What is the Lightning Network?

eclair

LND

Orfeas Stefanos Thyfronitis Litos

University of Edinburgh

20,000 tx/s

7 tx/s

insta*

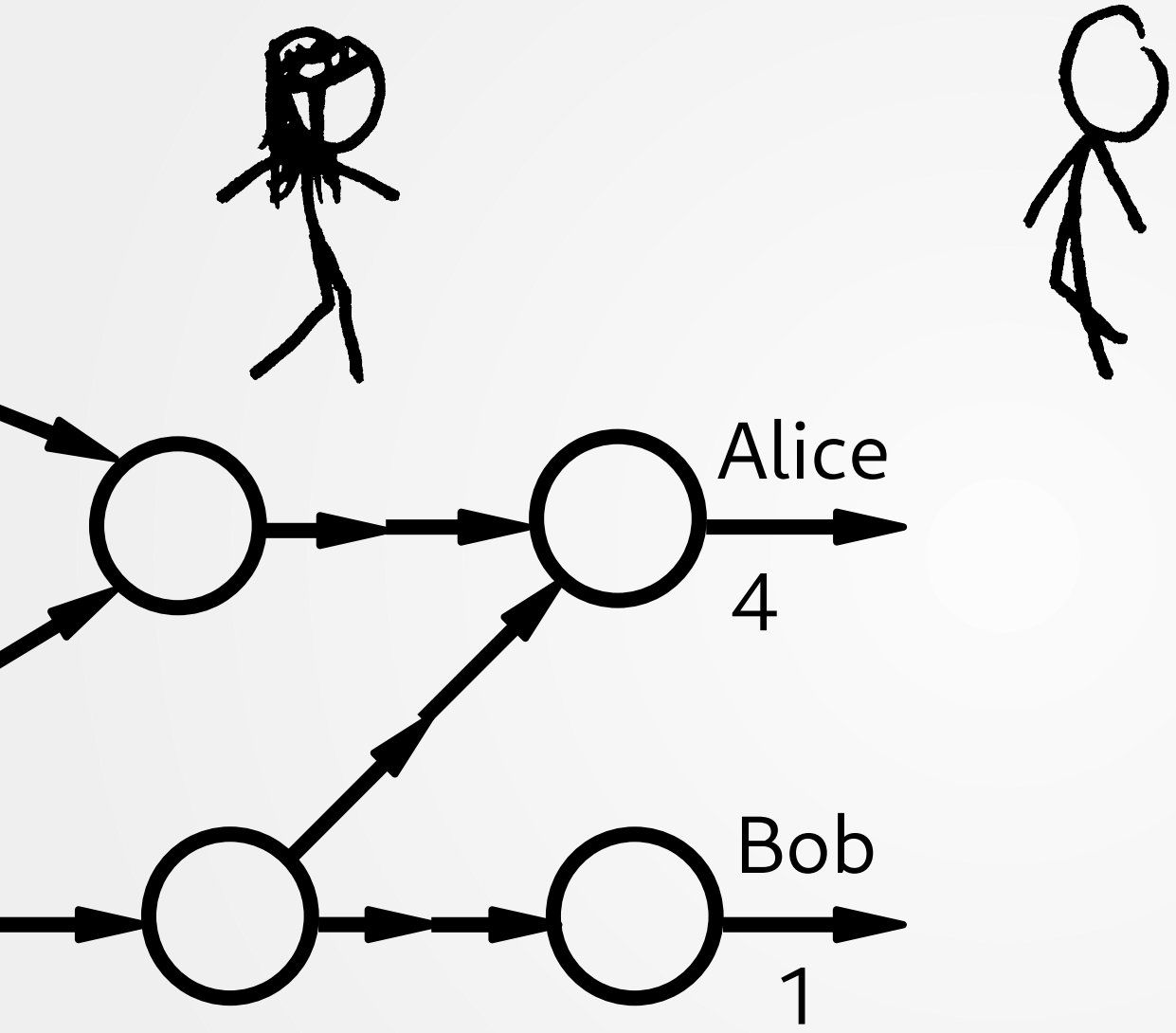
1 hour

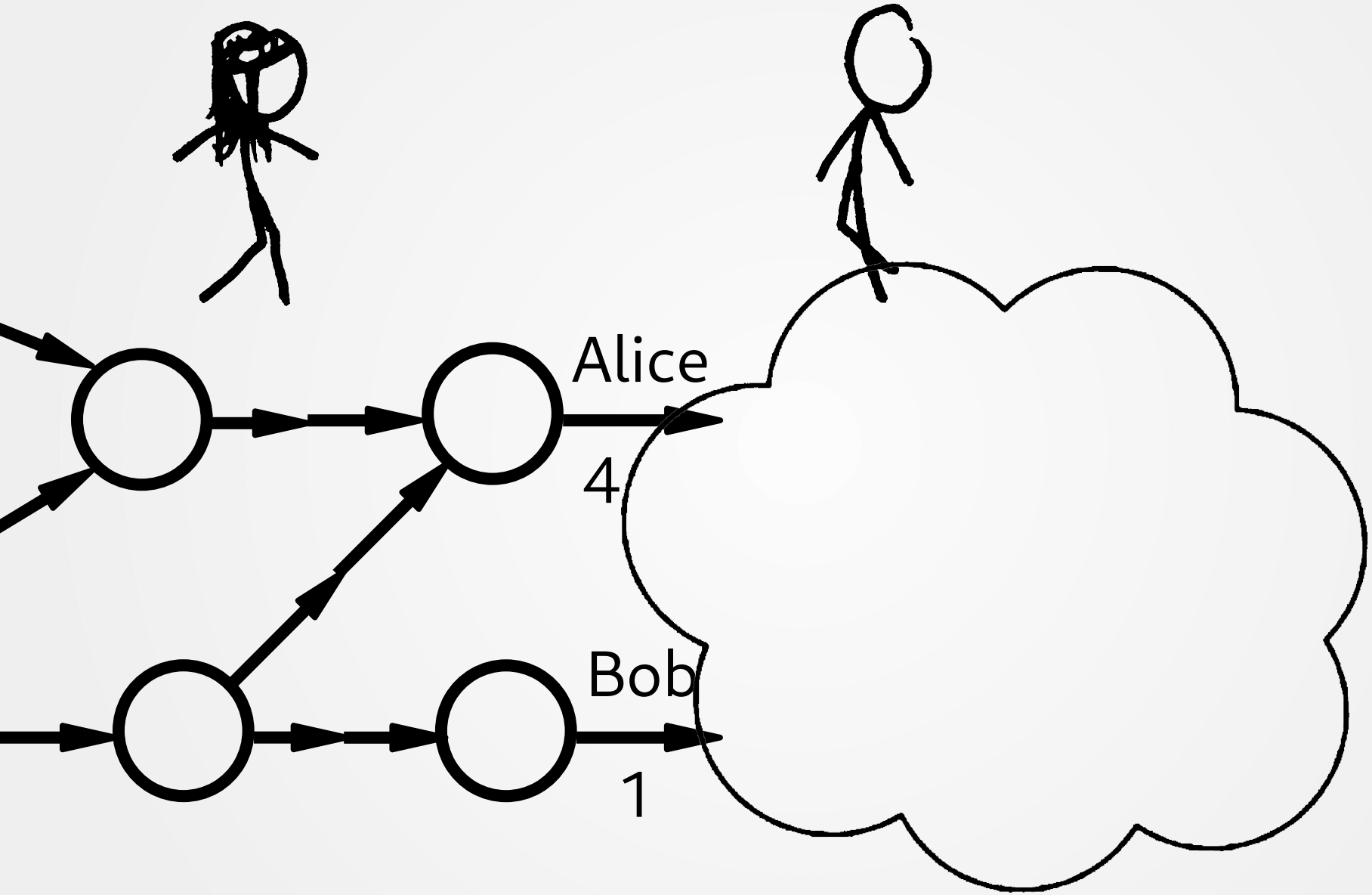
Problem
All txs validated by all wallets

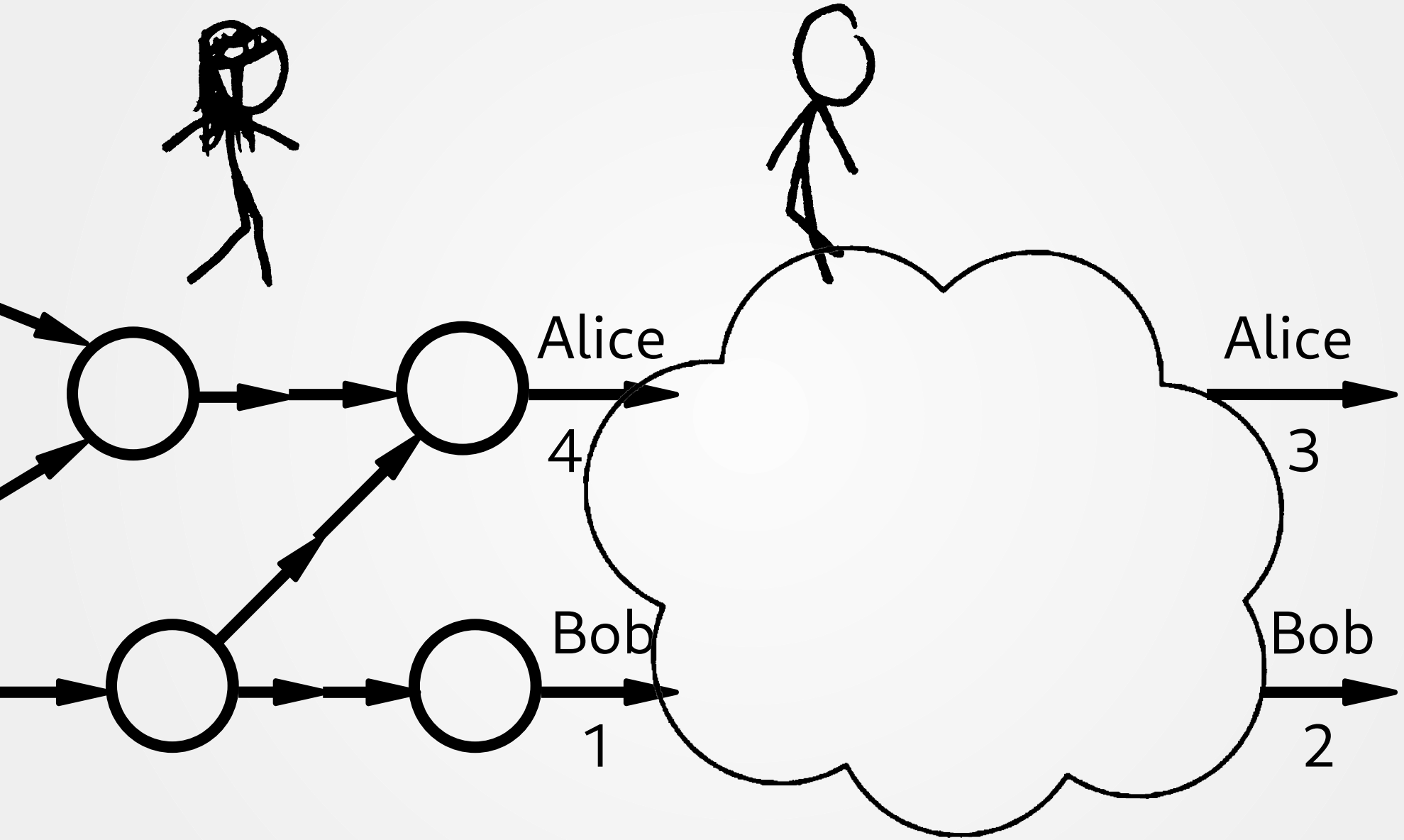
Problem
All txs validated by all wallets

