FastPay

High-Performance Byzantine Fault Tolerant Settlement

FastPay

Acknowledgments

Mathieu Baudet

George Danezis

Alberto Sonnino

Facebook Novi

What is FastPay?

A distributed (BFT) system

A standalone system

- An RTGS setting cross-bank payments

A side infrastructure

- Side chain to reduce latency of payments

What is FastPay?

A distributed (BFT) system

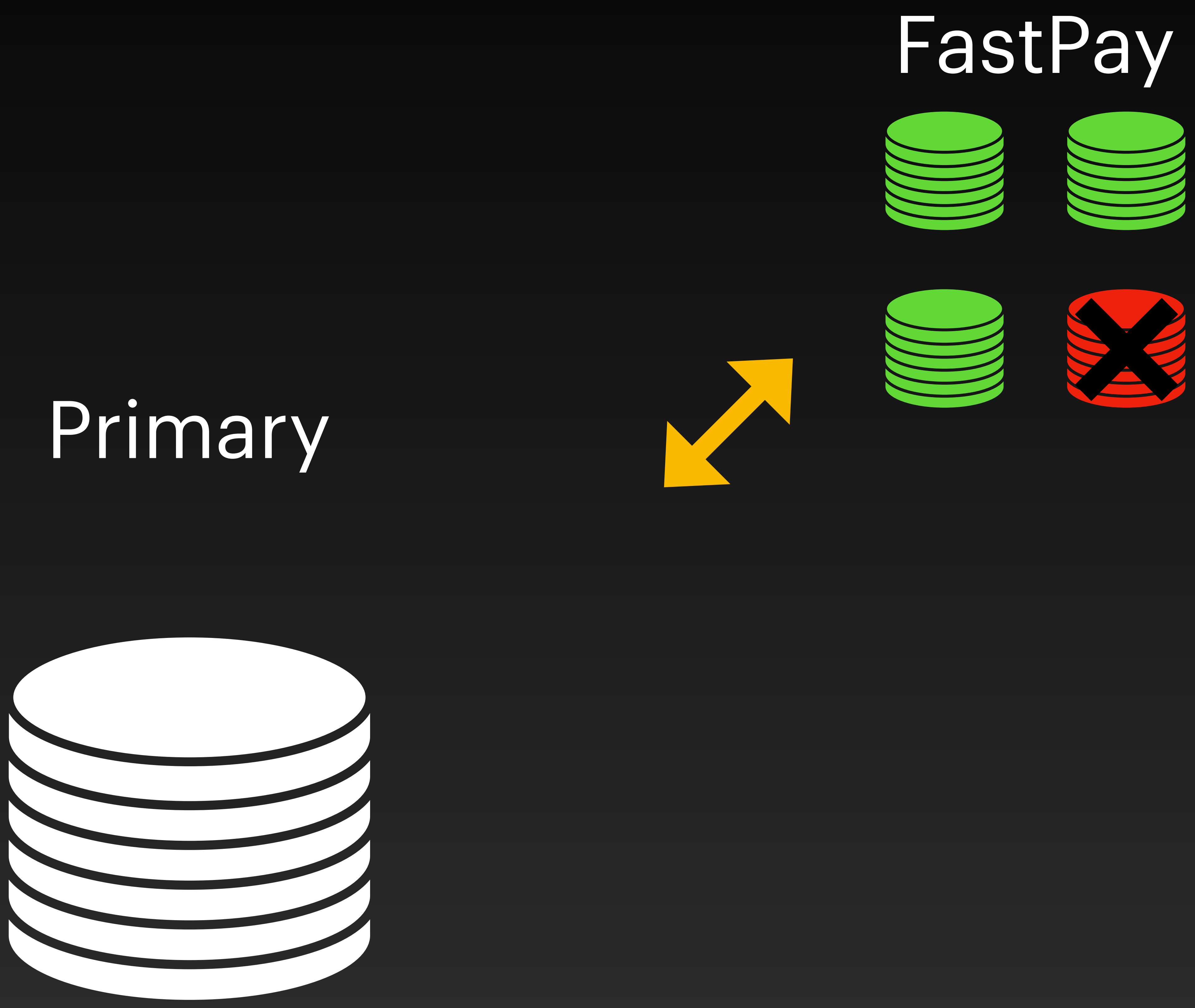
A standalone system

- An RTGS setting cross-bank payments

A side infrastructure

- Side chain to reduce latency of payments

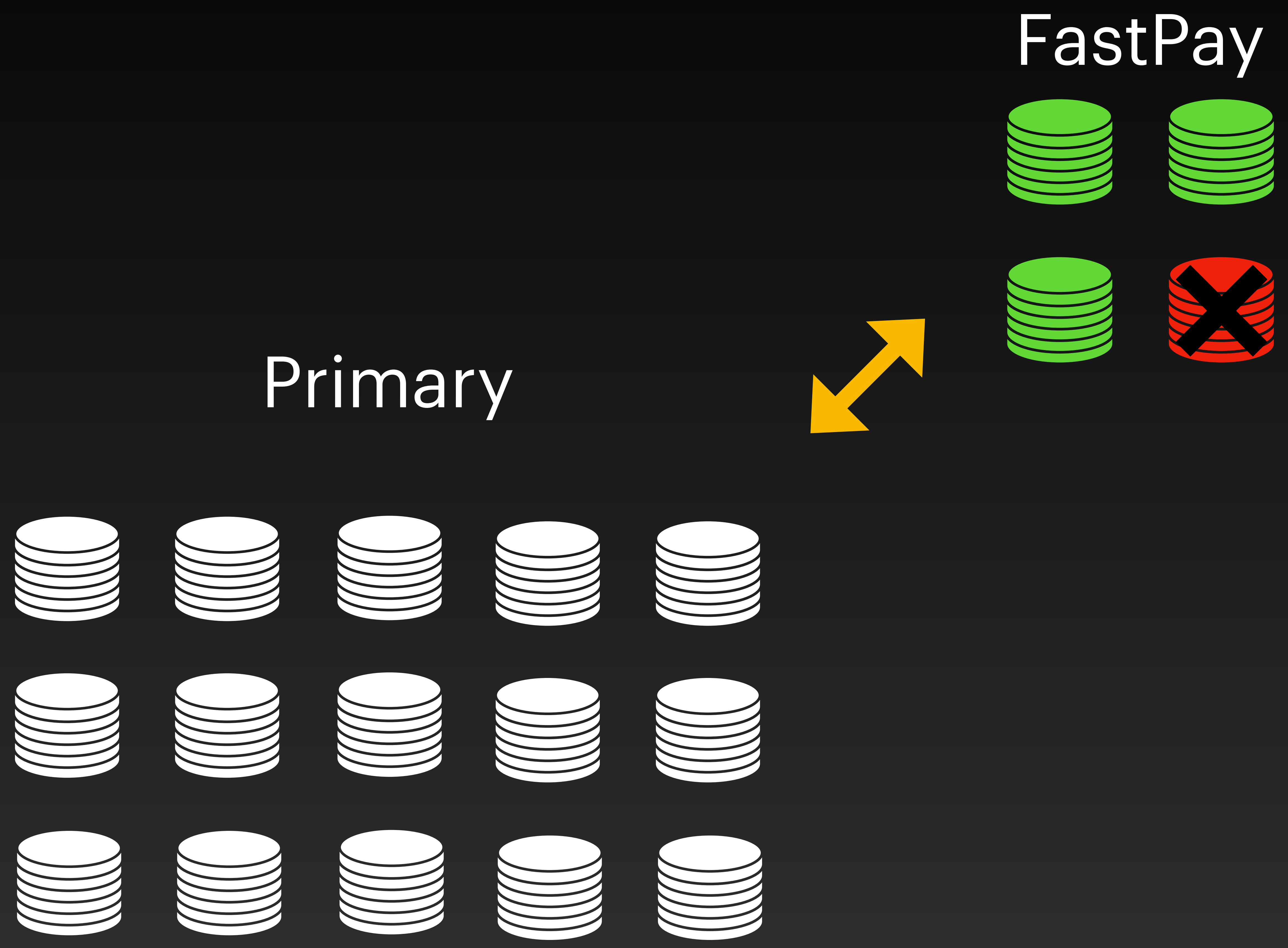
Overview



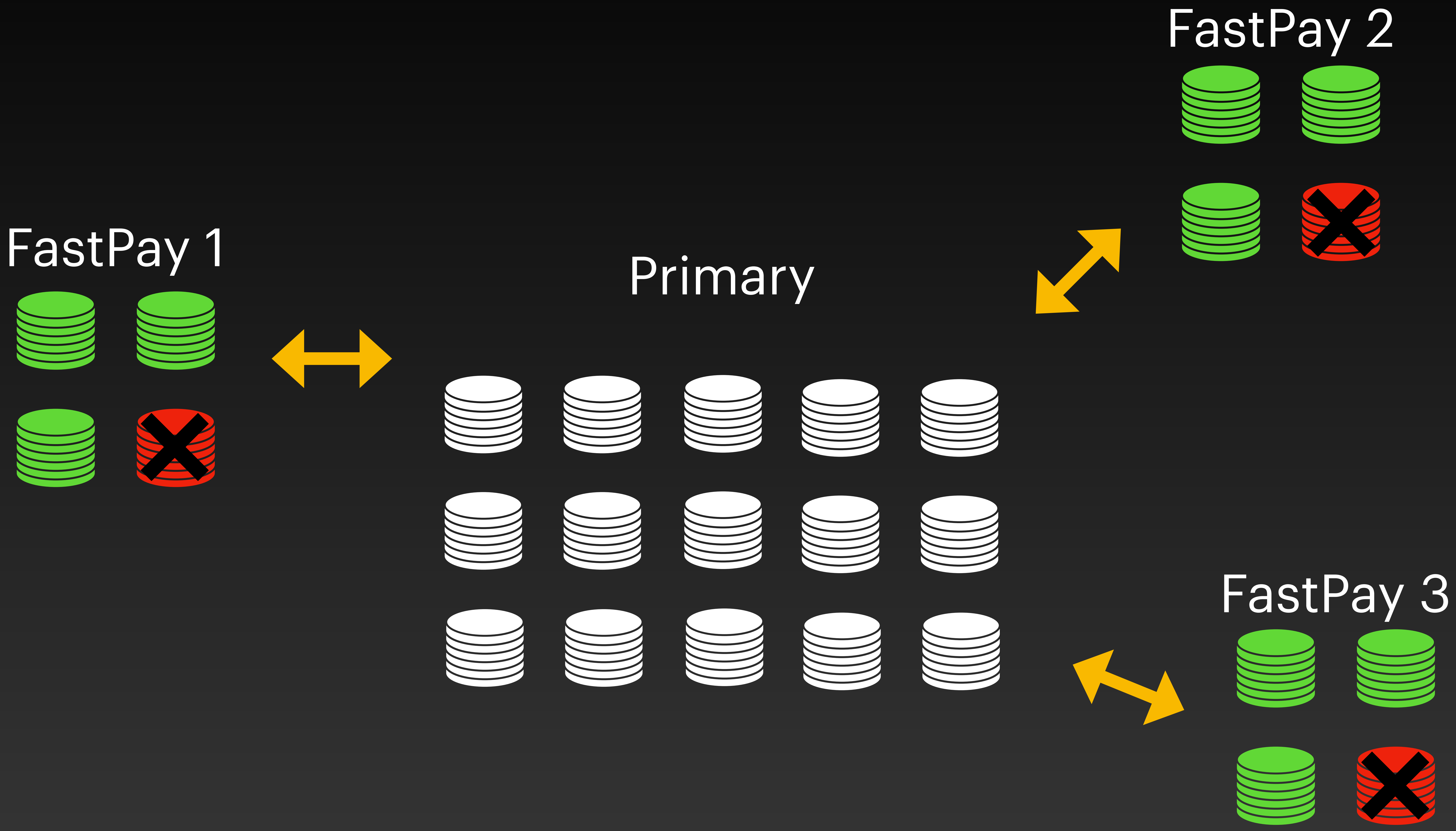
FastPay

Primary

Overview



Overview



Make it practical for retail payment at physical points of sale

This requires extremely low latency

What do we need?

Properties

What we want

- Low latency
- BFT reliance
- Fast finality
- Hight capacity

Current industry

?

Centralized systems

Slow Finality

In summary

What we want

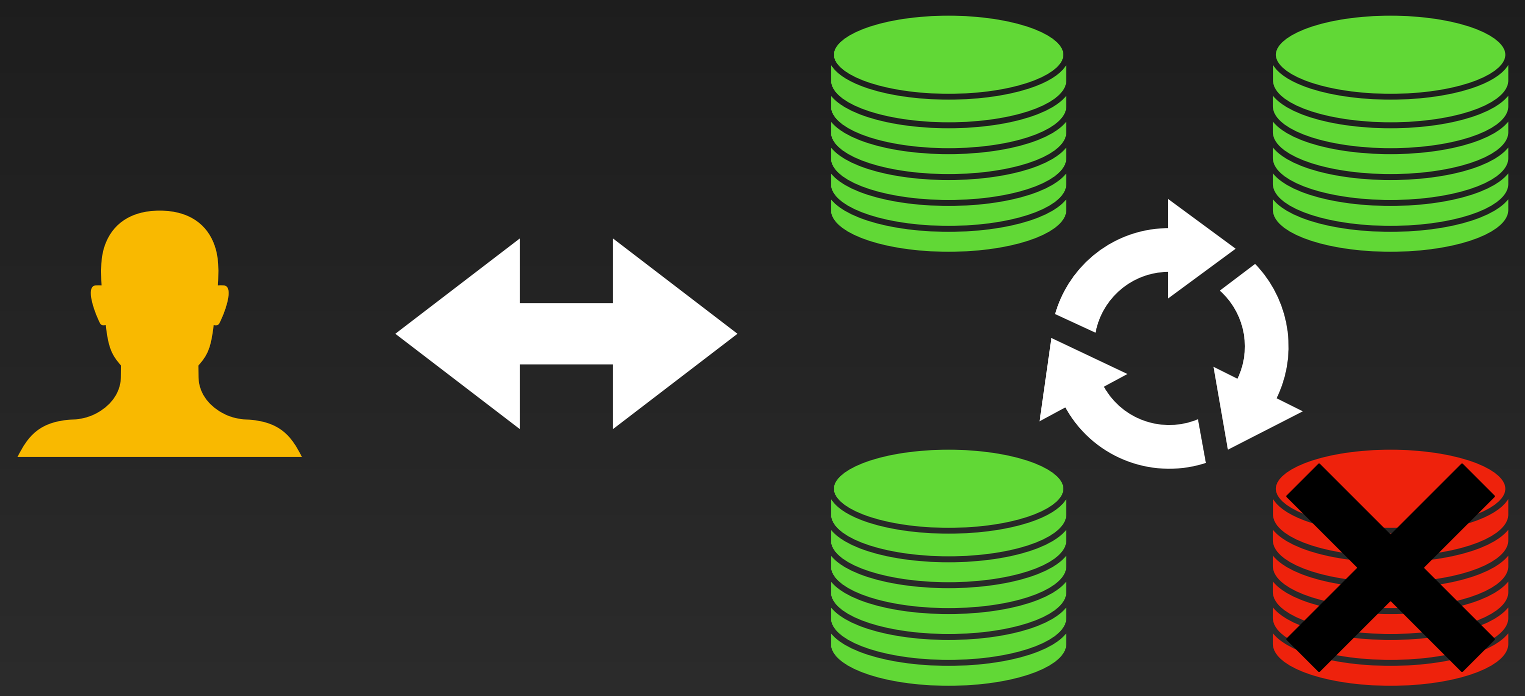
- Low latency
- BFT reliance
- Fast finality
- Hight capacity

Current industry

- Low latency (not settled)
- Centralized
- Slow finality
- Hight capacity (not settled)

