



# Commit-Chains Summary



## NOCUST

Off-chain ledger state:  
**user balances**

Fungible payments

Slower delayed finality

Lightweight clients

Instant finality support

Atomic Off-chain Swap (TEX)

Regular online presence to watch  
malicious state changes

## NOCUST-ZKP

- trusted setup for ZK  
+ users without incoming  
transaction can stay offline  
+ non-interactive challenge

## Plasma (Cash)

Off-chain ledger state:  
**coin serial number**

Non-Fungible payments

Rapid delayed finality

Large amounts of history data

No instant finality support

No known feasibility for swaps

Regular online presence to watch  
malicious withdrawals

# The good, bad and ugly of Commit Chains



**Recipient can be  
offline to receive a  
transaction**



**Limited censorship  
resistance**



**No decentralization**



**No collateral for delayed  
finality**

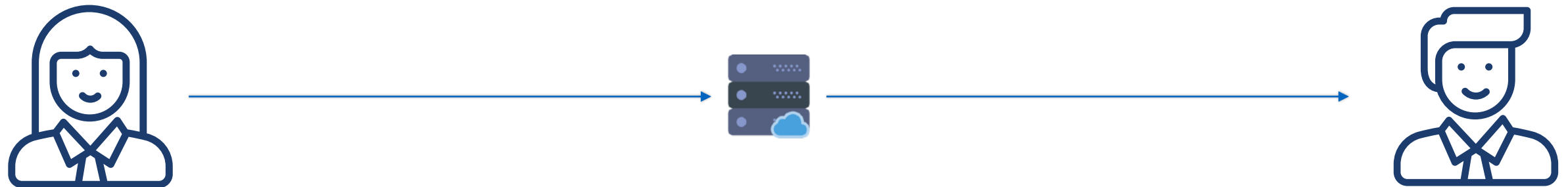


**Instant and free  
onboarding**



**Data availability  
challenges**

# What if we have a blockchain that scales significantly (wrt. latency and volume)?



## 2nd Factor and Location Verification:

Do you really want to spend these coins?

-> Get notified and act upon misbehavior.

## Privacy:

Off-Chain transactions are not broadcast, **may** increase privacy  
Privacy is lost towards commit-chain operators.