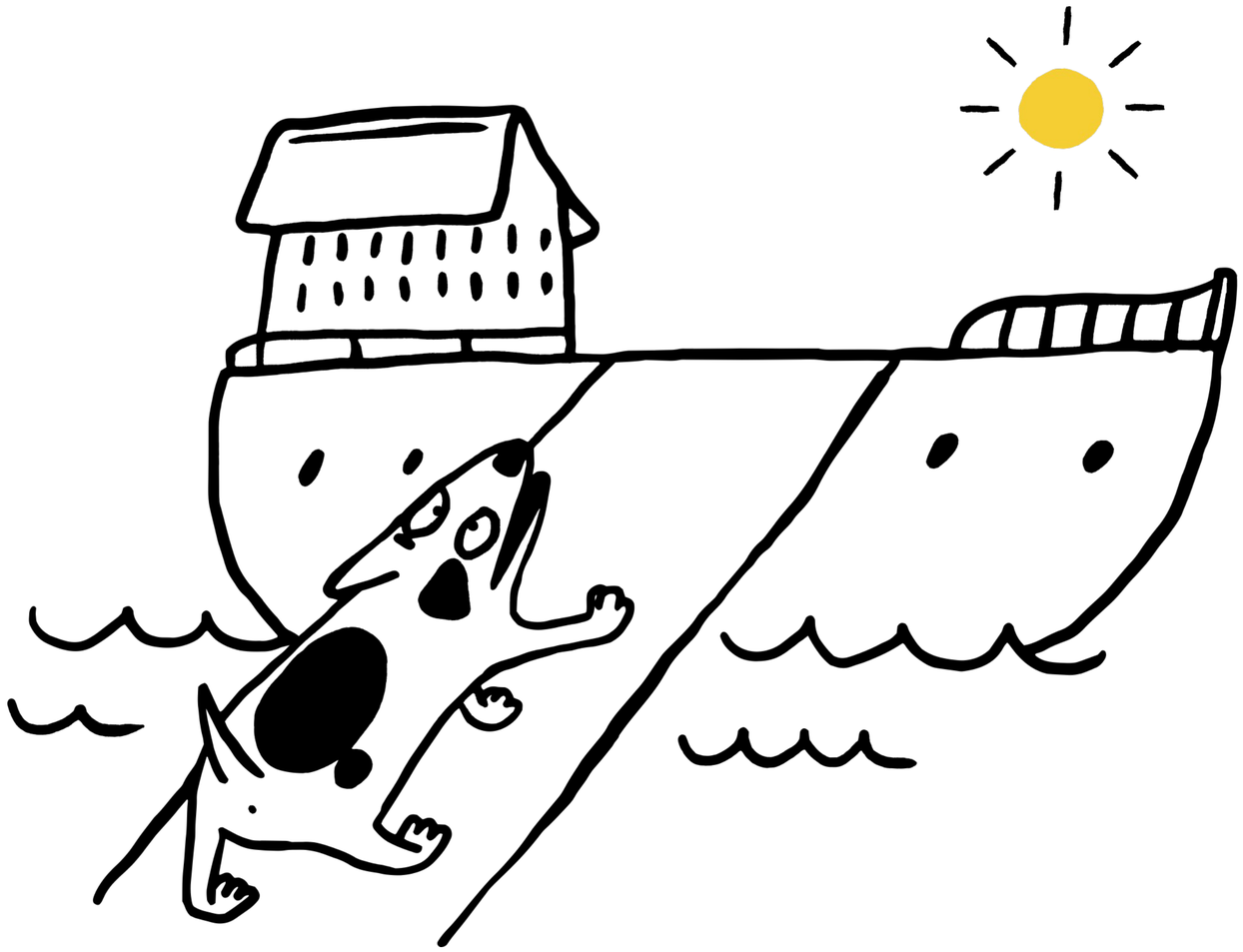
Ark & ecash:

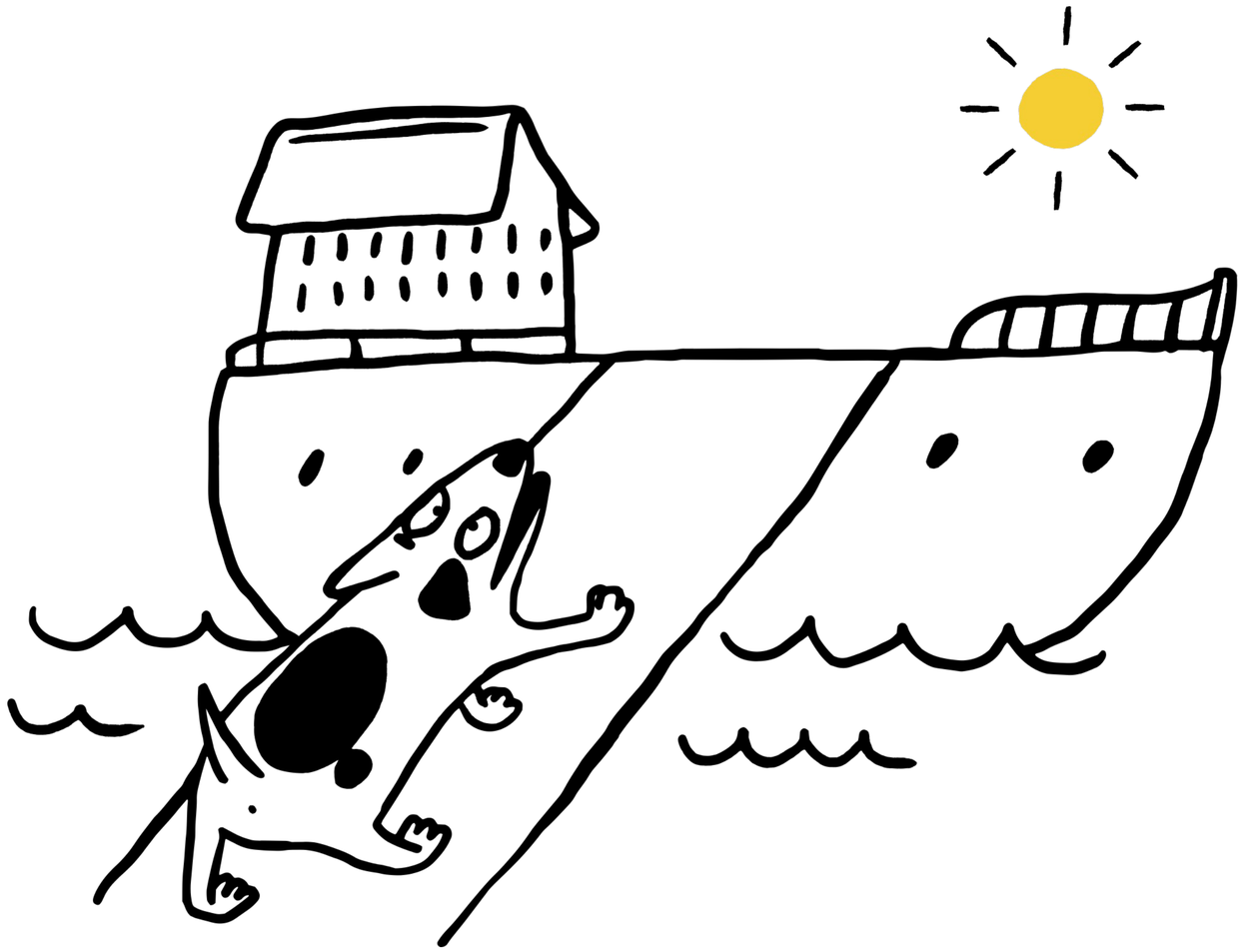
enemies or friends?