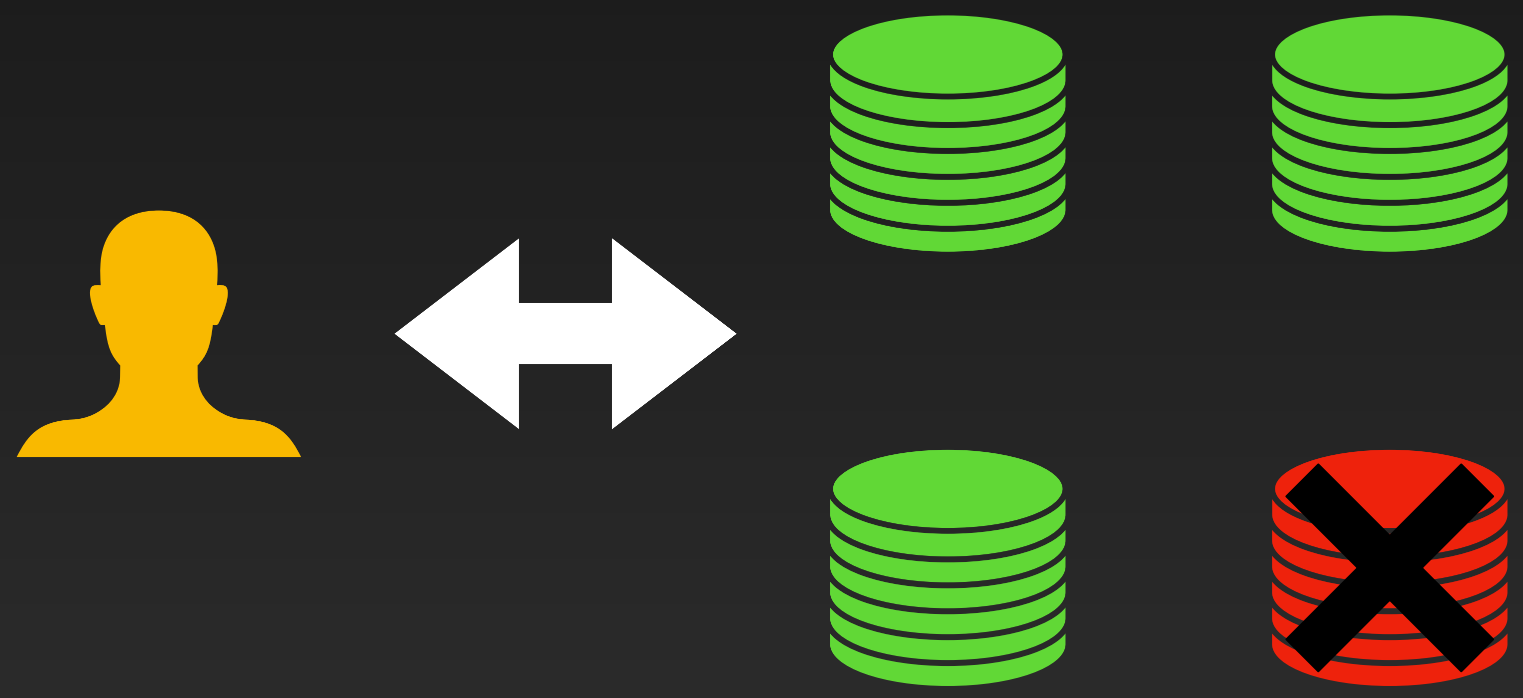
Difference with blockchains

Blockchains



Byzantine Consensus

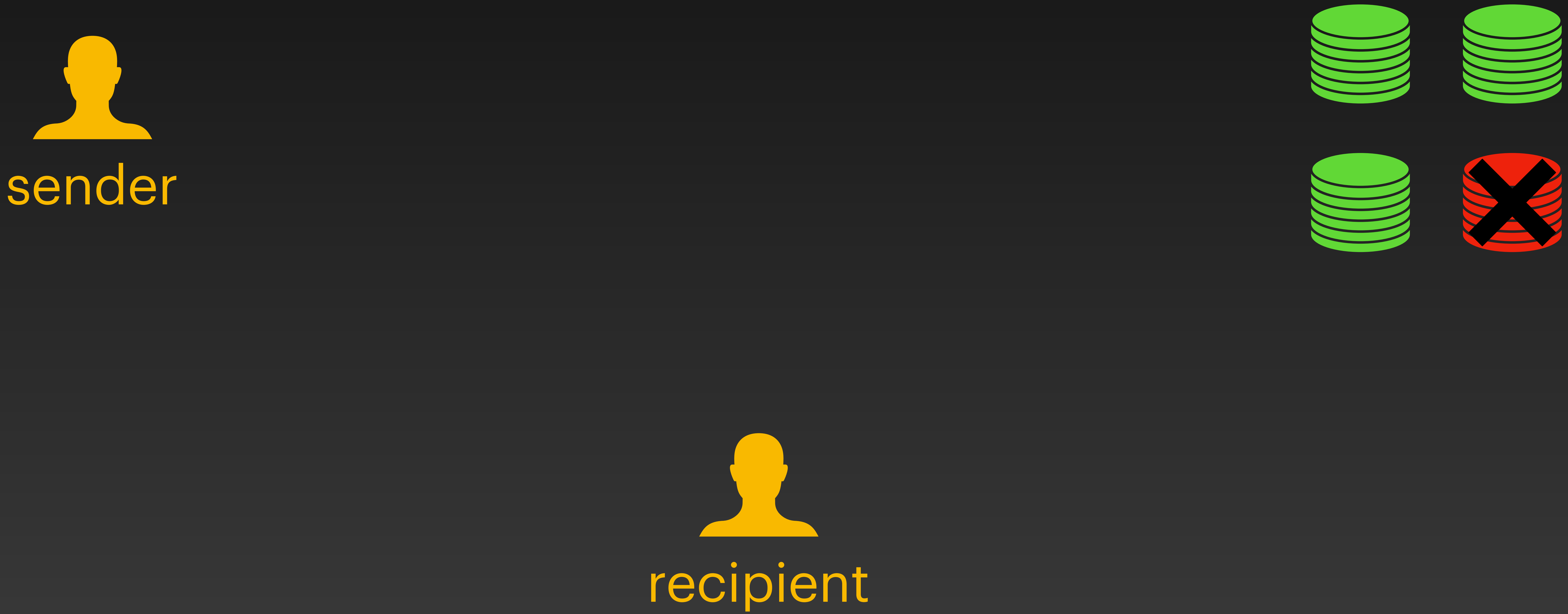
FastPay



Byzantine Consistent Broadcast

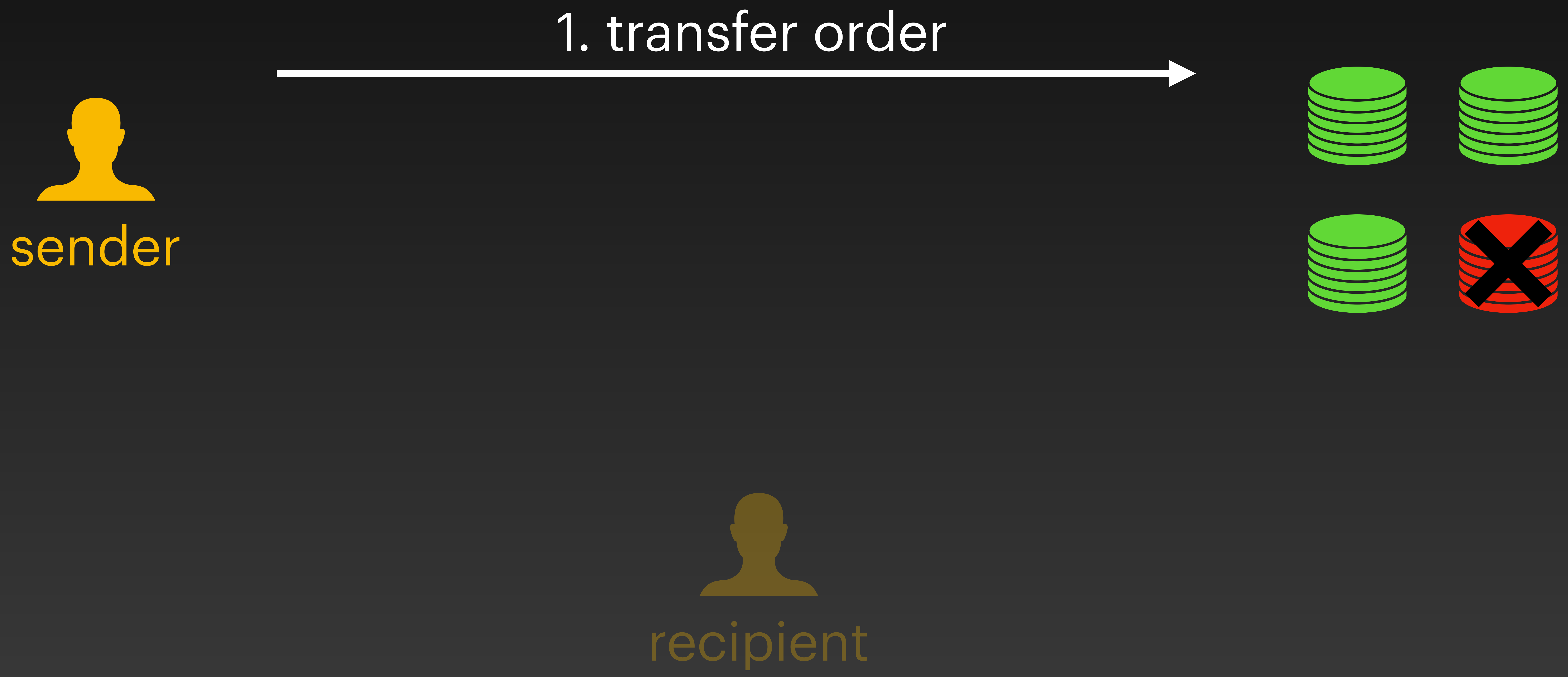
FastPay

How does it work?



FastPay

How does it work?