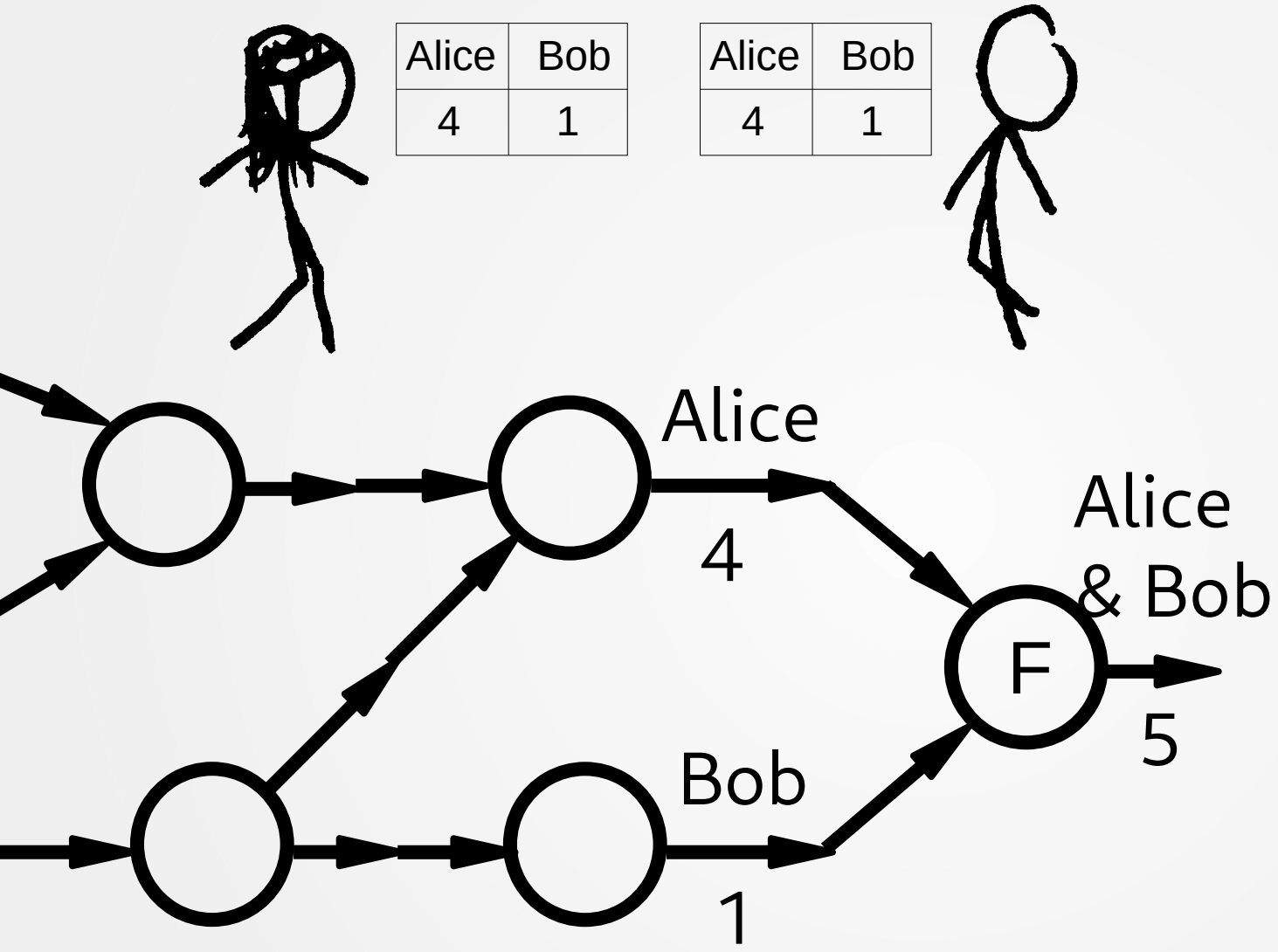
Solution
- Move most txs off-chain
- Resolve disputes on-chain

