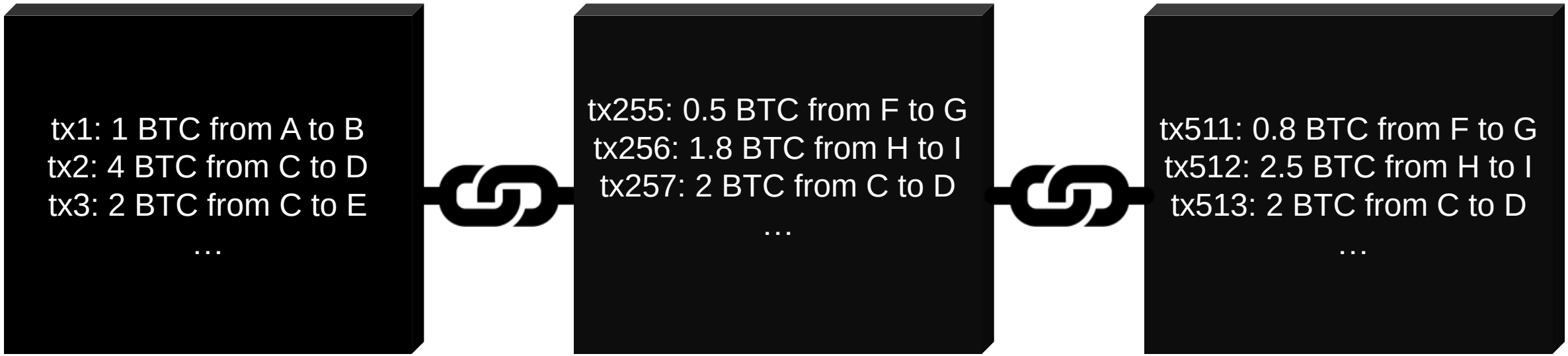
ETH zürich

Teechain: Scalable Blockchain Payments using Trusted Execution Environments

Cryptocurrencies

- Most popular: Bitcoin
- Driving technology: Blockchain
  - Peer-to-peer transaction based ledger
- Transactions from and to addresses