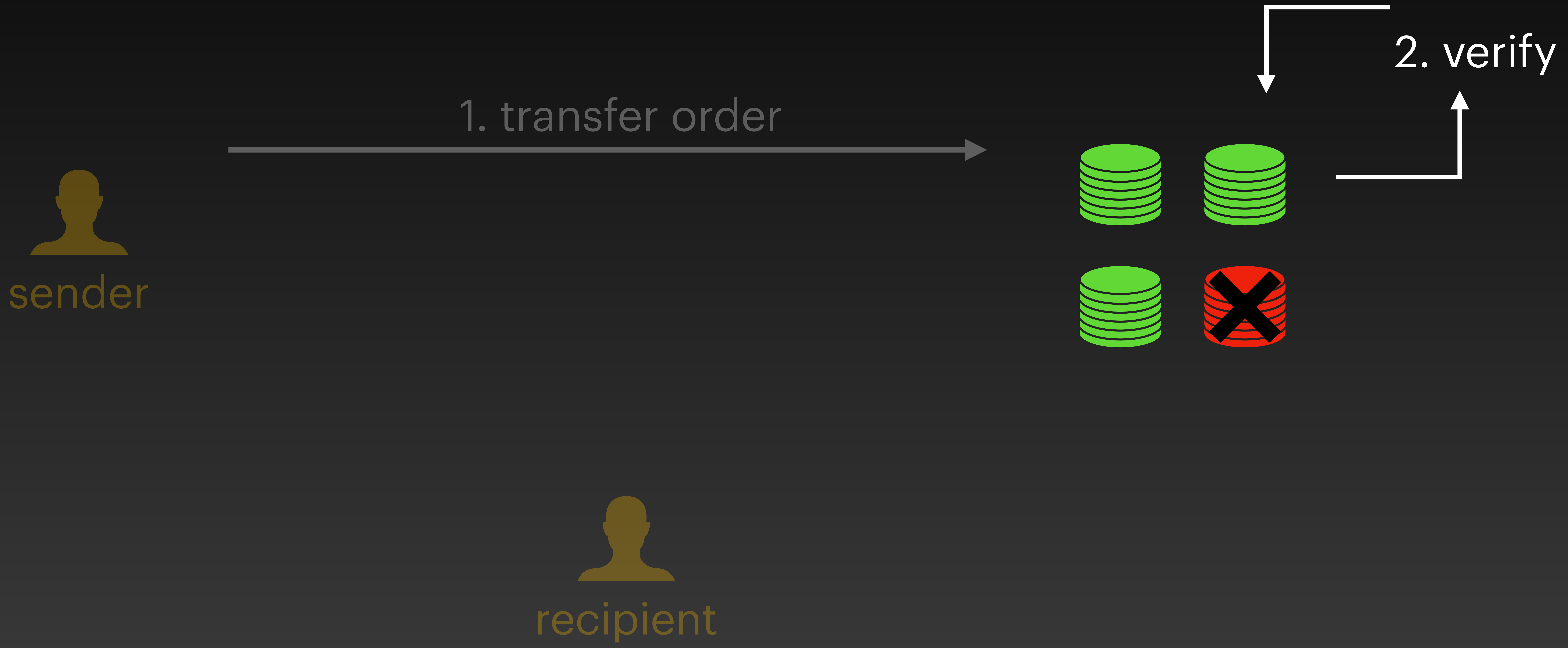
1. transfer order

sender

recipient

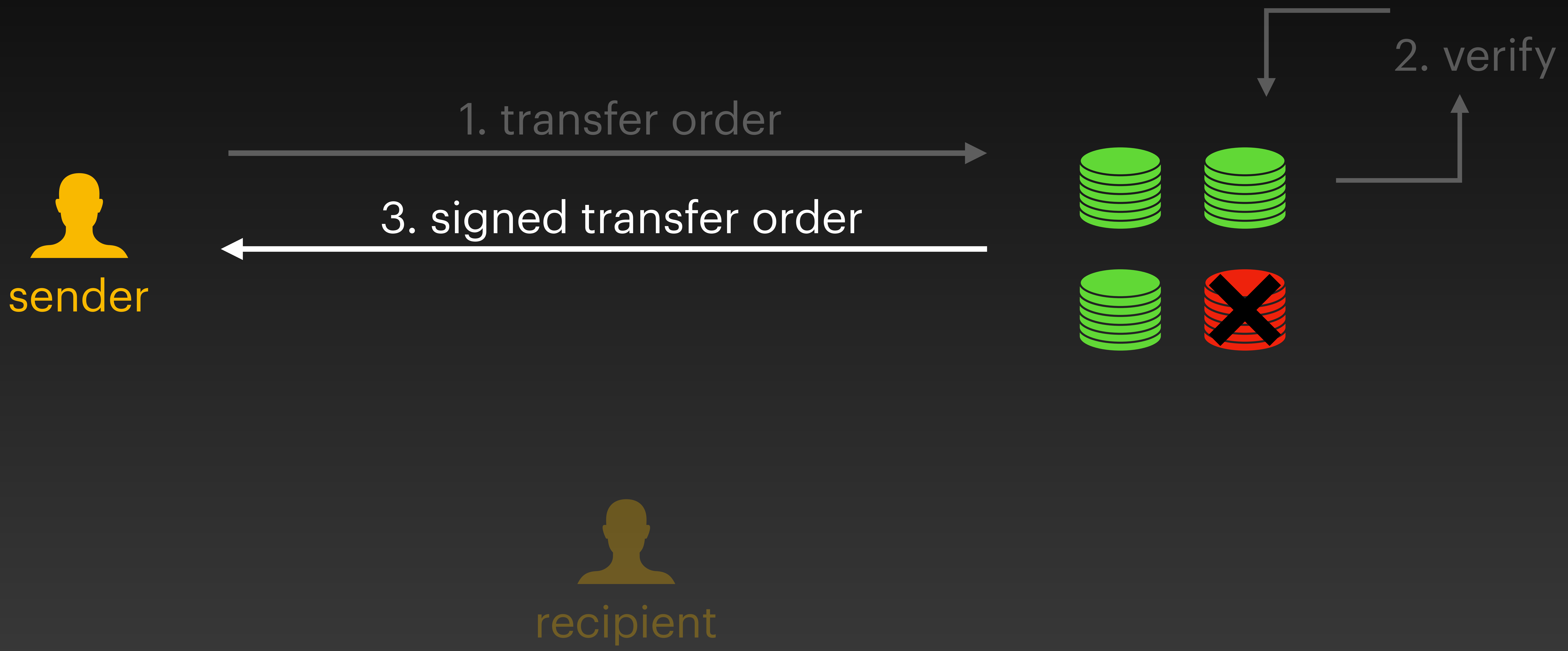
FastPay

How does it work?



FastPay

How does it work?



2. verify

1. transfer order

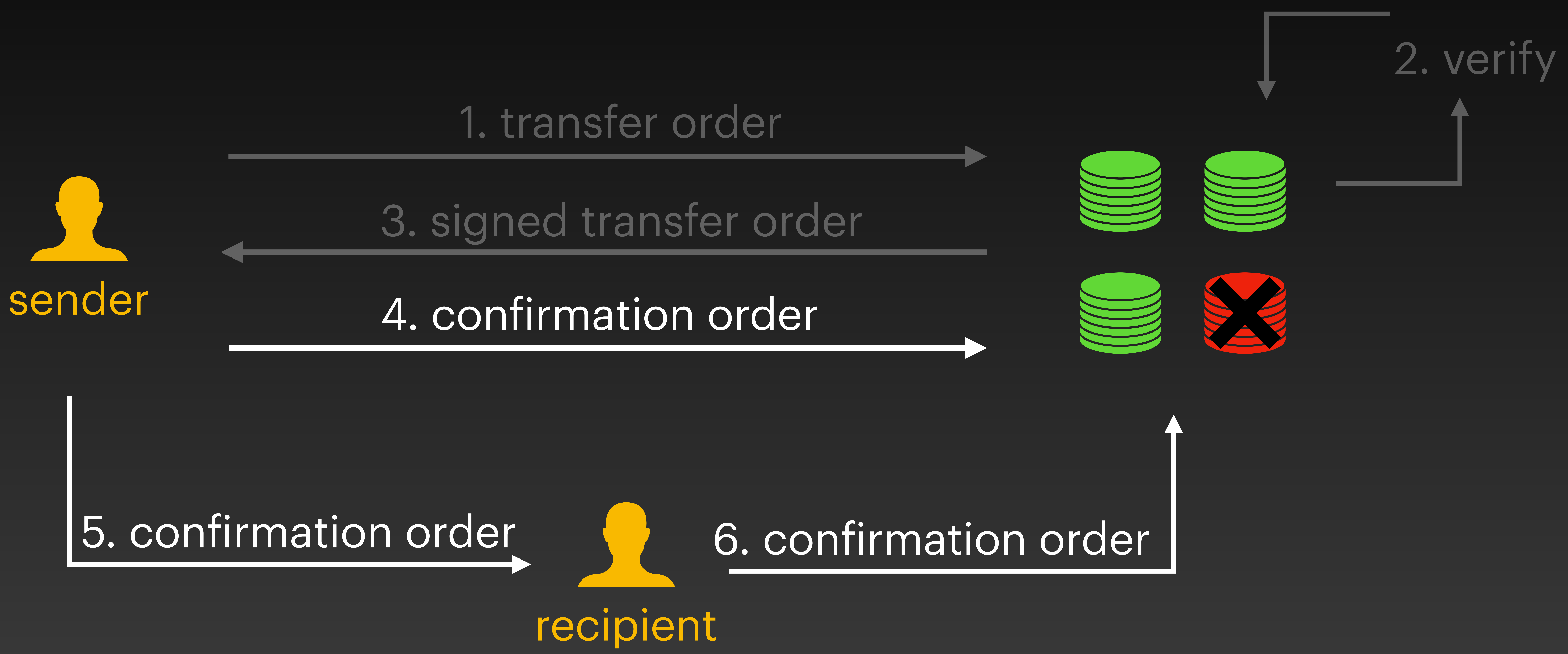
3. signed transfer order

sender

recipient

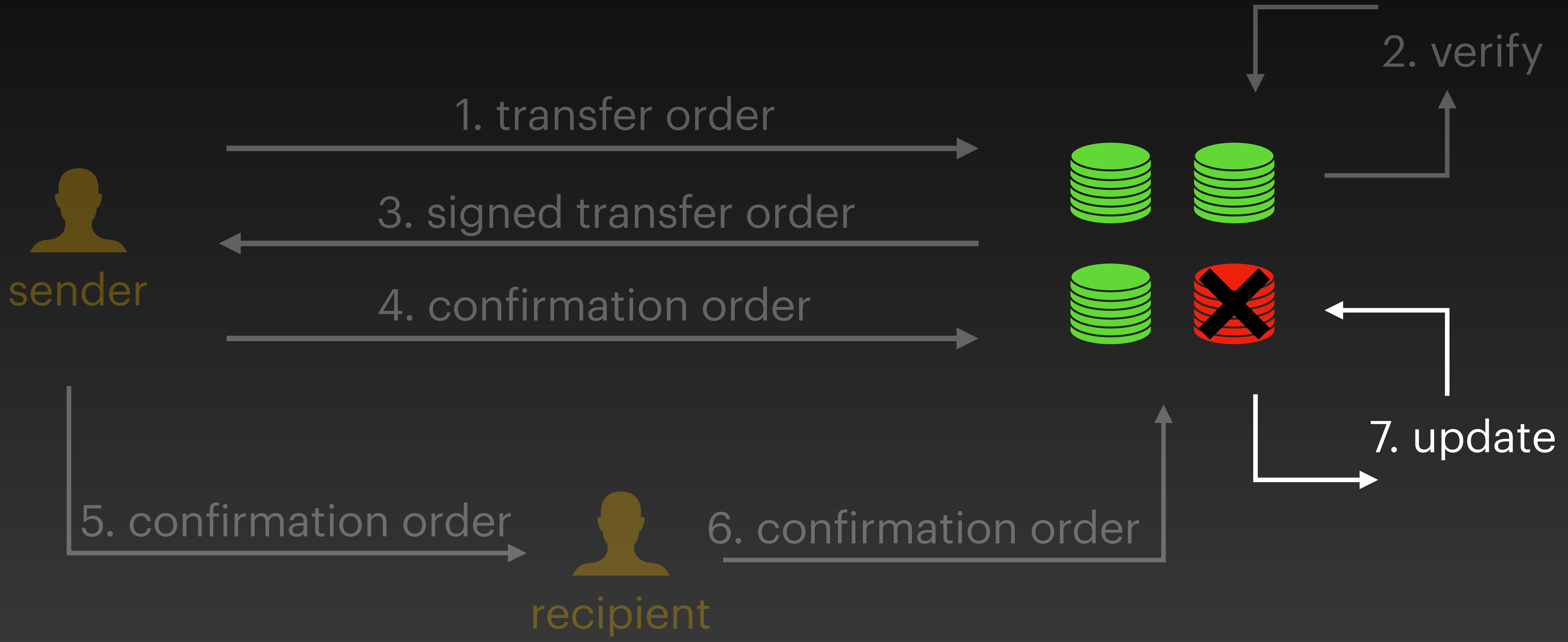
FastPay

How does it work?



