

What is the Lightning Network?



eclair

Orfeas Stefanos
Thyfronitis Litos



University of Edinburgh

VISA

20,000 tx/s

bitcoin

7 tx/s

Problem

All txs validated by all wallets

Problem

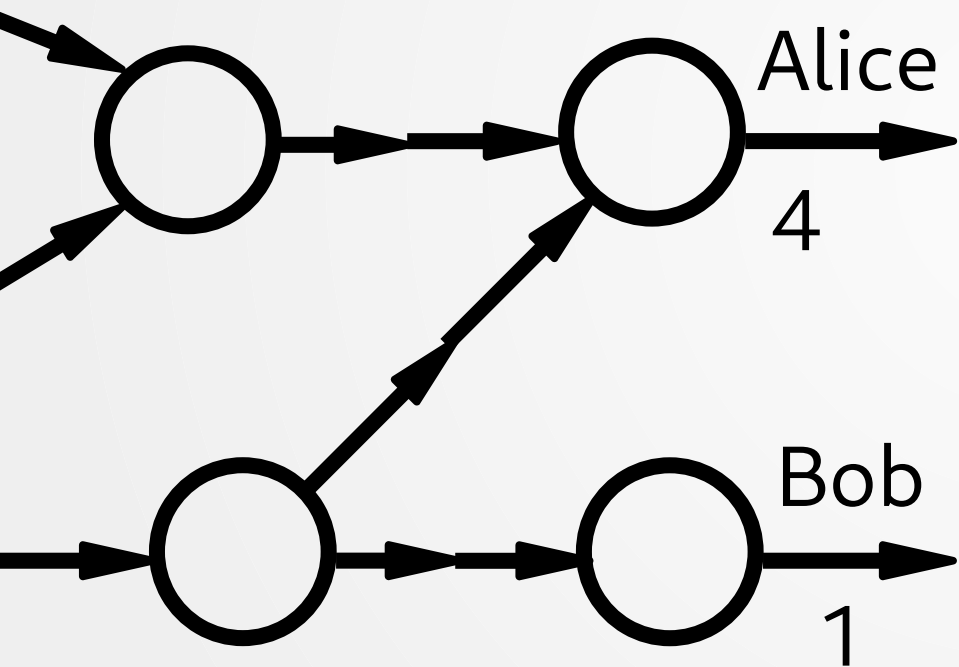
All txs validated by all wallets

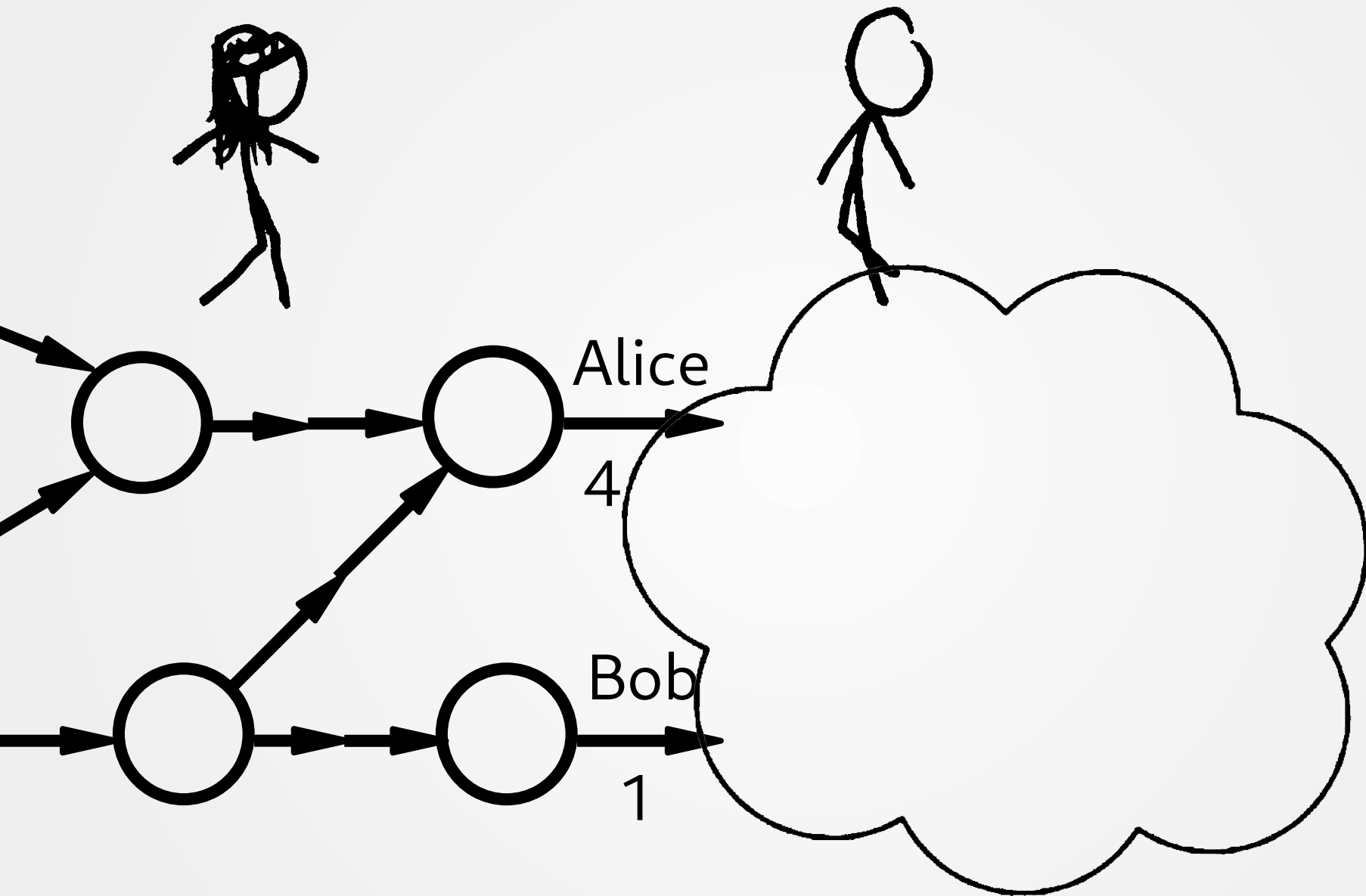
Solution

- Move most txs off-chain
- Resolve disputes on-chain

Part 1

2-party channels