Part 1
2-party channels


Alice
4
Bob
1

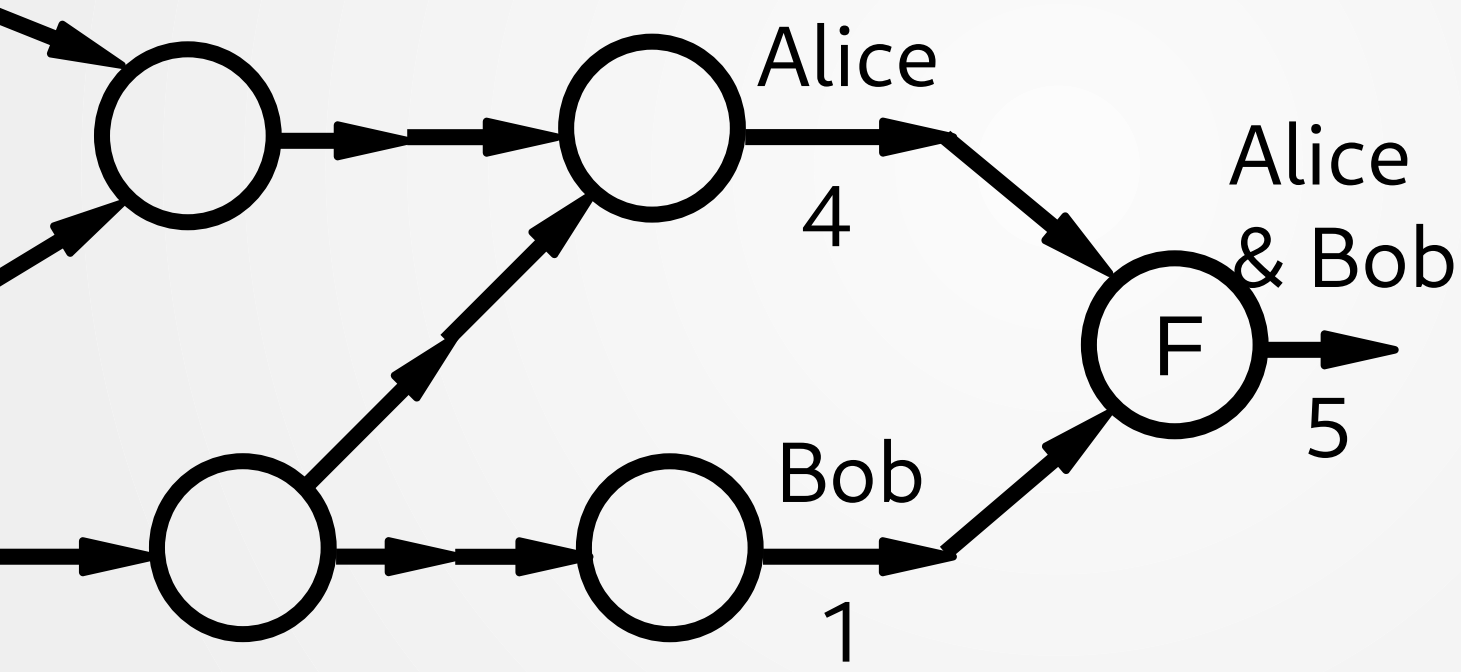

Alice
4
Bob
1


Alice
4
Alice
3
Bob
1
Bob
2


Alice
Bob
4
1
Alice
Bob
4
1
Alice
4
Alice
& Bob
F
5
Bob
1

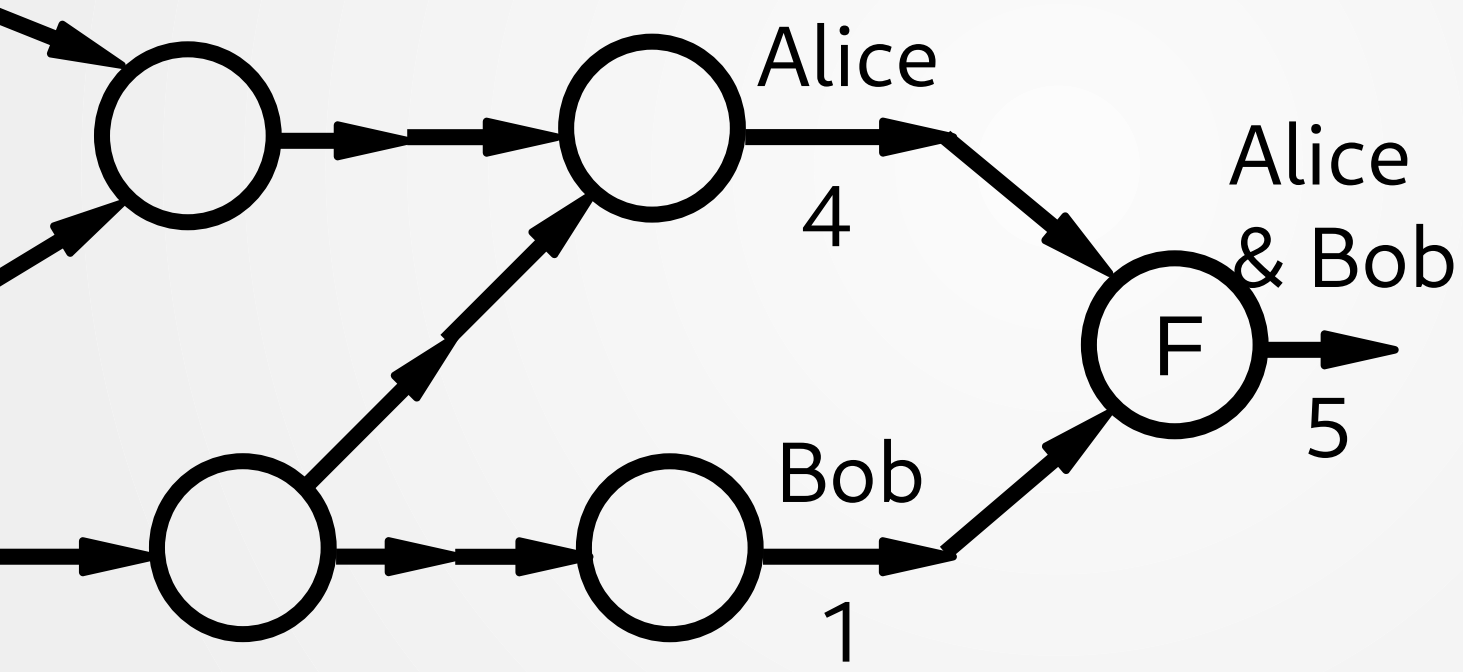
Alice	Bob
4	1
1	4

Alice	Bob
4	1
1	4



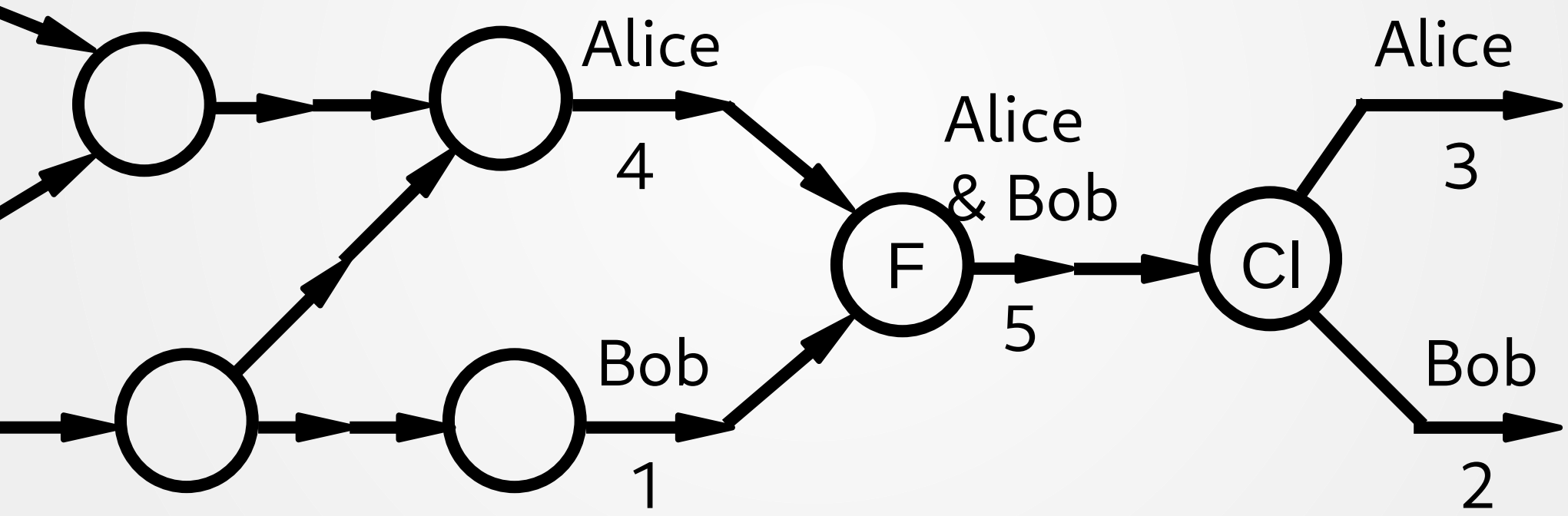
Alice	Bob
4	1
1	4
…	
3	2

Alice	Bob
4	1
1	4
…	
3	2



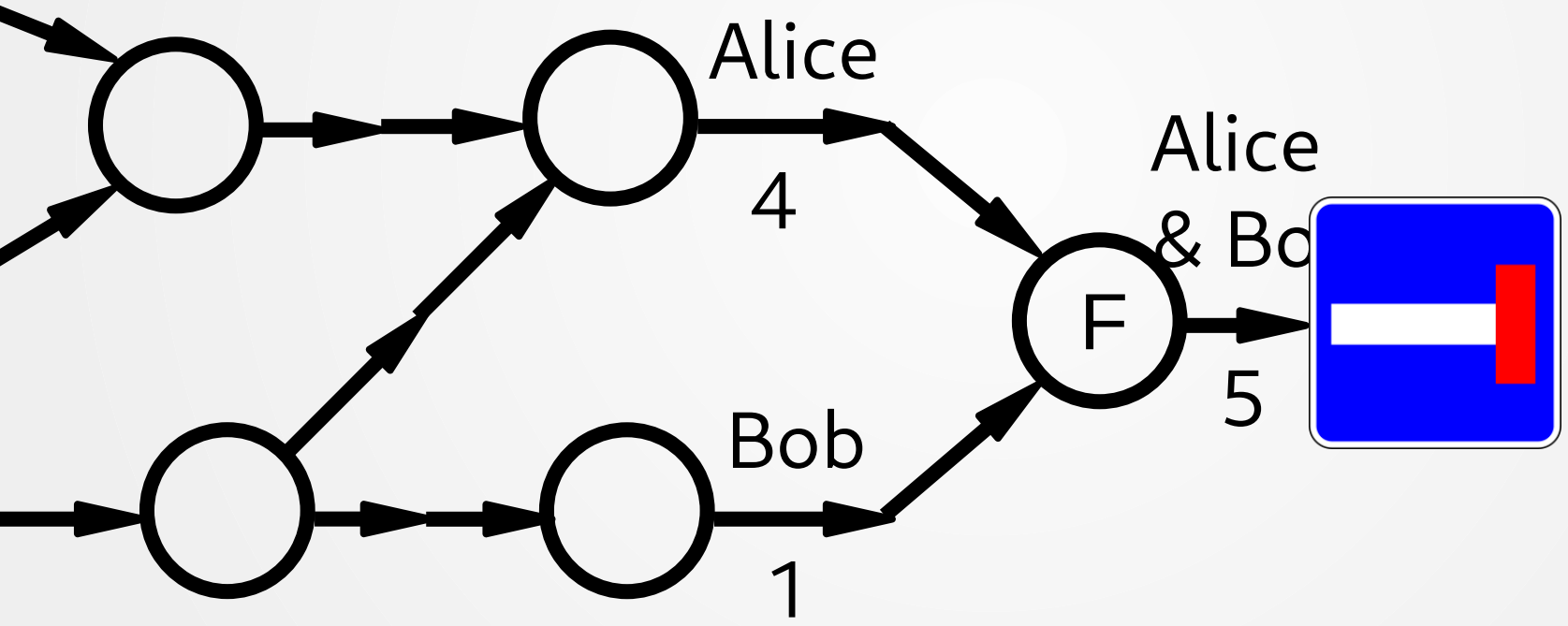
Alice	Bob
4	1
1	4
…	
3	2

Alice	Bob
4	1
1	4
…	
3	2



Alice	Bob
4	1
1	4
…	
3	2

Alice	Bob
4	1
1	4
…	
0.1	4.9

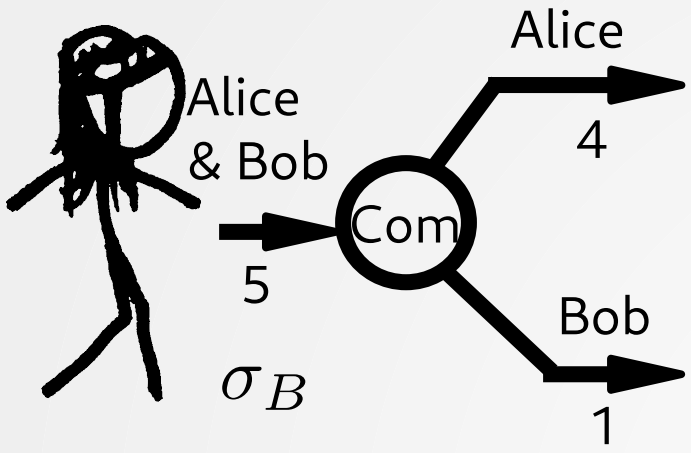


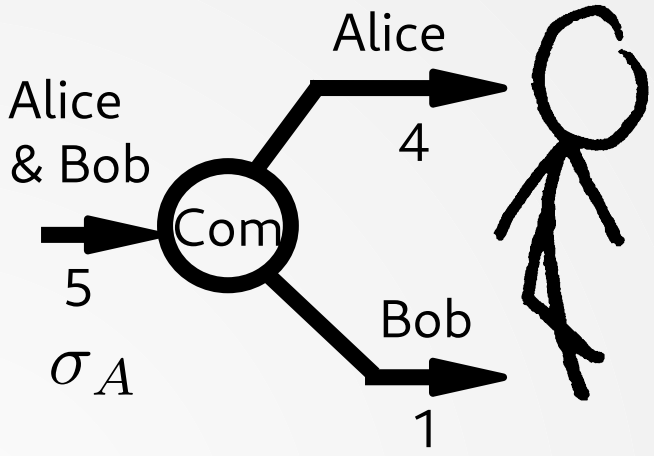
