Ark

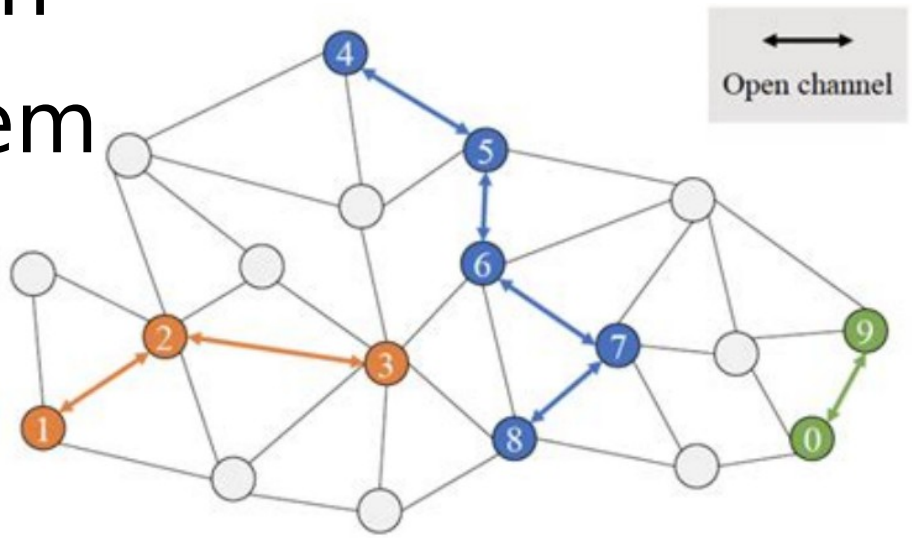
a new Bitcoin layer 2 protocol

Who am I?

- Steven Roose
- Bitcoin dev for over 10 years
- Liquid team @ Blockstream
- rust-bitcoin

Lightning Network

- off-chain payment protocol
- connected graph of two-party channels
- channels made on-chain
- inbound liquidity problem



What is Ark?

- new off-chain protocol for Bitcoin
  - → interoperable with Lightning
- sharing UTXOs with many users: VTXOs
  - → exchanging VTXOs for new VTXOs