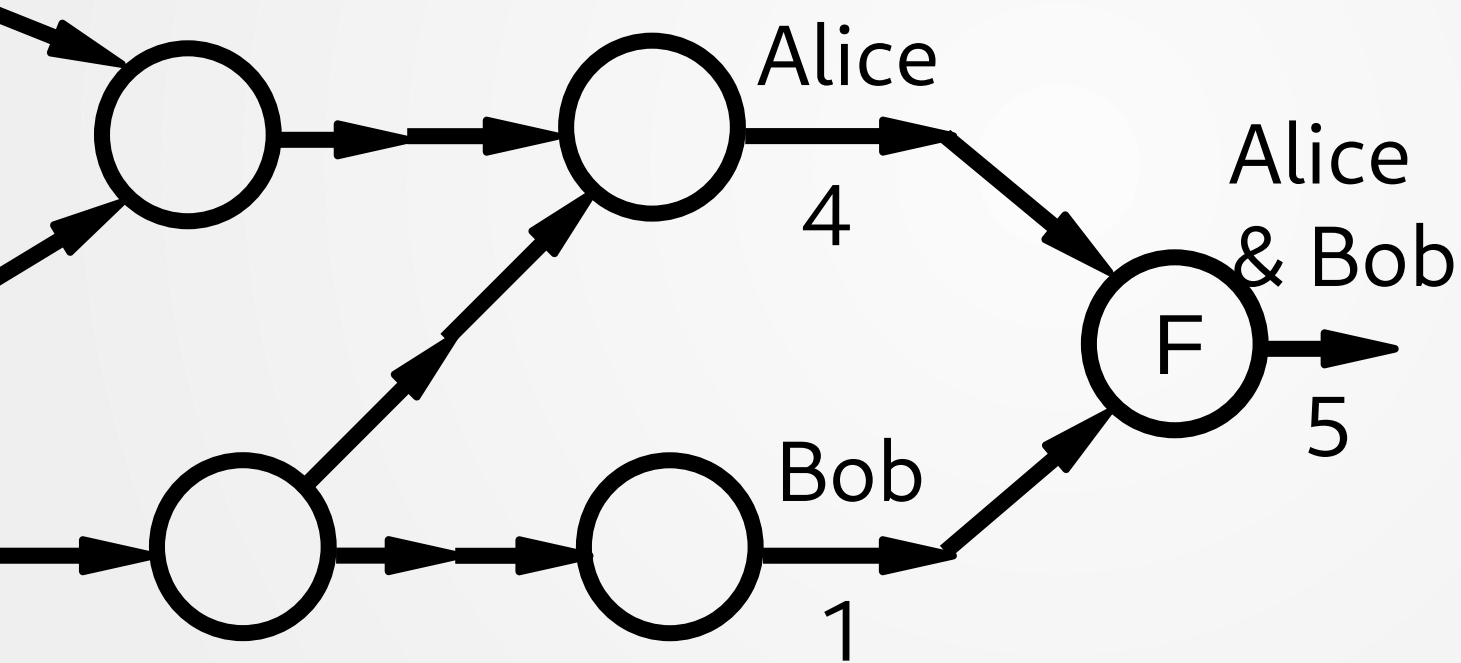






Alice	Bob
4	1

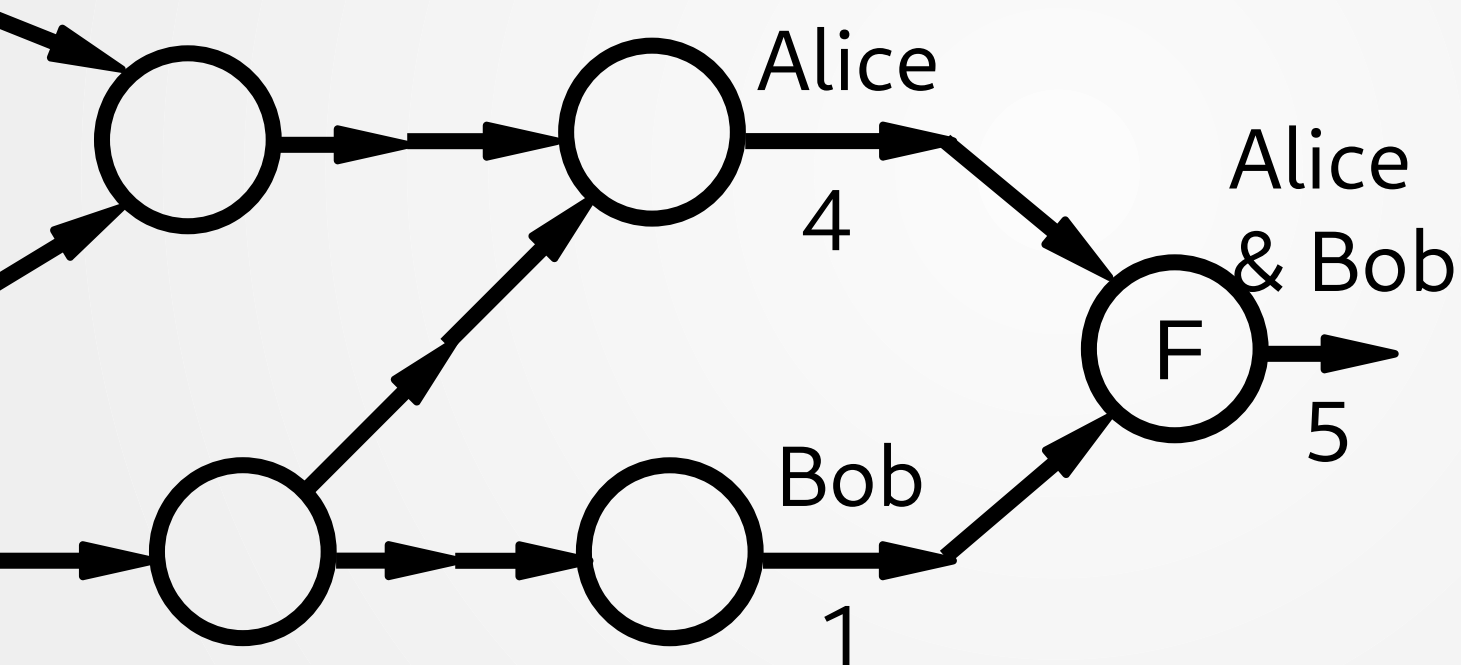
Alice	Bob
4	1





Alice	Bob
4	1
1	4

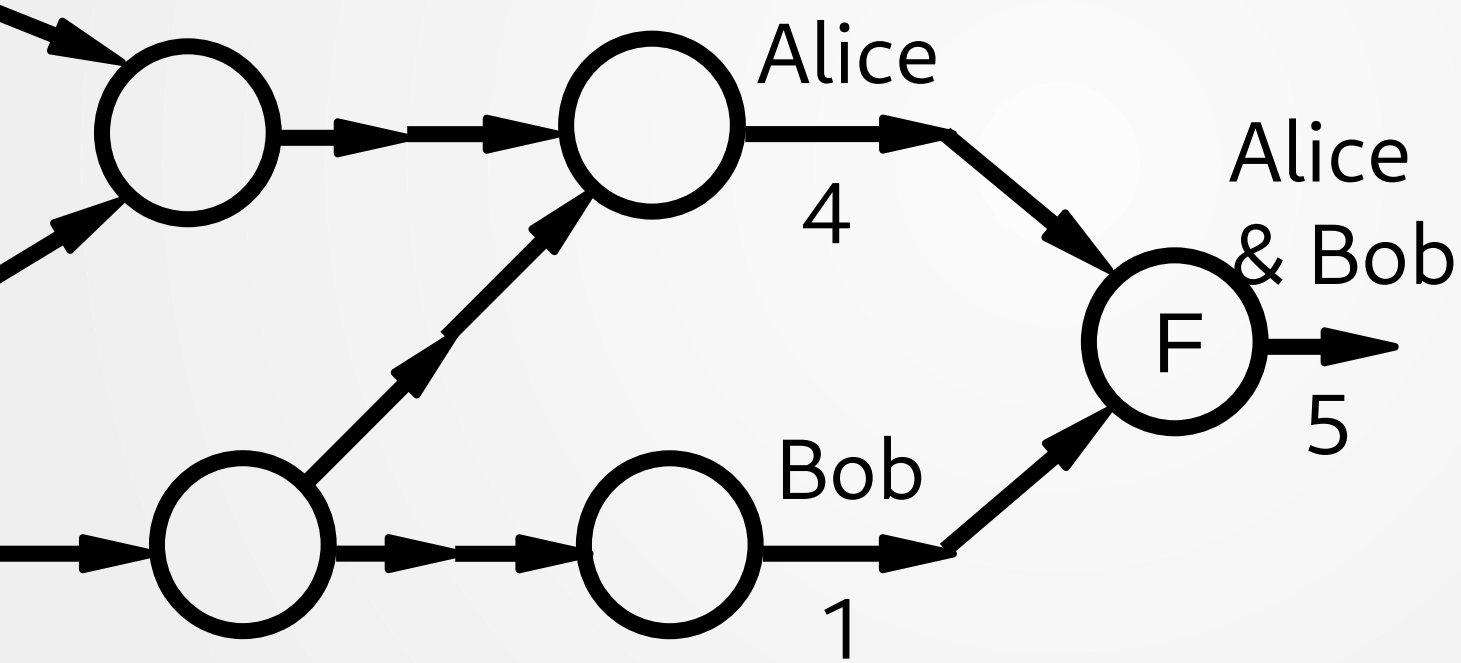
Alice	Bob
4	1
1	4





Alice	Bob
4	1
1	4
...	
3	2

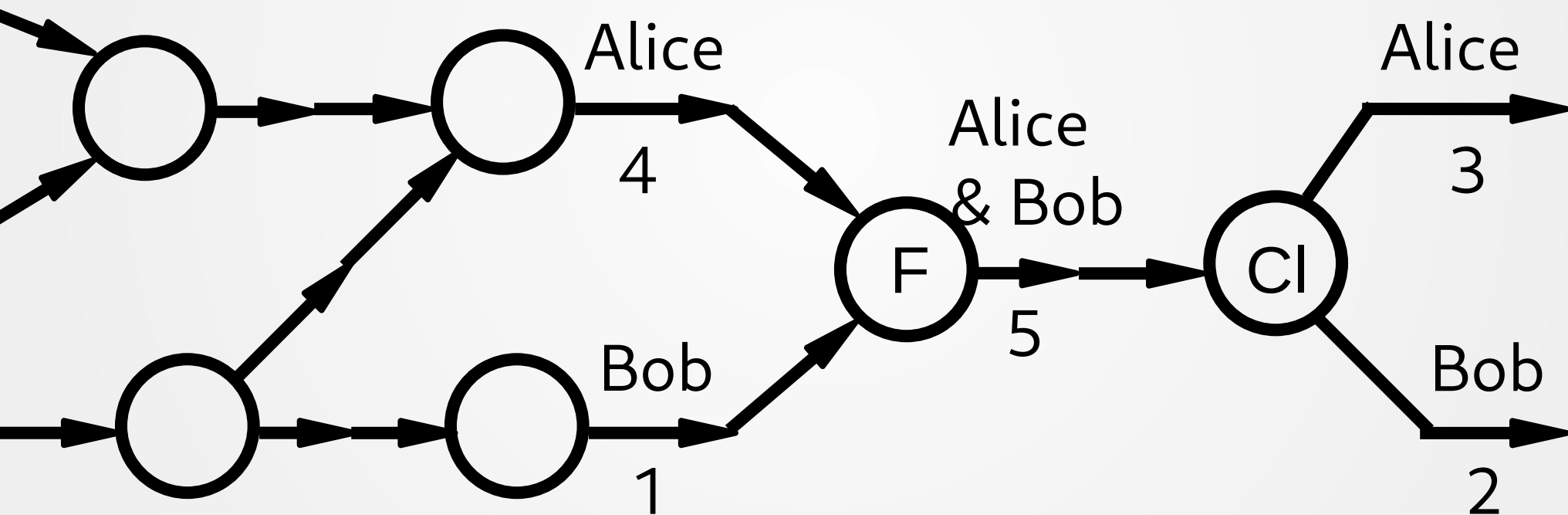
Alice	Bob
4	1
1	4
...	
3	2





Alice	Bob
4	1
1	4
...	
3	2

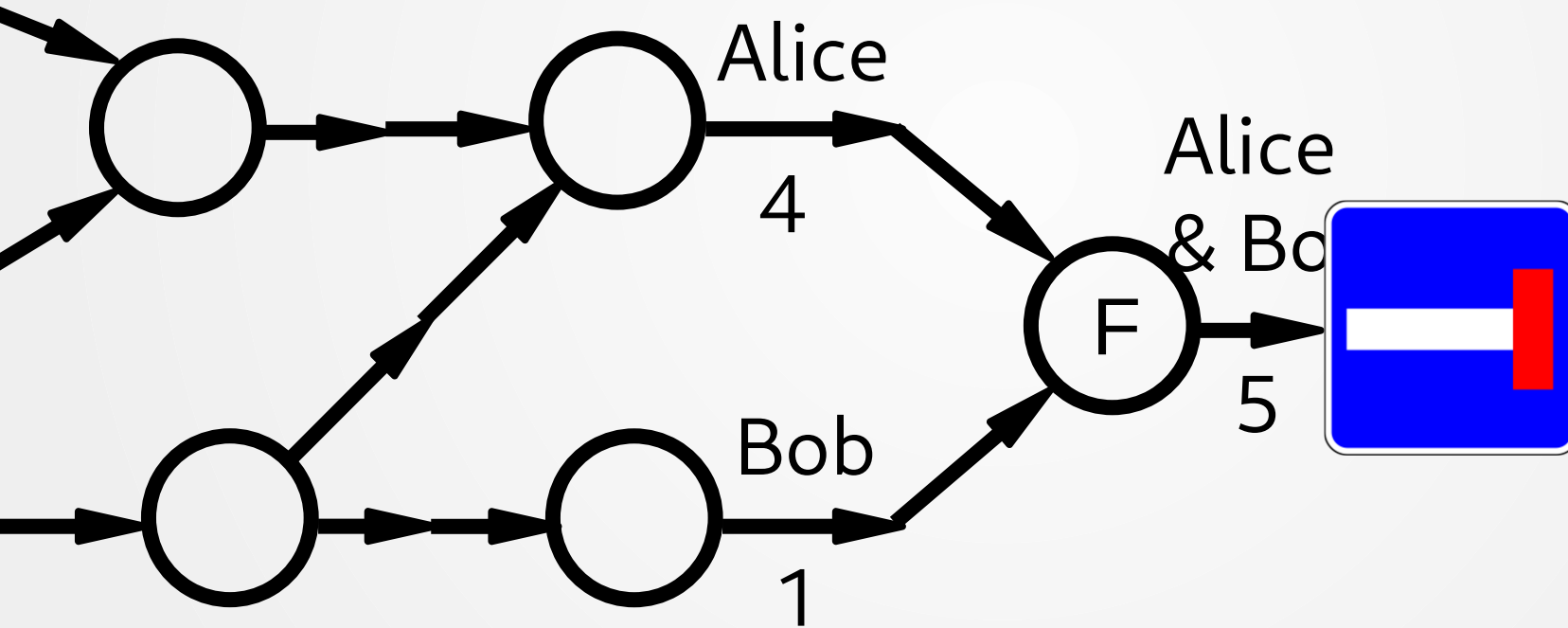
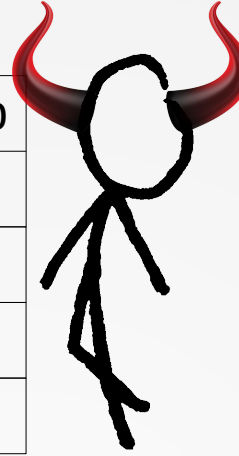
Alice	Bob
4	1
1	4
...	
3	2