Alice

4

Bob

1


Alice
Alice
& Bob
Com
4
5
Bob
σ_B
1

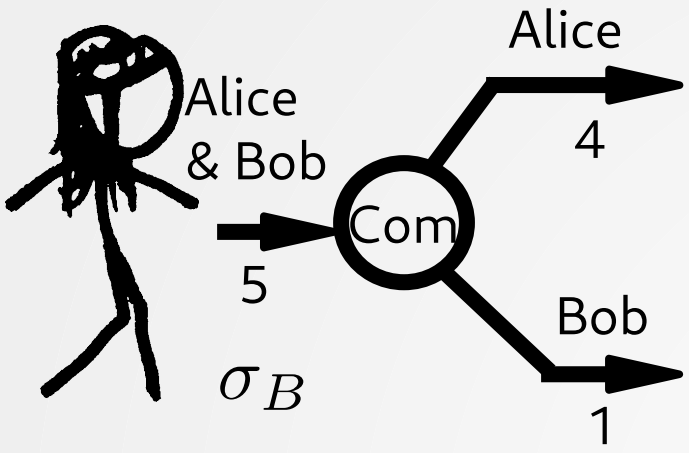

Alice
Alice
& Bob
4
Com
5
Bob
σ_A
1

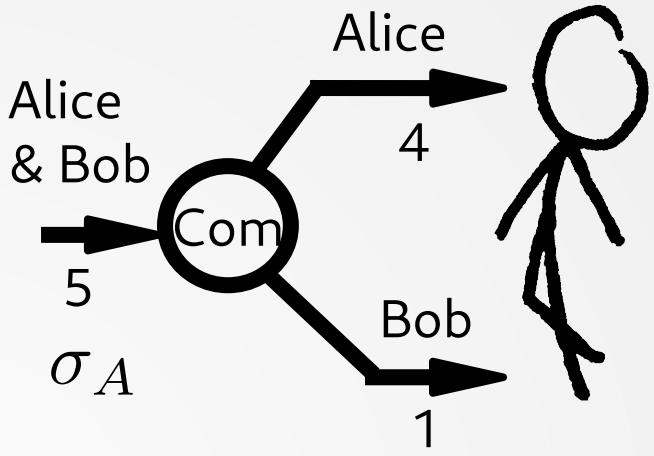
Alice

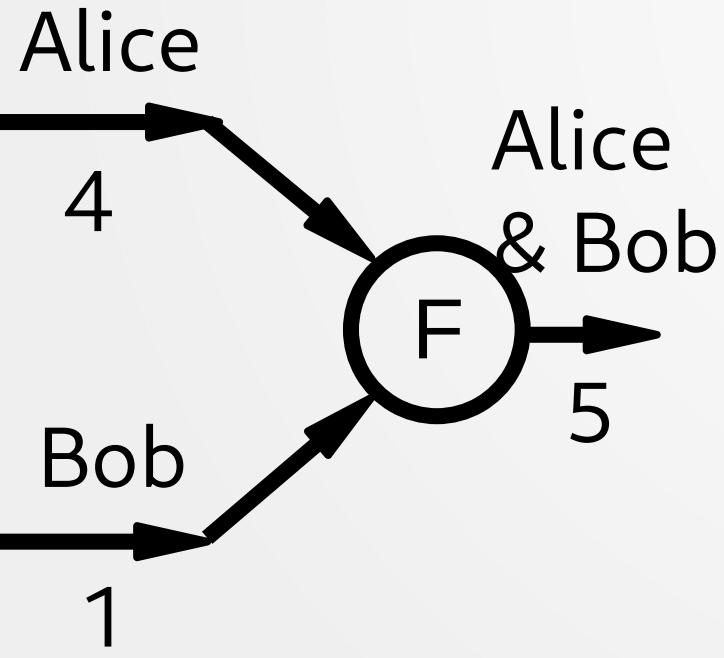
4

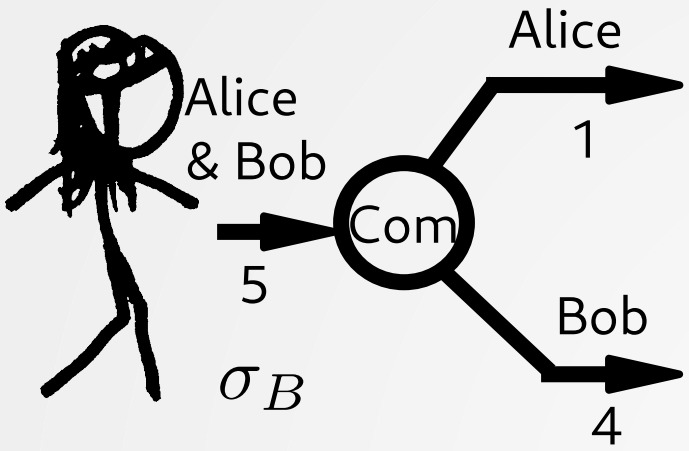
Bob

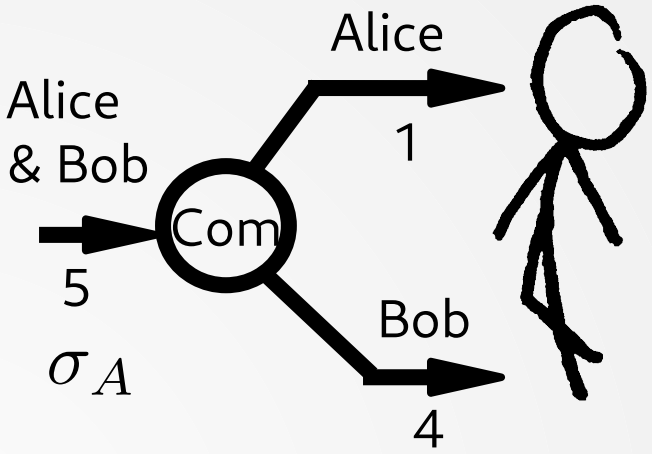
1

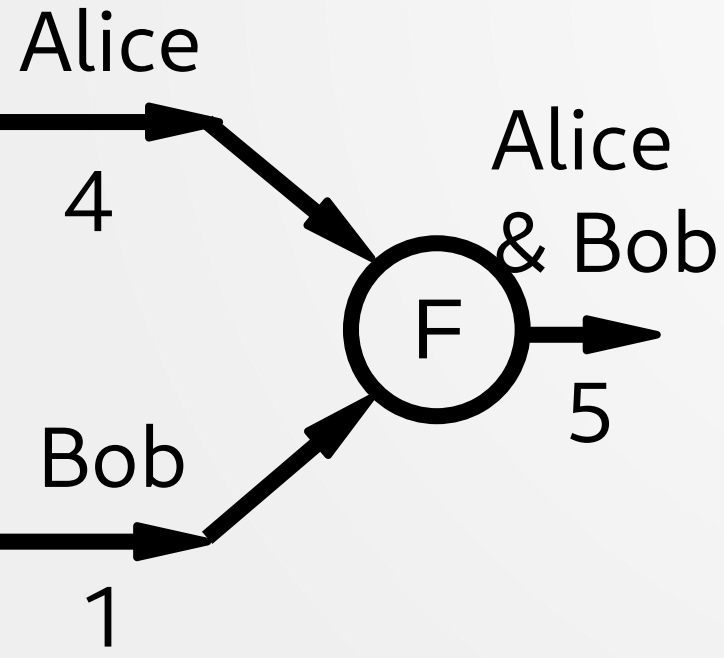

Alice
Alice
& Bob
Com
4
5
Bob
1
σ_B

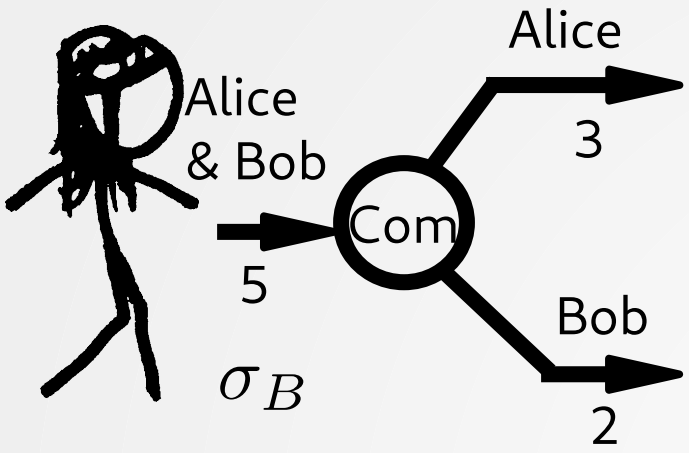

Alice
Alice
& Bob
Com
4
5
Bob
1
σ_A

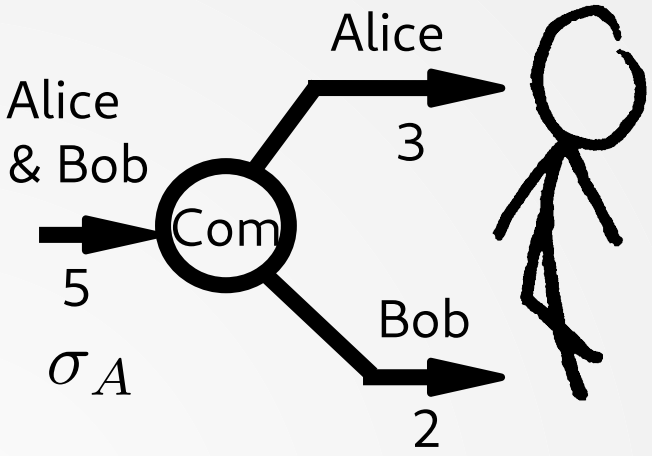

Alice
4
Alice
& Bob
F
5
Bob
1

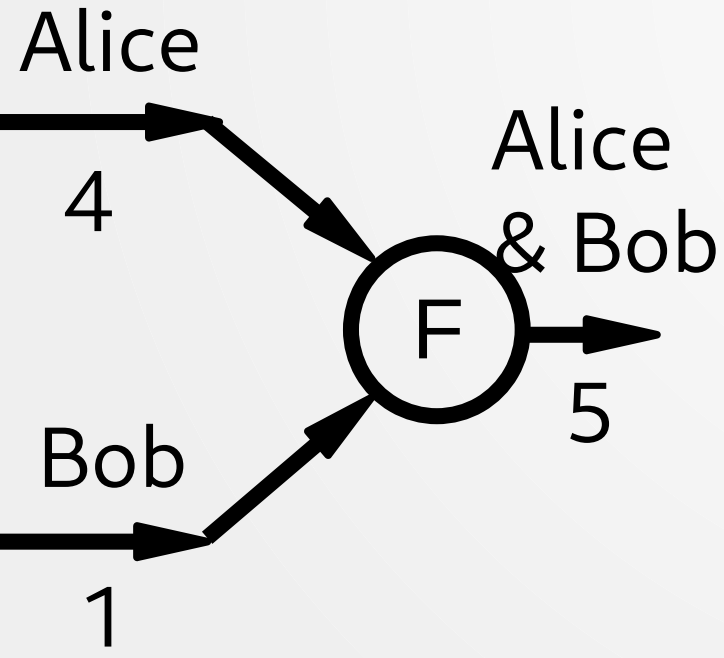