on-chain

4 BTC

off-chain

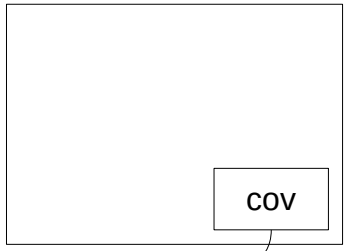

on-chain
cov
4 BTC
off-chain
A
1 BTC
B
1 BTC
C
1 BTC
D
1 BTC

on-chain

4 BTC

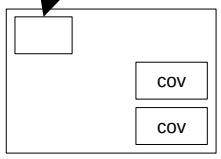
off-chain

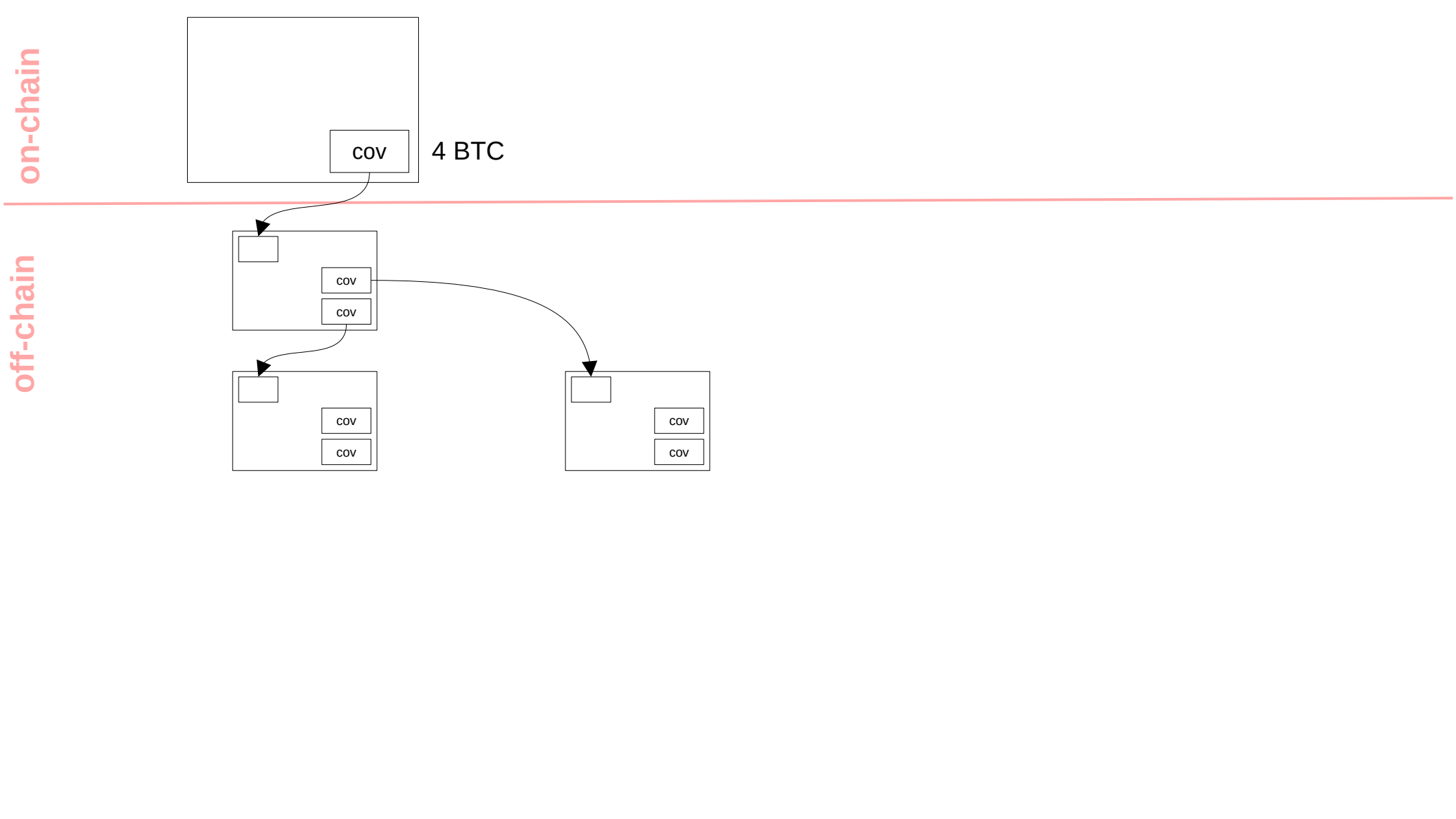
on-chain