second

Ark & ecash:

obviously friends !! ❤



second

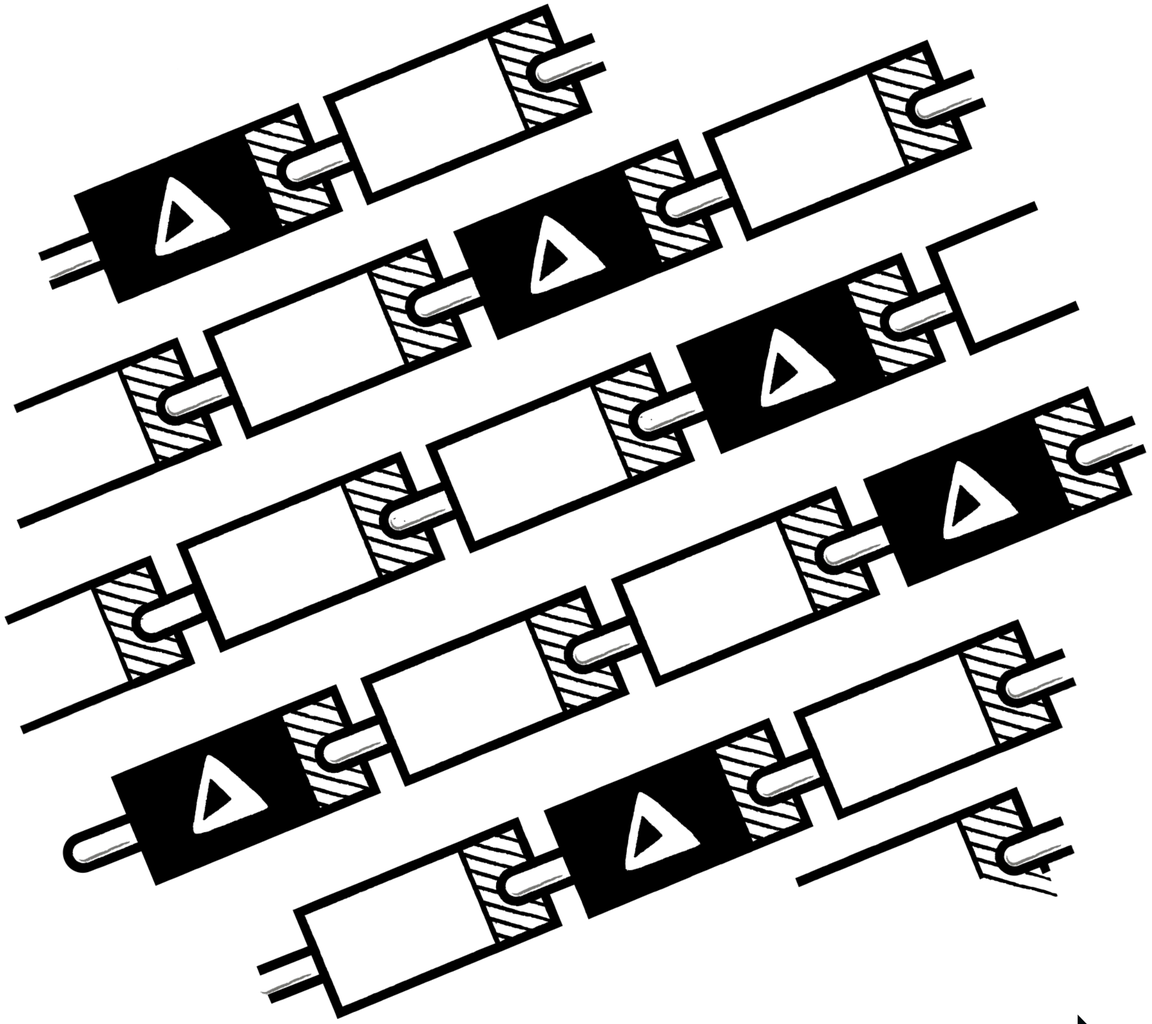
Ark

shared UTXOs → VTXOs

atomic exchange of VTXOs

VTXOs are refreshed in rounds

fast direct transfers → “arkoor”



second

ecash

exchange btc for ecash tokens

custodial mints (multi-sig)

blinded transactions

tokens have superpowers

second

So how do they compare?