Alice	Bob
4	1
1	4
...	
3	2

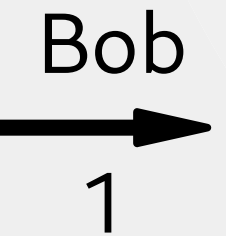
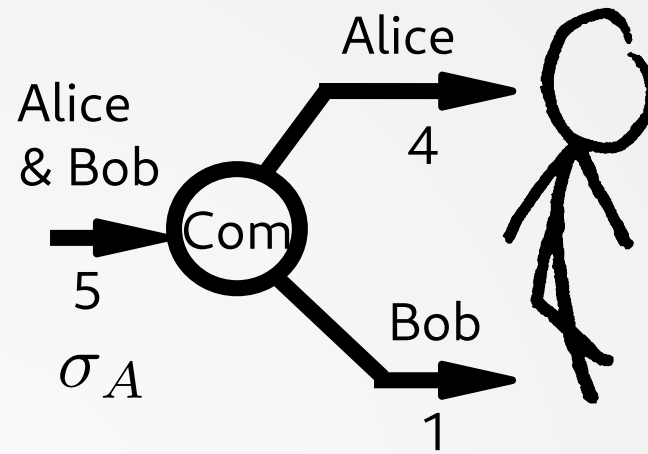
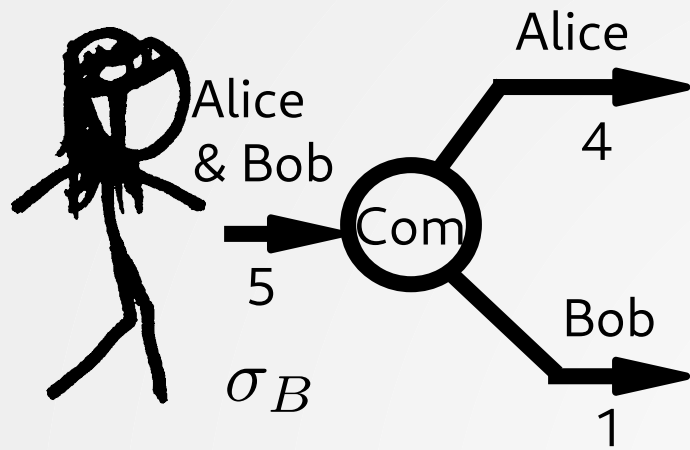
Alice	Bob
4	1
1	4
...	
0	5

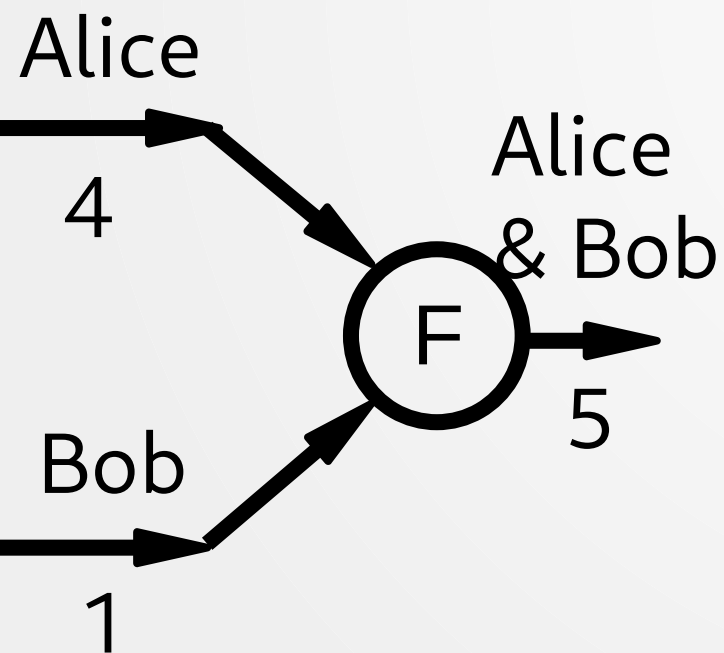
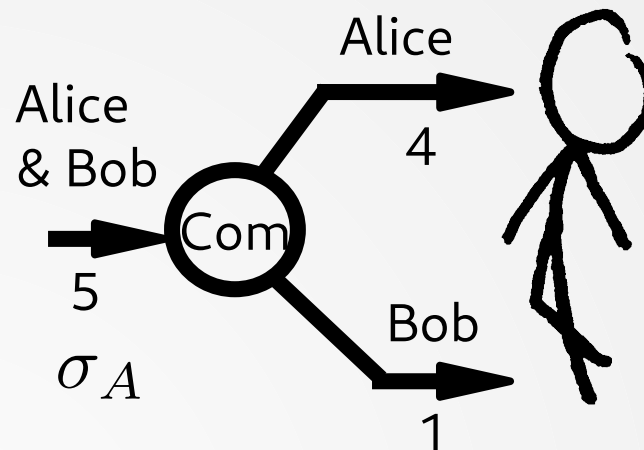
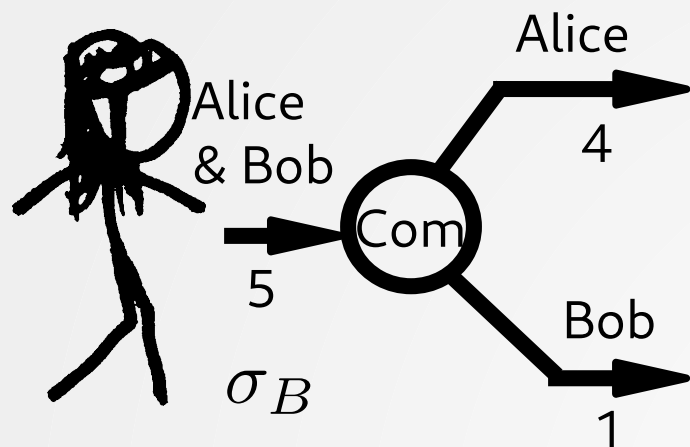


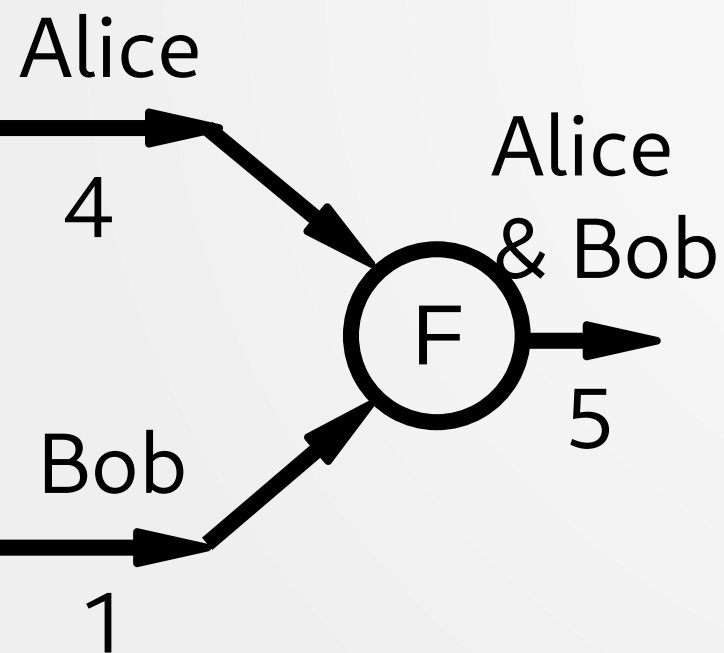
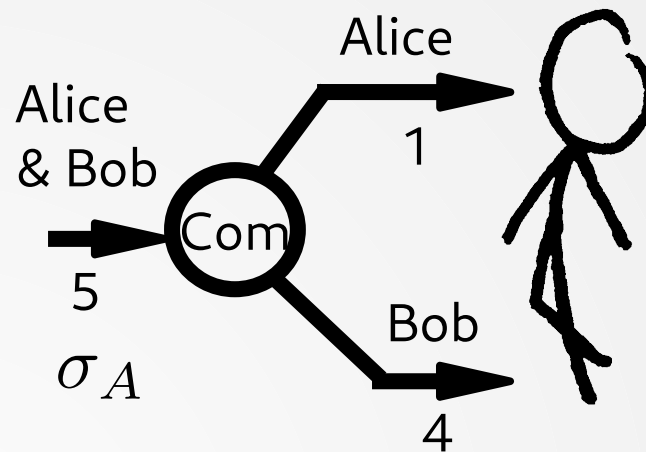
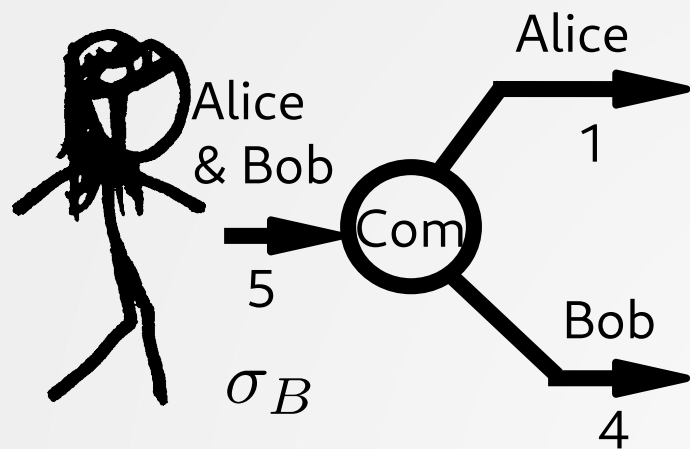