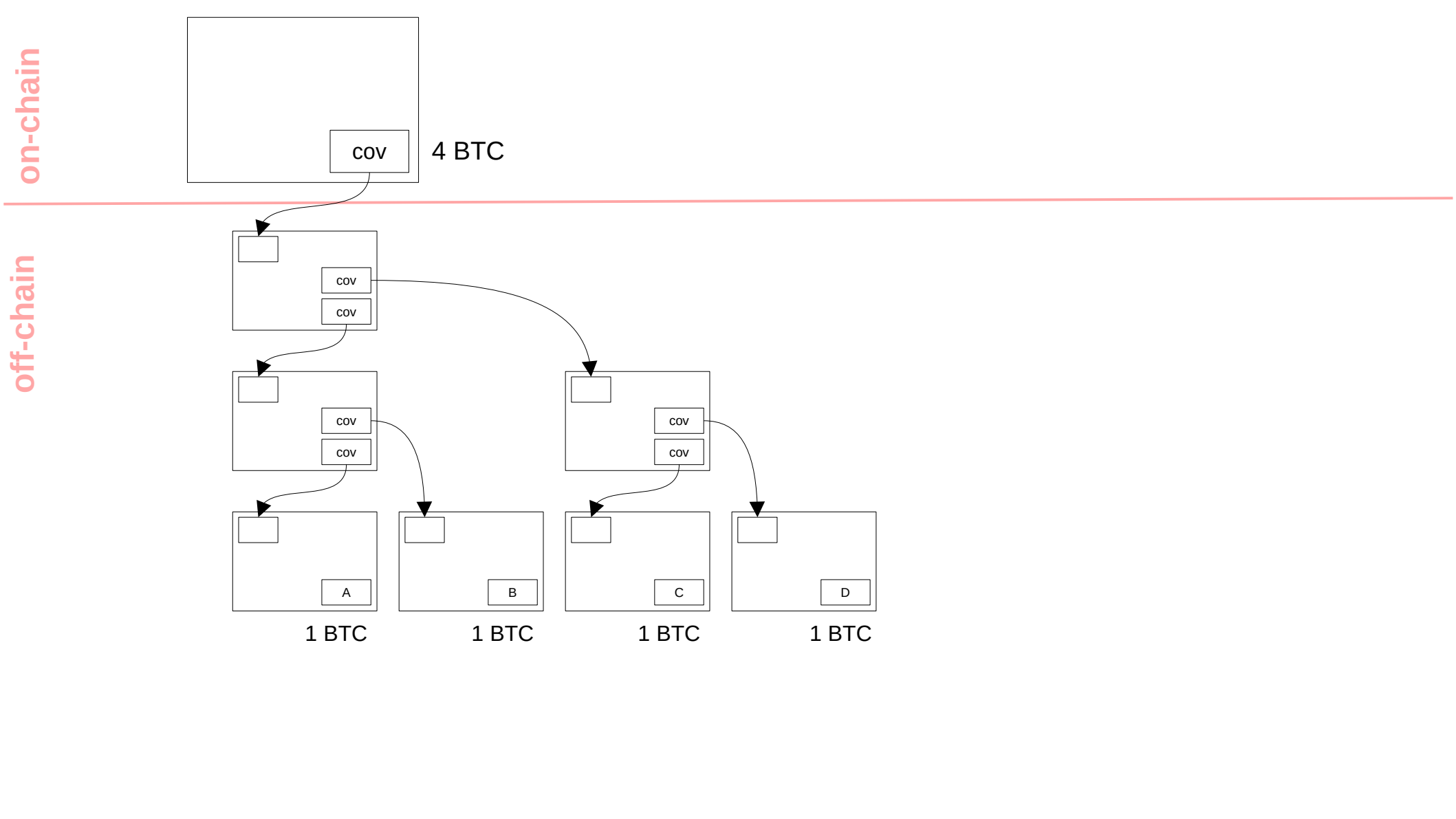


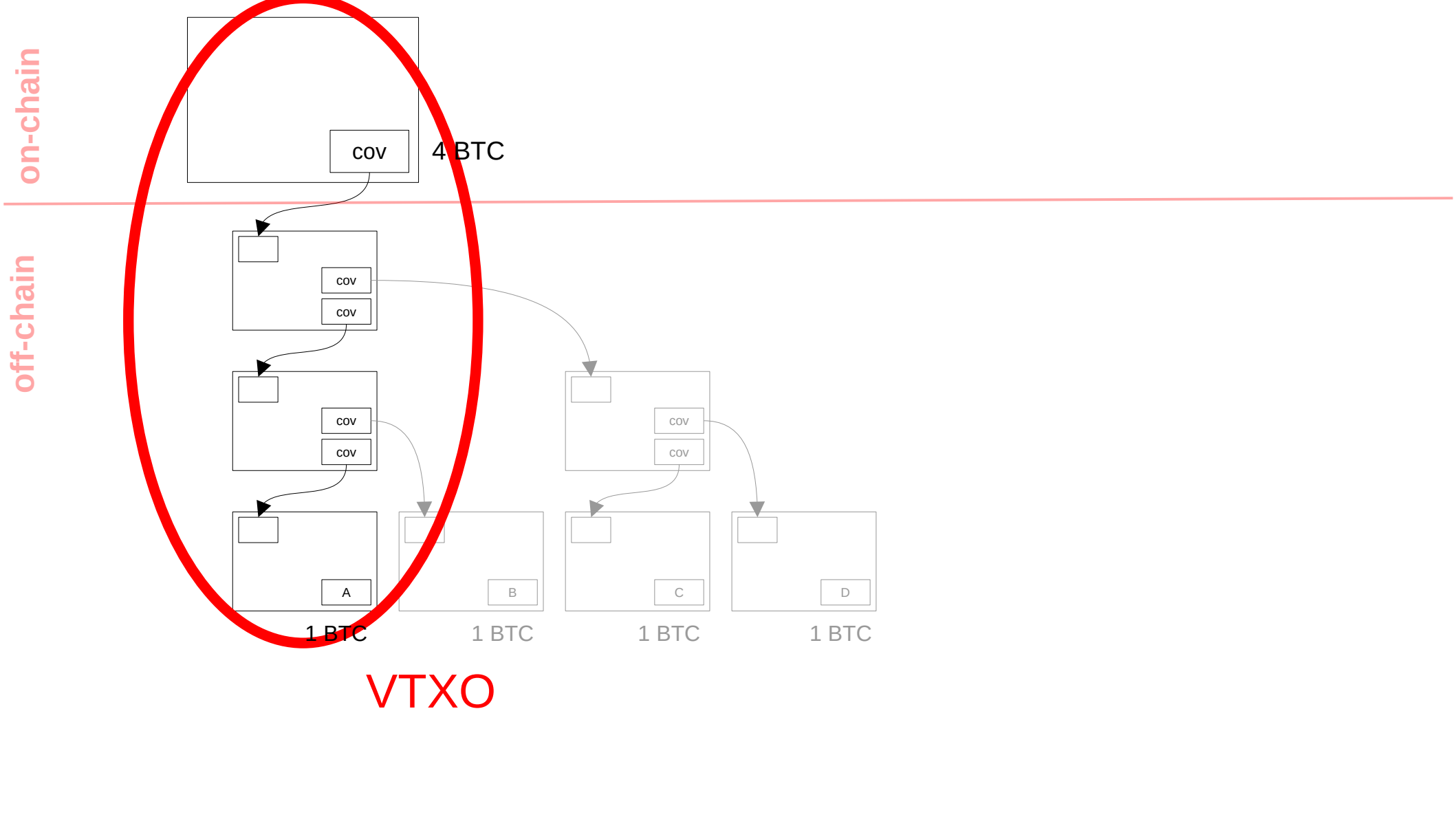
4 BTC

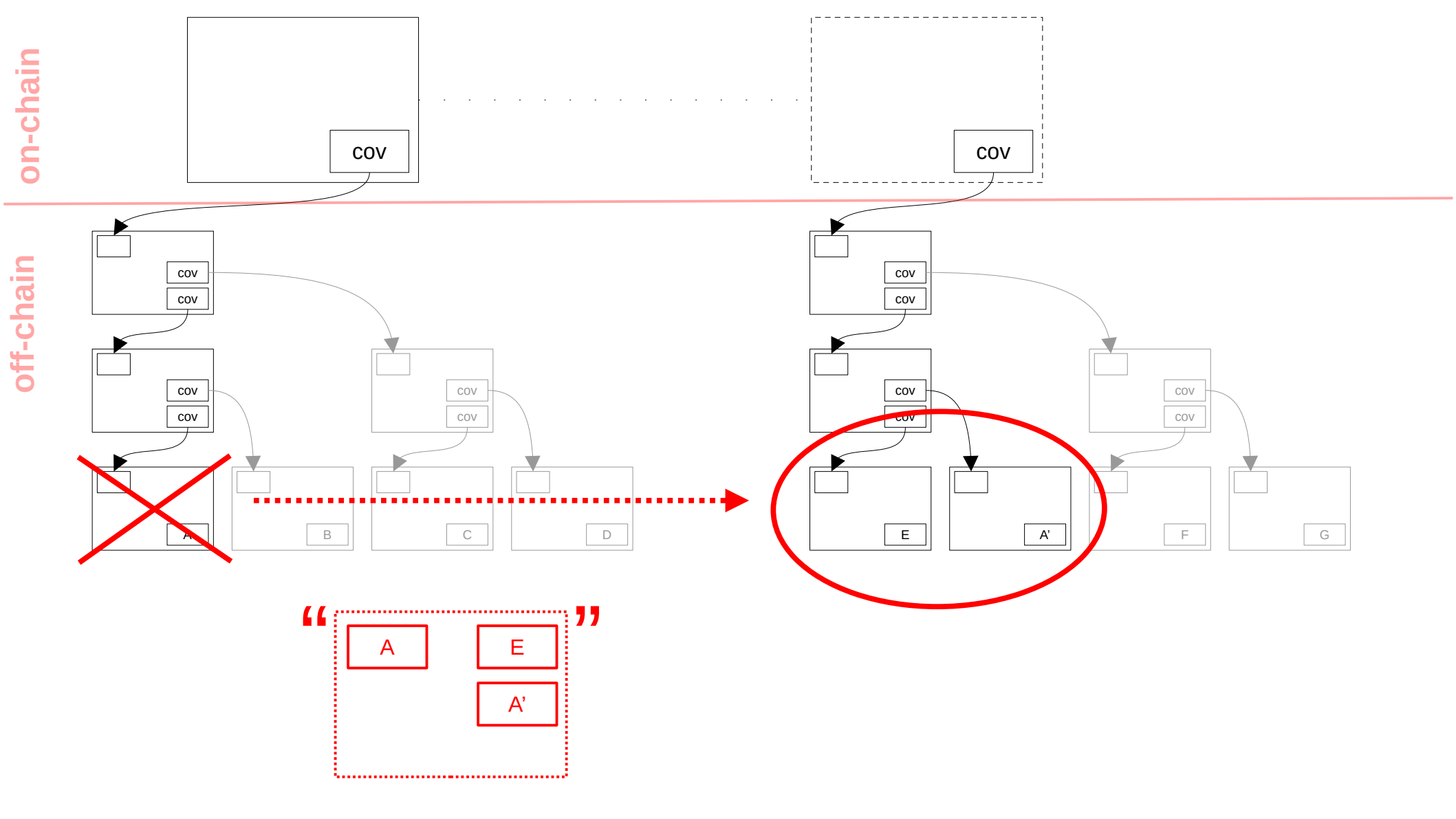
off-chain




on-chain
cov
4 BTC
off-chain
cov
cov
cov
cov
cov
cov


on-chain
cov
4 BTC
off-chain
cov
cov
cov
cov
cov
cov
cov
cov
A
B
C
D
1 BTC
1 BTC
1 BTC
1 BTC


on-chain
off-chain
cov
4 BTC
cov
cov
cov
cov
cov
cov
A
B
C
D
1 BTC
1 BTC
1 BTC
1 BTC
VTXO


on-chain
off-chain
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
A
B
C
D
E
A'
F
G
“
A
E
A’
”