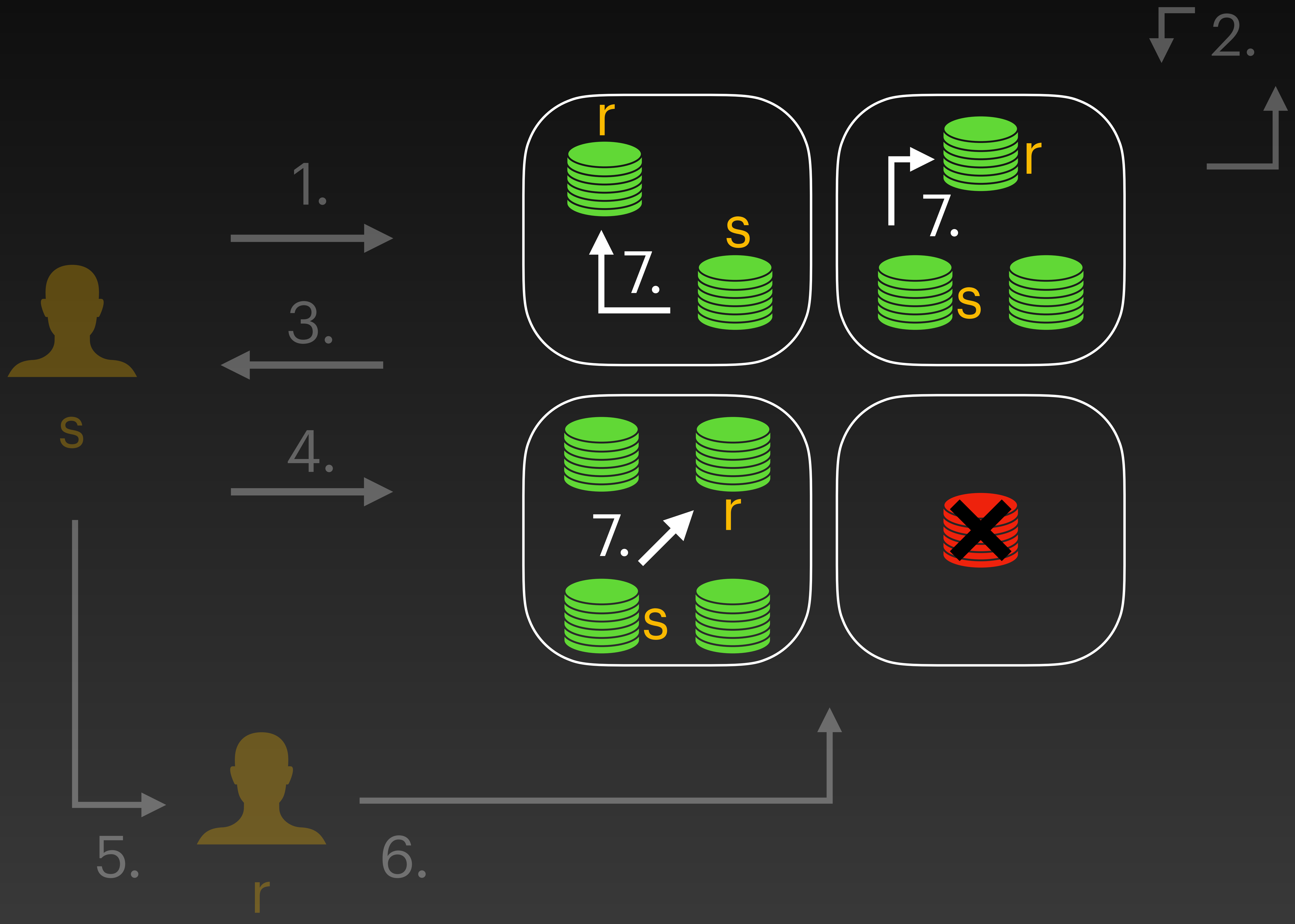
FastPay

How does it work?