second

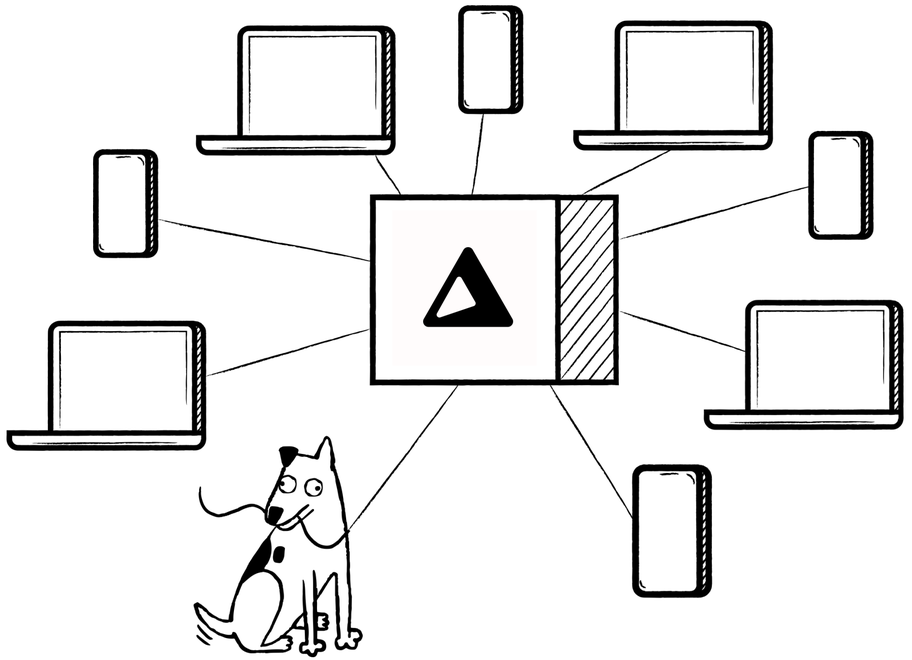
hub-and-spoke

client-server protocols

no p2p required

central coordinator*

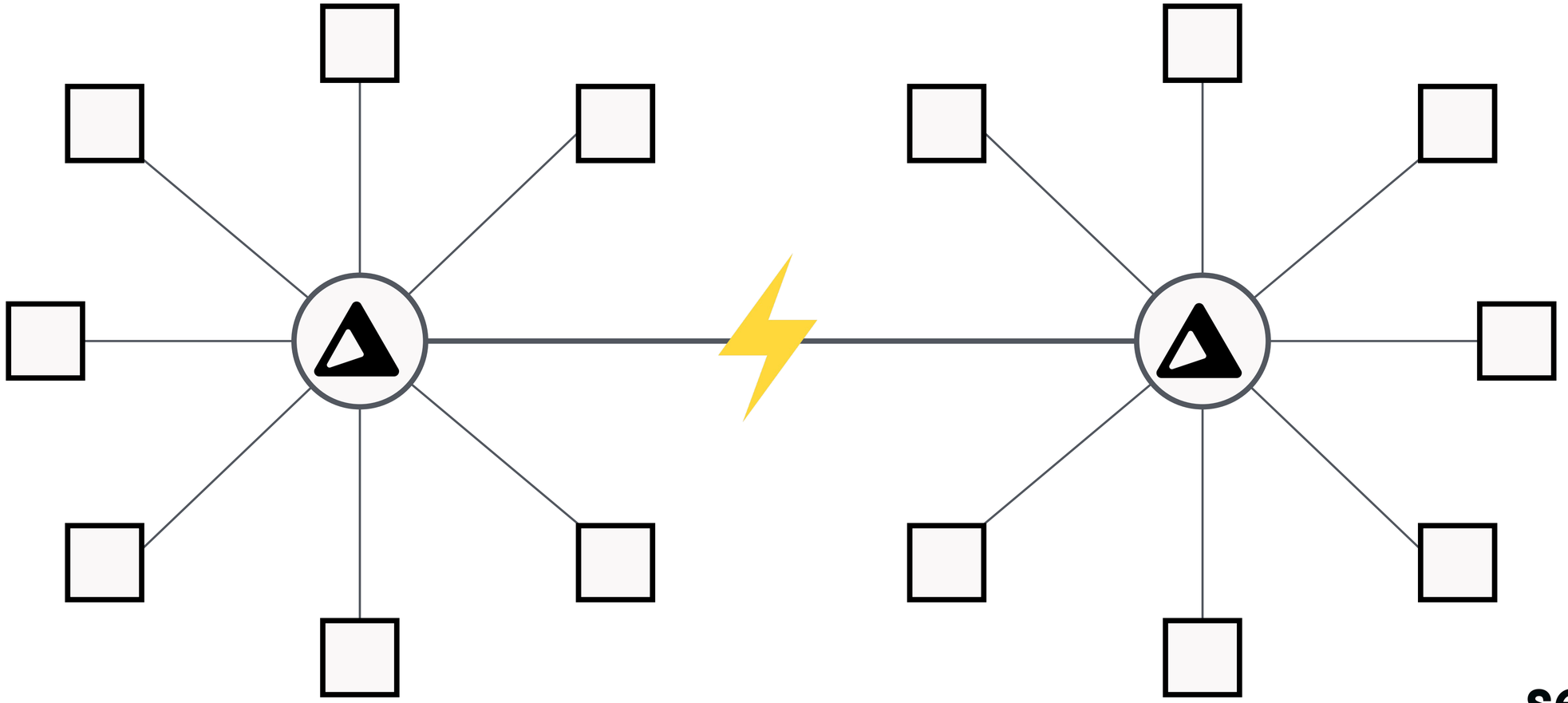
bridging over Lightning



*:

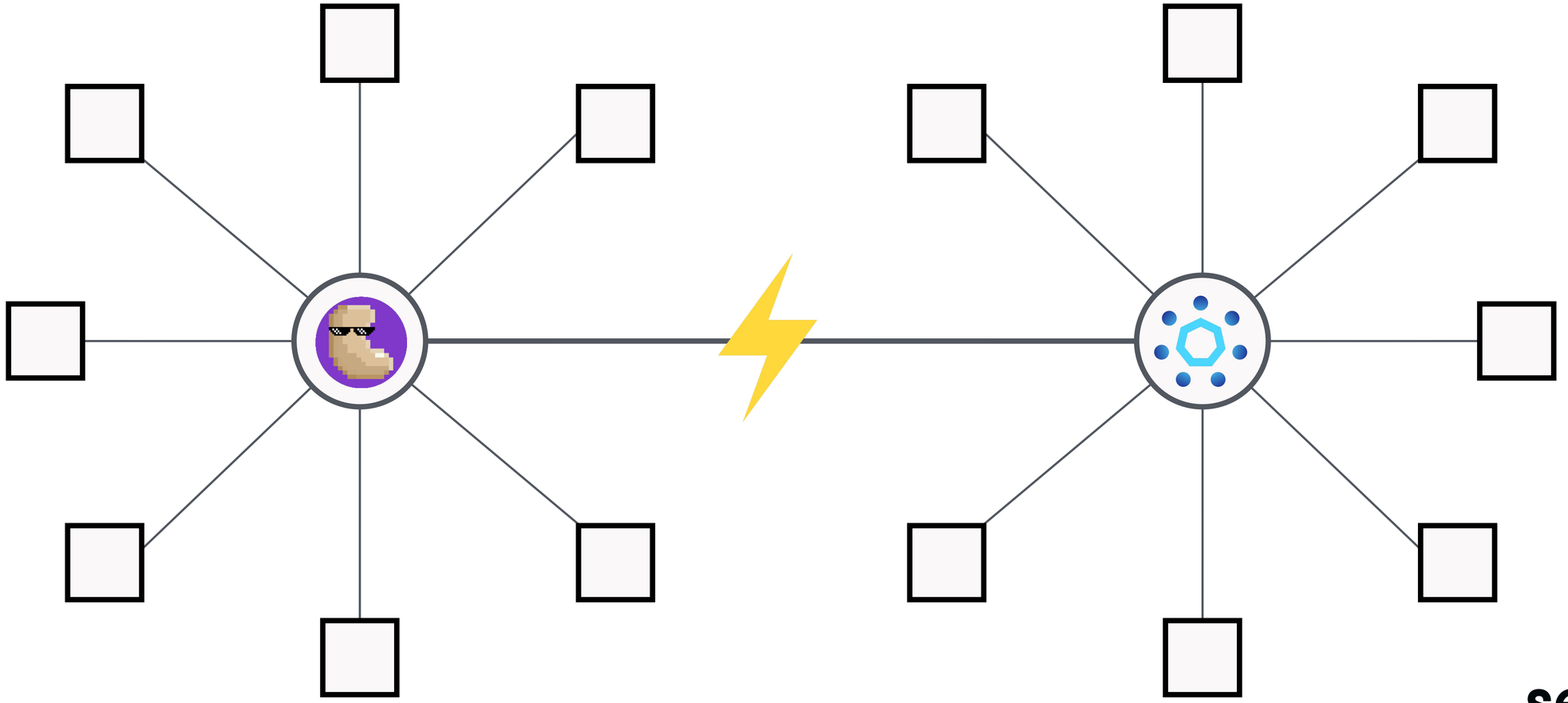
second

hub-and-spoke



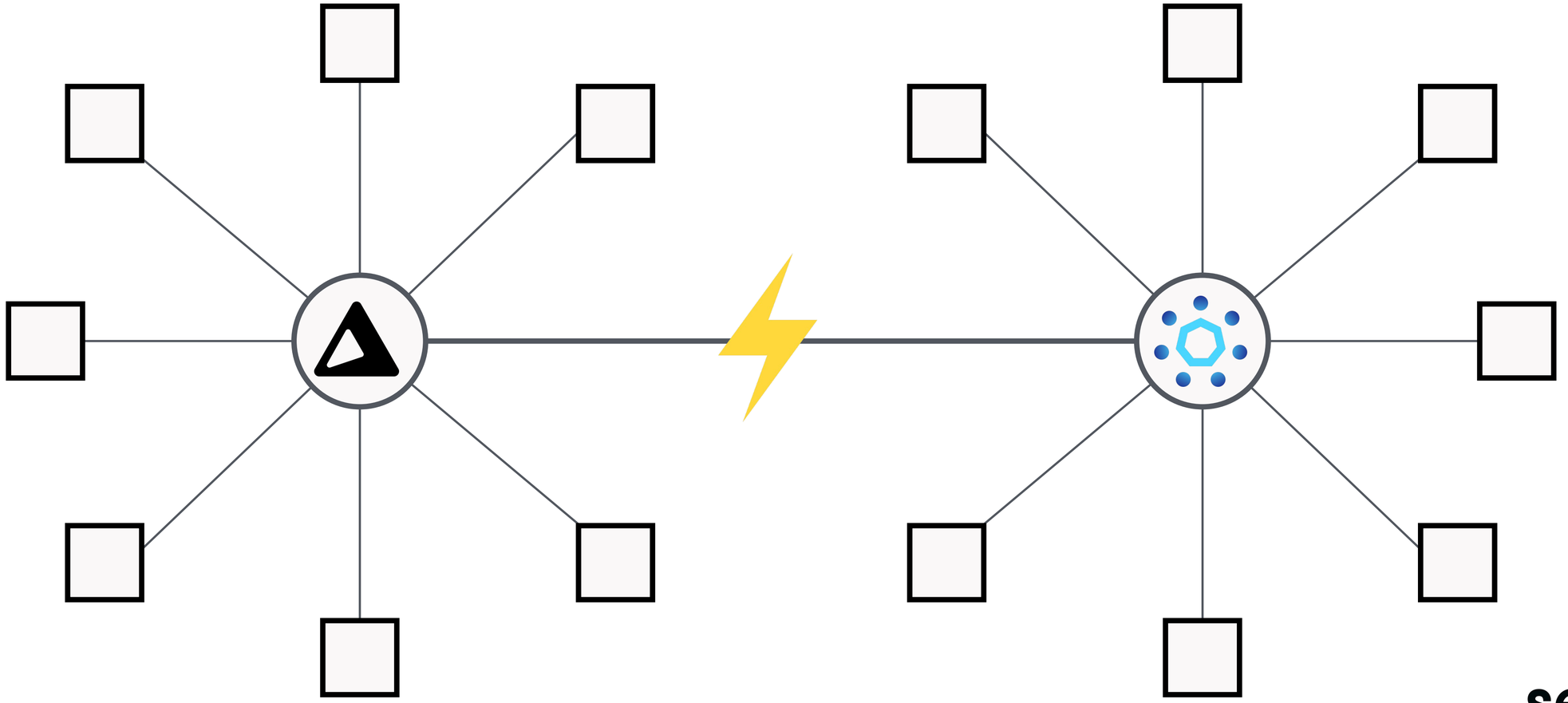
second

hub-and-spoke



second

hub-and-spoke



second

custody

ecash is inherently custodial

mint holds the money

users exchange IOUs

* audits:
  proof-of-reserves