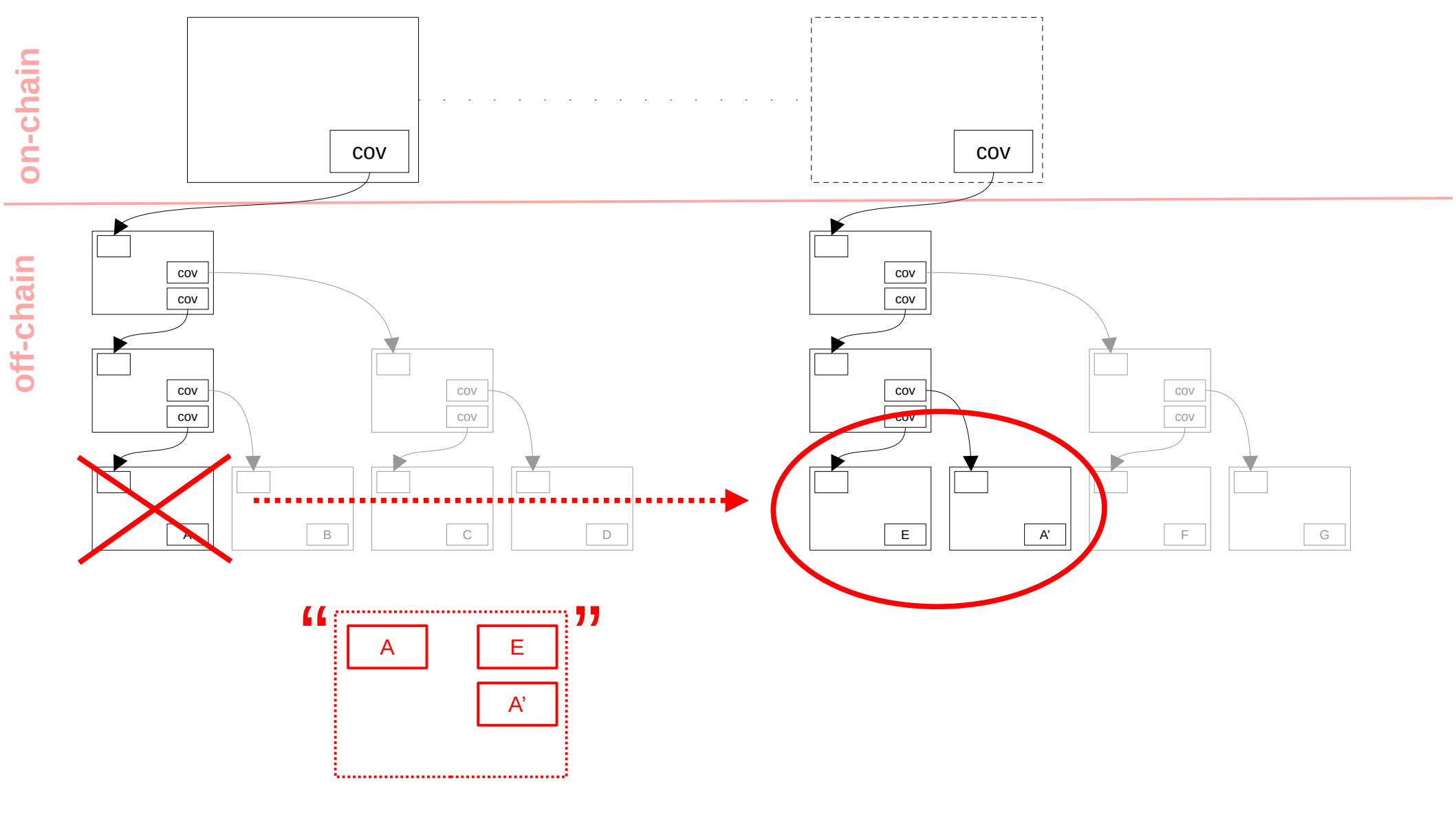
Ark Payments

- efficient UTXO-style off-chain txs
- users 100% in control of money
- anyone can receive
  - no channel or inbound liquidity required!
- Ark rounds by Ark Service Provider
  - scheduled at fixed time intervals
  - liquidity required from ASP
- VTXO expiry

Out-of-Round Payments

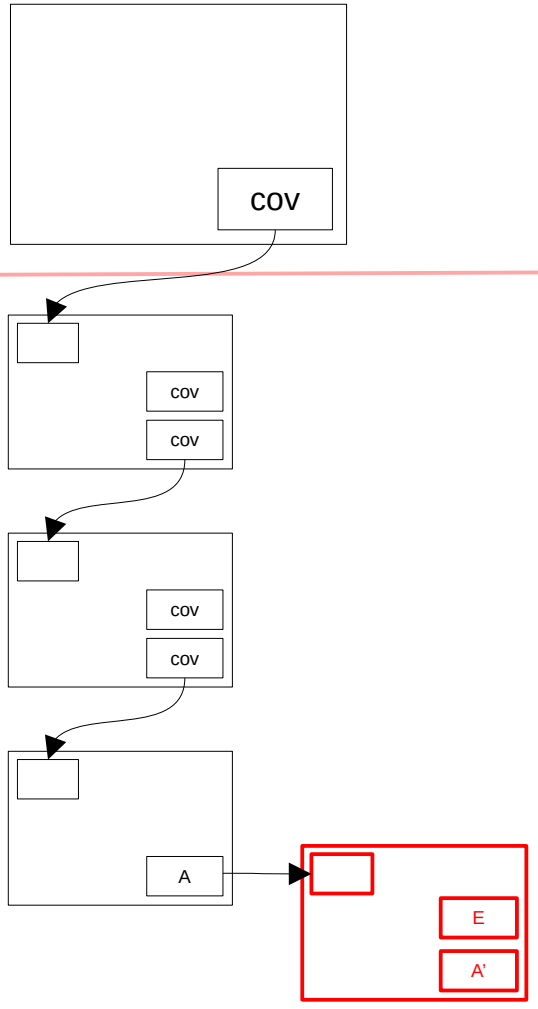
- we can send a VTXO directly
  - → without participating in a round
  - → instant & no liquidity fee
- “Somsen Shortcut”
- Arkoor