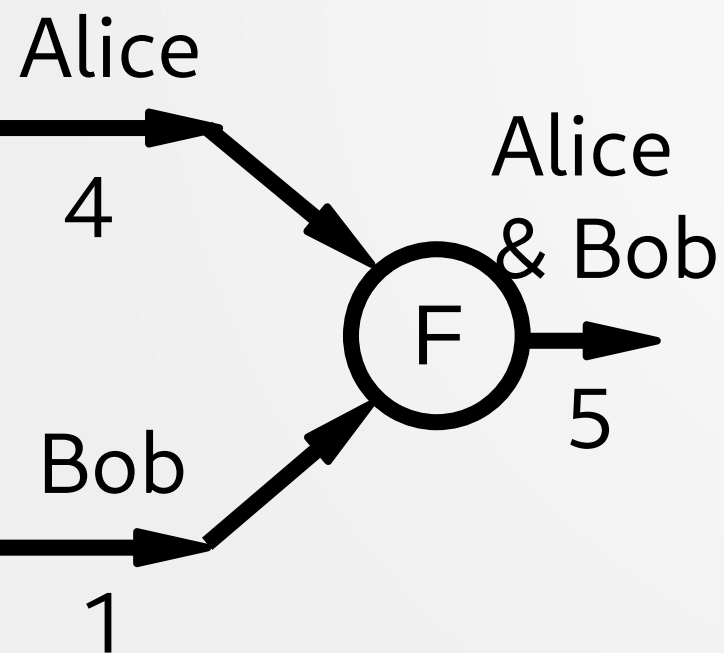
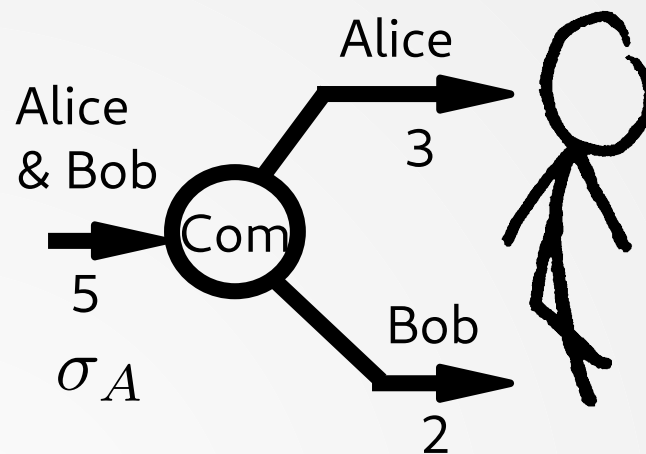
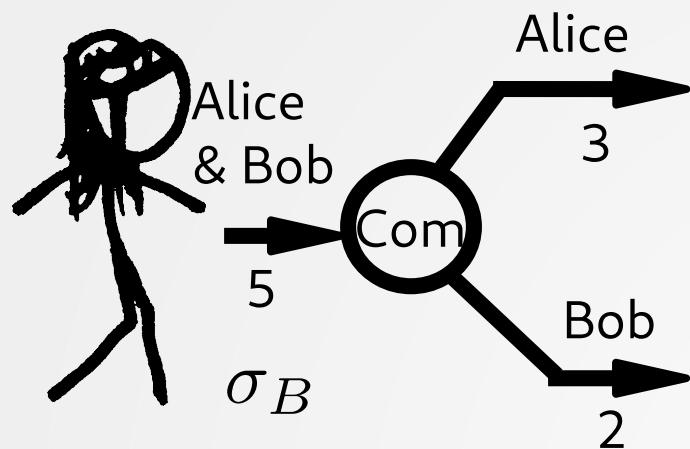
Alice
→
4

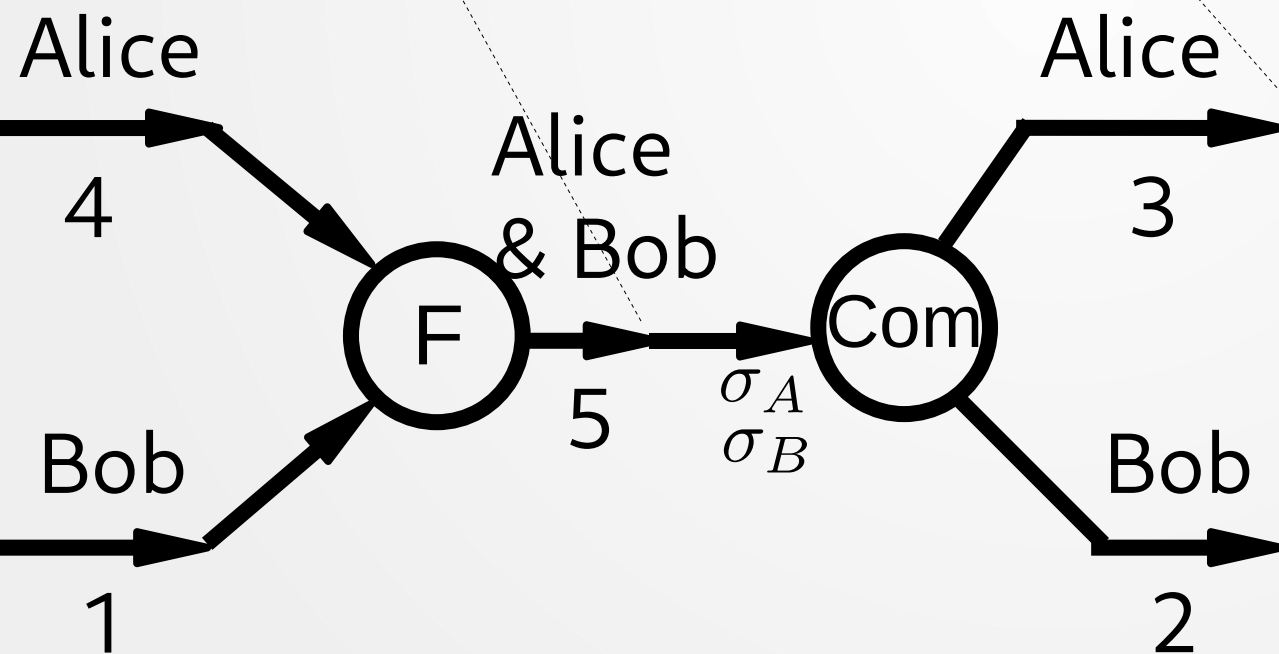
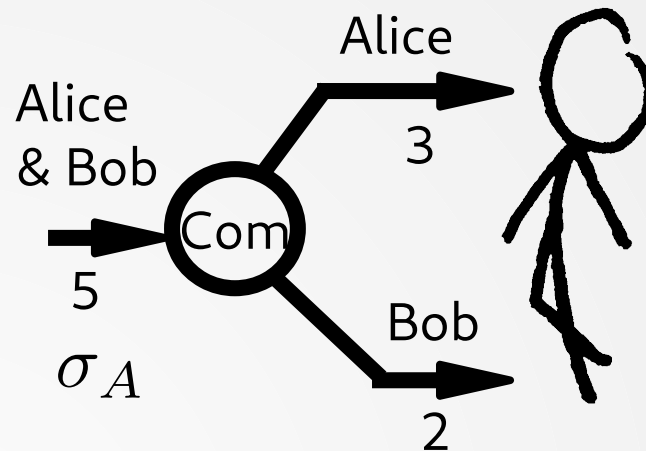
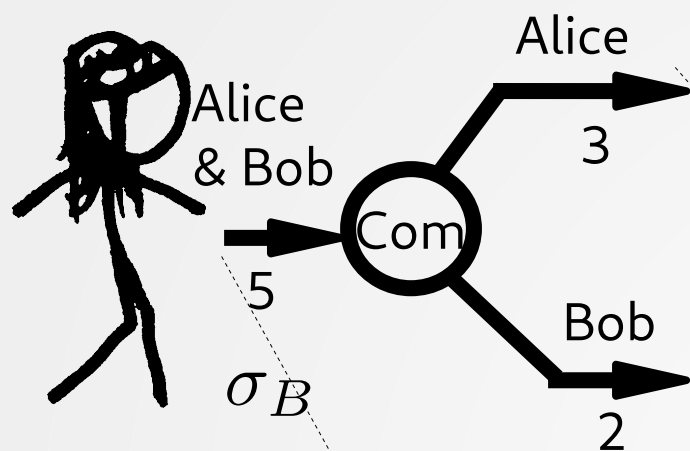
Bob
→
1

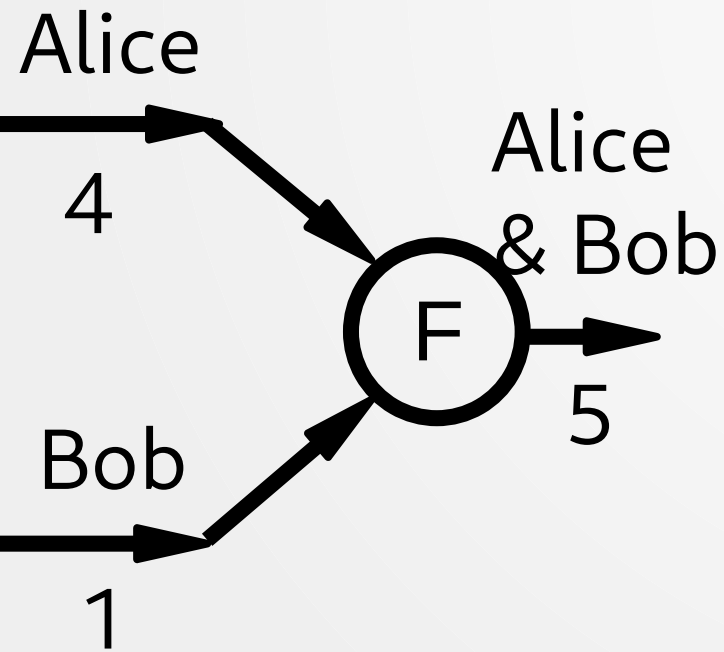
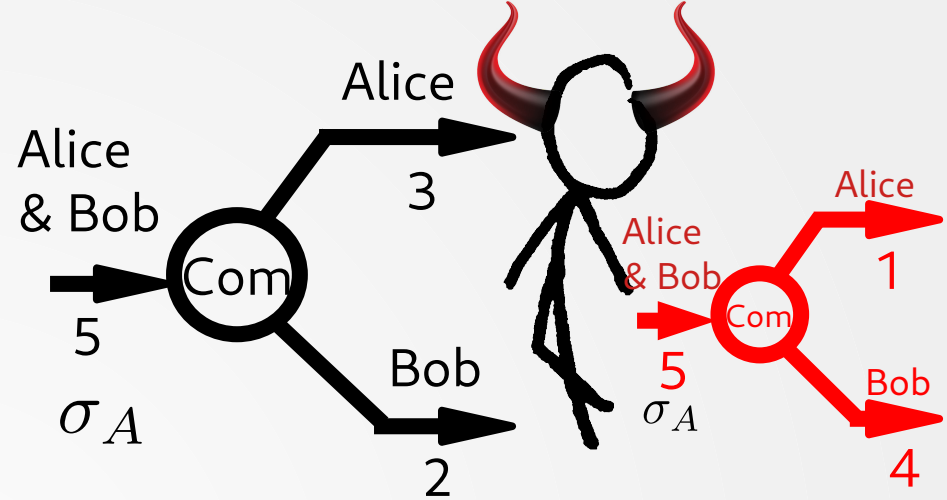
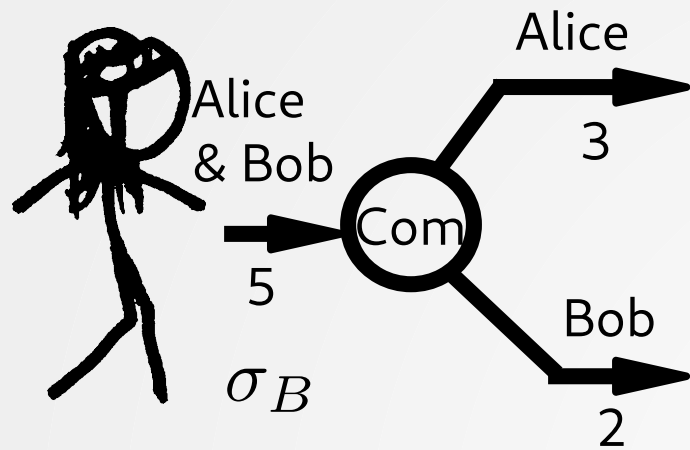