  proof-of-liabilities

second

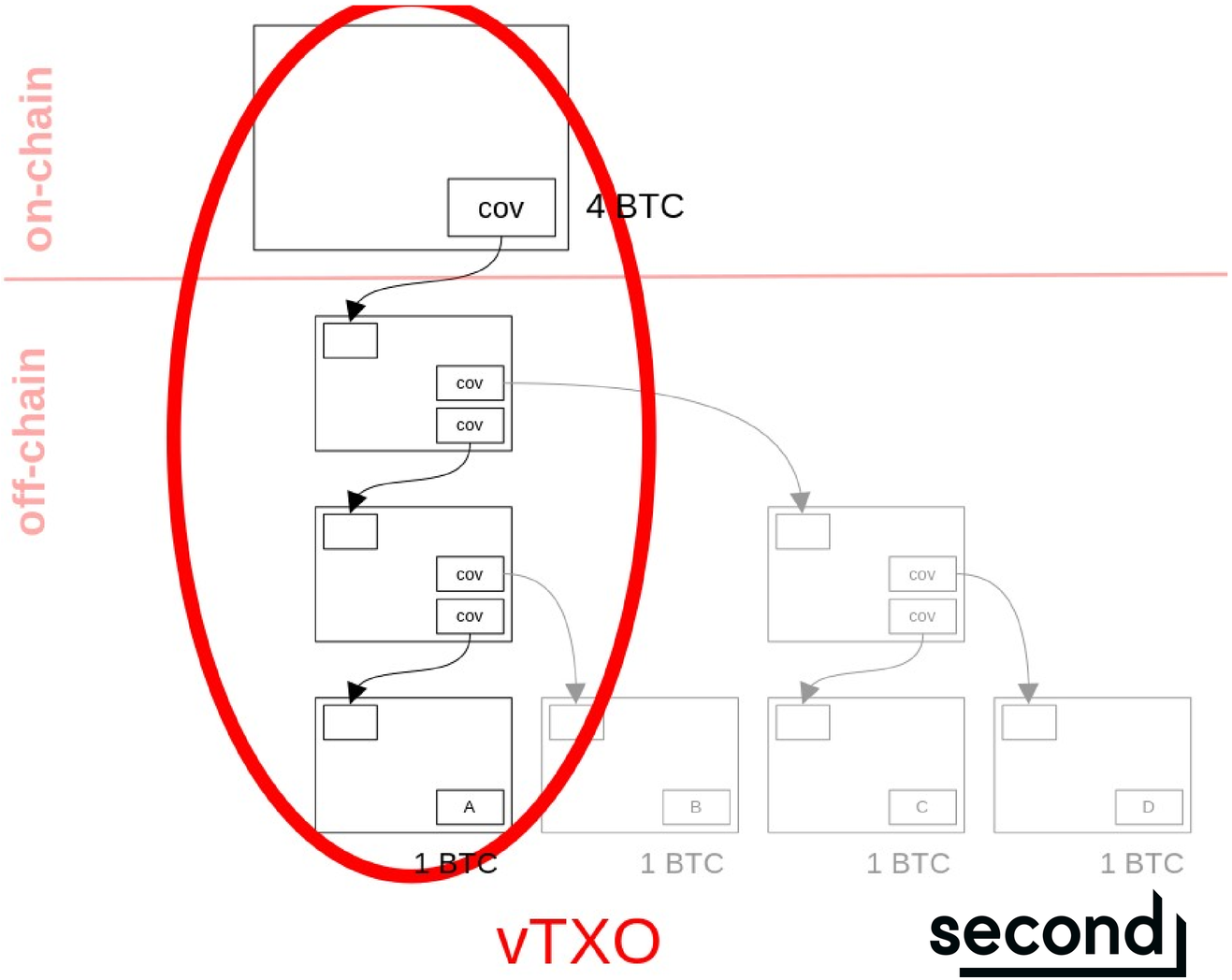
unilateral exit

non-custodial
→ true second layer™

can always go on-chain

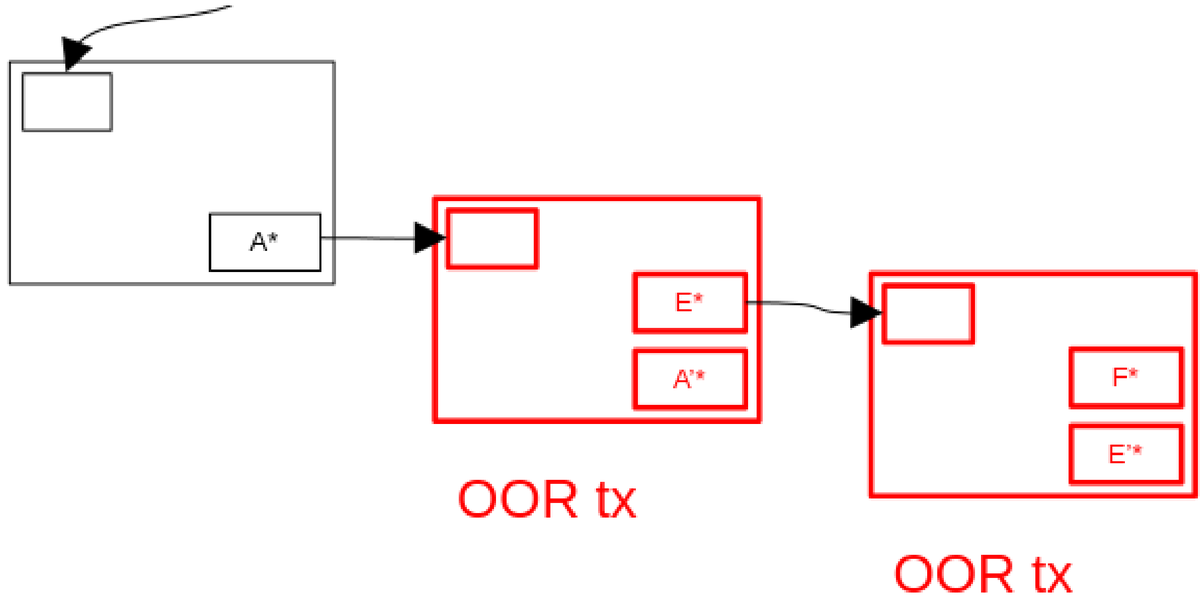
the exit path **is** the VTXO

limitation on small amounts



bitcoin transactions

VTXOs **are** UTXOs (++)

