# What is the Lightning Network?

Orfeas Stefanos Thyfronitis Litos

University of Edinburgh

# Problem

All txs validated by all wallets

Problem

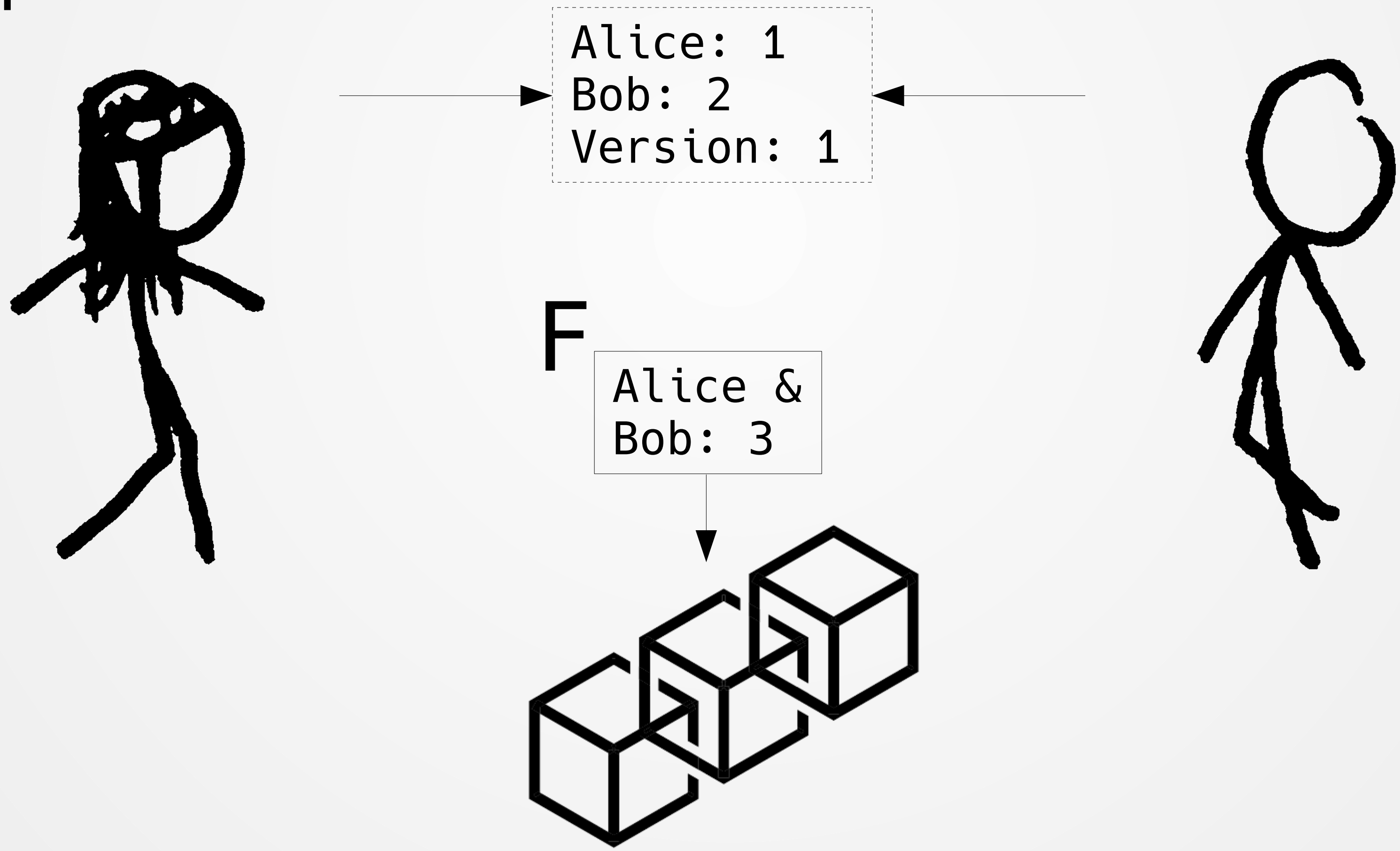