Alice
Alice
& Bob
Com
1
5
Bob
σ_B
4

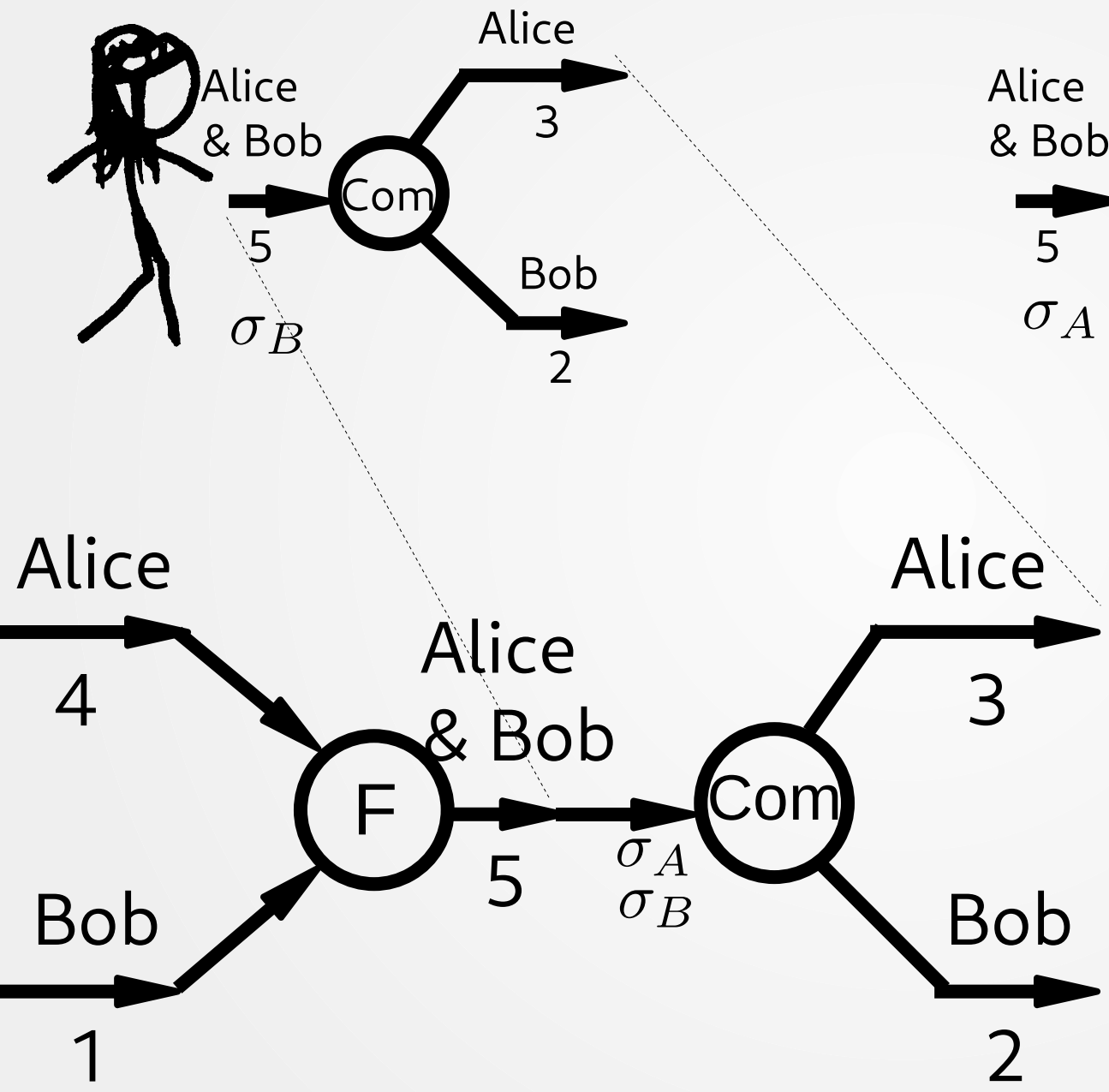

Alice
Alice
& Bob
1
Com
5
Bob
σ_A
4

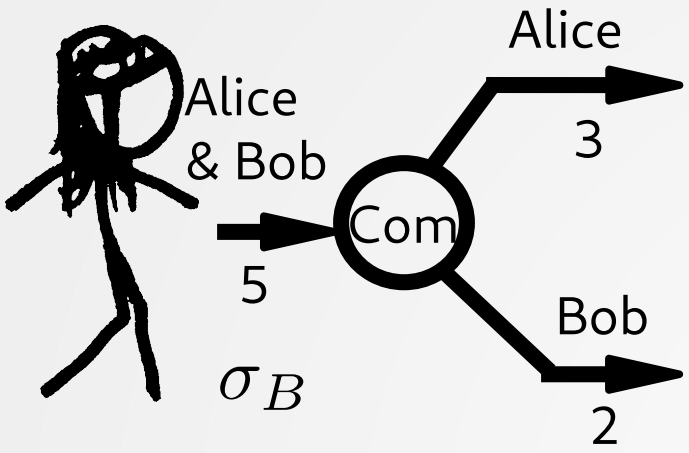

Alice
4
Alice
& Bob
F
5
Bob
1

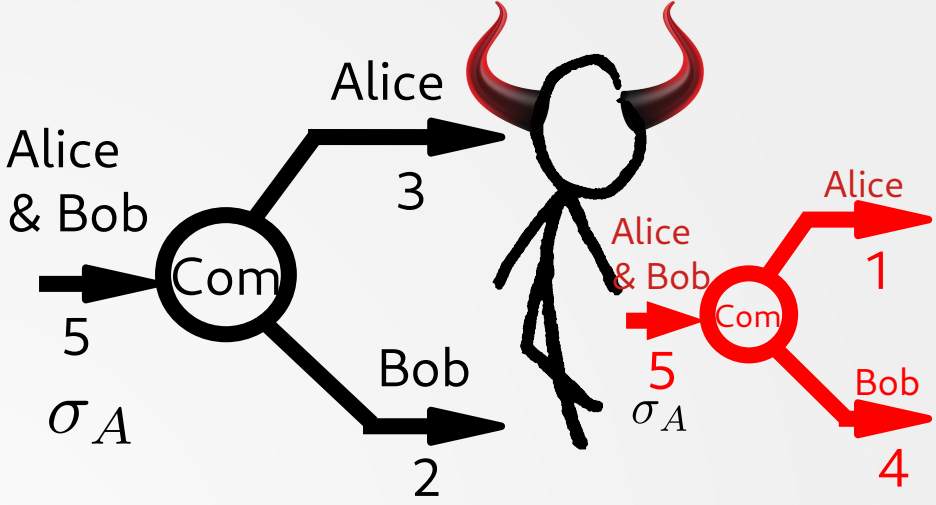

Alice
Alice
& Bob
Com
3
5
Bob
σ_B
2

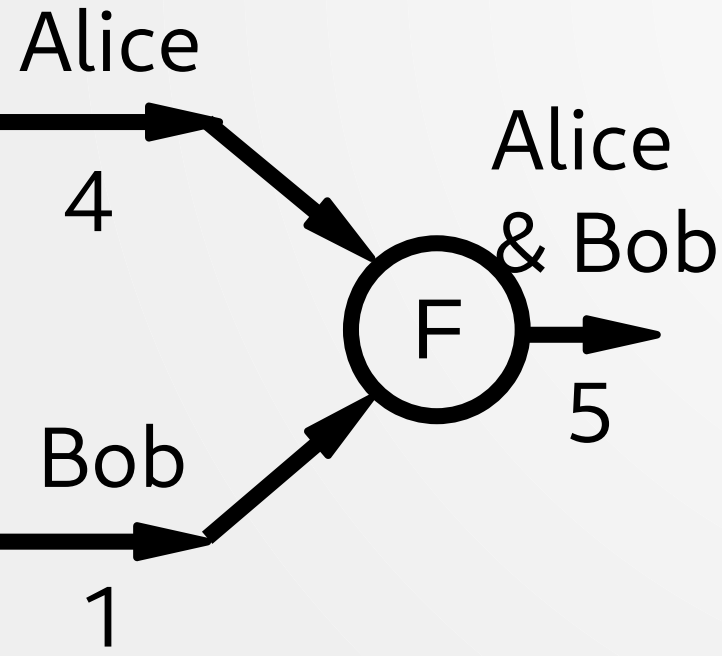

Alice
Alice
& Bob
3
Com
5
Bob
σ_A
2

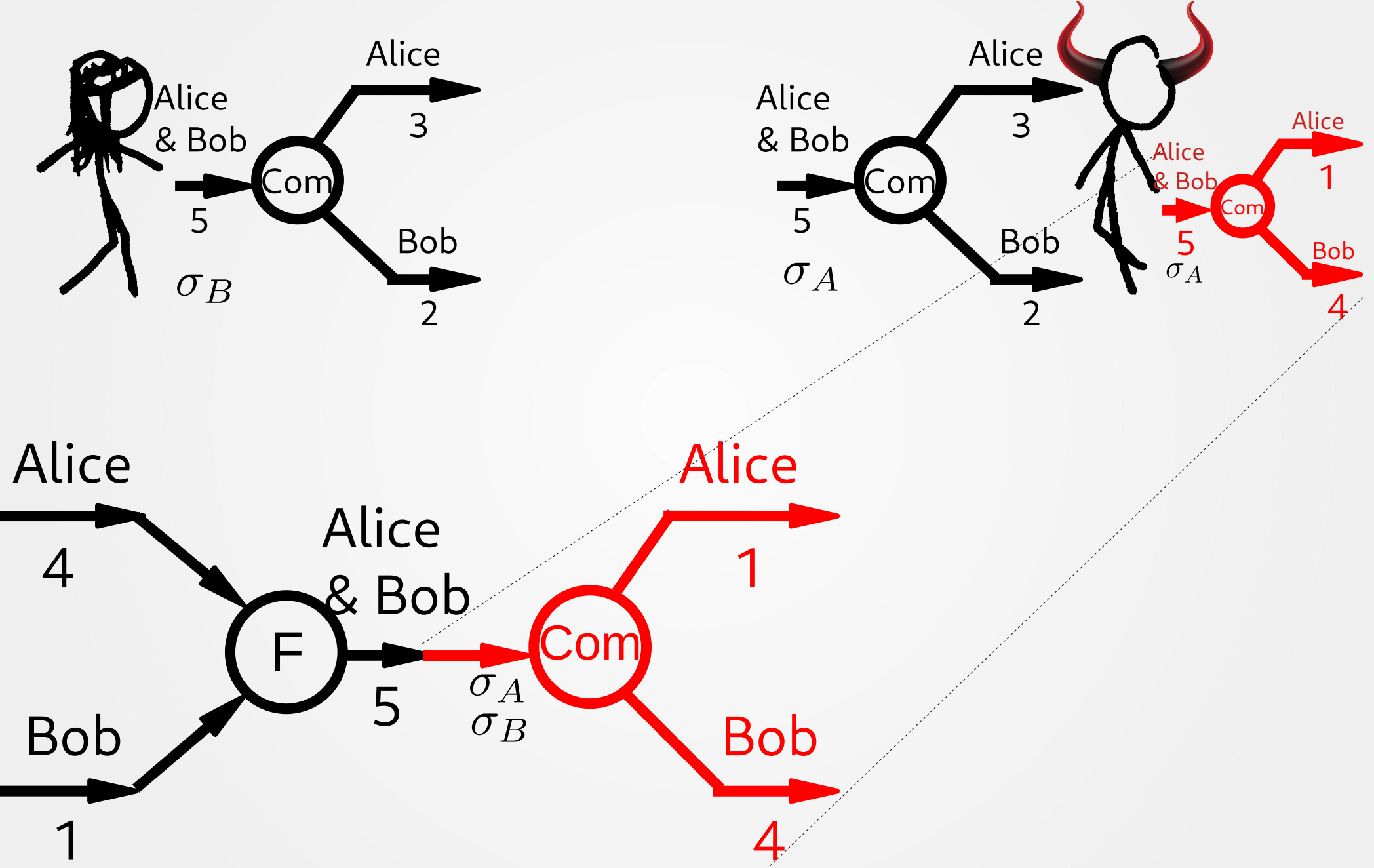

Alice
4
Alice
& Bob
F
5
Bob
1

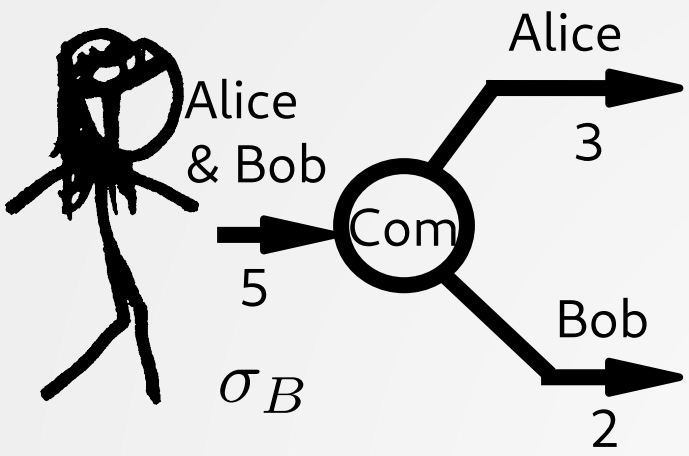

Alice
Alice
& Bob
Com
3
5
Bob
2
σ_B
Alice
Alice
& Bob
Com
3
5
Bob
2
σ_A
Alice
4
Alice
& Bob
F
5
Com
Alice
3
Bob
1
σ_A
σ_B
Bob
2