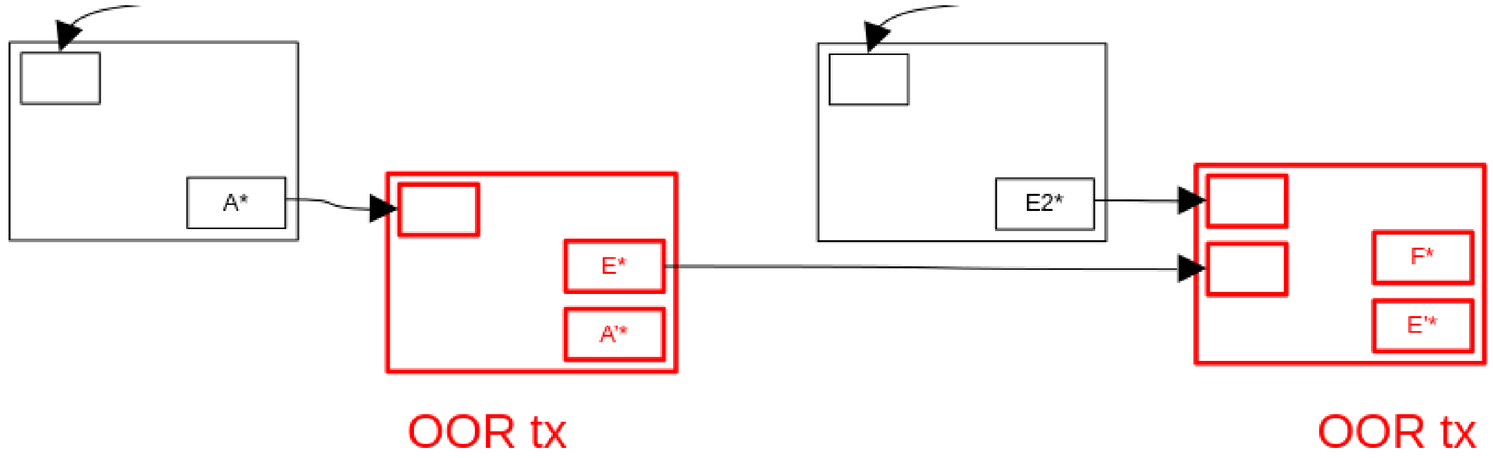


second

bitcoin transactions

VTXOs **are** UTXOs (++)

multiple inputs

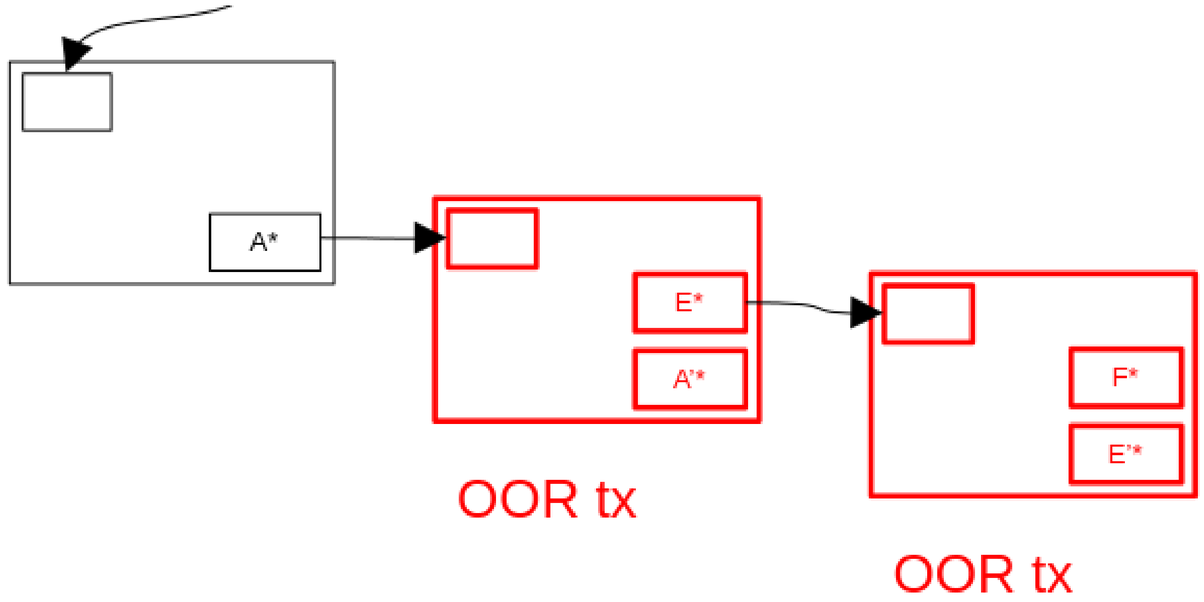


second

bitcoin transactions

VTXOs **are** UTXOs (++)

complex scripts:
- → multi-sig
- → Lightning channels
- → DLCs
- → ???