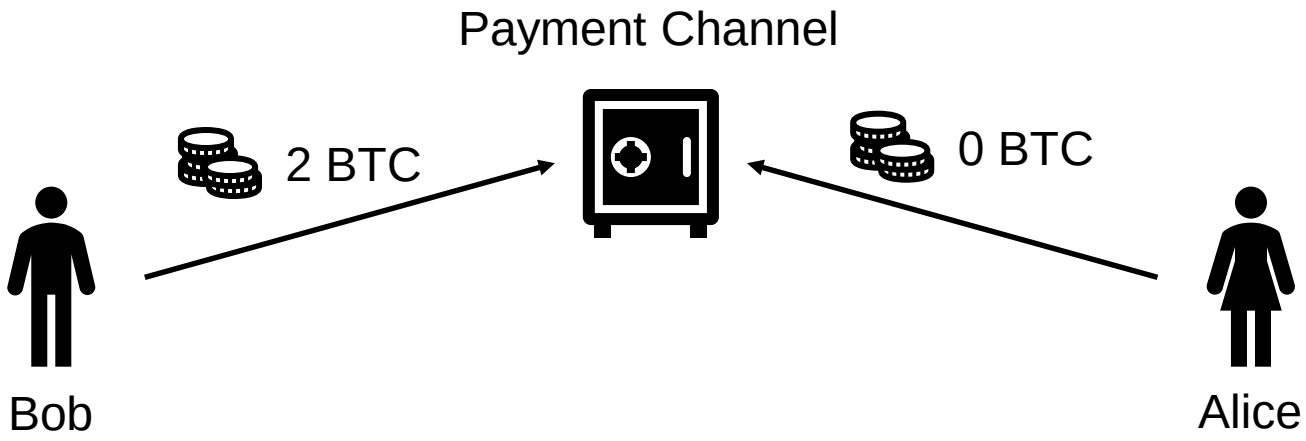
The blockchain



Shortcomings of Bitcoin

- Not scalable
- High fees
- Environmental issues
- Security vulnerabilities

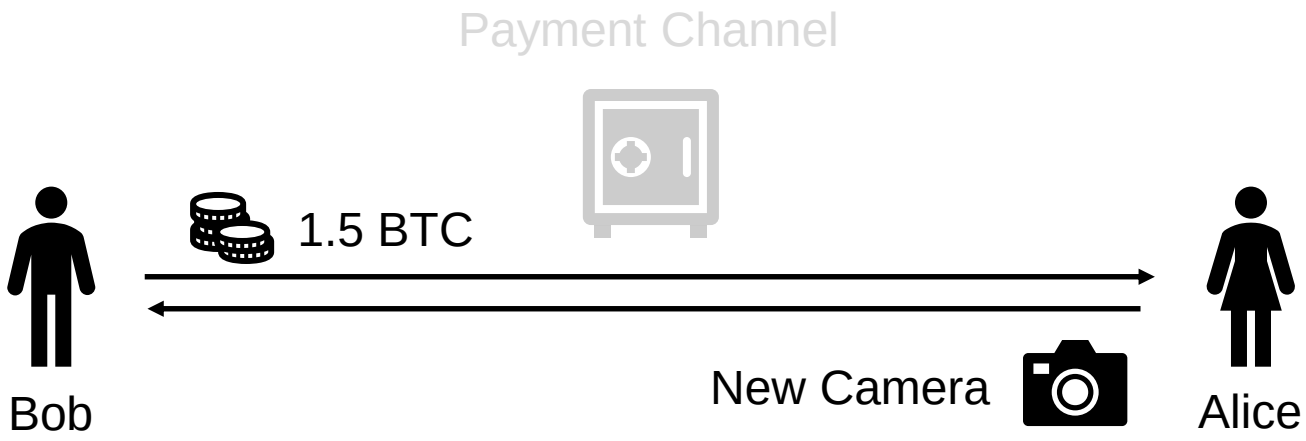
Payment channels: Setup

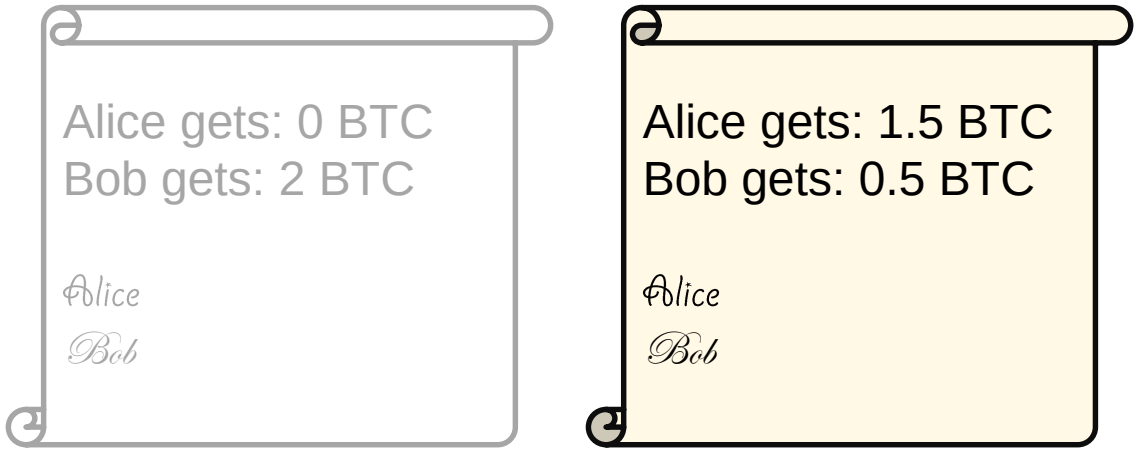


Alice gets: 0 BTC
Bob gets: 2 BTC

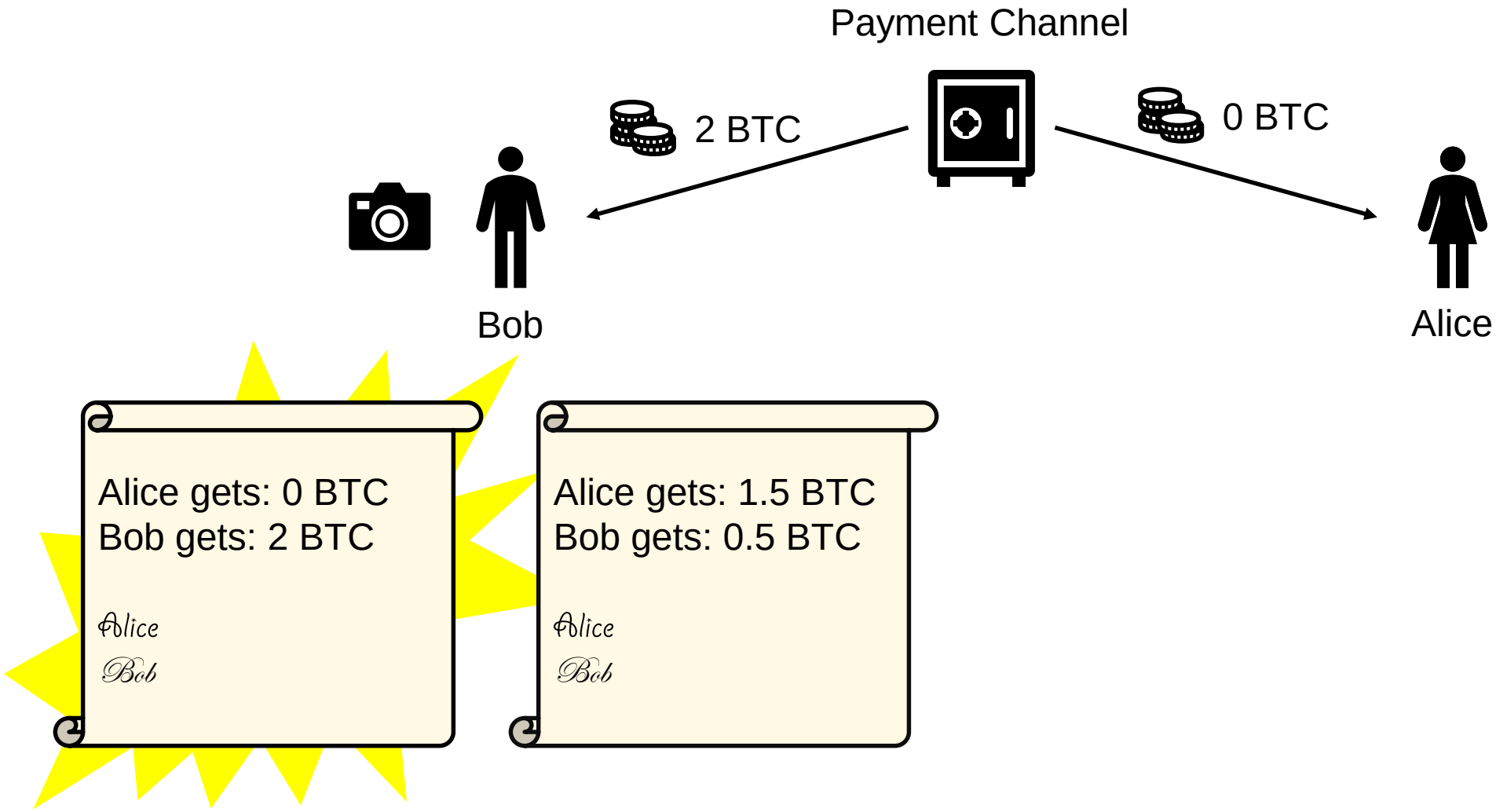
Alice
Bob

Payment channels: Payment





Payment channels: Problems