All txs validated by all wallets

Solution

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

# Enter payment channels

## Open

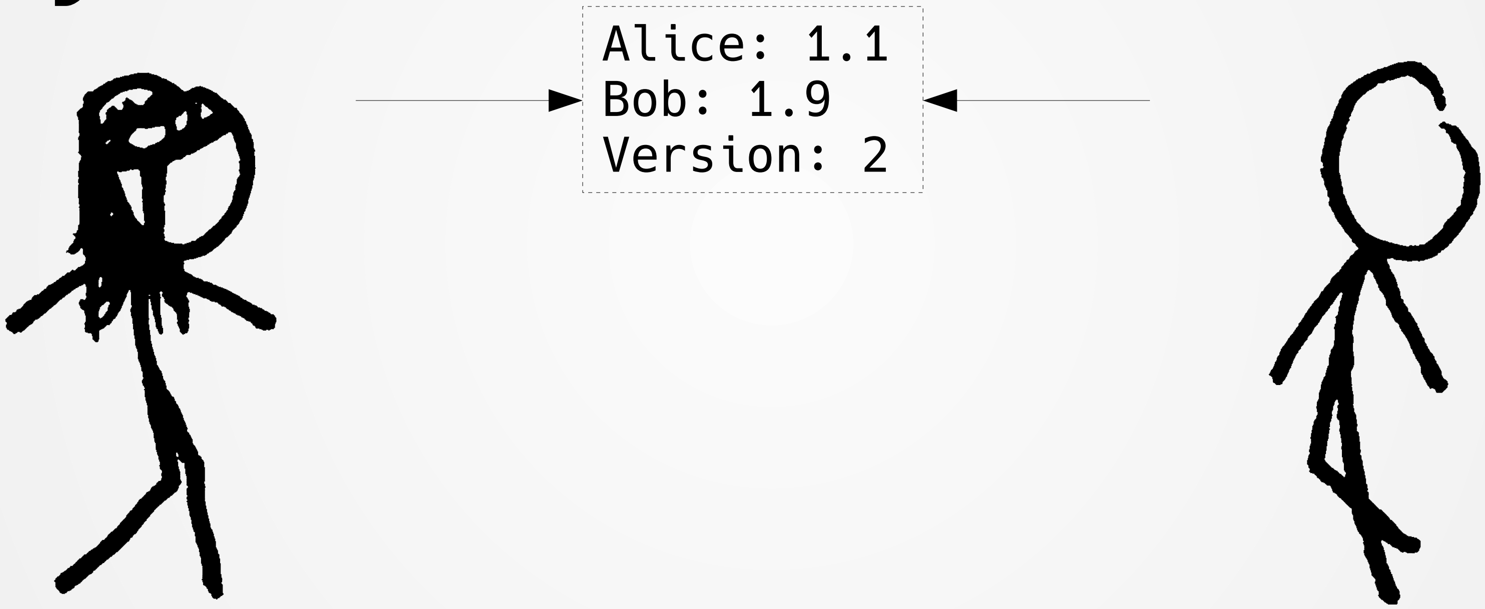


