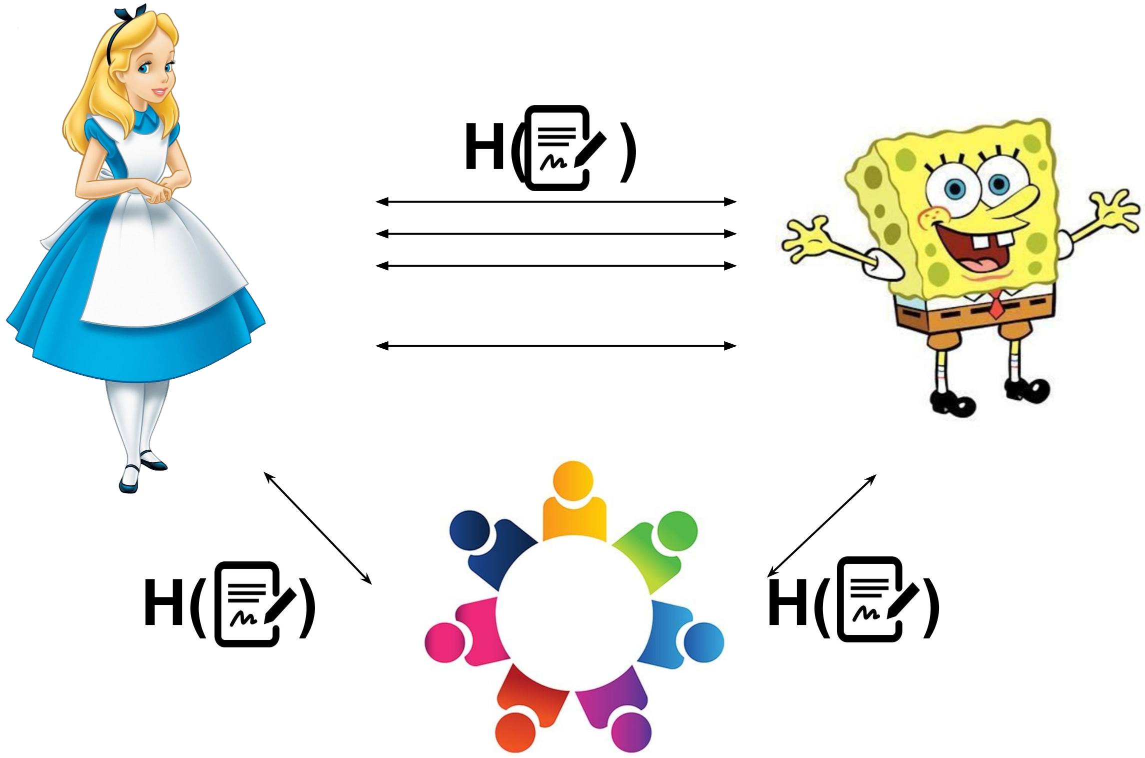
1) Consensus is costly
2) Privacy is important
3) Incentives are critical