on-chain
off-chain
cov
cov
cov
cov
cov
cov
A

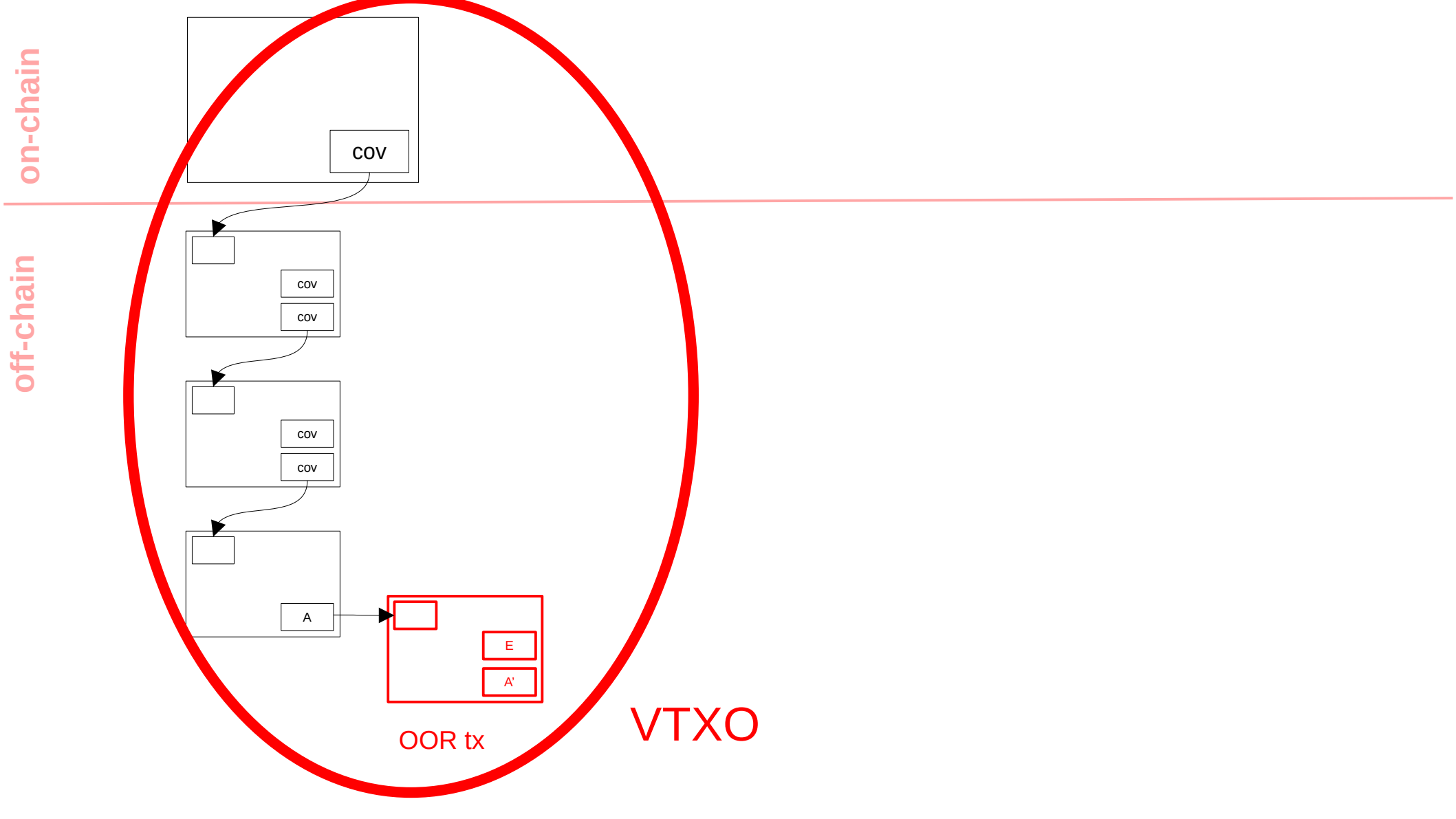

on-chain
off-chain
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
A
B
C
D
E
A'
F
G
“
A
E
A’
”