Alice: 1
Bob: 2
Version: 1

F

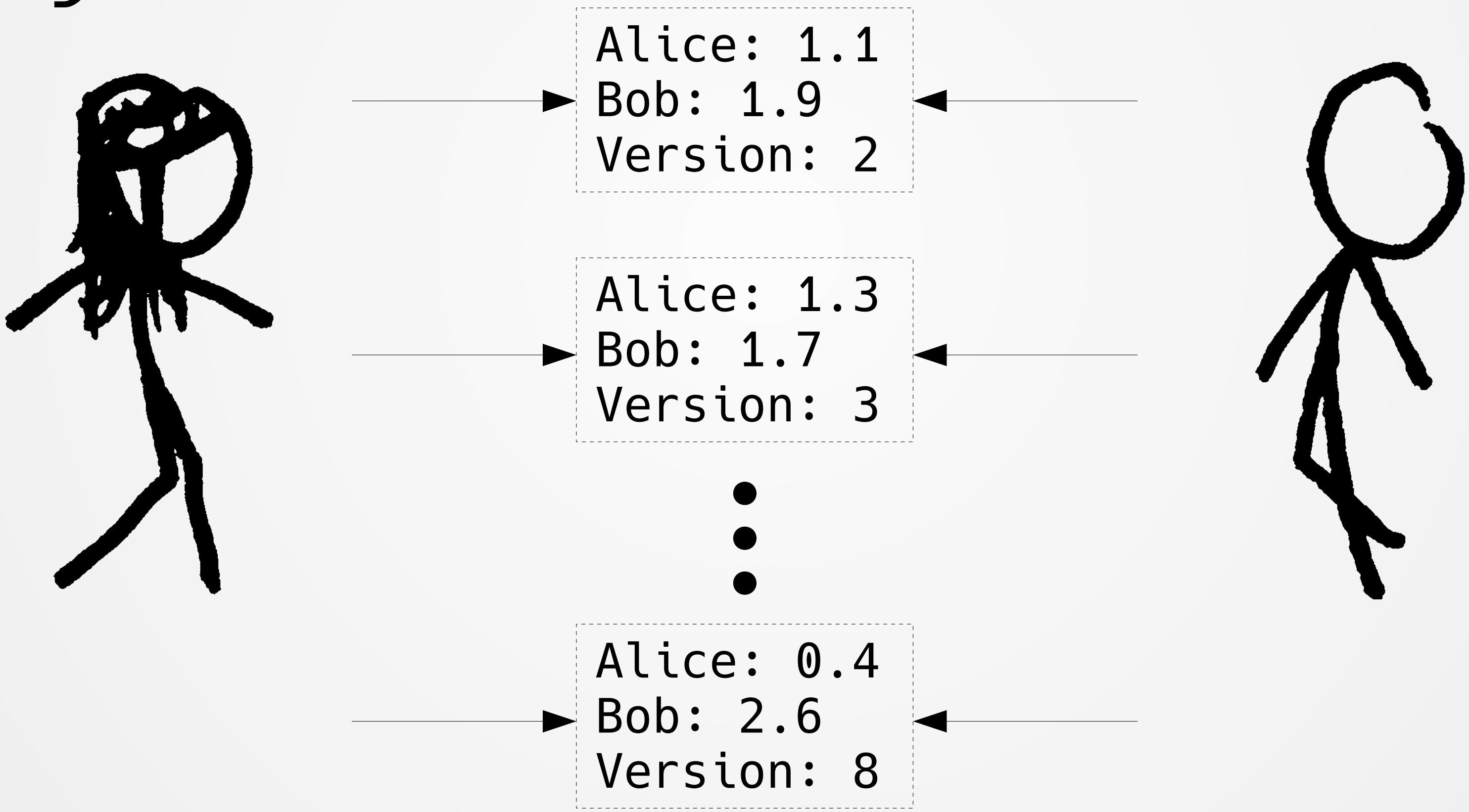
Alice &
Bob: 3

# Pay



Alice: 1.1
Bob: 1.9
Version: 2

# Pay



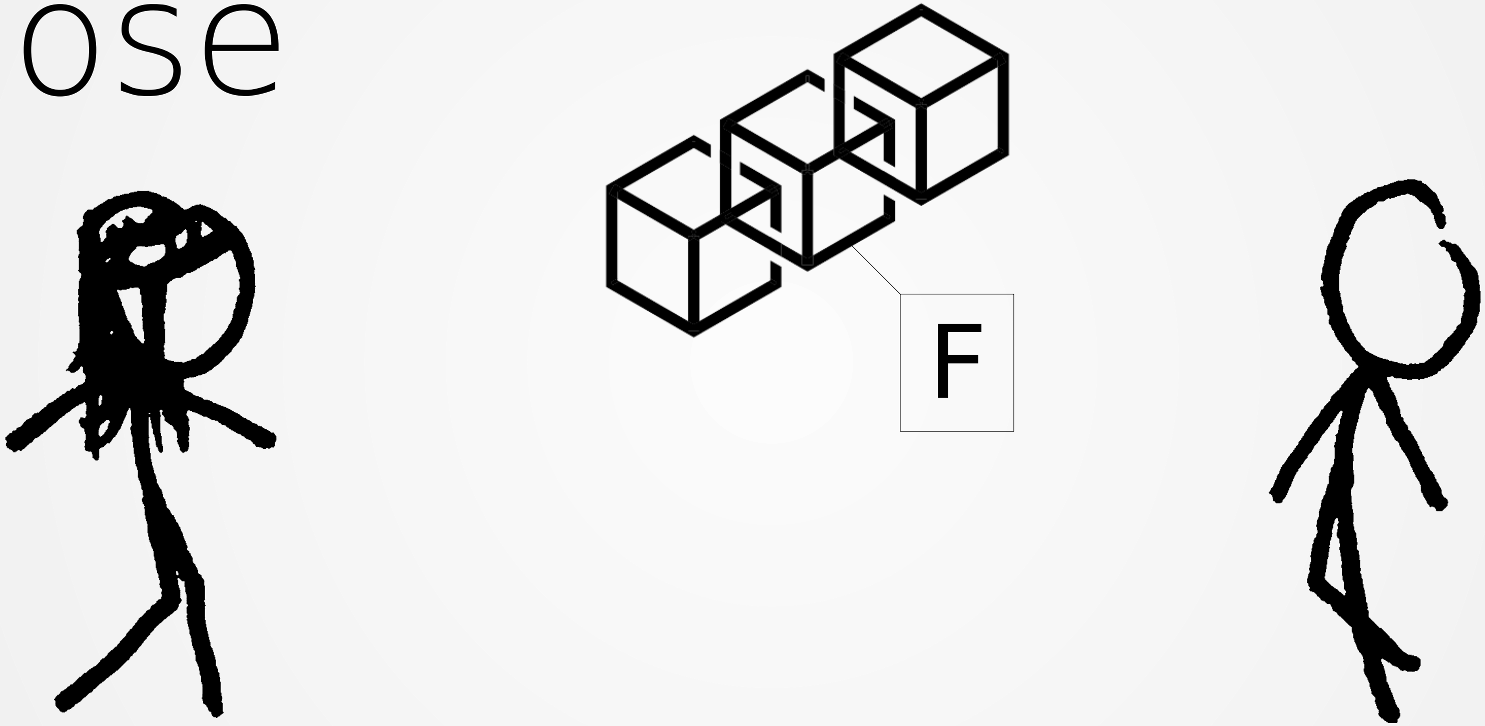