Payment channels: Solutions

- Timelocks
- Lightning network

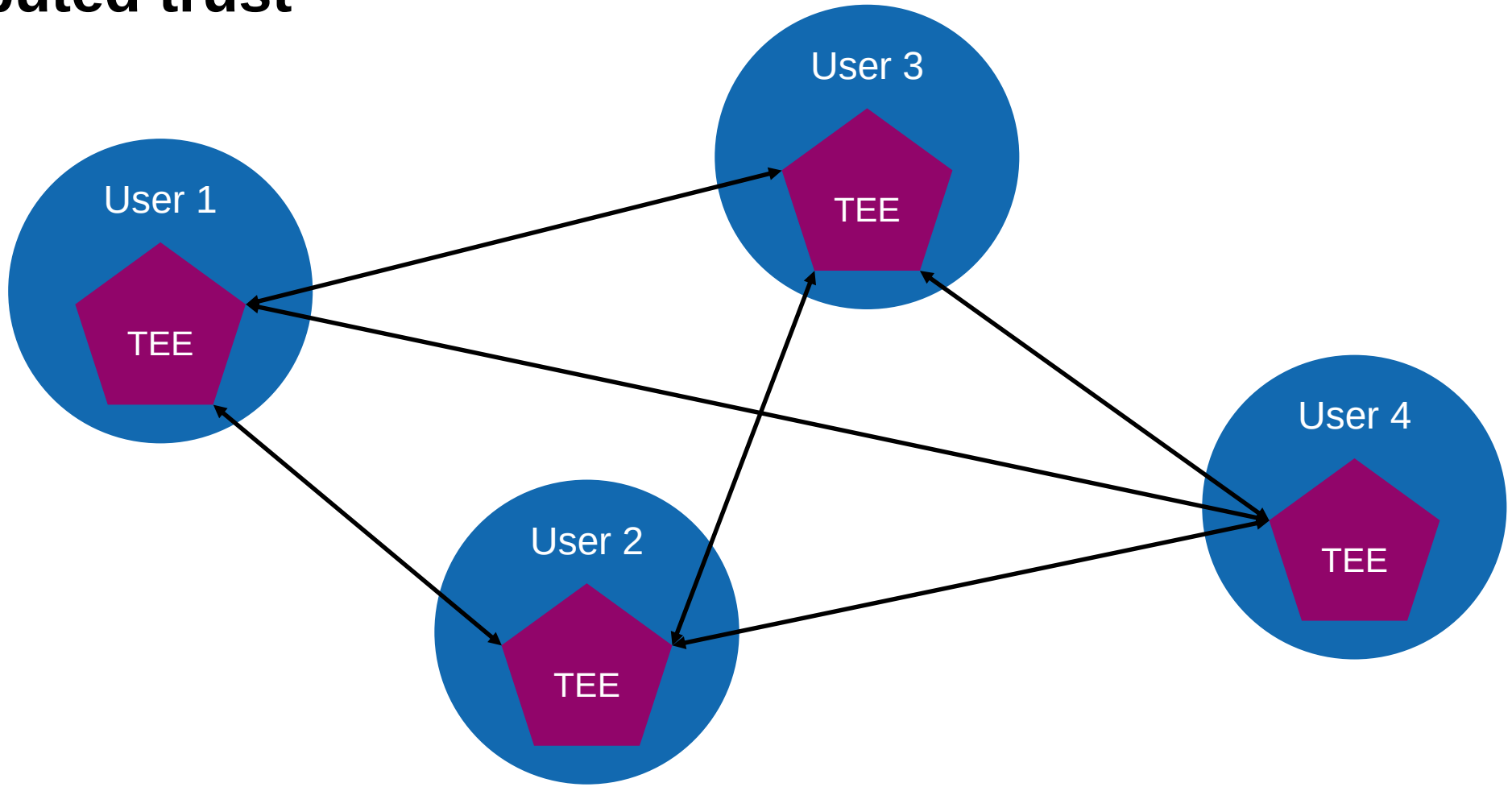
Teechain payment channels

- Establish trust relationship between users
- Protected channel state until termination

Establishing trust

- Shift root of trust to hardware using trusted execution environments (TEEs)
- Intel SGX
  - Fully isolated
  - Encrypted memory
  - Remote attestation