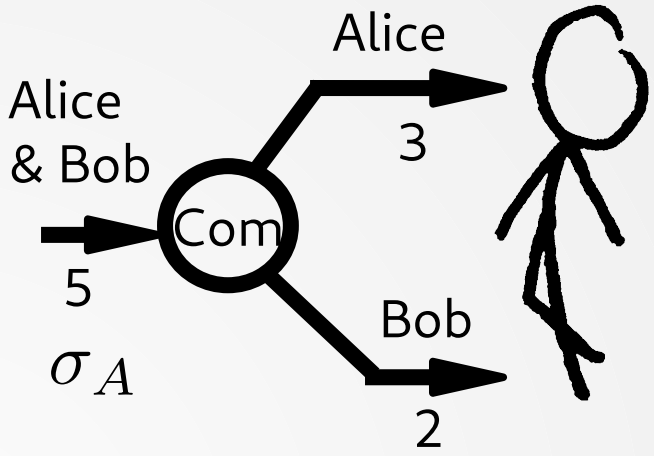

Alice
& Bob
Com
5
3
2
Alice
Bob
σ_B

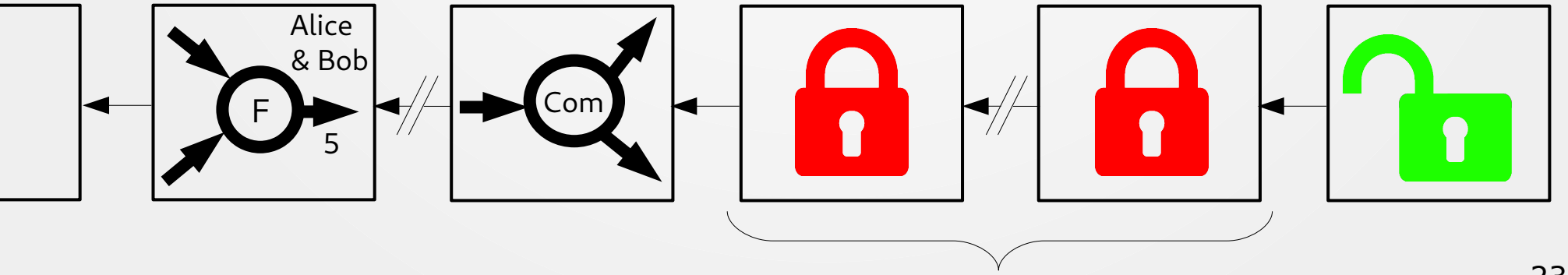

Alice
& Bob
Com
5
3
2
Alice
Bob
σ_A
Alice
& Bob
Com
5
1
4
Alice
Bob
σ_A


Alice
4
Alice
& Bob
F
5
Bob
1

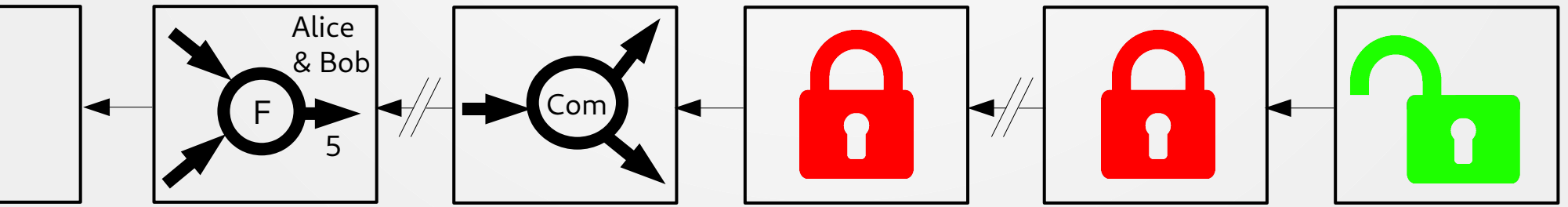

Alice
& Bob
Com
5
σ_B
Alice
3
Bob
2
Alice
& Bob
Com
5
σ_A
Alice
3
Bob
2
Alice
& Bob
Com
5
σ_A
Alice
1
Bob
4
Alice
4
Bob
1
F
Alice
& Bob
5
σ_A
σ_B
Com
Alice
1
Bob
4