Alice: 1.1
Bob: 1.9
Version: 2

Alice: 1.3
Bob: 1.7
Version: 3

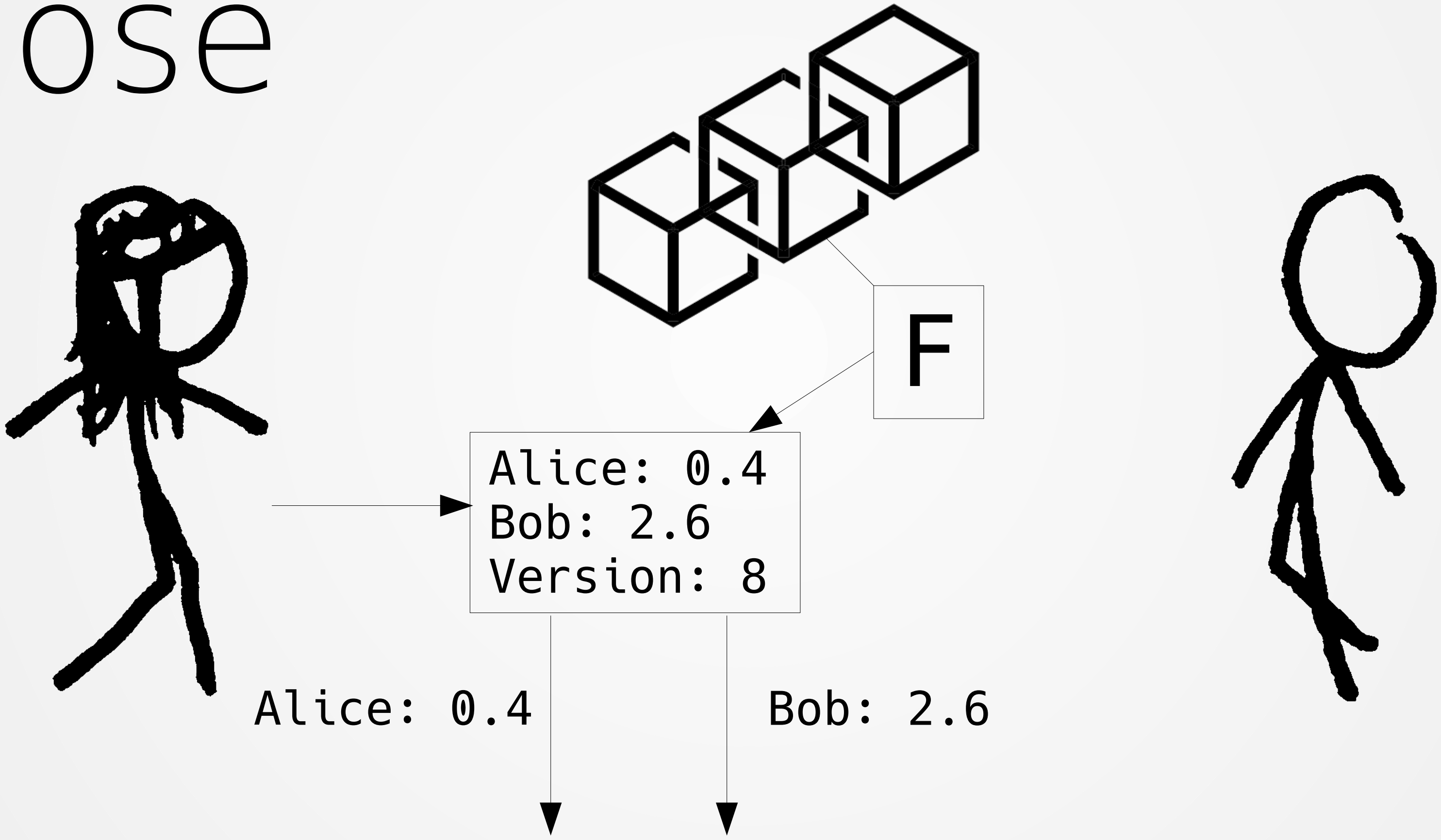
⋮

Alice: 0.4
Bob: 2.6
Version: 8