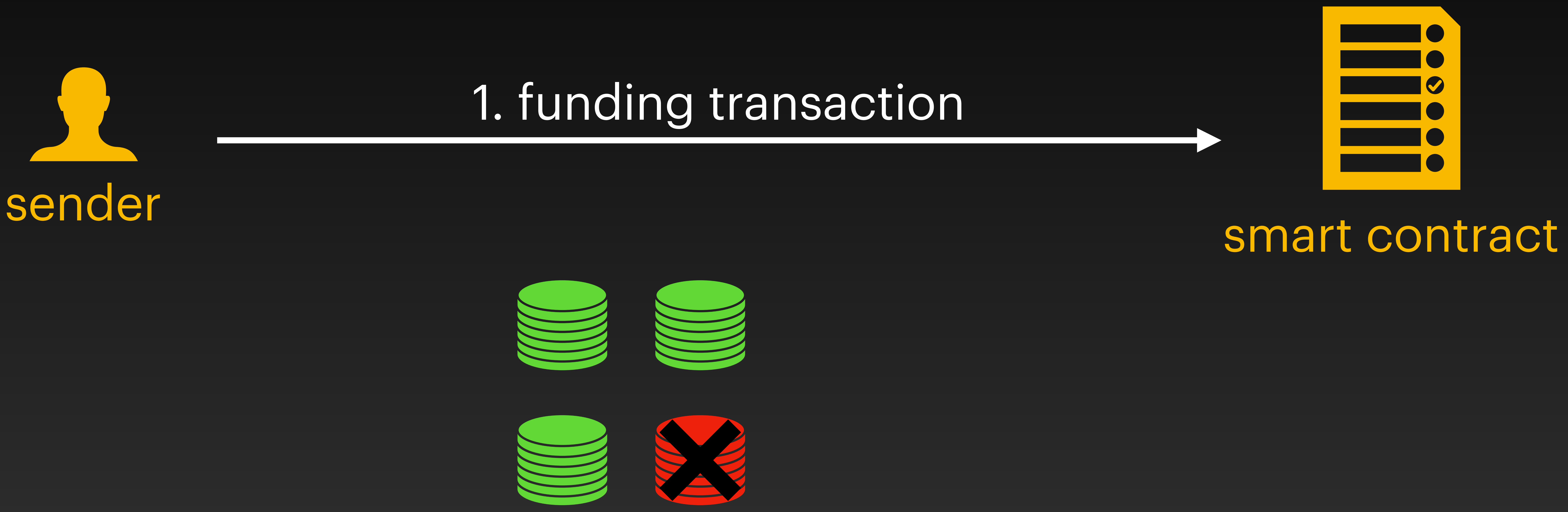
FastPay

Increasing capacity



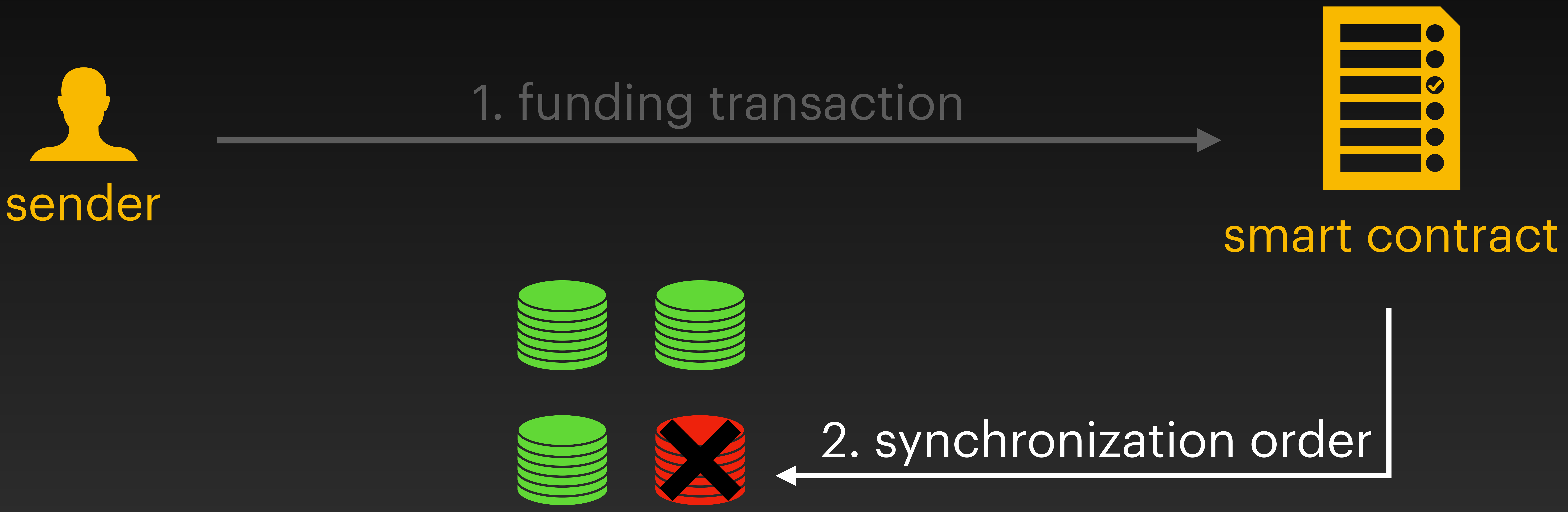
FastPay

From primary infrastructure to FastPay



FastPay

From primary infrastructure to FastPay



sender

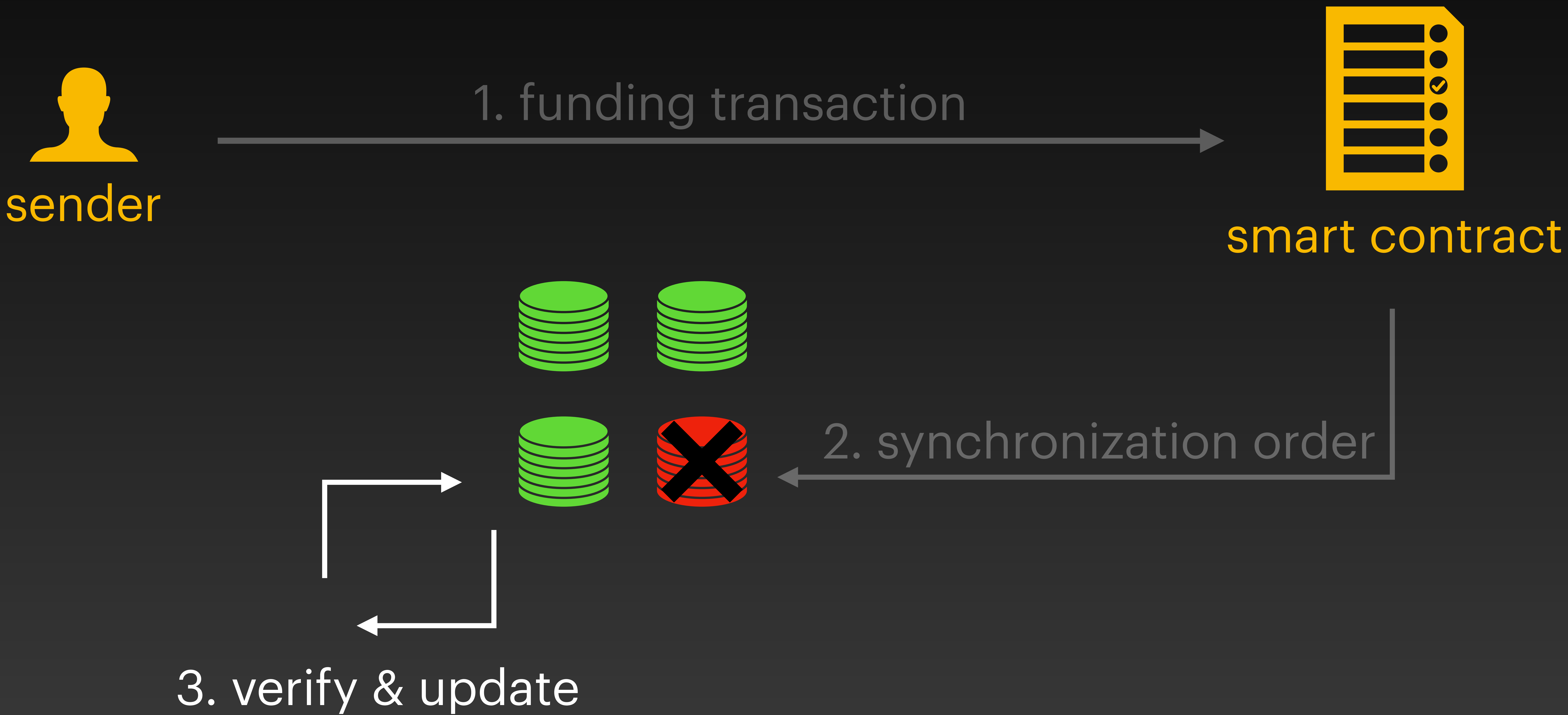
1. funding transaction

smart contract

2. synchronization order

FastPay

From primary infrastructure to FastPay



sender

1. funding transaction

smart contract

2. synchronization order

3. verify & update

FastPay

Implementation

- Written in Rust
- Networking: Tokio & UDP
- Cryptography: ed25519-dalek

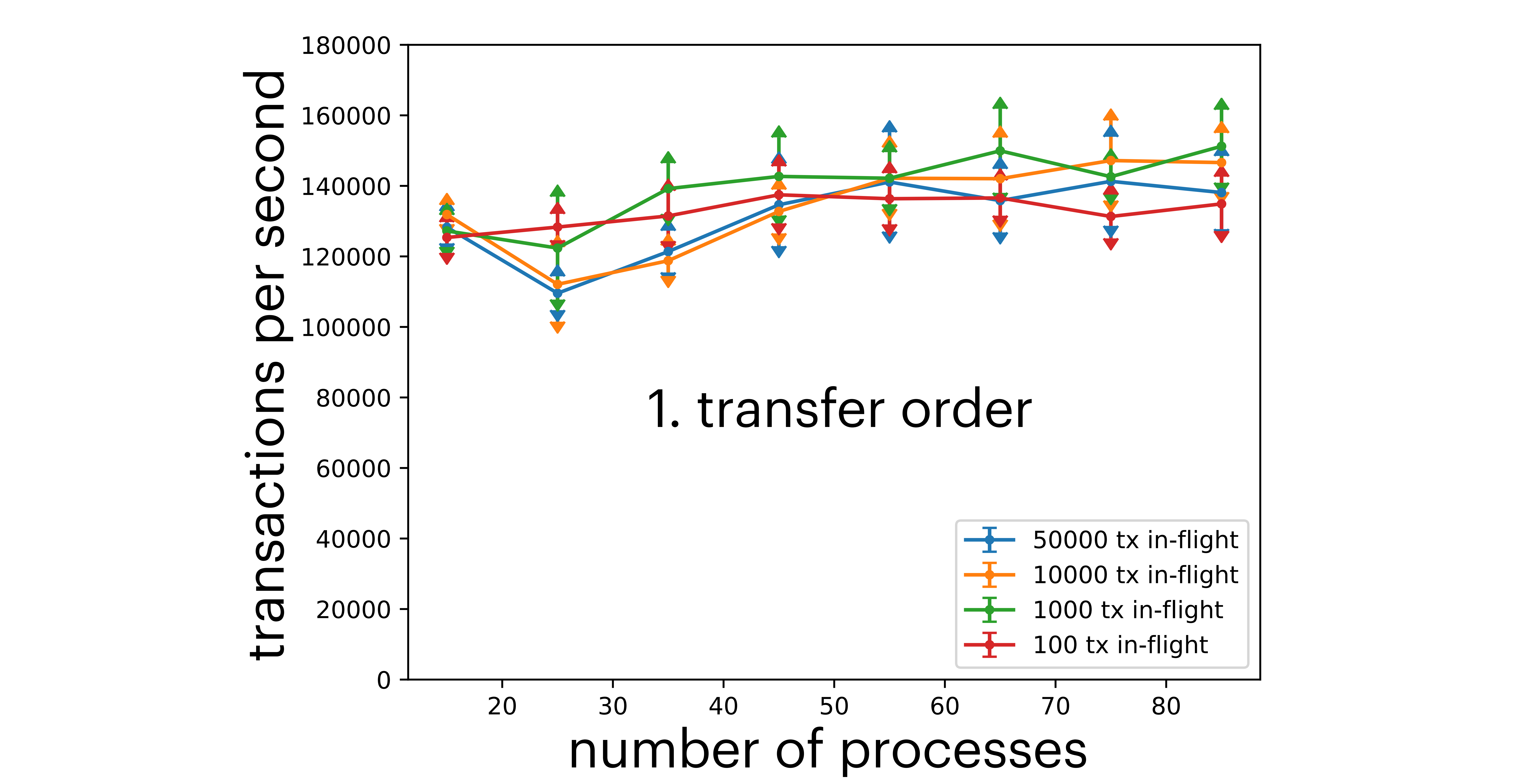
https://github.com/novifinancial/fastpay