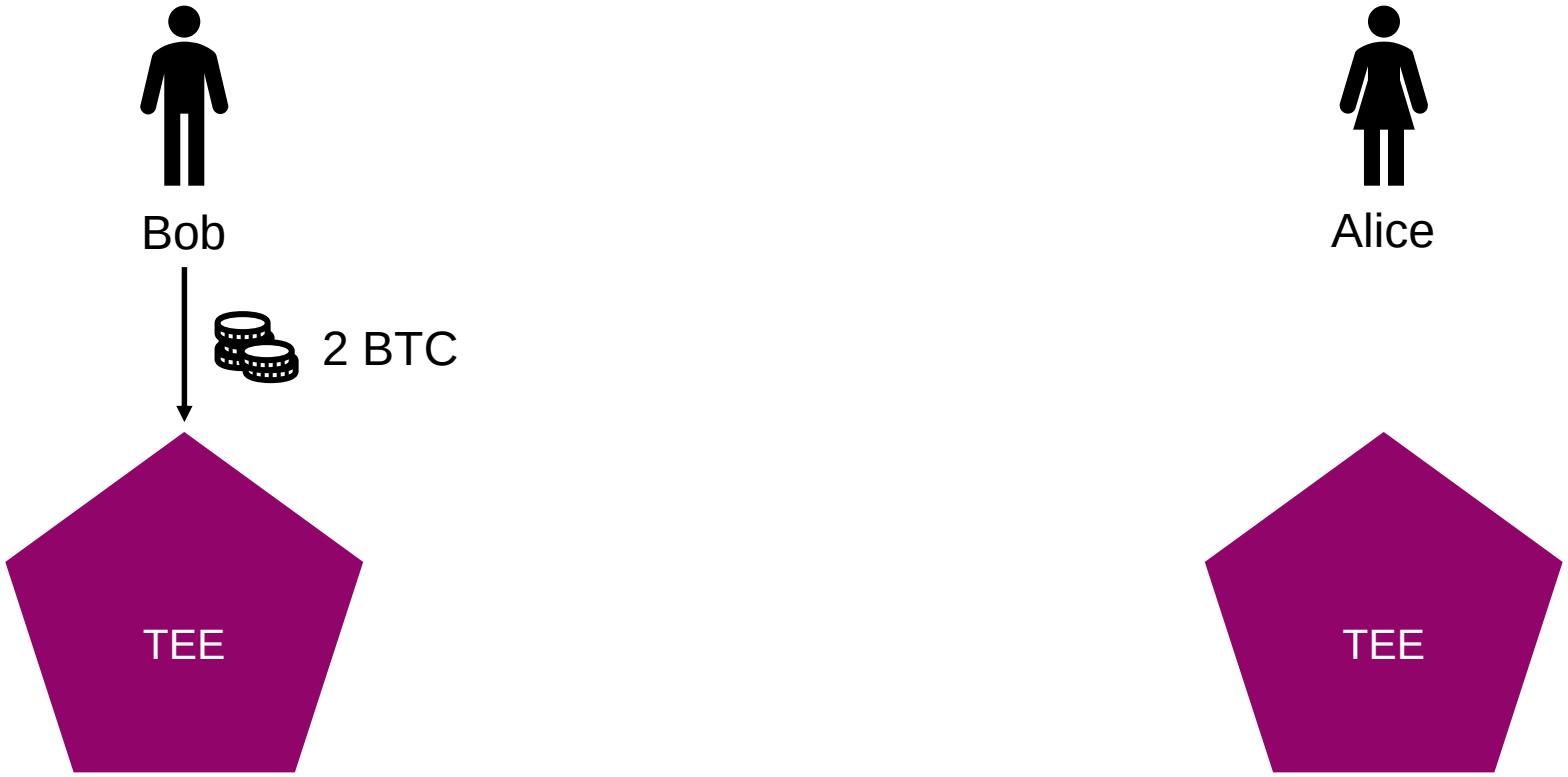
Distributed trust



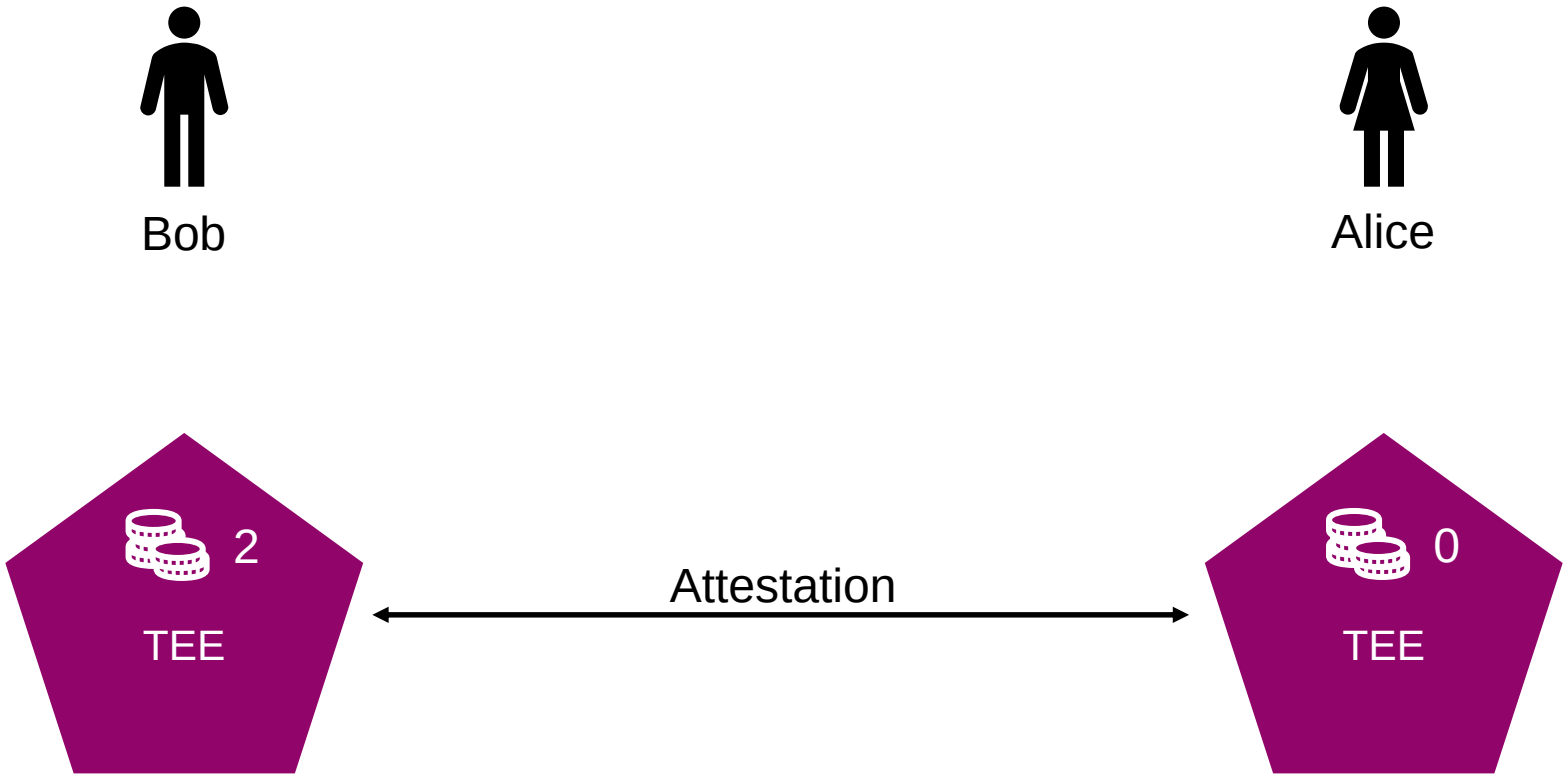
Establishing trust

- Users trust:
  - The blockchain
  - Own TEE (i.e. Intel)
  - Own environment
  - Remote TEE
  - Teechain code