# Close



# Close



F

Alice: 0.4
Bob: 2.6
Version: 8

Alice: 0.4

Bob: 2.6

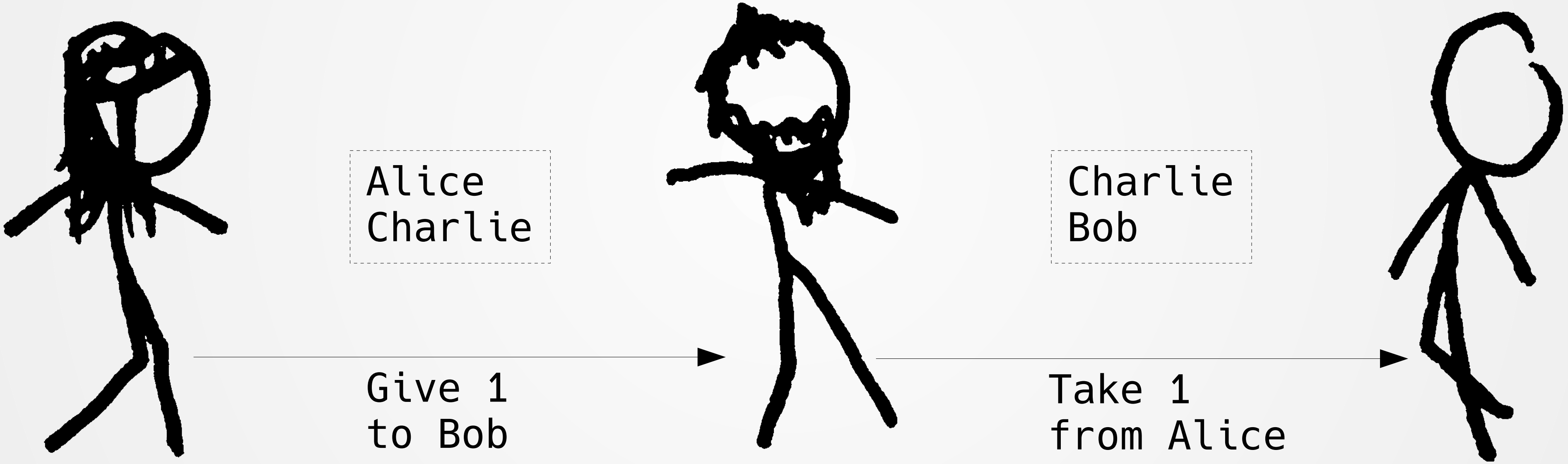
# Multi-hop payments

```
Alice
Charlie
```

```
Charlie
Bob
```