second

privacy

both private from the public

ecash has perfect
privacy from operator

Ark can come very close

second

blind signatures

the back-bone of ecash

Ark can use blind signatures for rounds
→ similar to WabiSabi

more VTXOs increase exit cost

second

cost

ecash is virtually free
  → both txs and holding

Ark holding has perpetual cost
  → 30-day expiry → periodic refresh
  → rounds: fixed + fractional

arkoor txs virtually free
  → might want to refresh afterwards

significant costs only at exit time

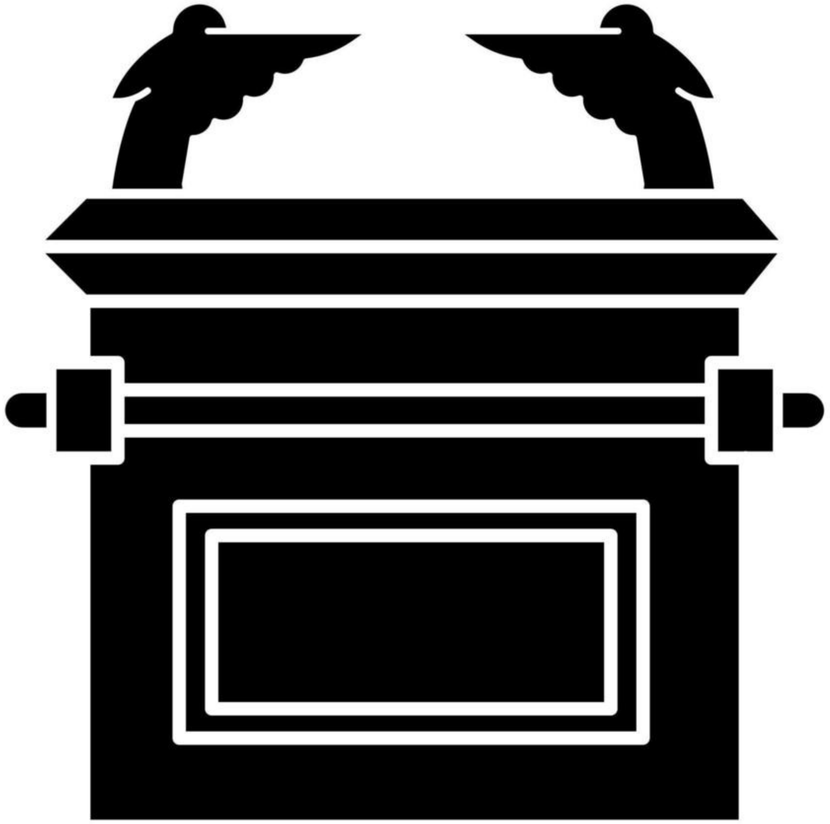
second

covenants

ecash doesn’t need covenants!

clArk: covenant-less Ark

covenants super-charge Ark
→ OP_CTV / OP_TXHASH



second

So can we work together?