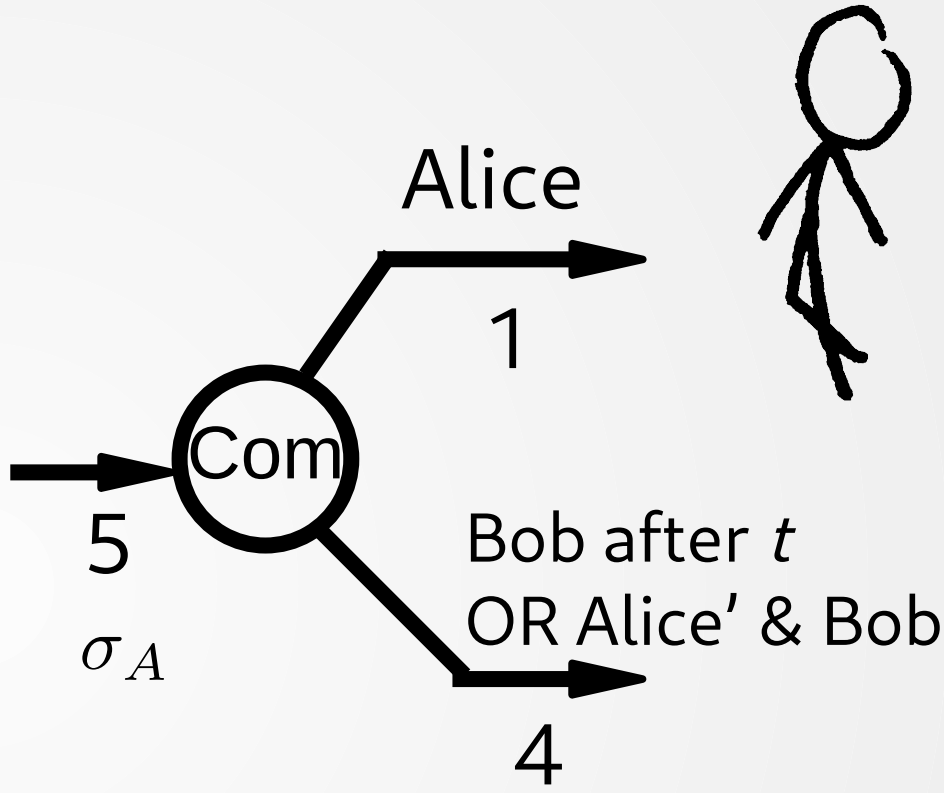


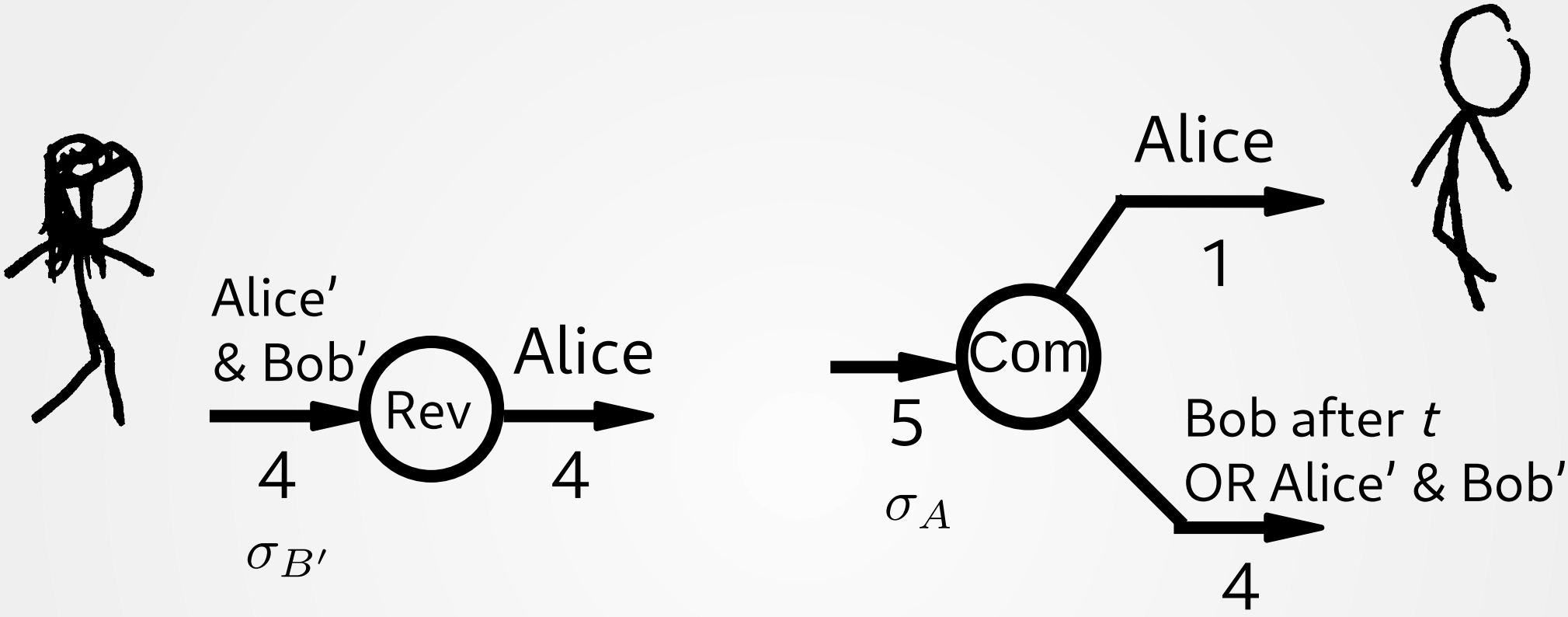


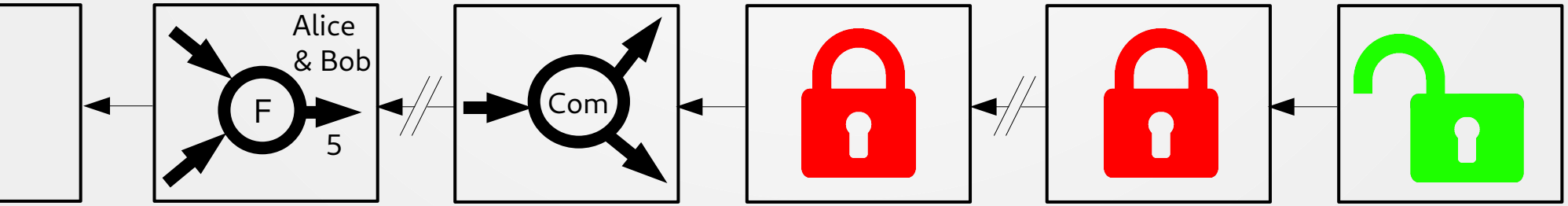
Dispute period



Dispute period t







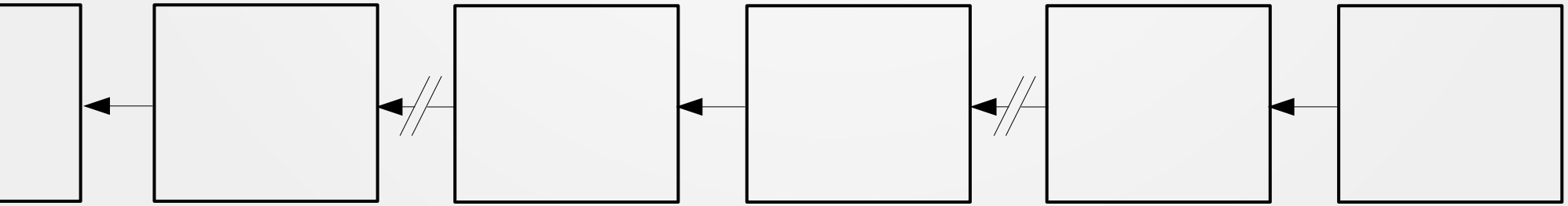
Dispute period t

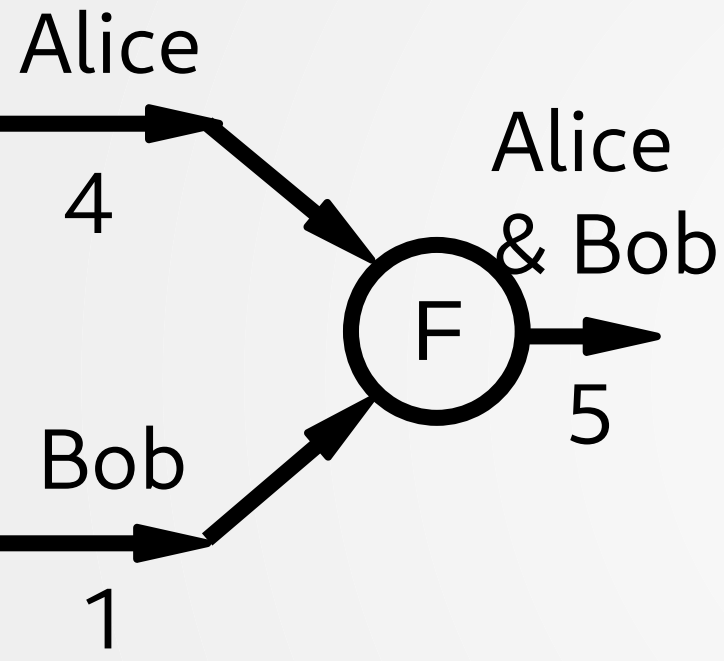
Alice

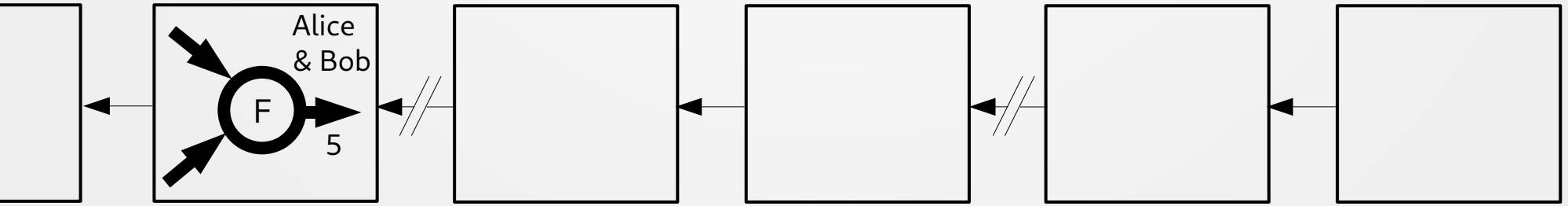
4

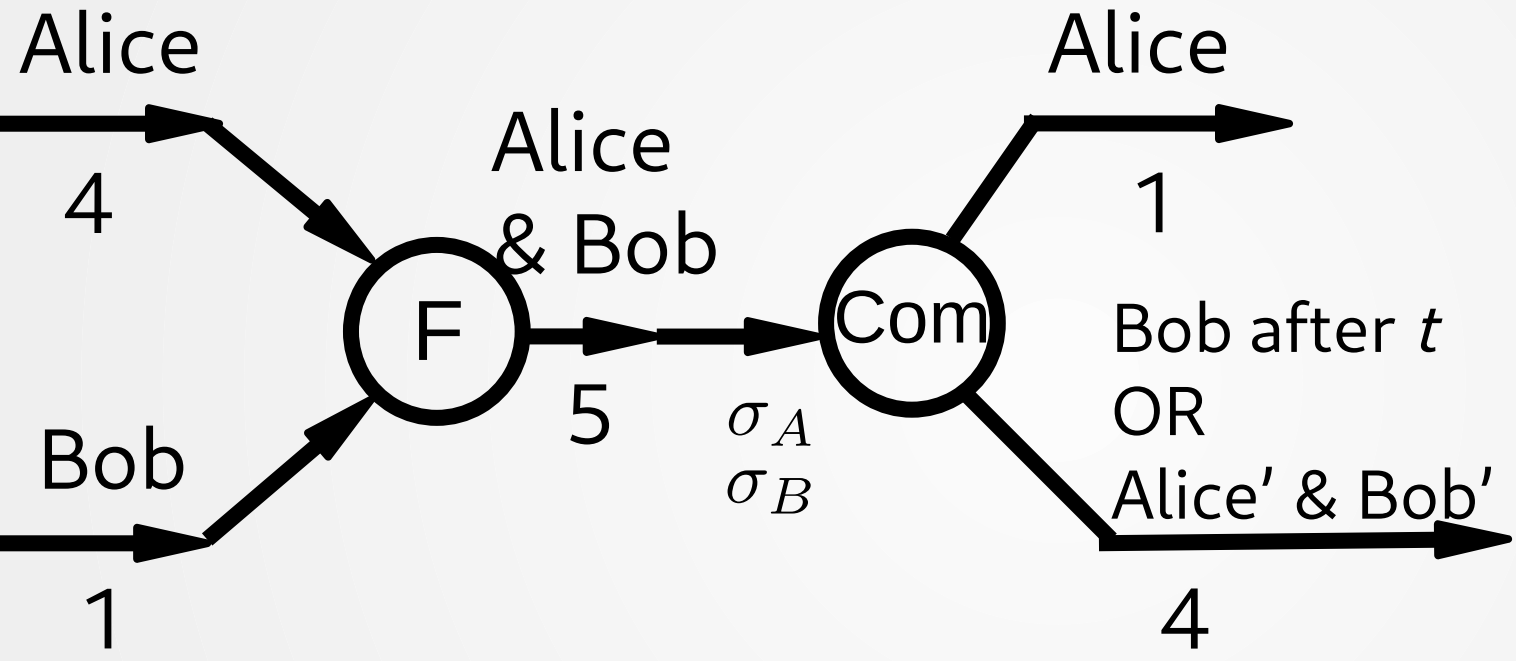
Bob

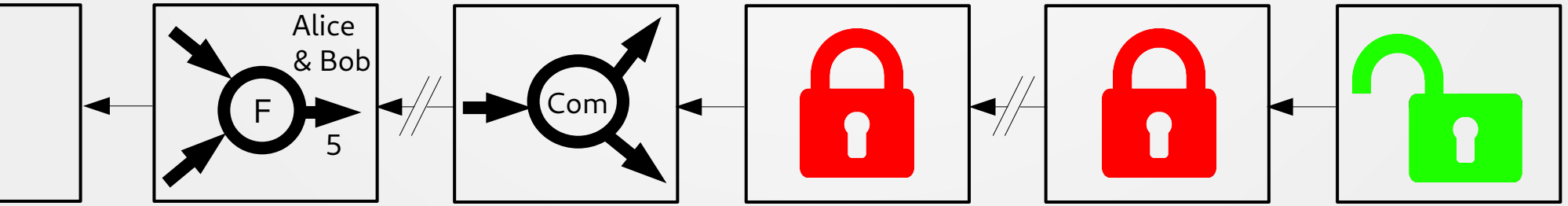
1



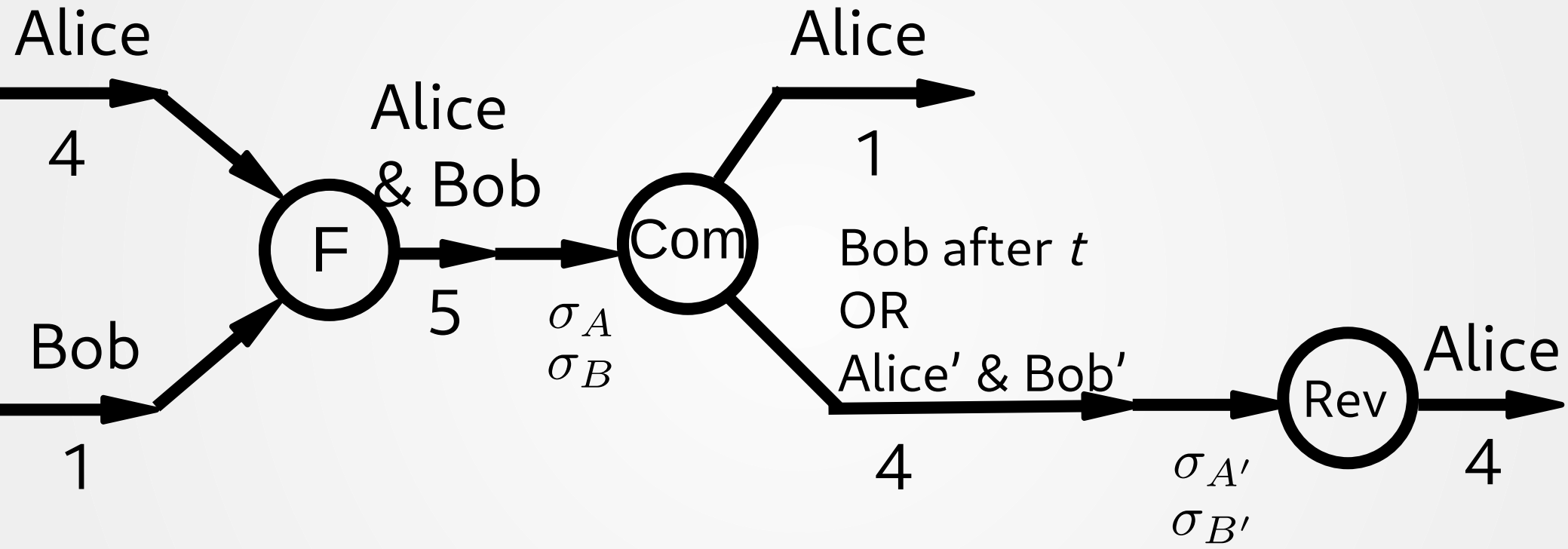

Alice
4
Bob
1
F
Alice
& Bob
5

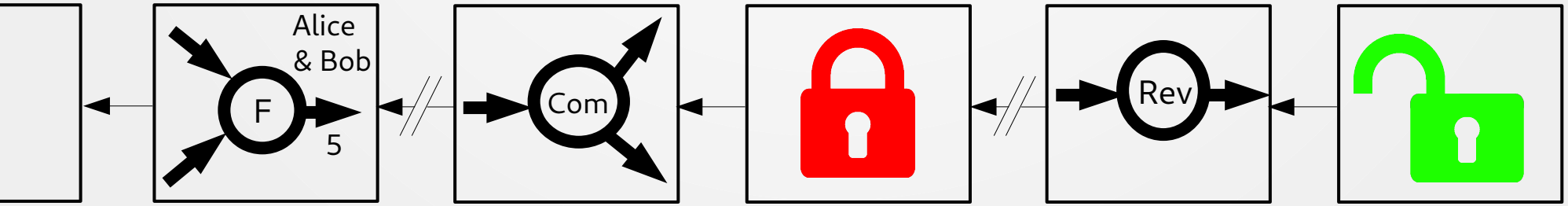

Alice
& Bob
F
5



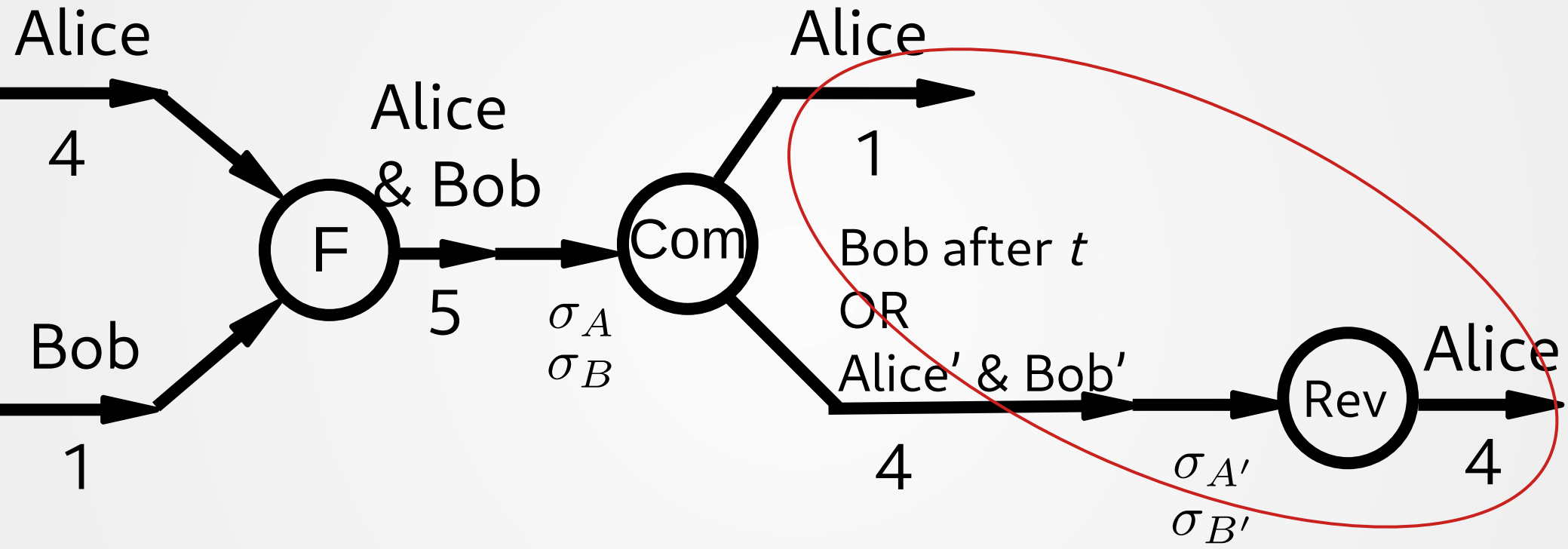


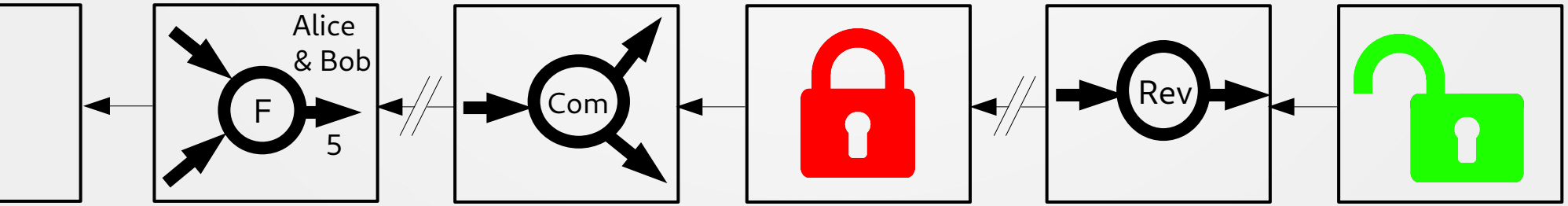
Dispute period t





Dispute period t





Dispute period t

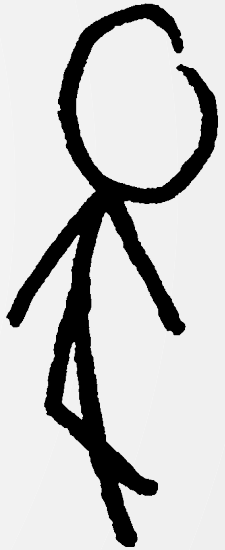
Part 2
Multi-hop payments

Multi-hop payments

```
Alice
Charlie
```

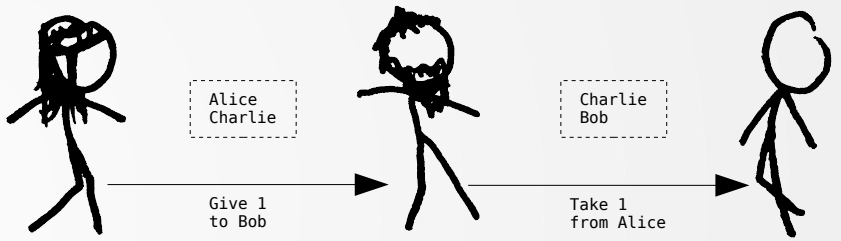
Charlie

```
Charlie