Charlie

# Multi-hop payments



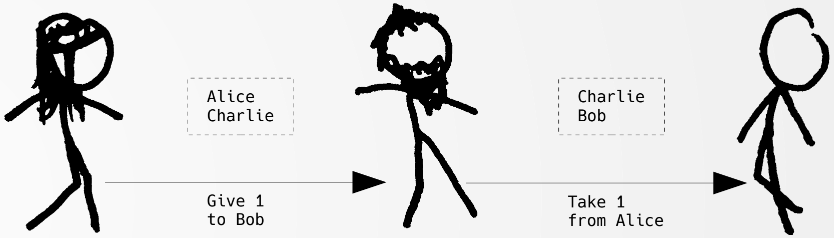
Alice
Charlie

Give 1
to Bob

Charlie
Bob

Take 1
from Alice

# Why no one can cheat?



Alice
Charlie

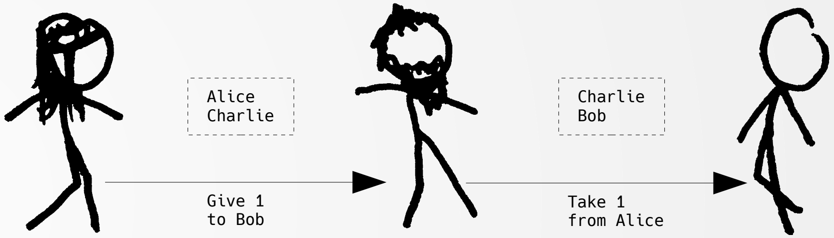
Charlie
Bob

Give 1
to Bob

Take 1
from Alice

# Why no one can cheat?

# HTLC

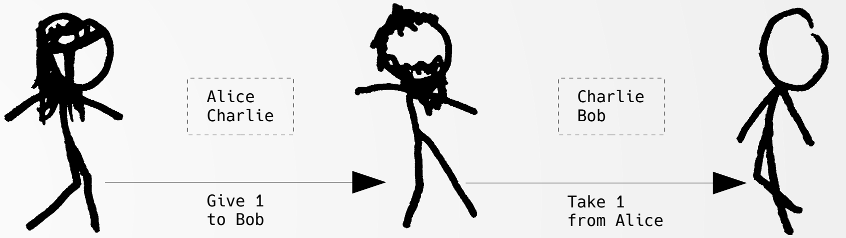


"I, Alice, promise to pay Charlie 1 coin if he reveals a preimage of **`0xabcdef`** within an hour"

# Why no one can cheat?

# HTLC

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

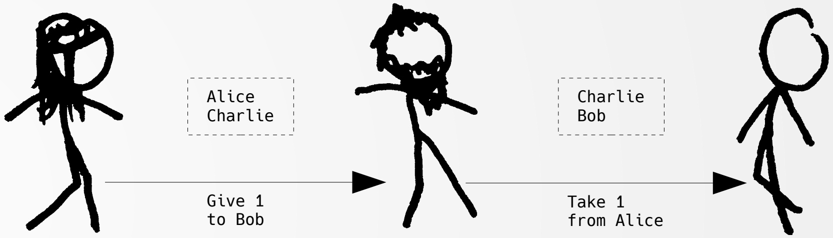


- Bob chooses random **R**, computes **h=H(R)**
- Bob sends **h** to Alice

# Why no one can cheat?

# HTLC

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



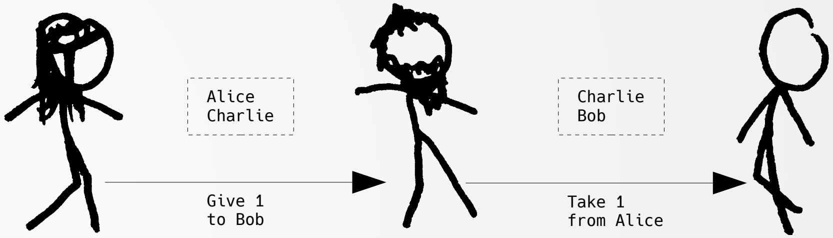
- Bob chooses random **R**, computes **h=H(R)**
- Bob sends **h** to Alice

- 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

# Our contribution

We prove LN secure (using UC)

Thank you!