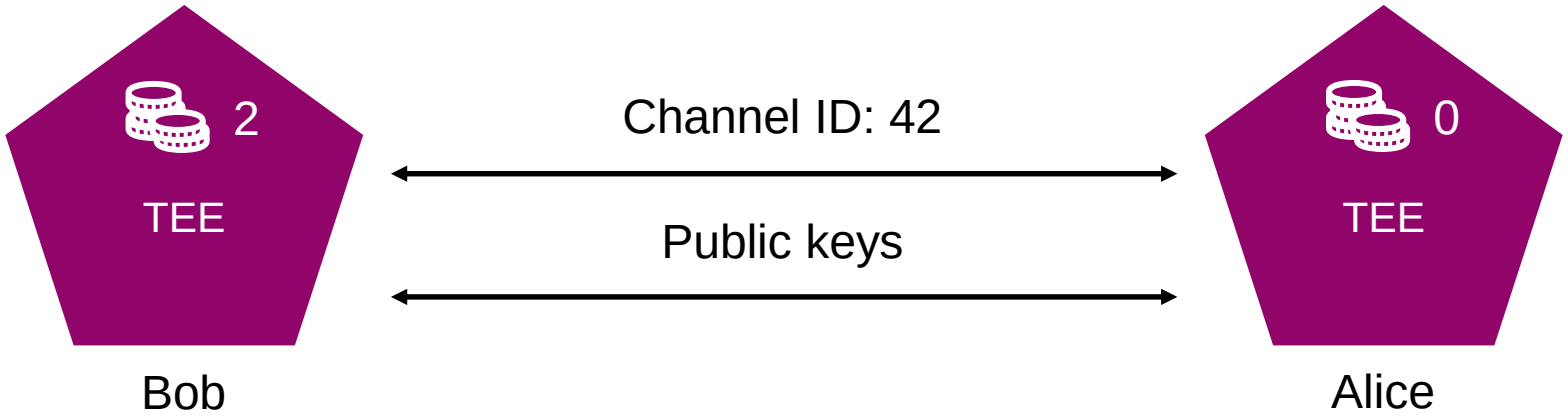
Single channel: Deposit



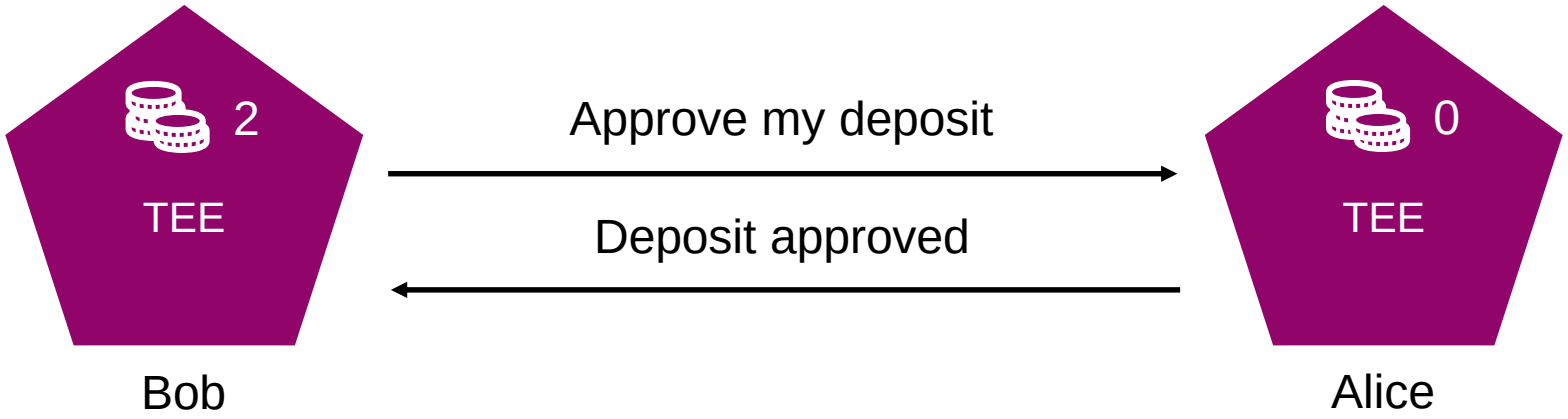
Single channel: Mutual attestation



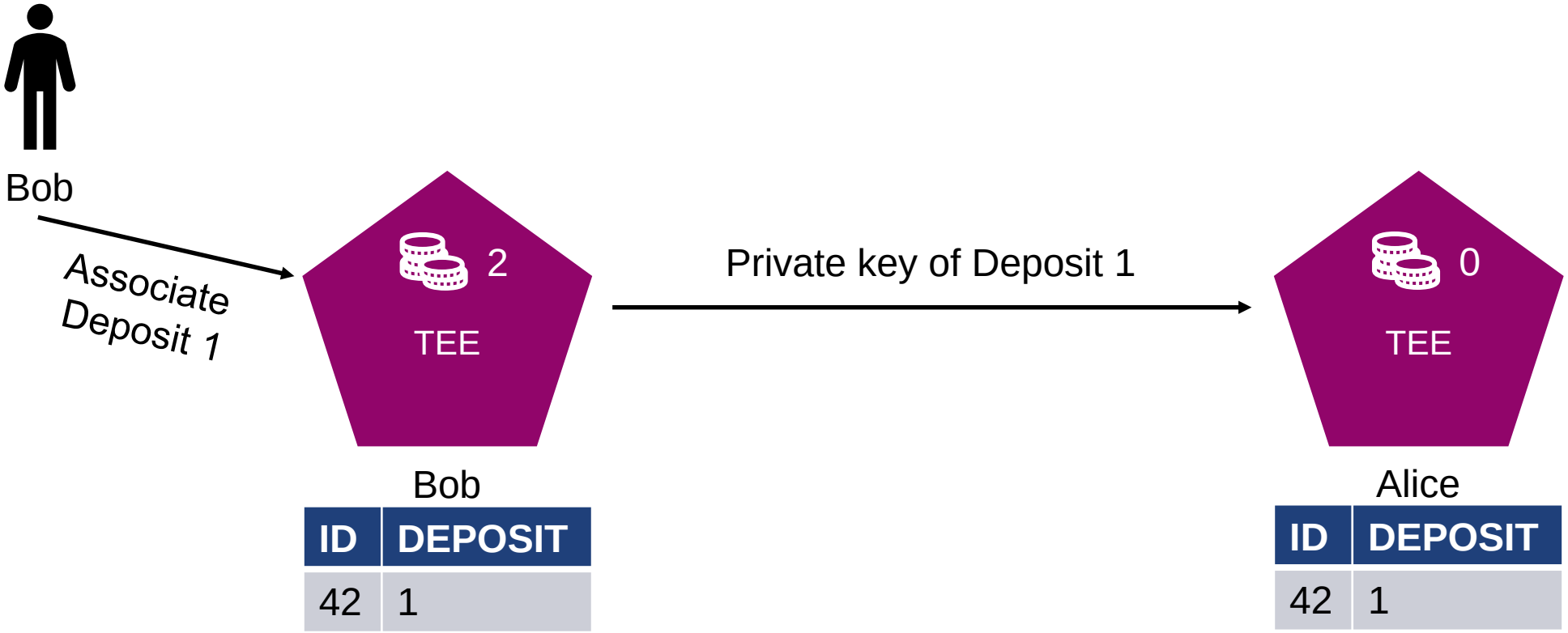
Single channel: Opening a channel



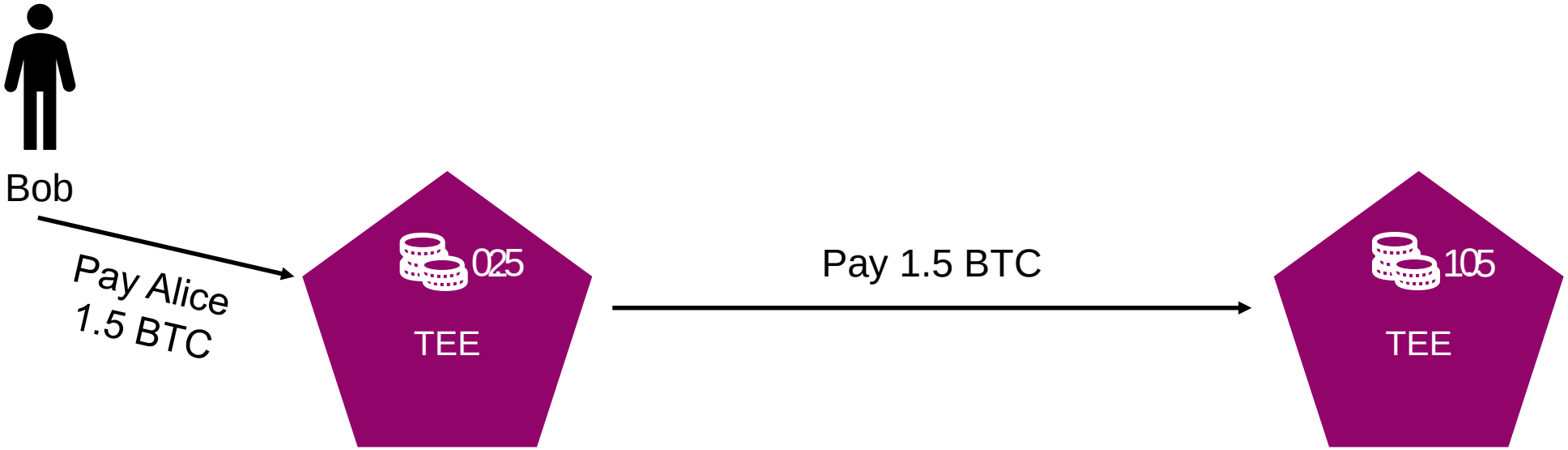
Single channel: Deposit approval



Single channel: Deposit association