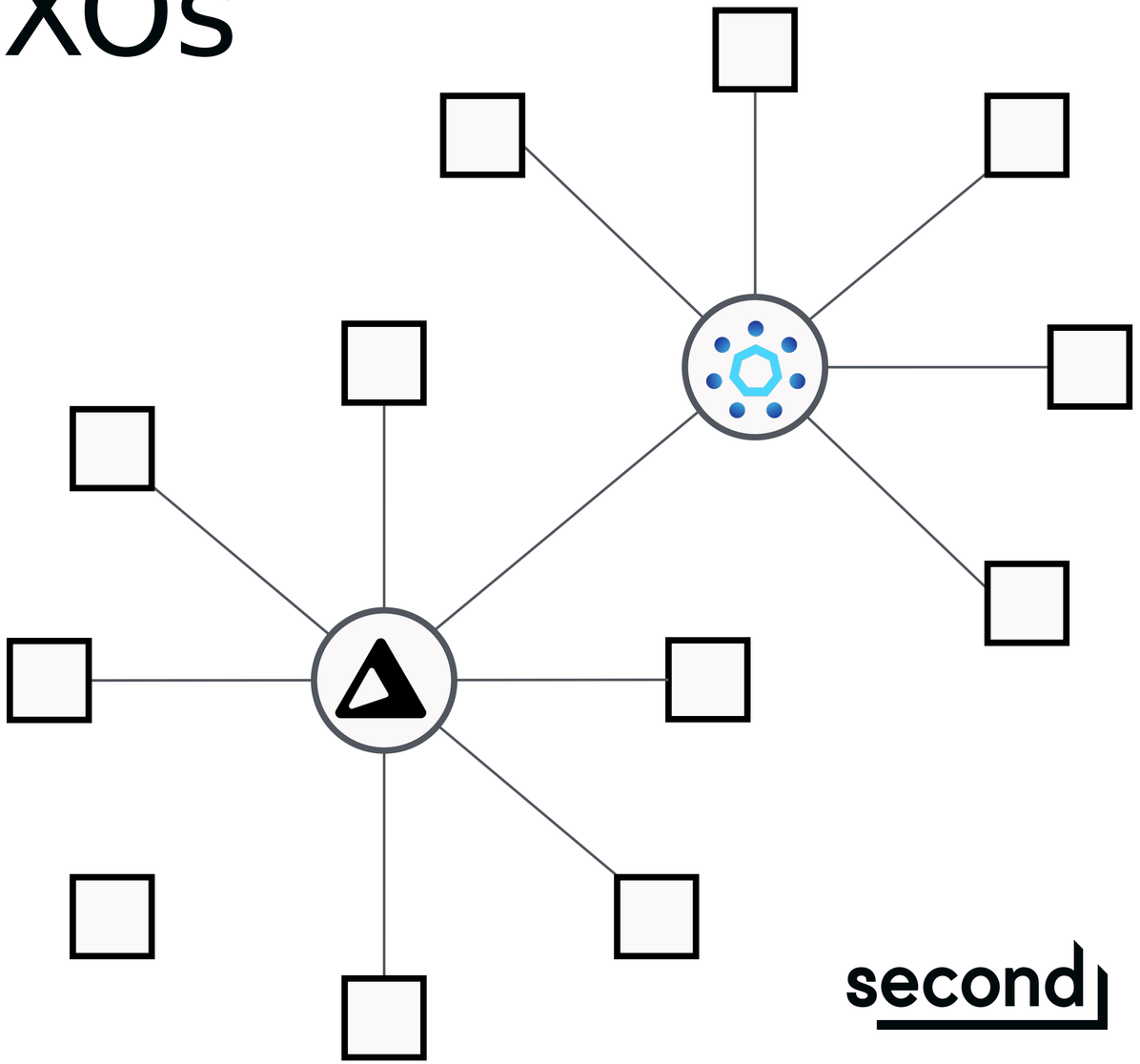
second

mints can own VTXOs

Ark has online requirements
→ mint is always online

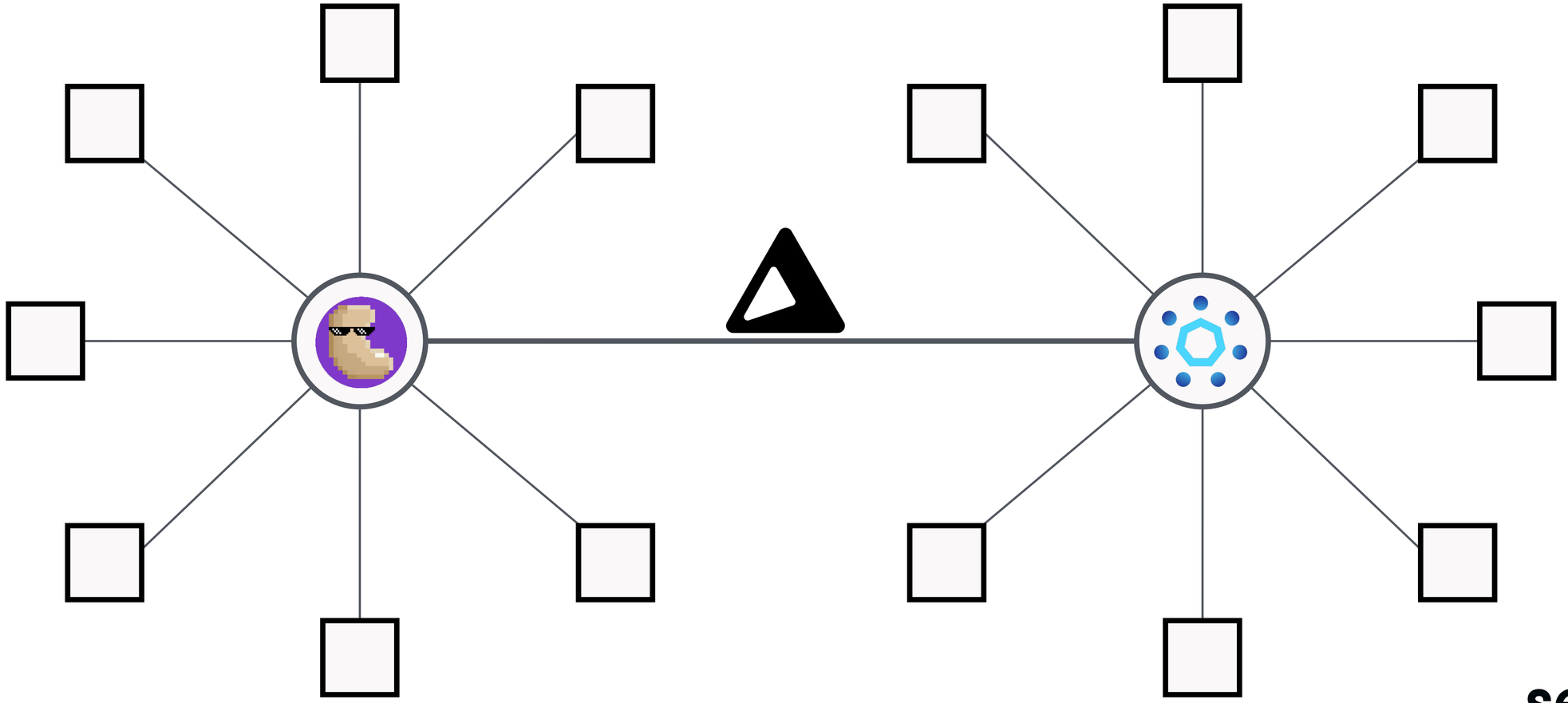
cheaper than on-chain

easier than Lightning



second

inter-mint Ark txs



second

What’s next for Ark?

Second just launched!

bark client in Rust

available for testing
→ codeberg.org/ark-bitcoin/bark

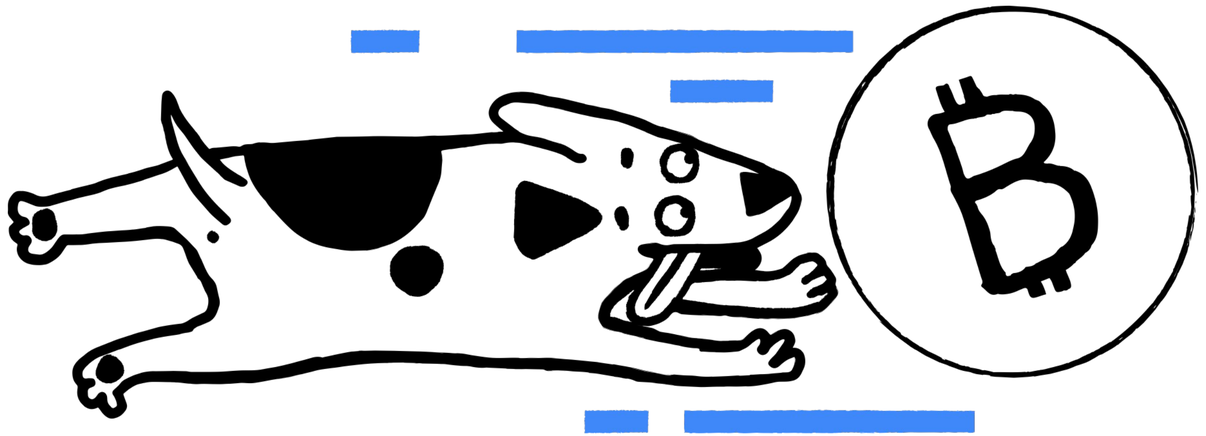
discussion on Telegram

ark-protocol.org

@ark_bitcoin

second

We’re hiring.



Come find me after the talk, or email steven@second.tech

second