FastPay

Throughput Evaluation

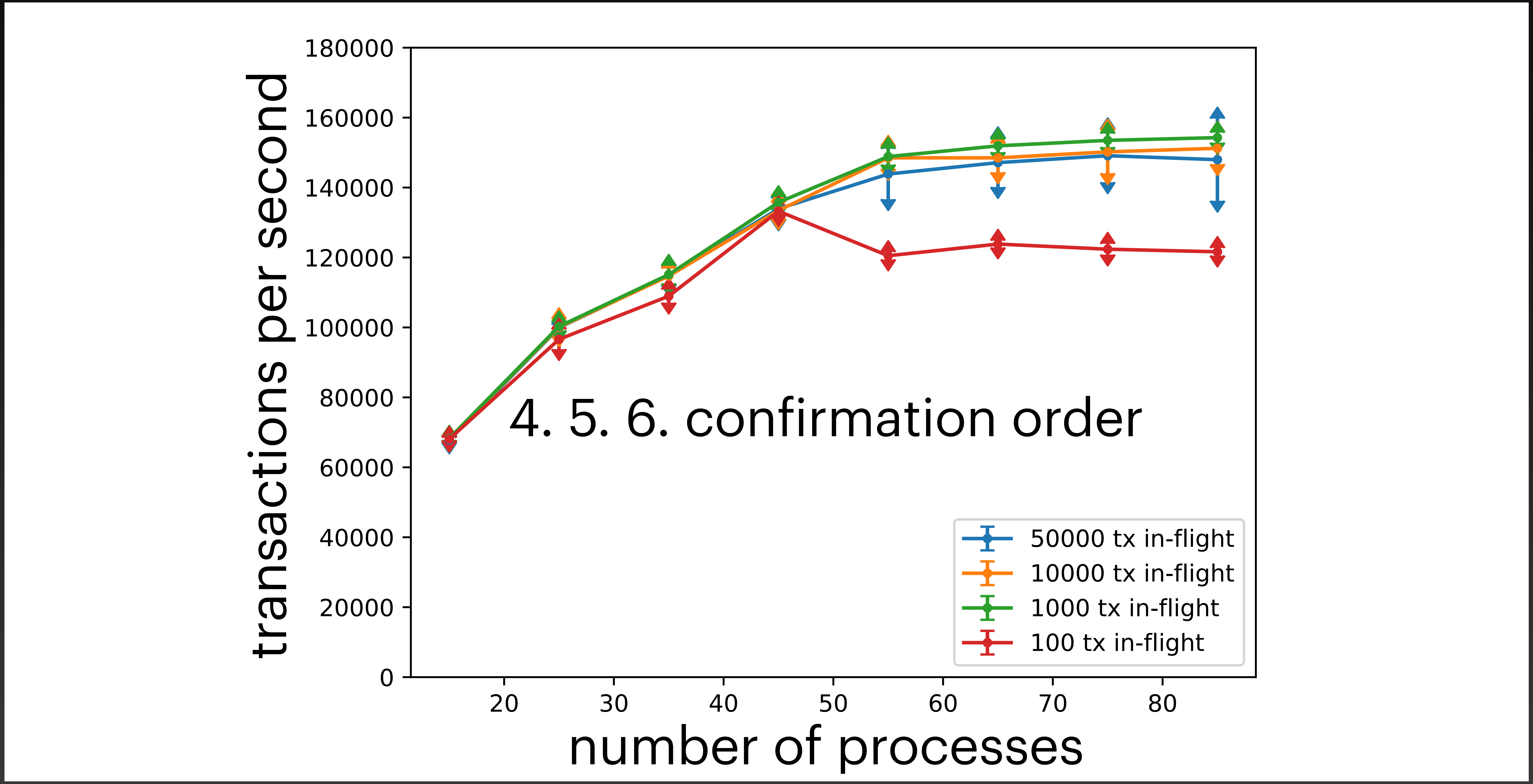
FastPay

High concurrency



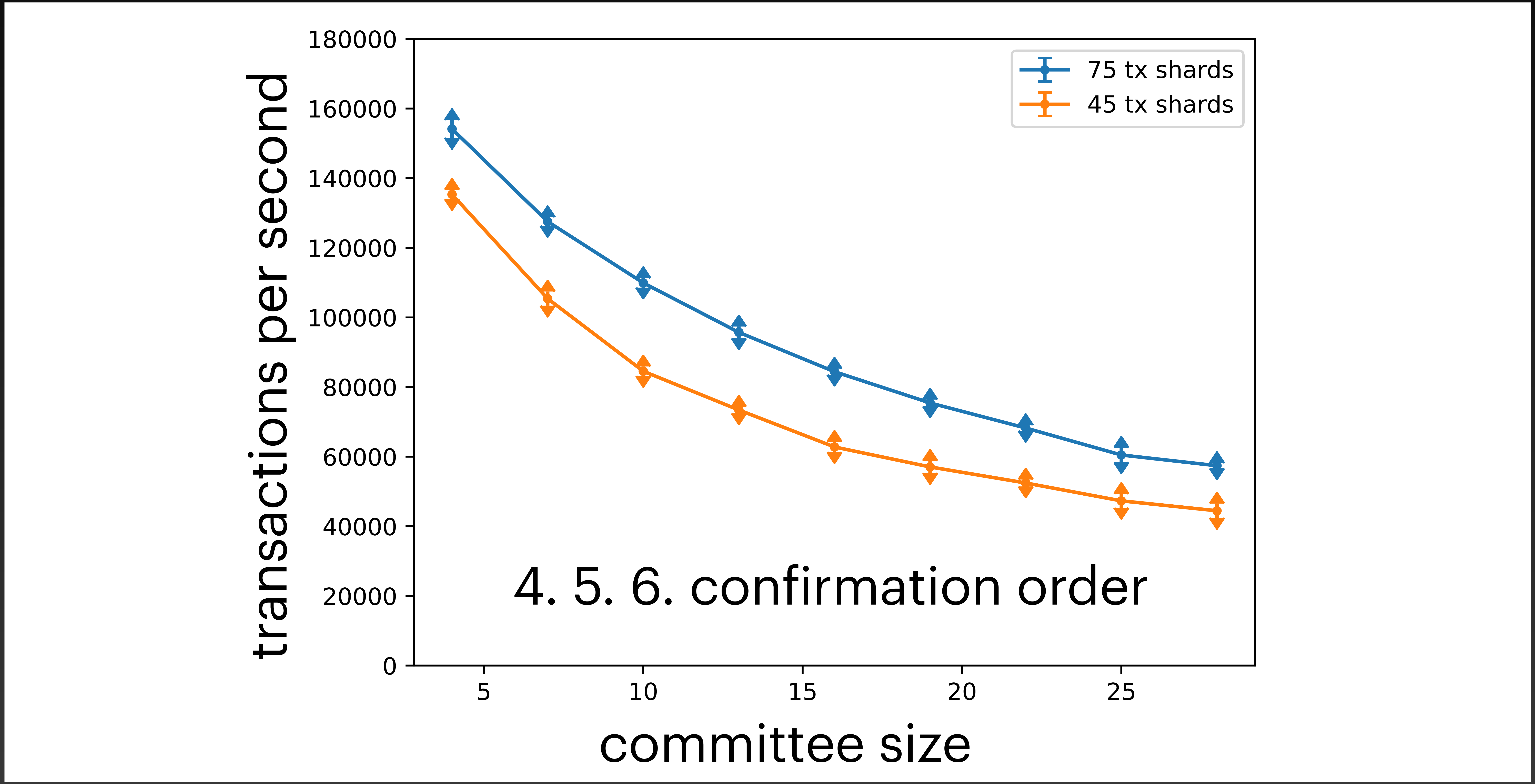
FastPay

High concurrency



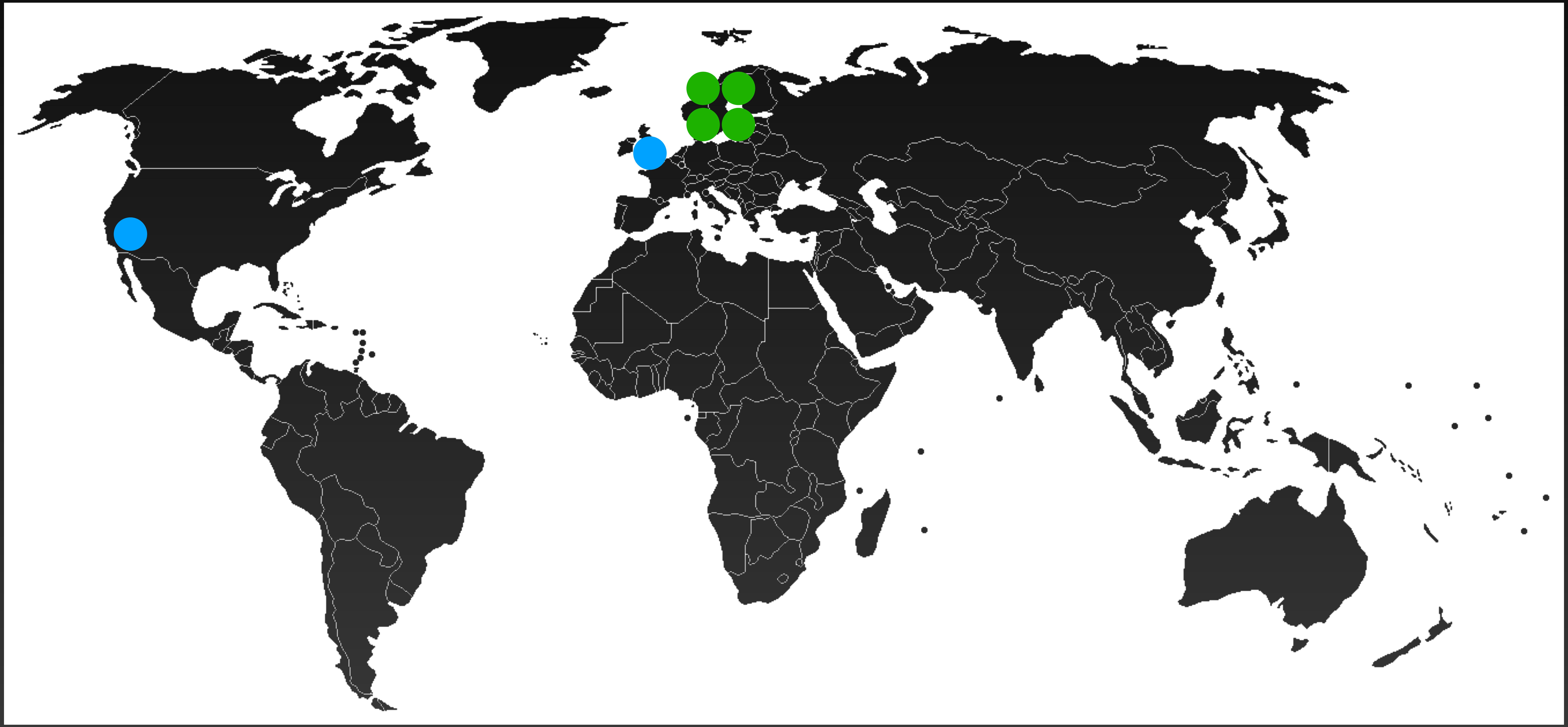
FastPay

Influence of the number of authorities



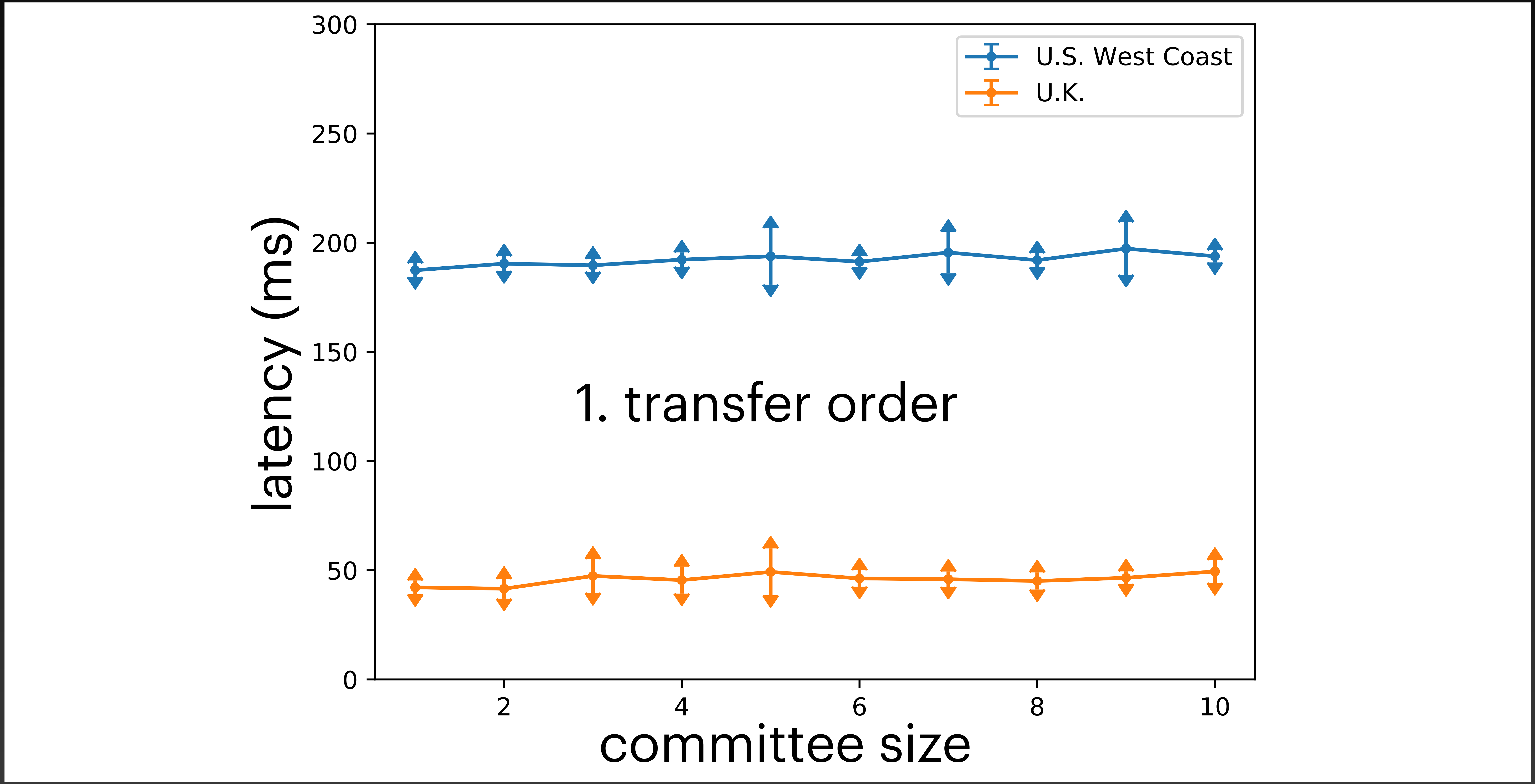