Single channel: Payment



Bob

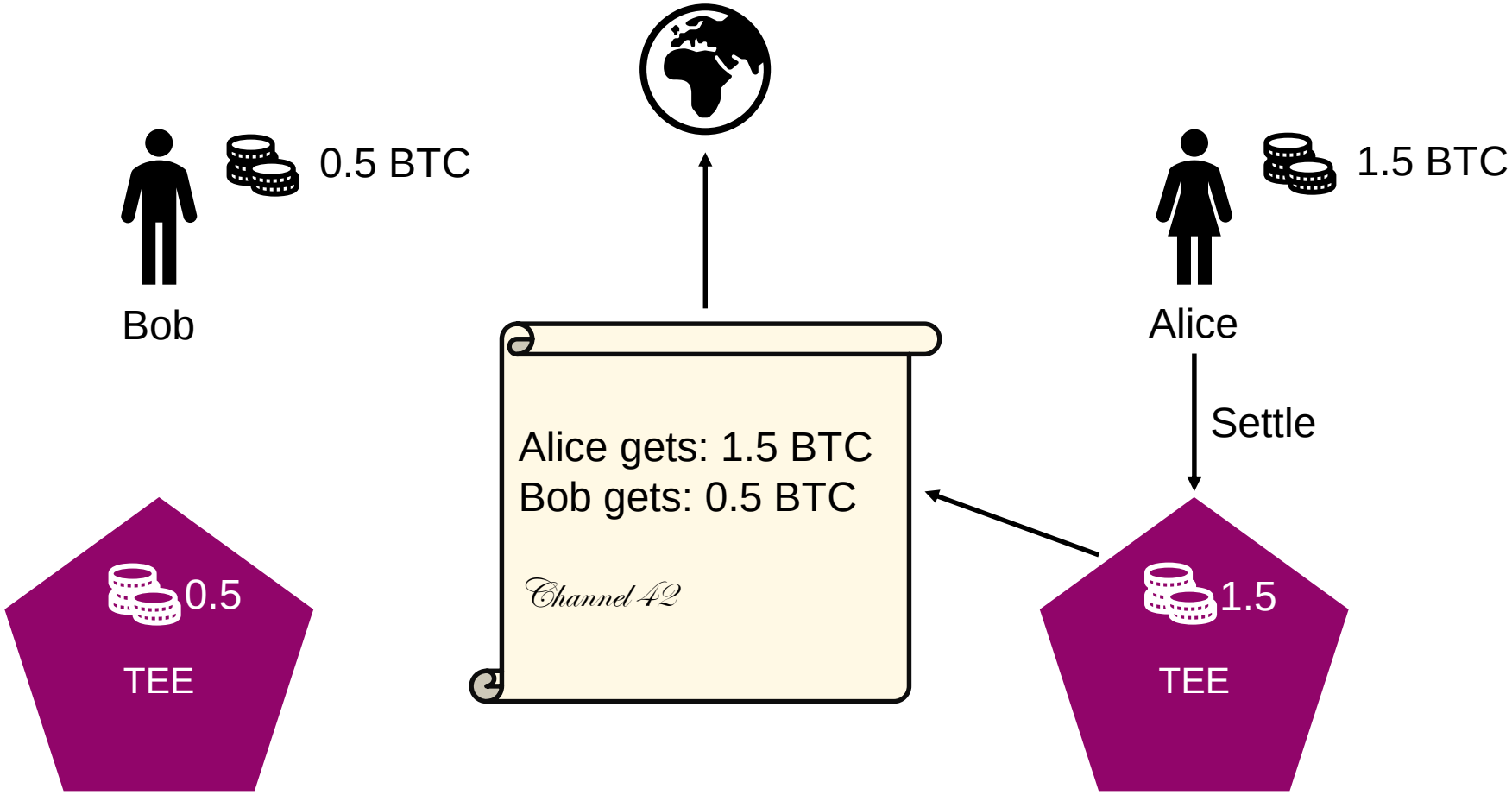
ID	DEPOSIT
42	1

Alice

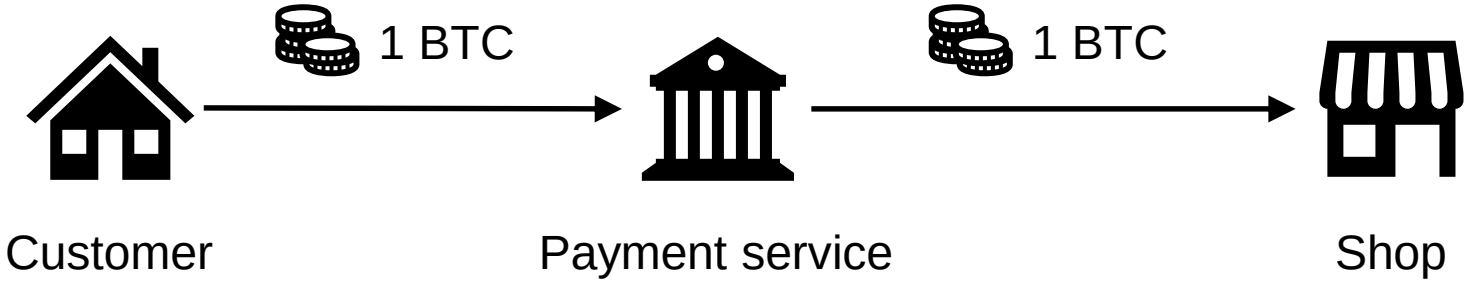
ID	DEPOSIT
42	1

Single channel: Settlement

Single channel: Settlement

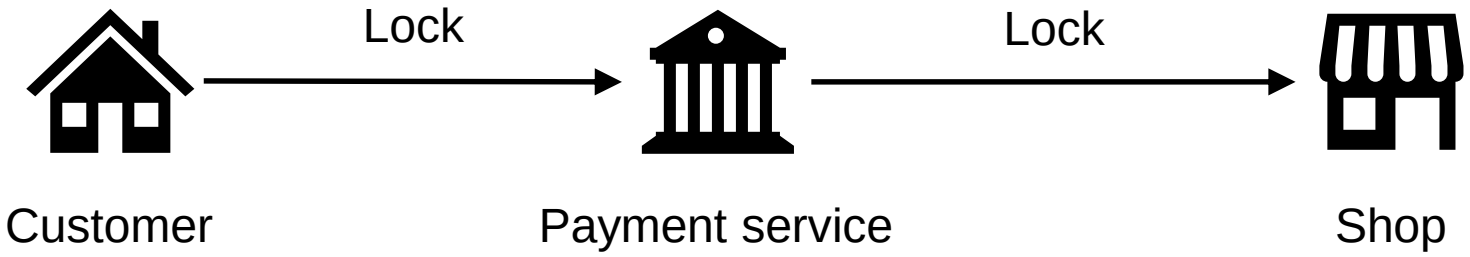


Payment chains



- Goals:
  - Atomicity
  - Robustness against nodes ejecting