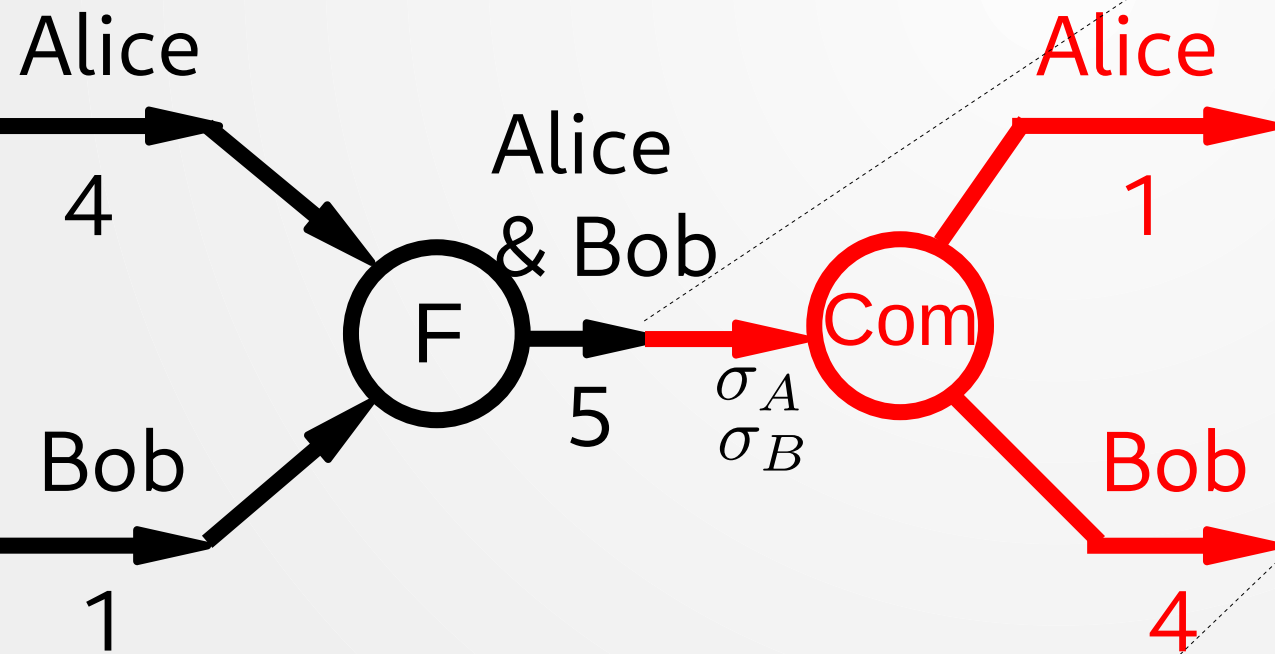
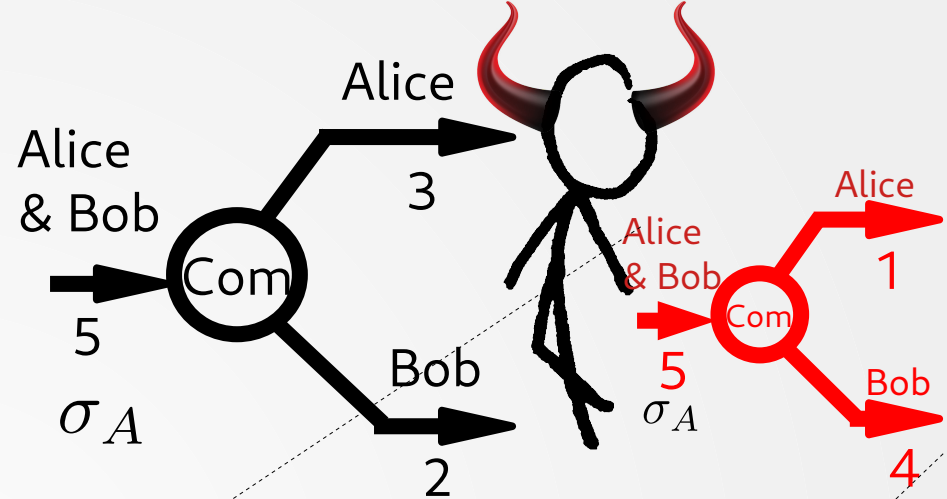
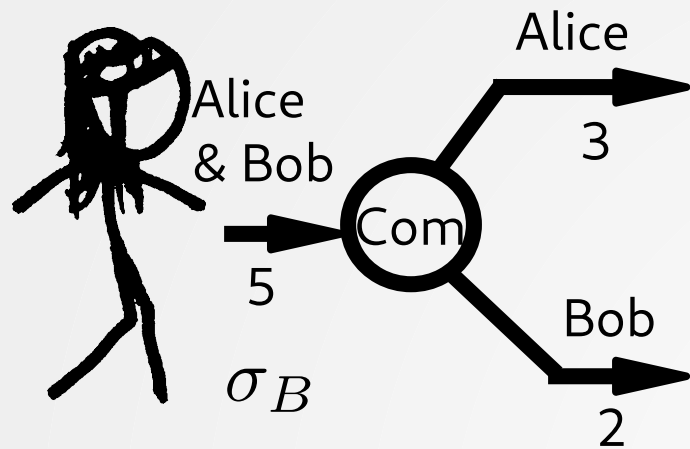


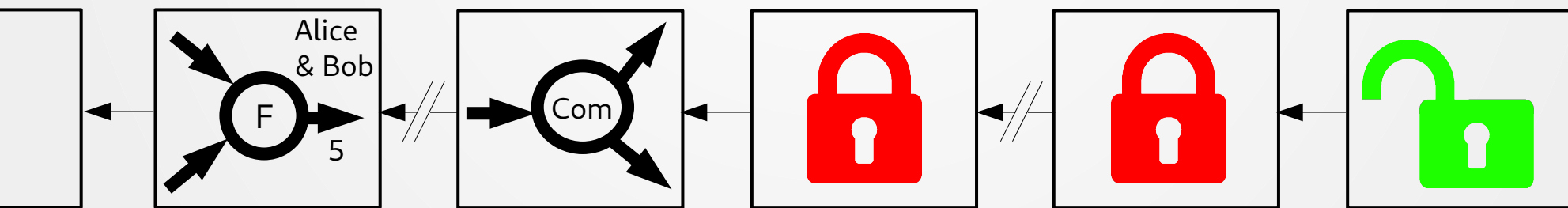
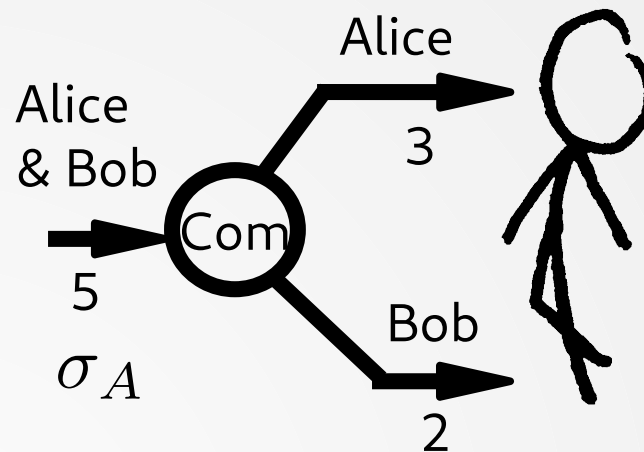
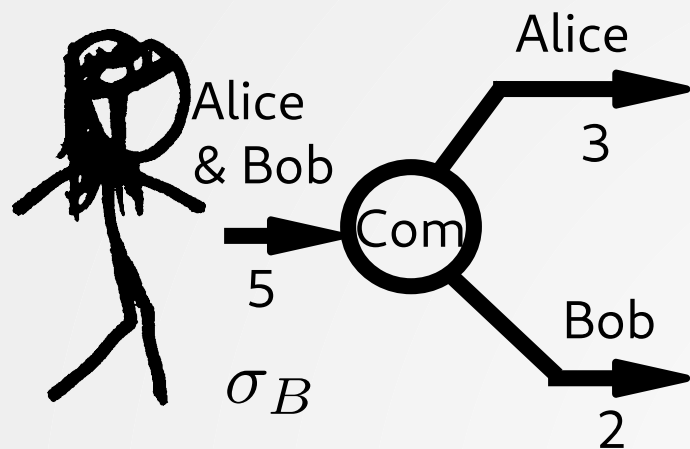


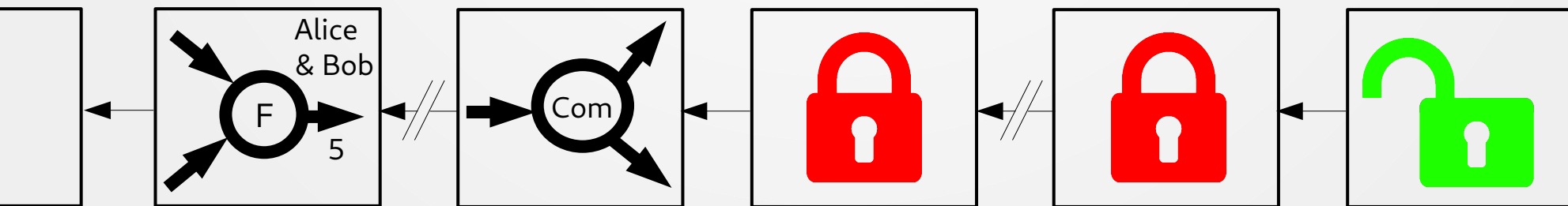
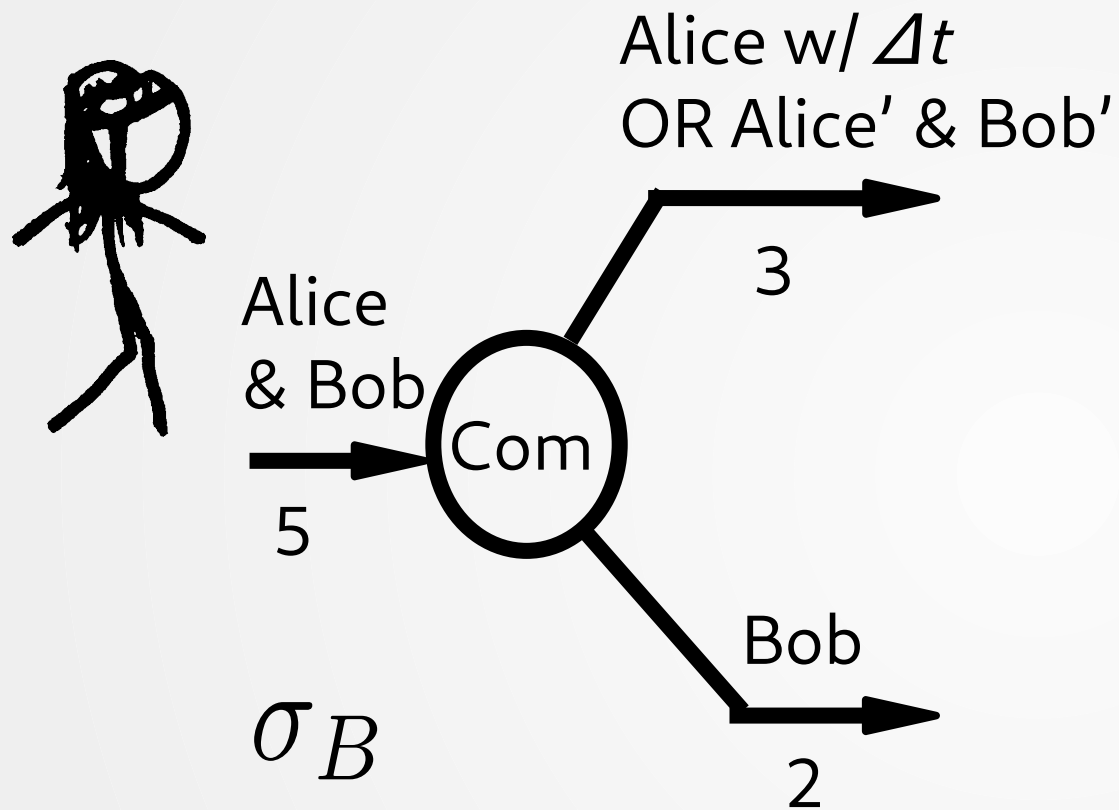