FastPay

Latency setup



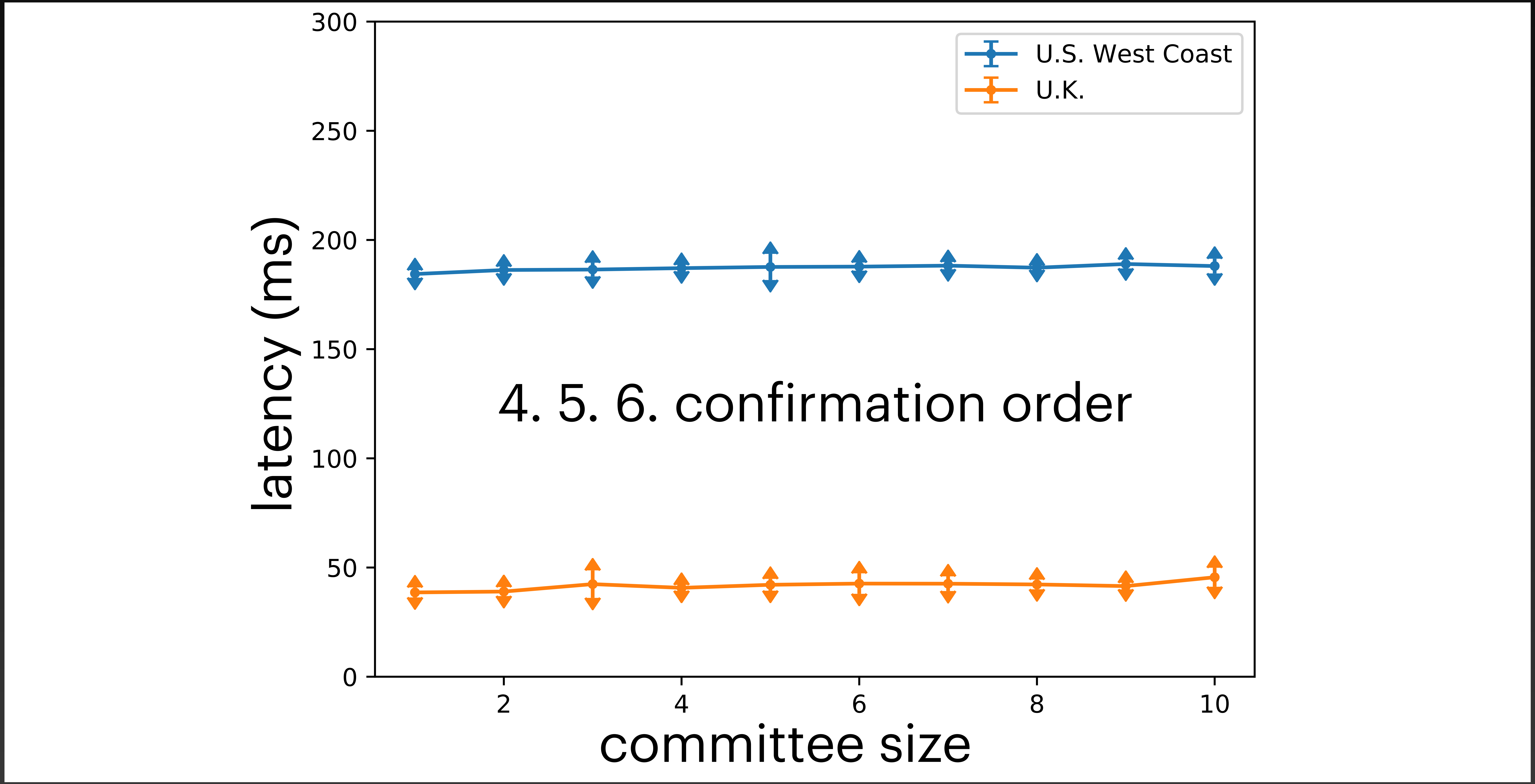
FastPay

Latency



FastPay

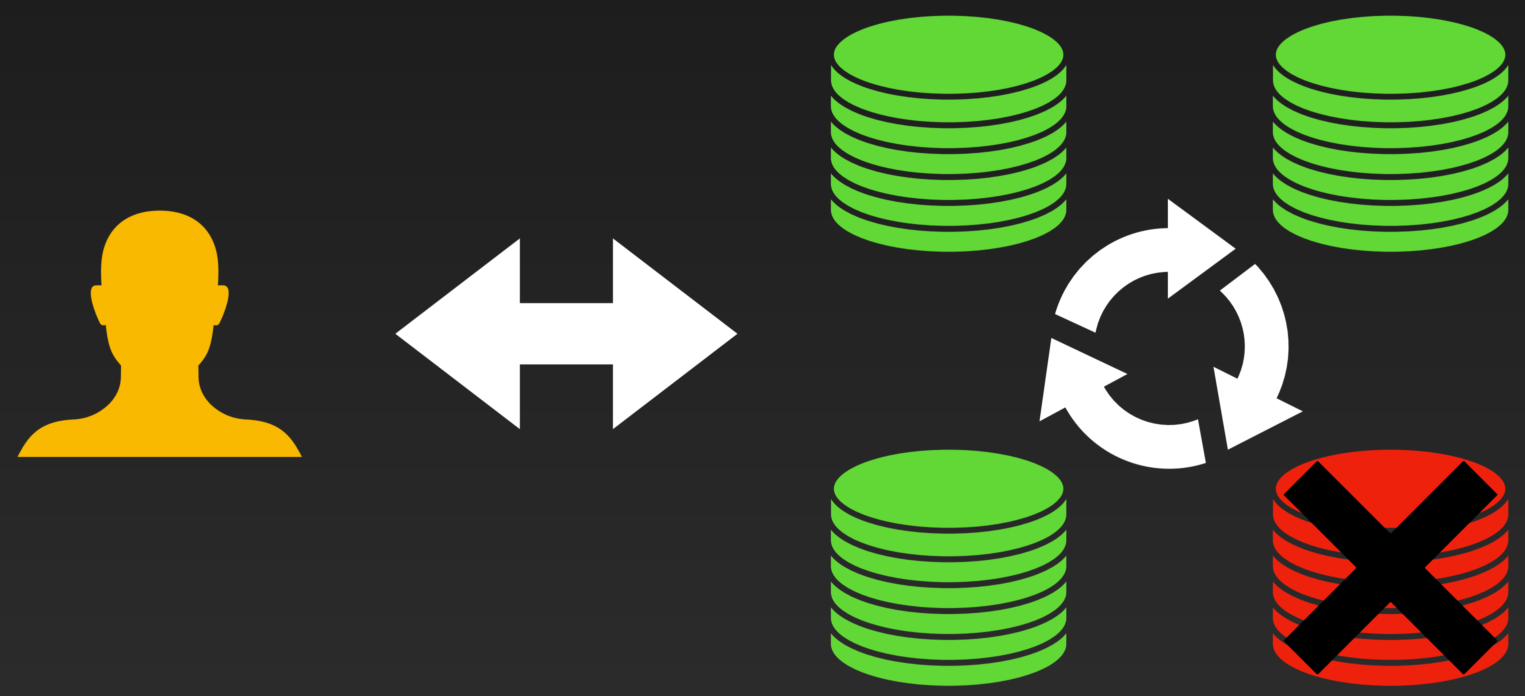
Latency



4. 5. 6. confirmation order

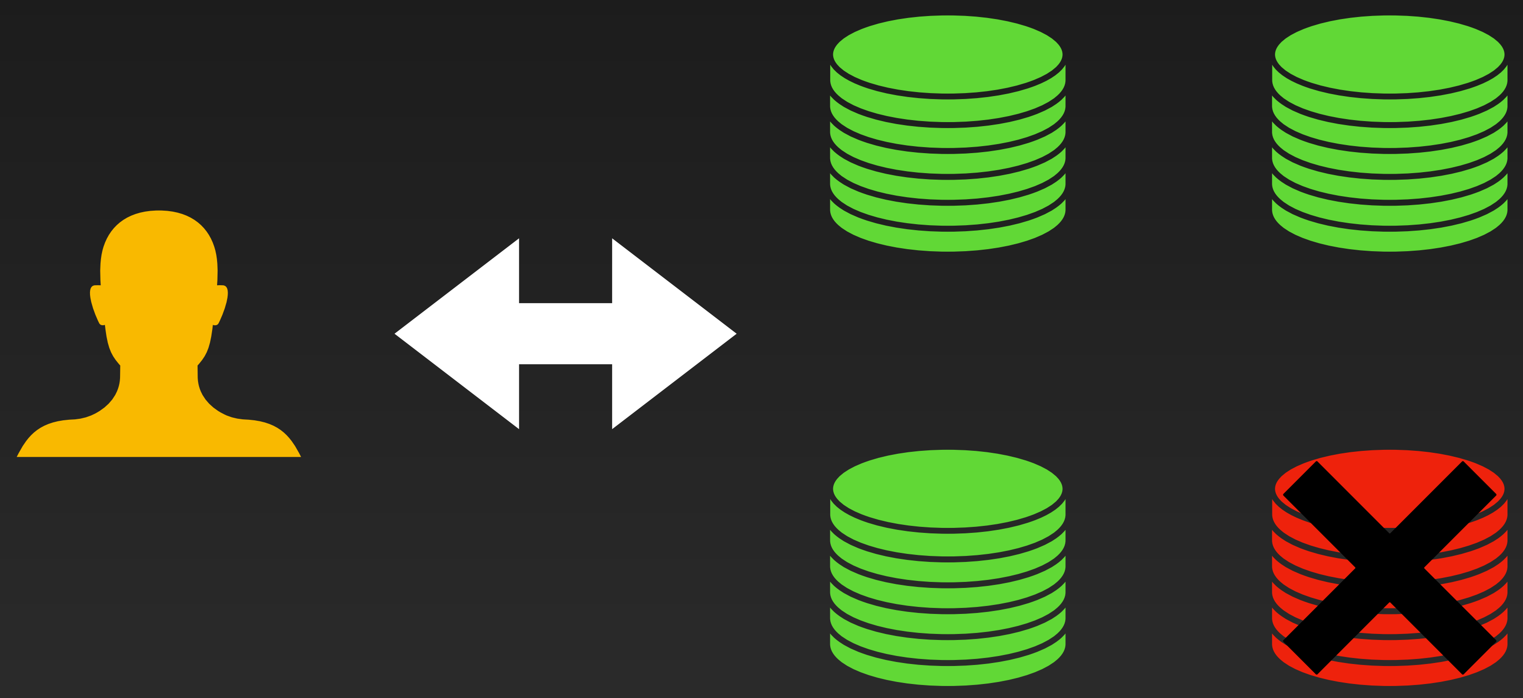
Worst-case efficiency

Blockchains



Bad leader can slow down the protocol

FastPay



No leader, nothing changes

Conclusion

FastPay

- Based on Byzantine Consistent Broadcast
- Simple design, low latency, high capacity, very robust

- **Paper:** https://arxiv.org/abs/2003.11506
- **Code:** https://github.com/novifinancial/fastpay

asonnino@fb.com

Alberto Sonnino