Bob
```



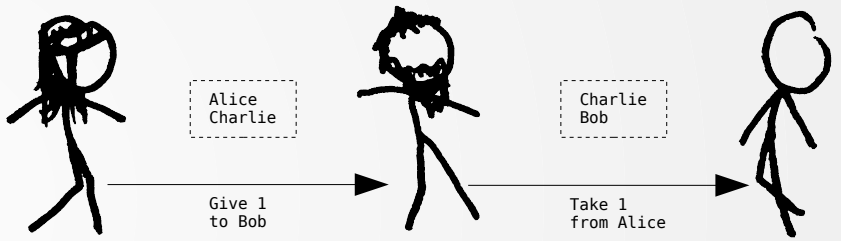
Multi-hop payments

Why no one can cheat?



Why no one can cheat?

HTLC

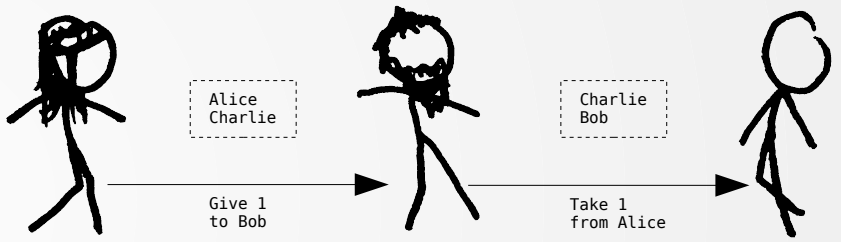


"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of **0xabcdef** within an hour"

Why no one can cheat?

HTLC

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

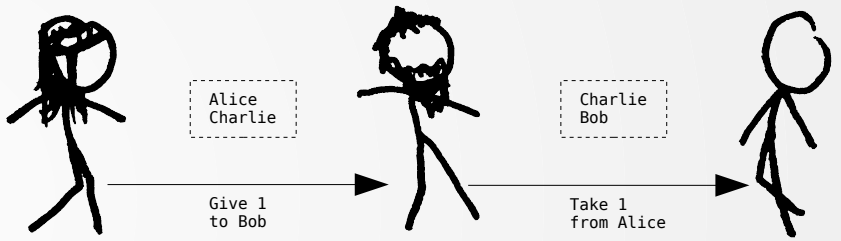


- Bob chooses random **R**, computes **h=H(R)**
- Bob sends **h** to Alice

Why no one can cheat?

HTLC

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

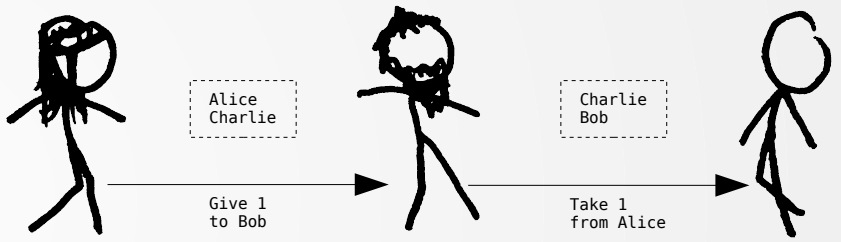


- Bob chooses random **R**, computes **h=H(R)**
- Bob sends **h** to Alice
- Alice signs an **h**-HTLC with Charlie
- Charlie signs an **h**-HTLC with Bob

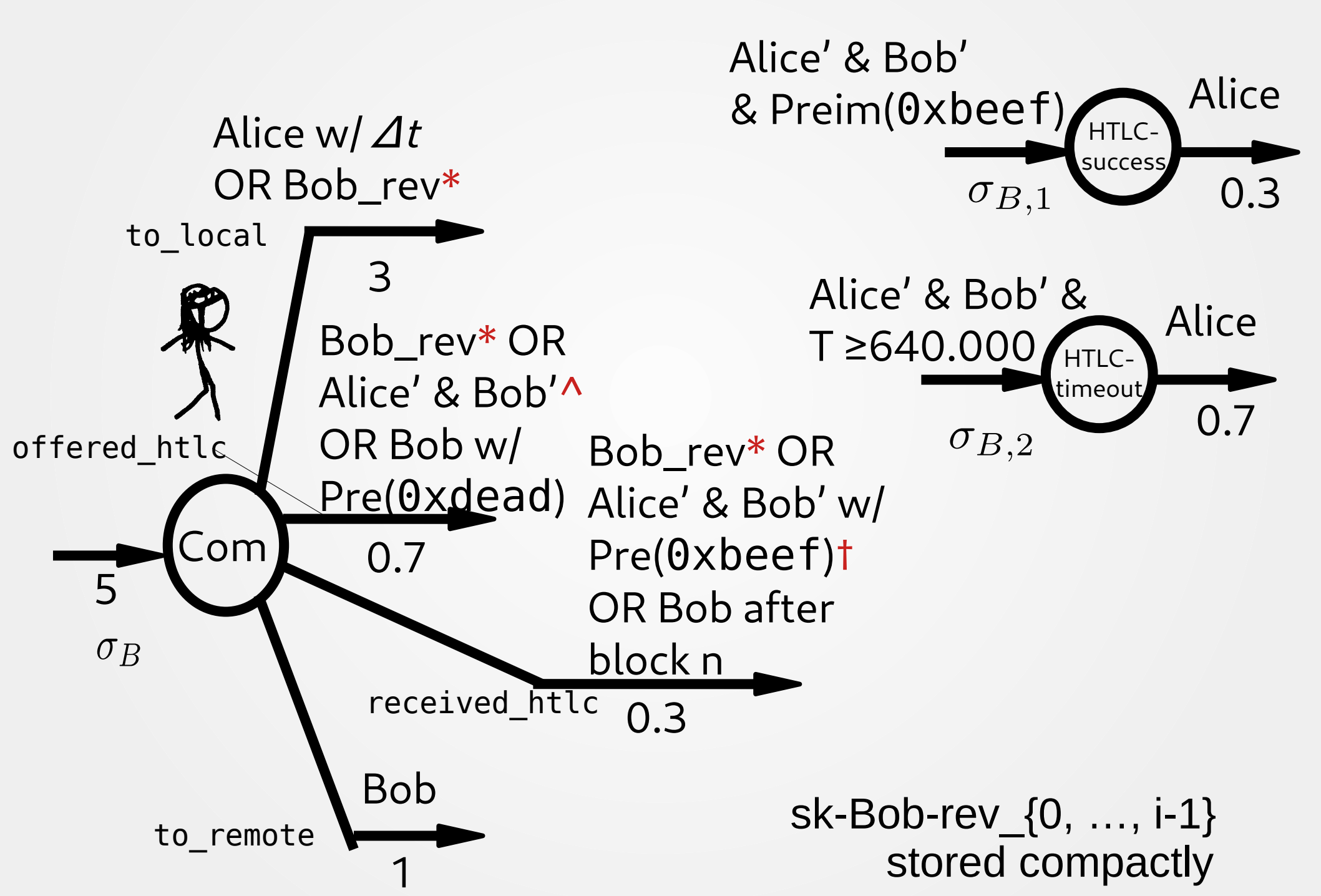
Why no one can cheat?

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!