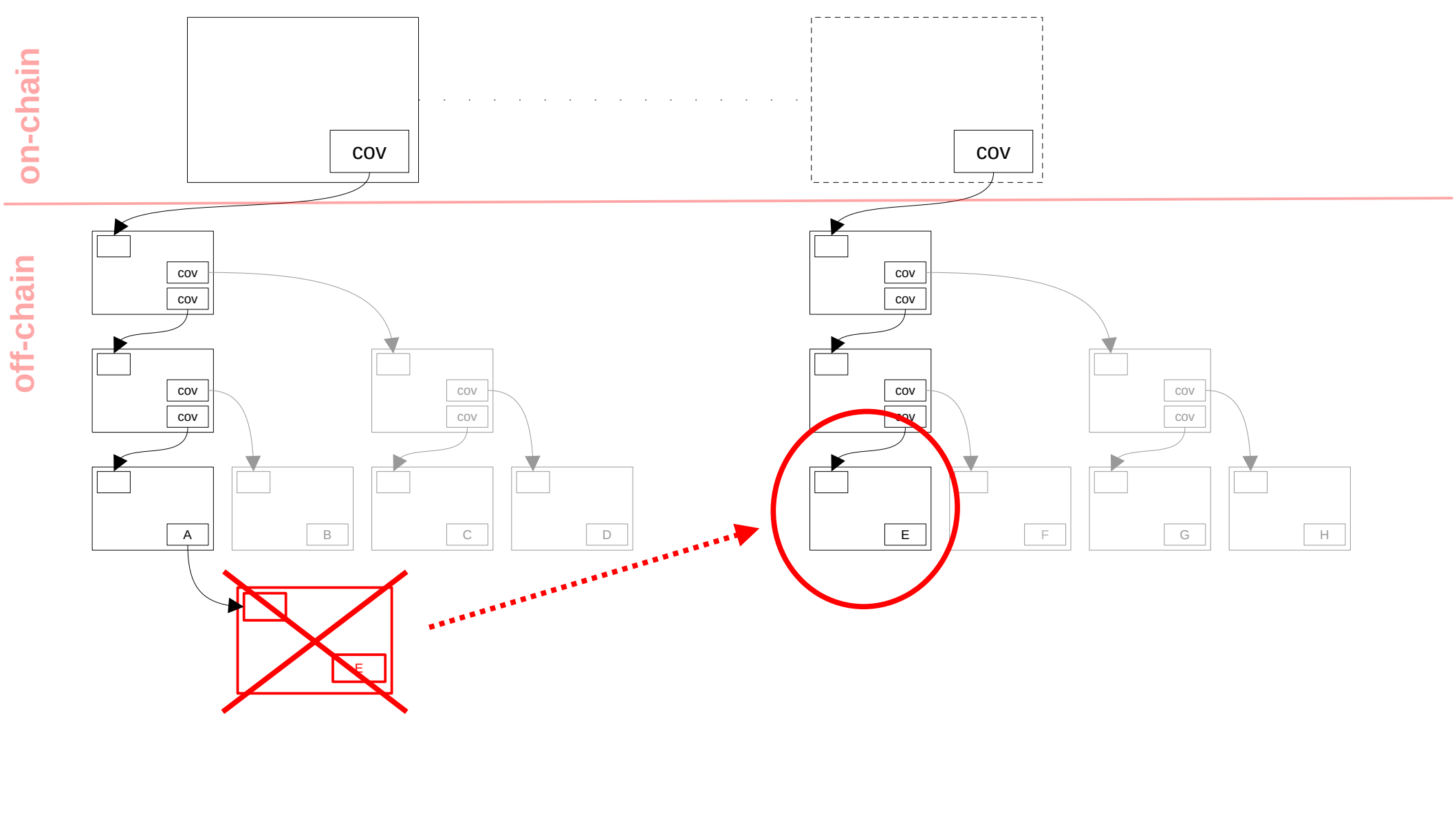
on-chain

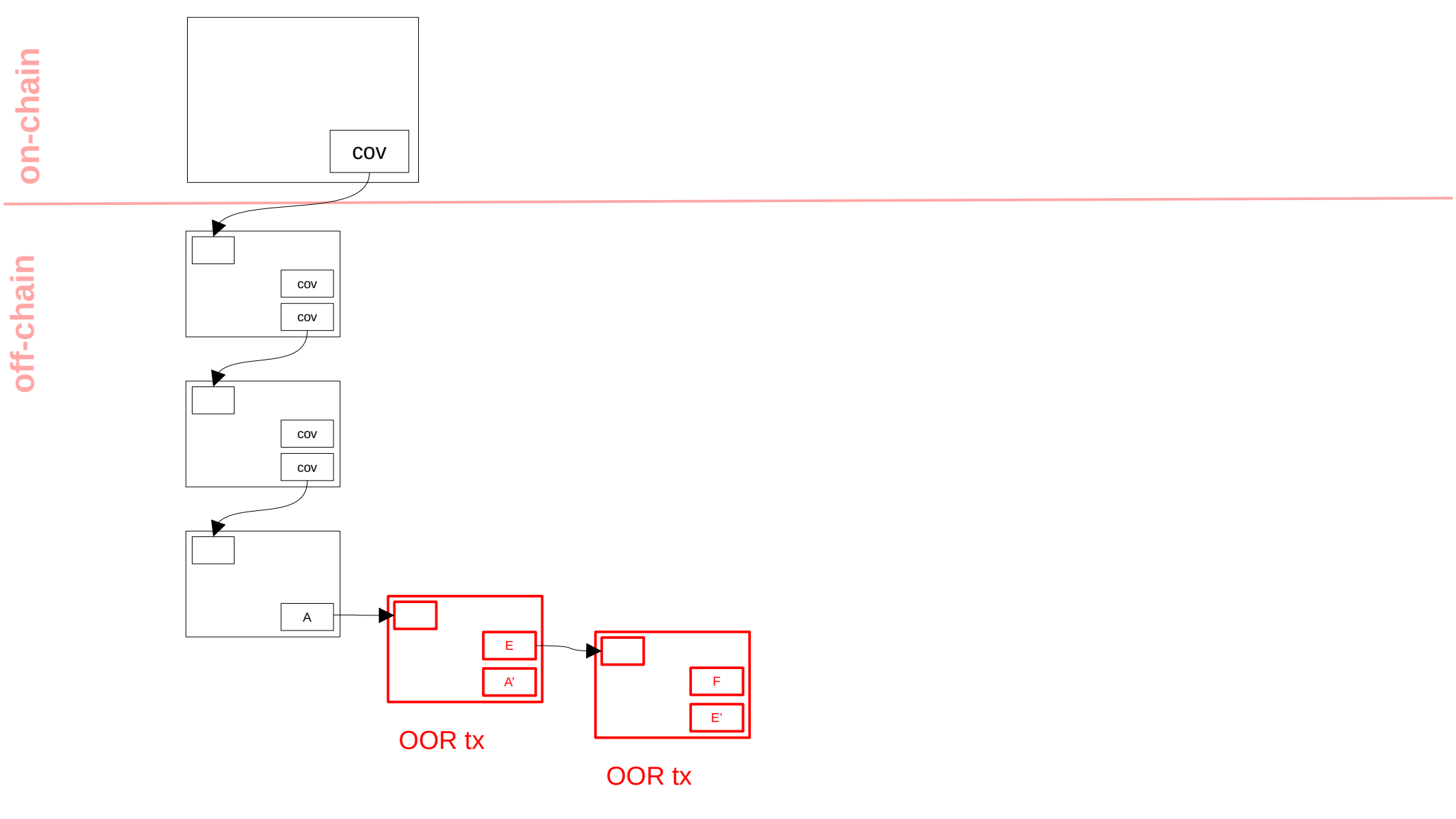
off-chain

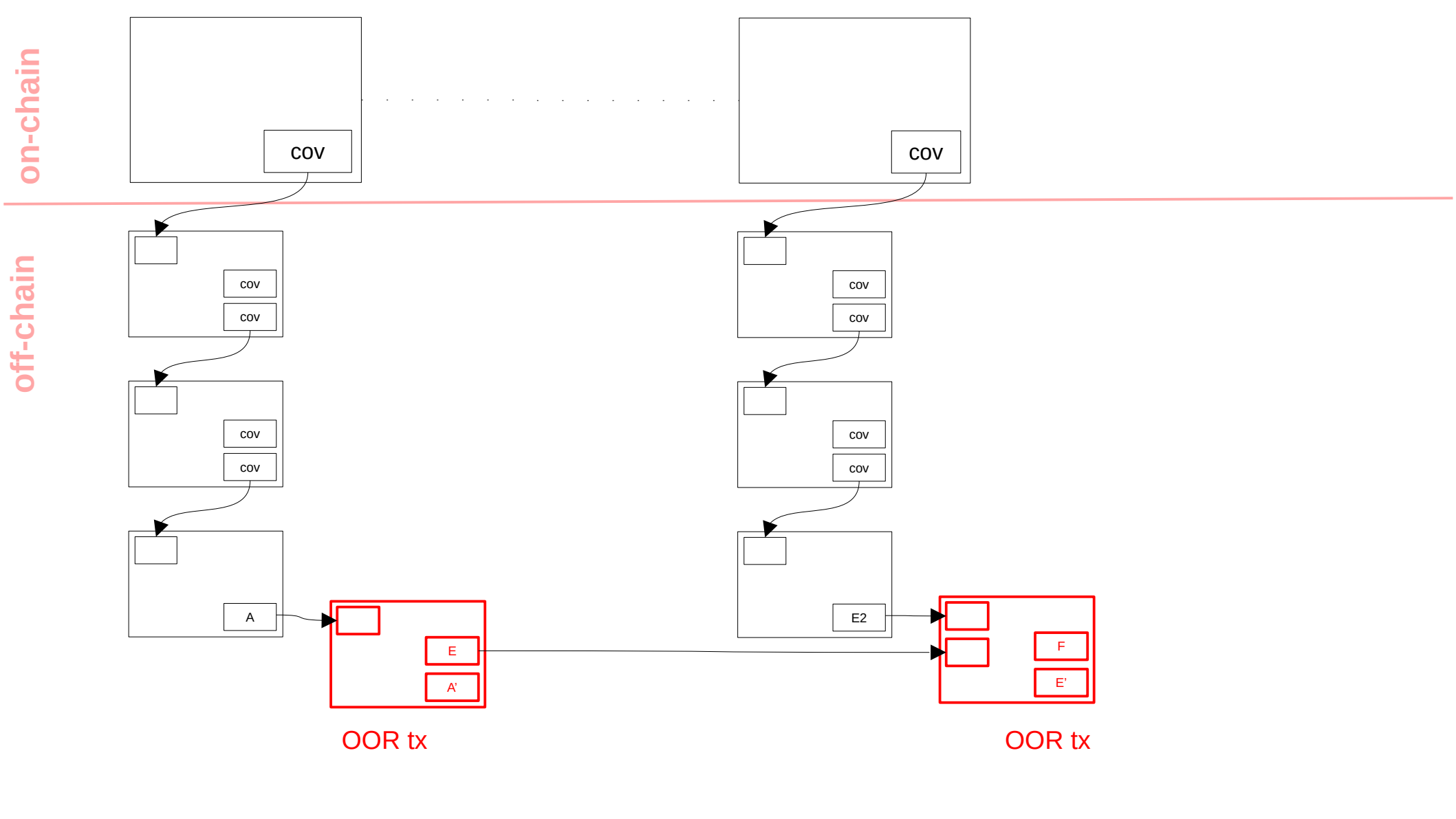


OOR tx


on-chain
off-chain
cov
cov
cov
cov
cov
cov
A
E
A'
OOR tx
VTXO


on-chain
off-chain
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
A
B
C
D
E
F
G
H
E


on-chain
off-chain
cov
cov
cov
cov
cov
cov
A
E
A'
F
E'
OOR tx
OOR tx


on-chain
off-chain
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
cov
A
E
A'
E2
F
E'
OOR tx
OOR tx

Out-of-Round Payments

- instant & no liquidity fee
- temporary state-chain model
  → opt-out

Lightning

- make Lightning payments from Ark
  - → similar to regular Ark (OOR) tx
  - → ASP functions as LSP
- create Lightning channels inside Ark
  - → Ark as “channel factory”
  - → cheap channels with expiry

State of the Ark

- impl of clArk on Bitcoin
  - → covenant-less Ark
  - → MuSig2 cosigning instead of covenants
- impl on Liquid using covenants

Thanks

- https://roose.io/presentations
- https://ark-protocol.org/
- Questions?