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

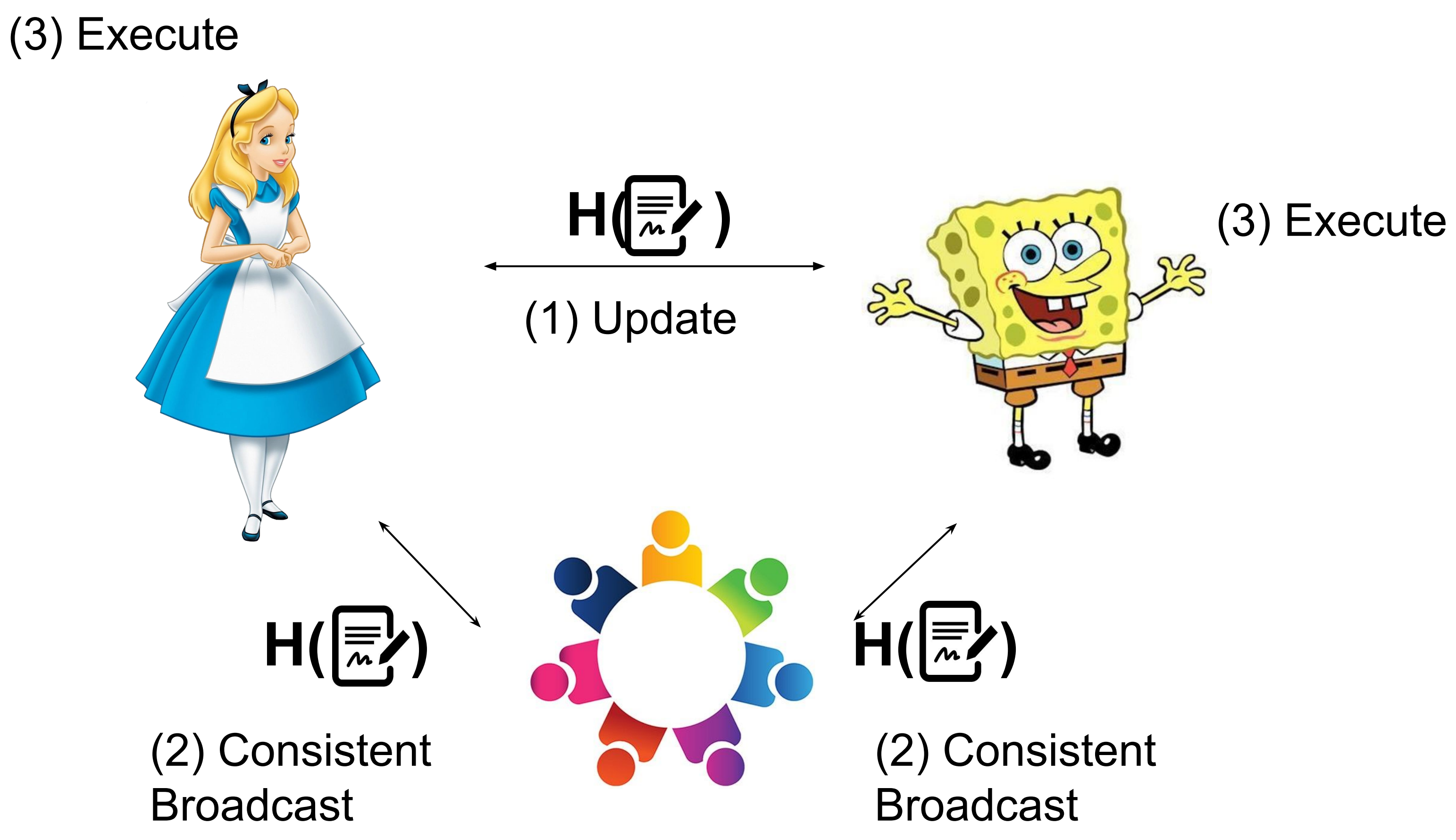
Encrypted State



➔ Privacy preserving

➔ Alice/Bob cannot publish a previous transaction

Brick Architecture



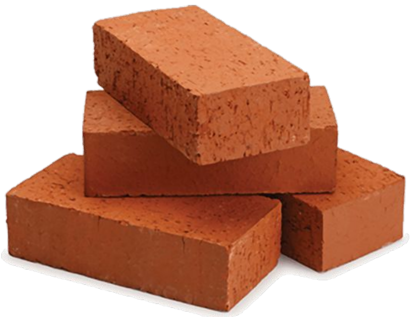
Incentives

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

- ➔ 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, Kokoris-Kogias, Wattenhofer. *Brick: Asynchronous State Channels*.]

Thank you!

Questions?

➔ Avarikioti, Tyfronitis-Litos, Wattenhofer. *Cerberus Channels: Incentivizing Watchtowers for Bitcoin*. Financial Cryptography and Data Security 2020.

➔ Avarikioti, Kokoris-Kogias, Wattenhofer. *Brick: Asynchronous State Channels.*