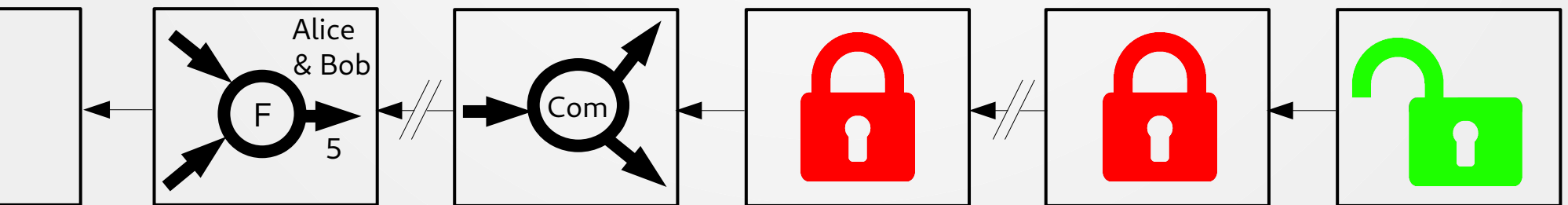
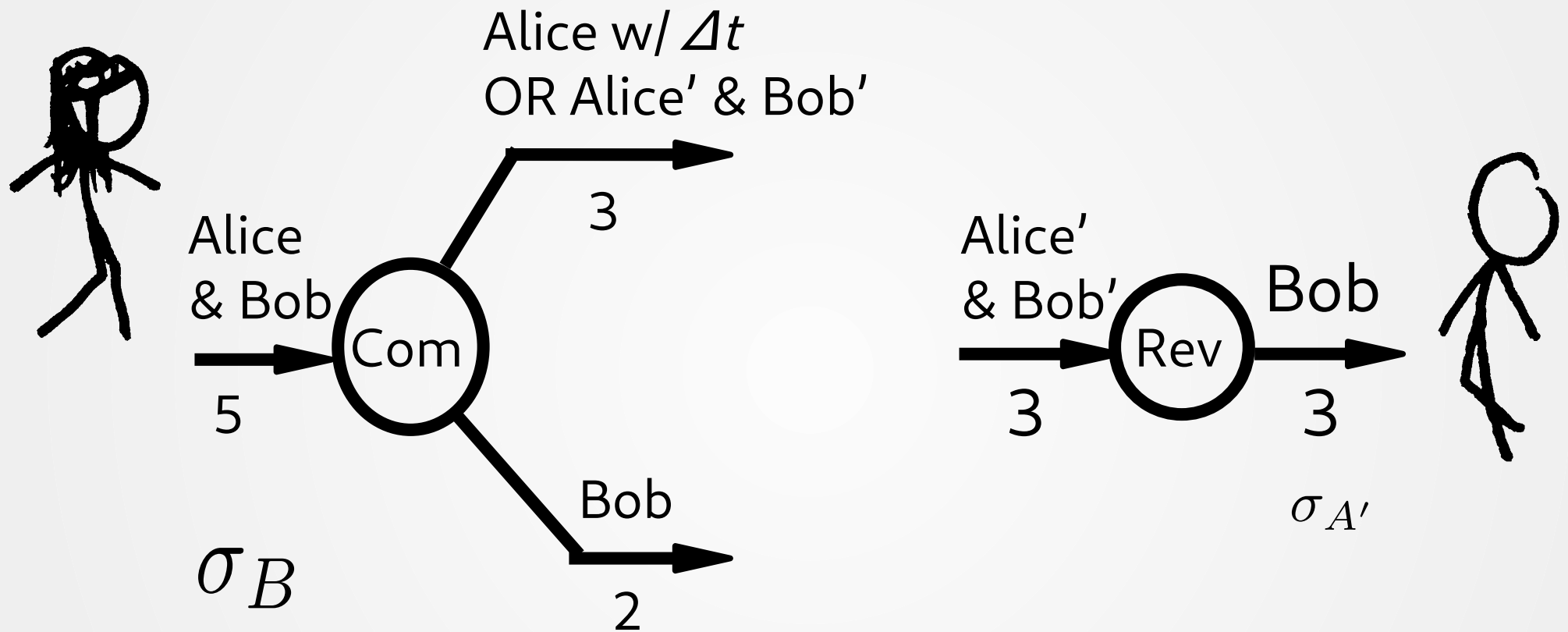








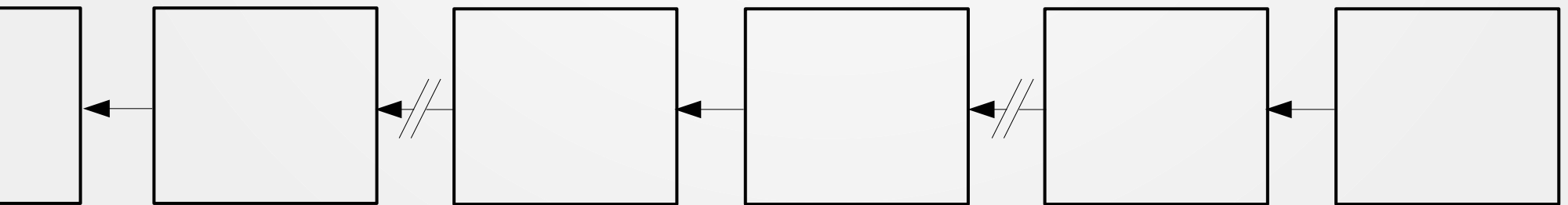
Dispute period t

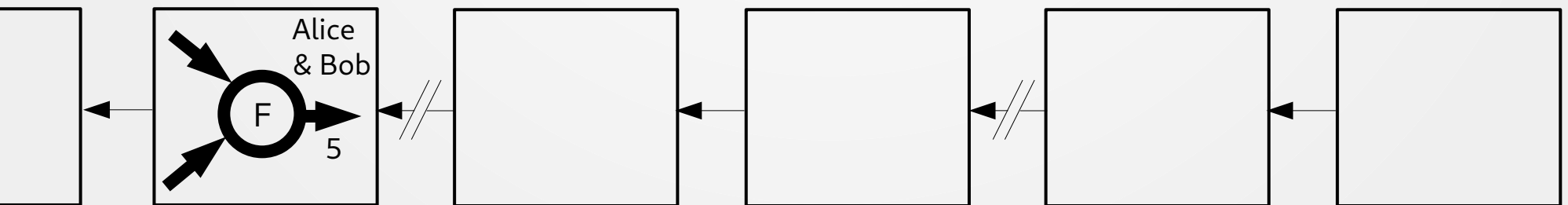
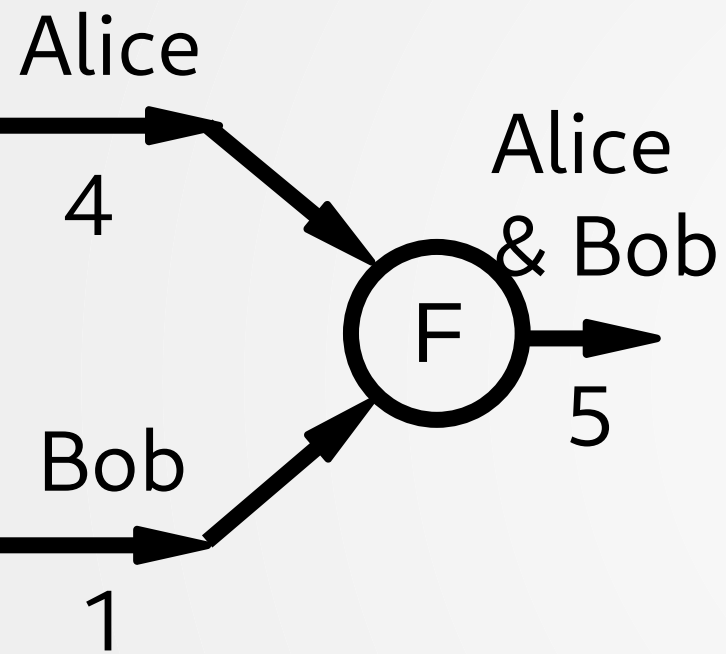