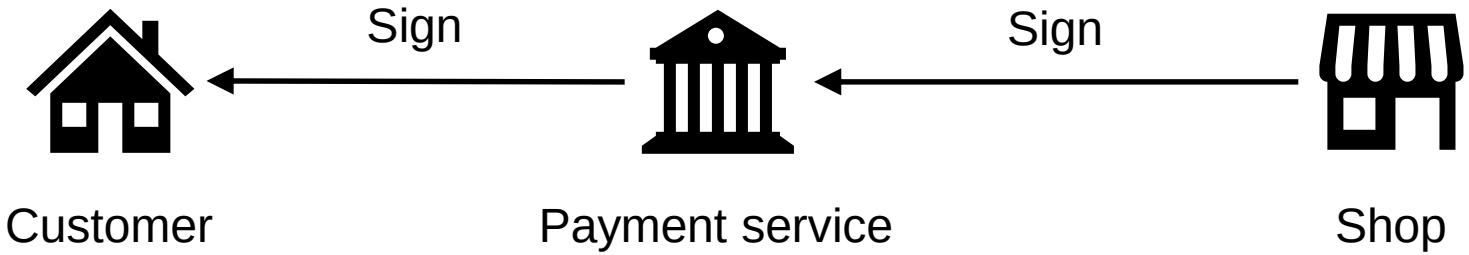
Payment chains: Lock (1)



- Check:
  - Channel idle
  - Enough funds available

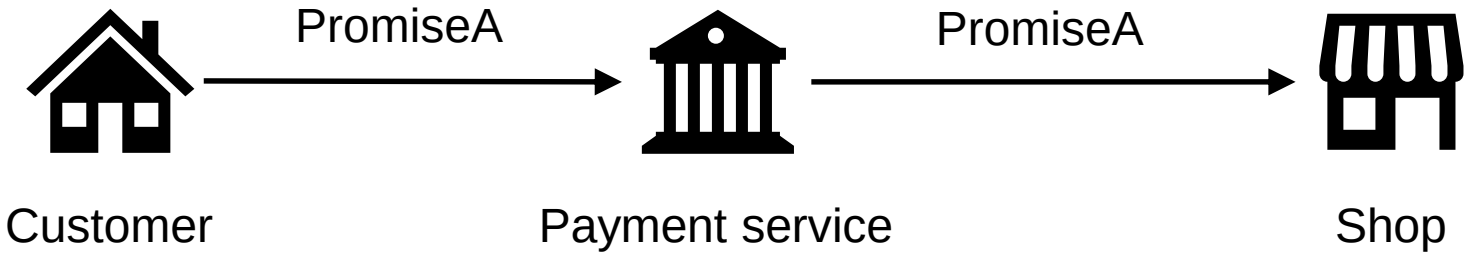
- Create `chainSettleTx`

Payment chains: Sign (2)



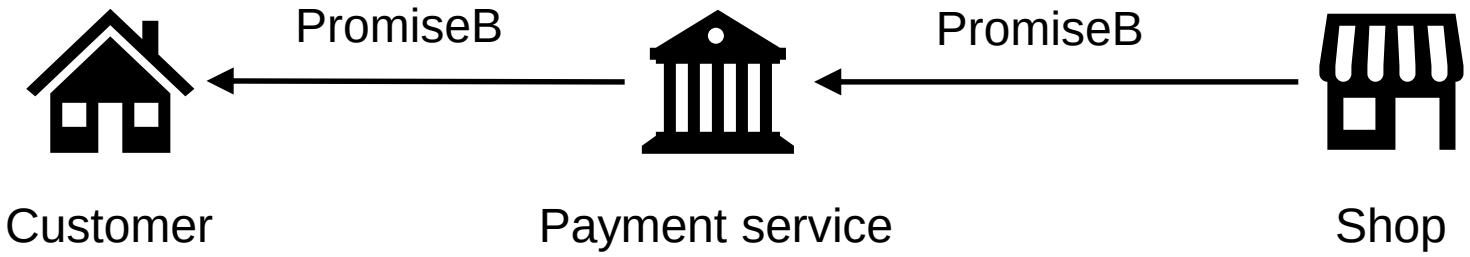
- Sign `chainSettleTx`

Payment chains: PromiseA (3)