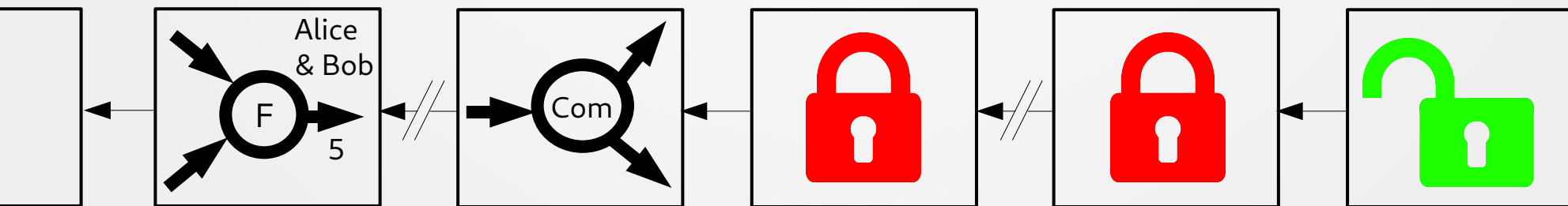
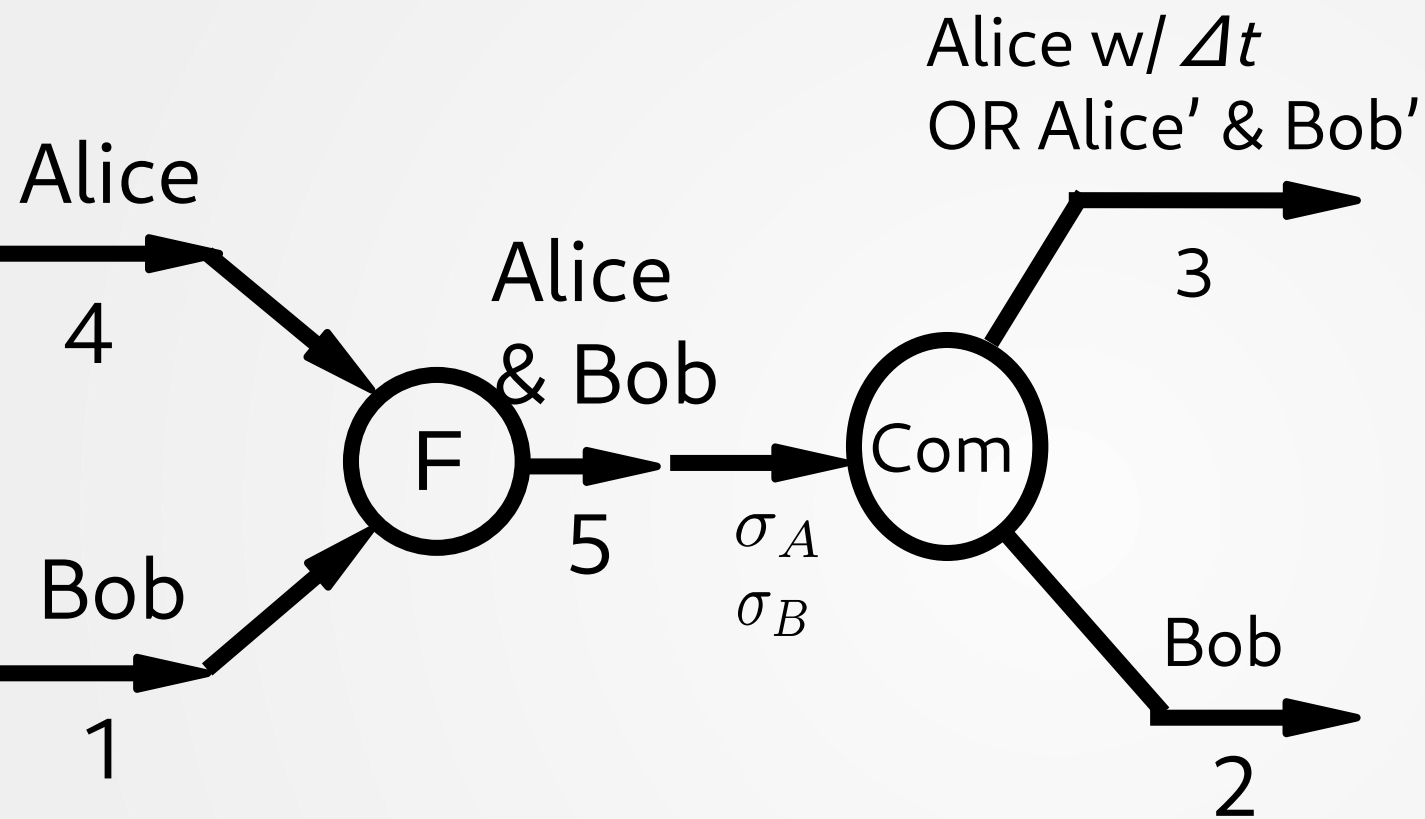
Dispute period t

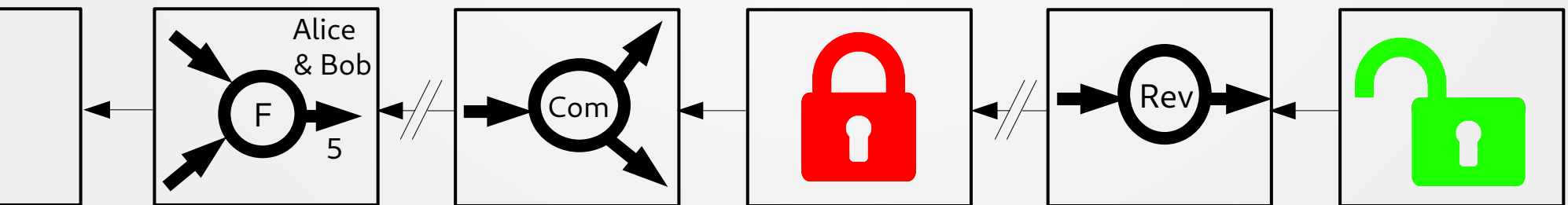
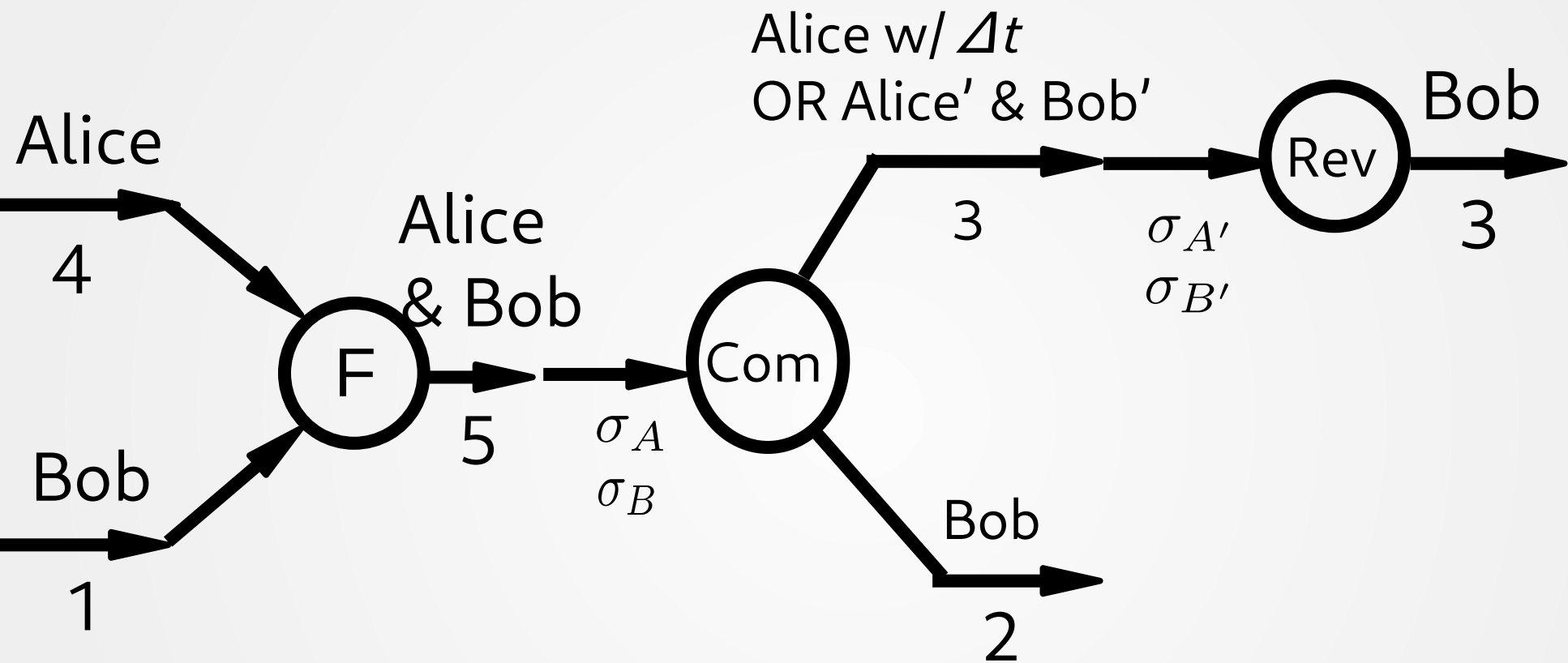
Alice
→
4

Bob
→
1

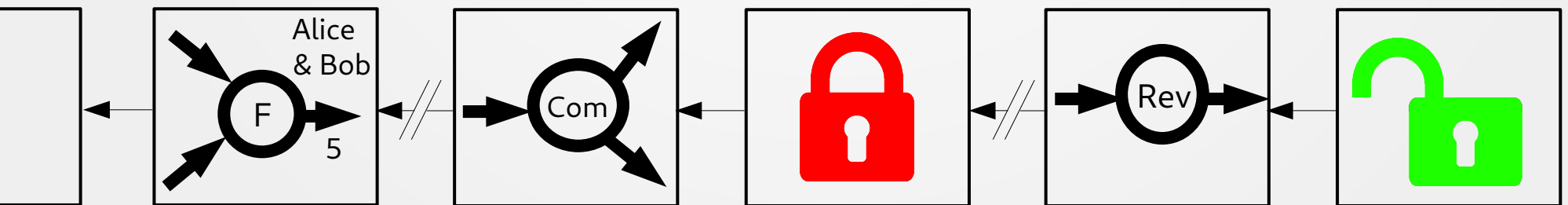
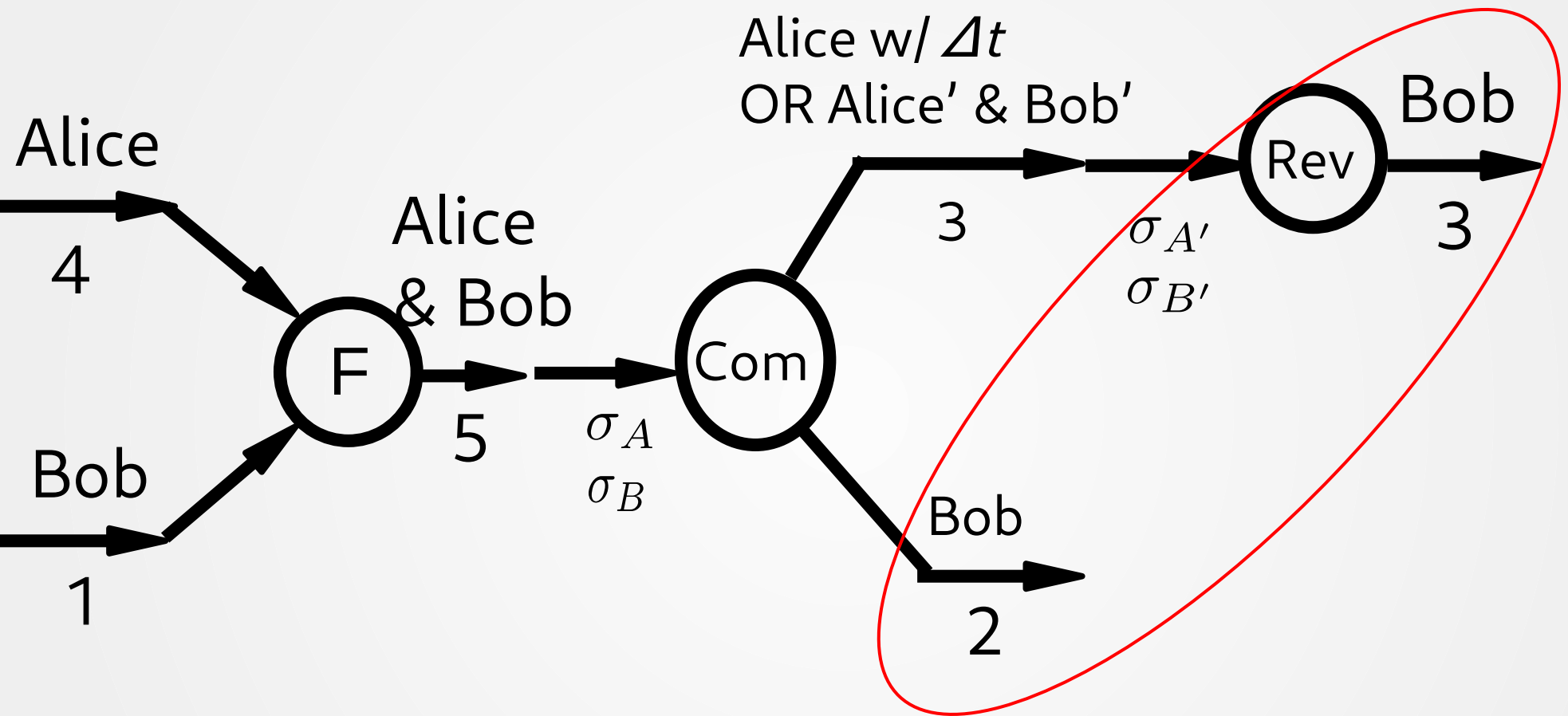