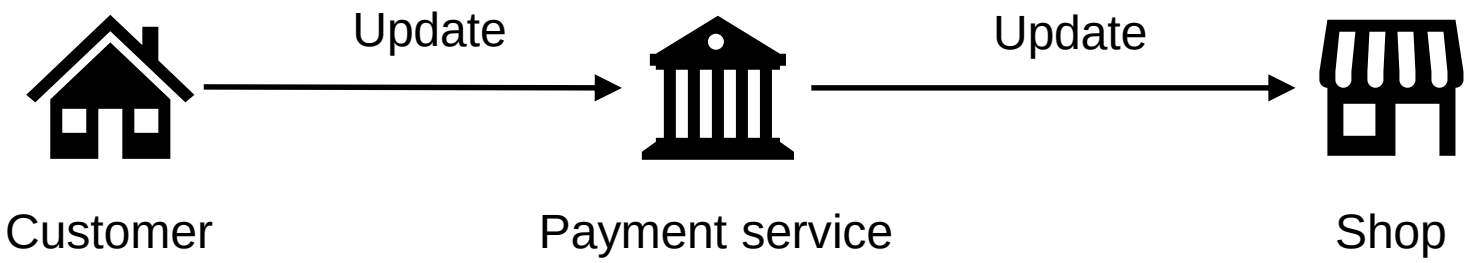
- Promise to not settle pre-payment
- Distribute `chainSettleTx`

Payment chains: PromiseB (4)



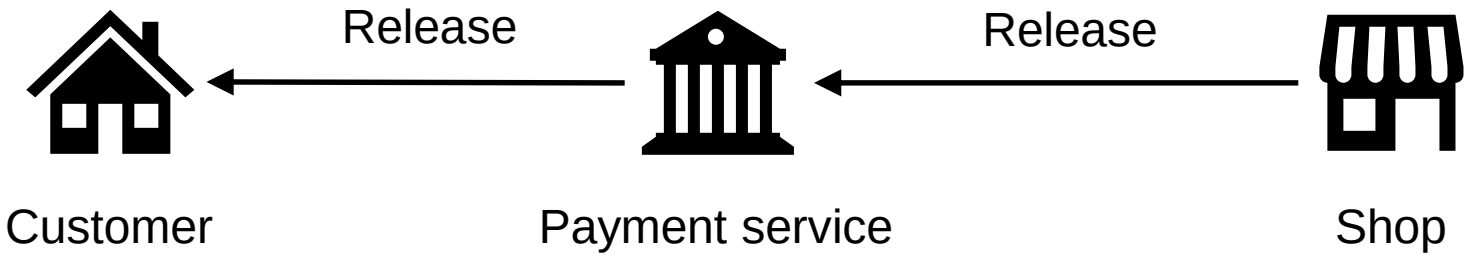
- Promise to correctly settle post-payment
- Update internal channel balances to post-payment

Payment chains: Update (5)



- Delete `chainSettleTx`

Payment chains: Release (6)

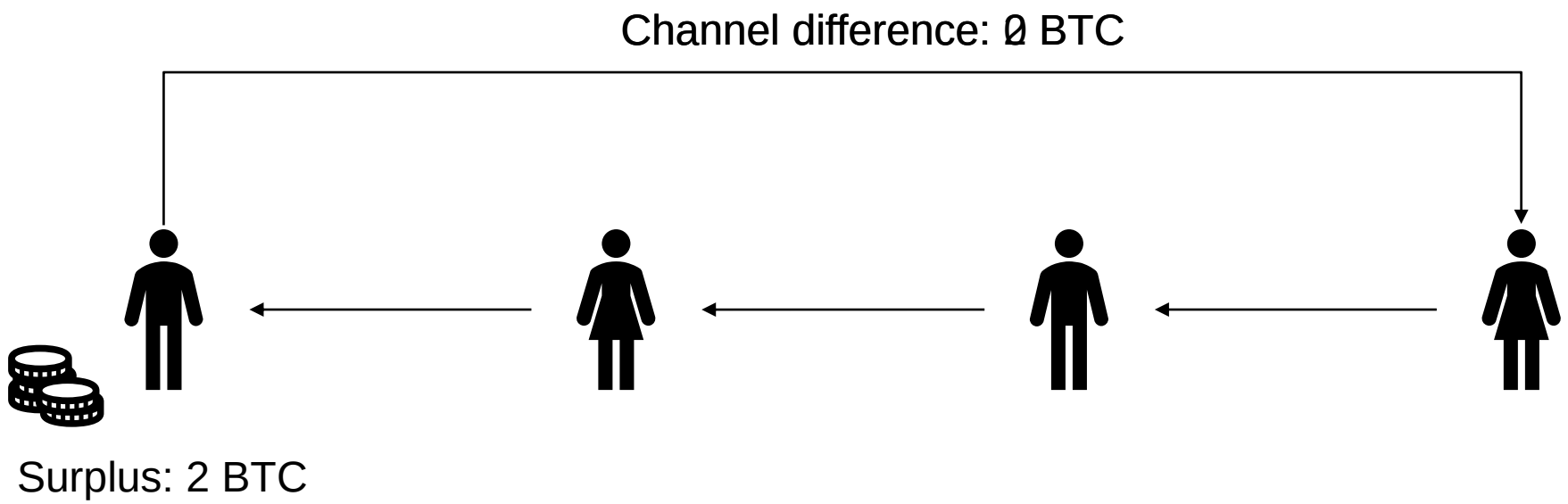


- Release the lock

Chain payment atomicity

- PromiseA transitions nodes to post-payment settling

Neutralize channels via chains



Fault tolerance

- Persistent storage
- Backup chains

Performance

Single channel performance	Throughput (tx/s)	Latency (ms ± stddev)
Lightning Network	1’000	387 ± 31
Teechain		
• No fault tolerance	111’000	86 ± 4.4
• Chain replication	33’000	123 ± 1.2
• Persistent storage	9.9	185 ± 0.3
Remote attestation and channel creation	N/A	2’100 ± 420

Performance

Two channel (chain) performance	Latency (ms ± stddev)
Lightning Network	0.91 ± 0.115
Teechain	
• No fault tolerance	2.28 ± 0.10
• Chain replication	3.3 ± 0.15
• Persistent storage	3.5 ± 0.11
UK1 -> UK2 with chain replication	0.22 ± 0.05

Security

- Secure channel setup (Diffie Hellman key exchange)
- Monotonically increasing counters against replay attacks
- Introducing hardware risks
  - Spectre adaptions
  - Side-channel attacks

Limitations

- Hardware constraints
- Performance highly dependent on fault tolerance
- Potential loss of funds

Questions