Dispute period t



Dispute period t

Part 2

Multi-hop payments

Multi-hop payments

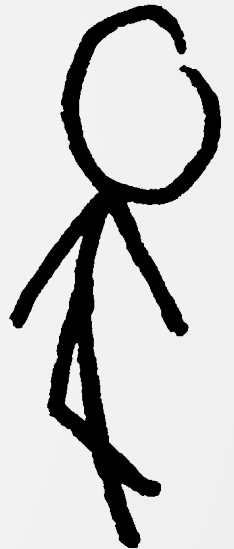


Alice
Charlie



Charlie

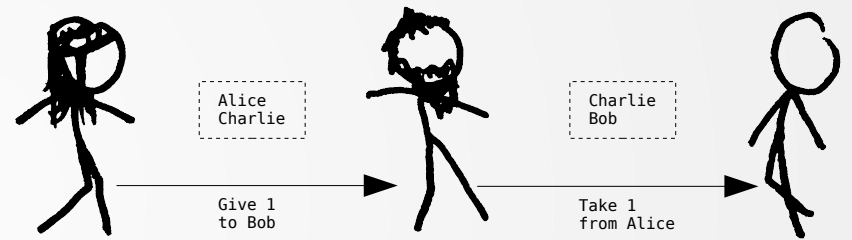
Charlie
Bob



Multi-hop payments

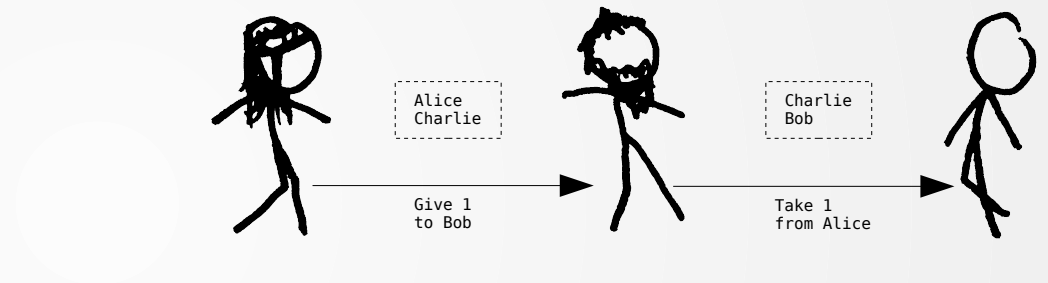


Why no one can cheat?



Why no one can cheat?

HTLC

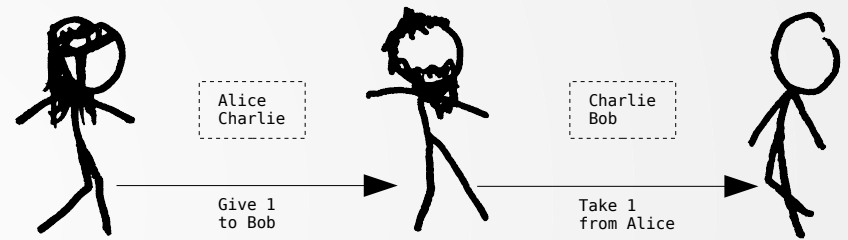


"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of **0xabcdef** within an hour"

Why no one can cheat?

HTLC

"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of `0xabcdef` within an hour"

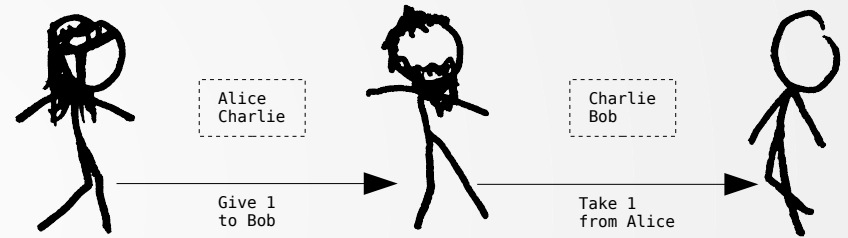


- Bob chooses random **R**, computes **$h=H(R)$**
- Bob sends **h** to Alice

Why no one can cheat?

HTLC

"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of `0xabcdef` within an hour"

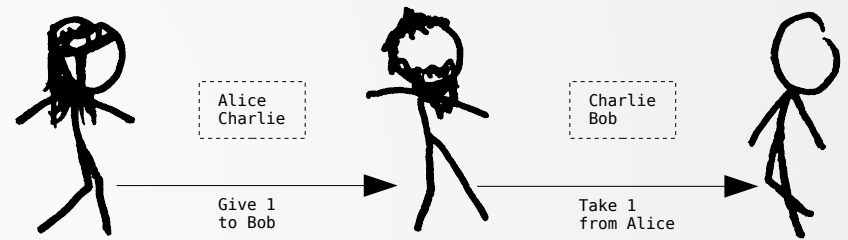


- Bob chooses random **R**, computes **$h=H(R)$**
- Bob sends **h** to Alice
- Alice signs an **h**-HTLC with Charlie
- Charlie signs an **h**-HTLC with Bob

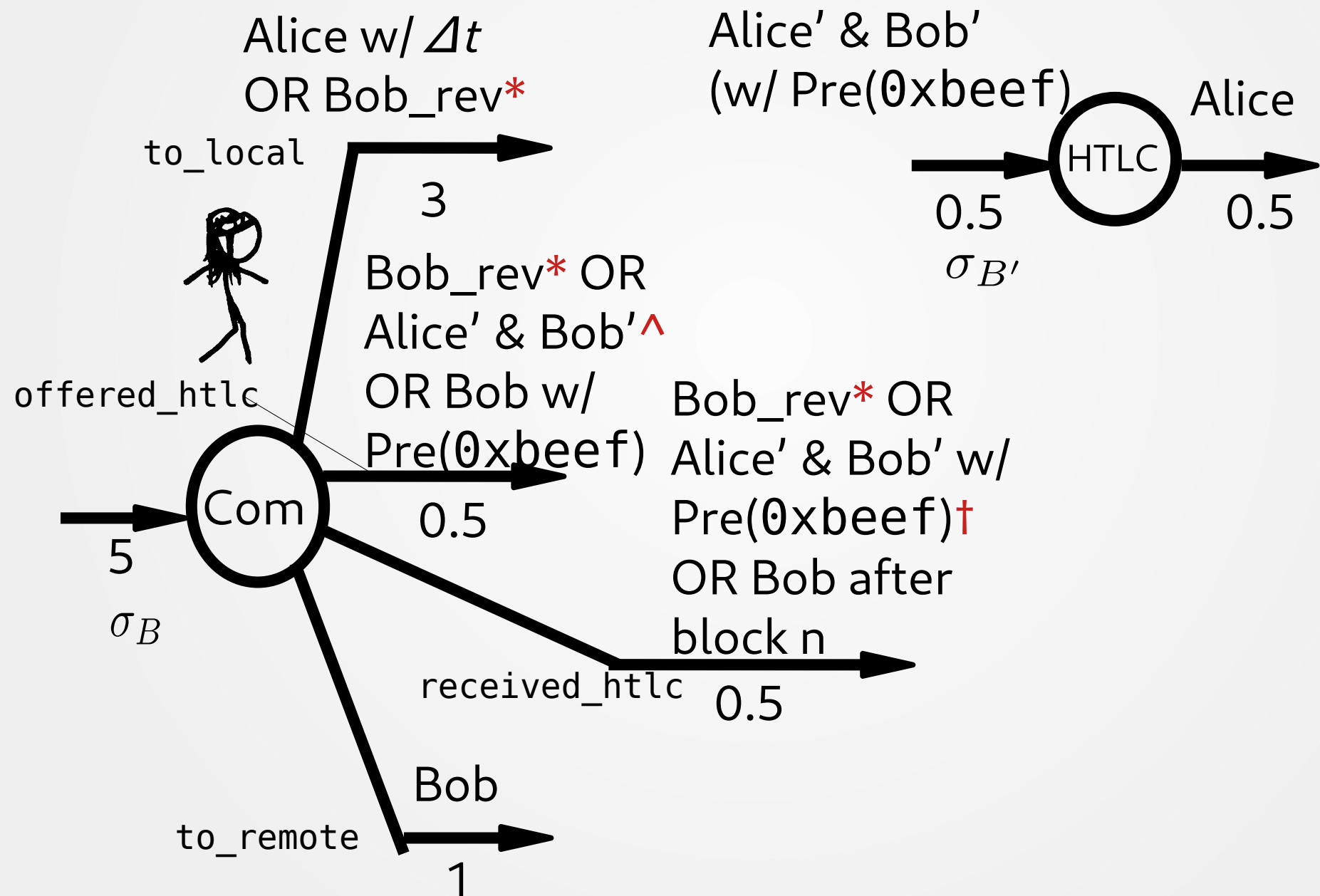
Why no one can cheat?

HTLC

"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of `0xabcdef` within an hour"



- Bob chooses random **R**, computes **$h=H(R)$**
- Bob sends **h** to Alice
- Alice signs an **h**-HTLC with Charlie
- Charlie signs an **h**-HTLC with Bob
- Bob reveals **R** to Charlie, gets 1
- Charlie reveals **R** to Alice, gets 1



*Revocation ^To HTLC-timeout TX †To HTLC-success TX

<https://github.com/lightningnetwork/lightning-rfc/>

Thank you!