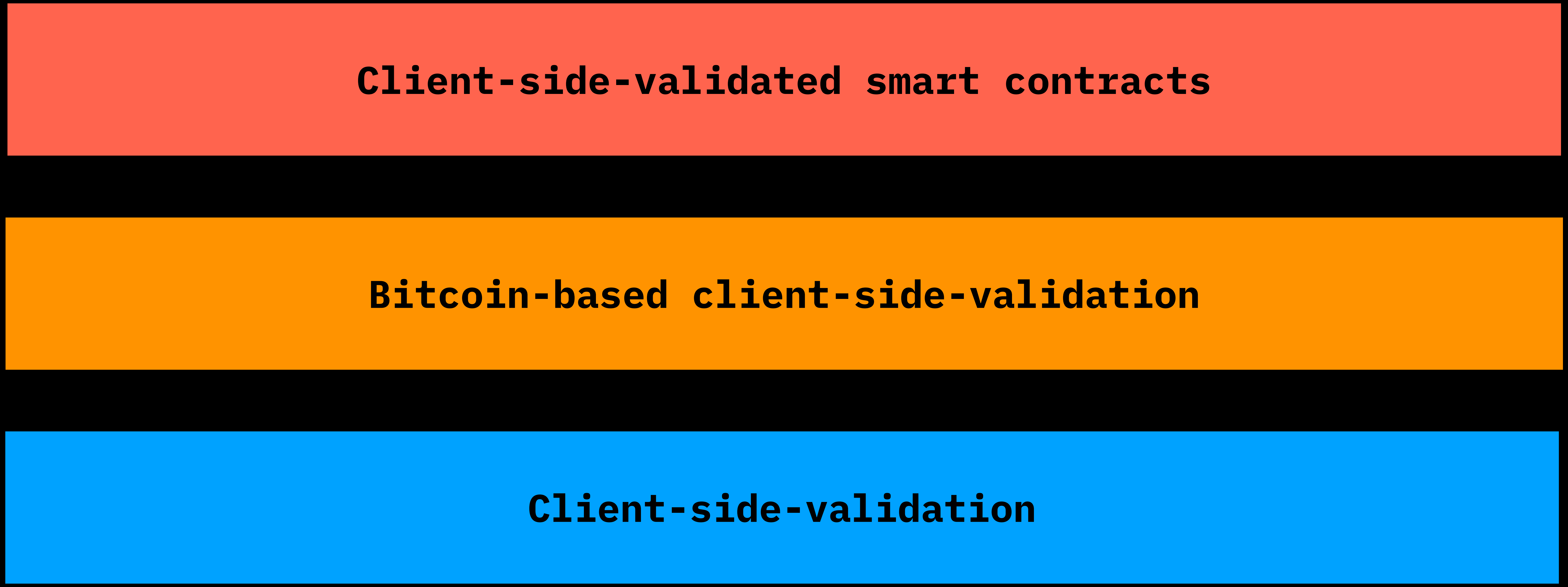
RGB: Private and scalable smart contracts for Bitcoin and Lightning Network – and beyond (DEX, DeFi)

by LNP/BP Standards Association

Client-side-validation

RGB stack

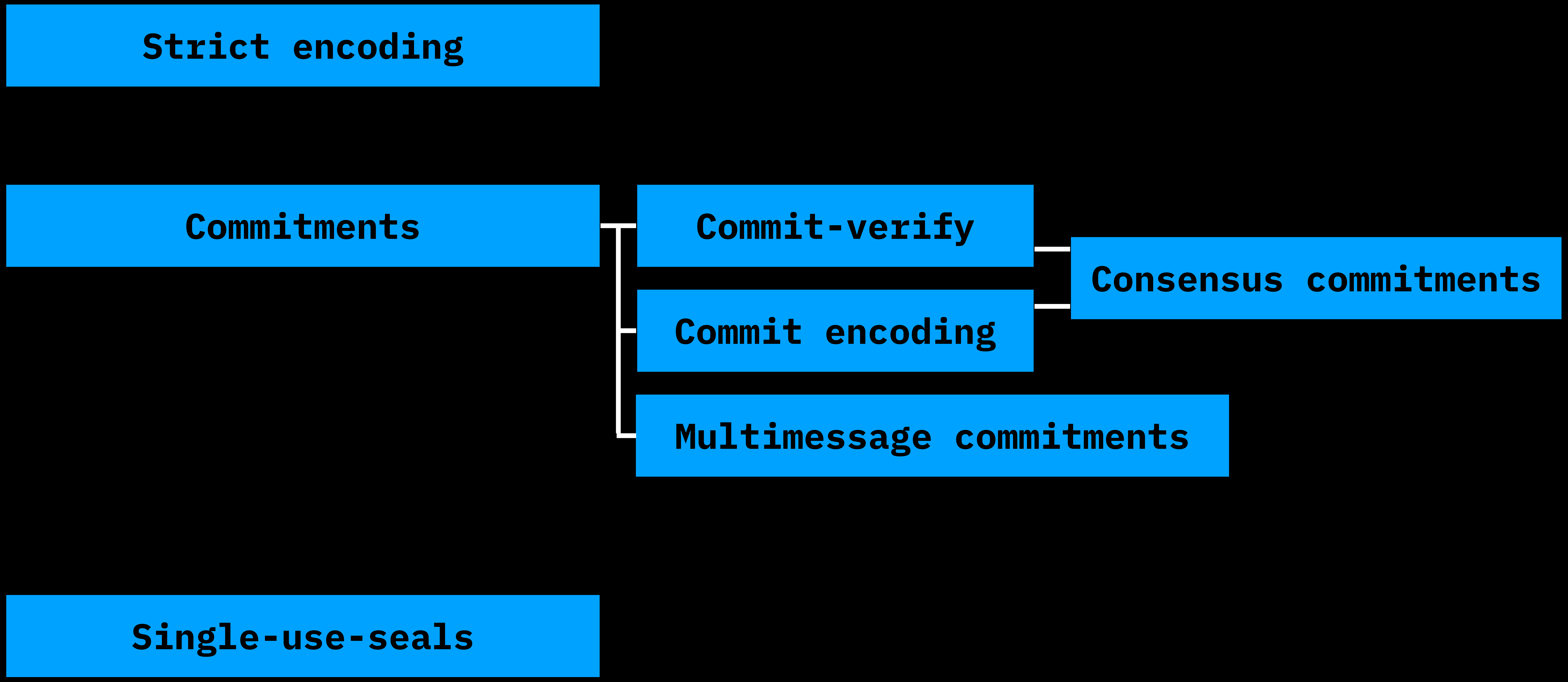


Client-side-validated smart contracts

Bitcoin-based client-side-validation

Client-side-validation

Client-side-validation



Strict encoding

Commitments

Commit-verify

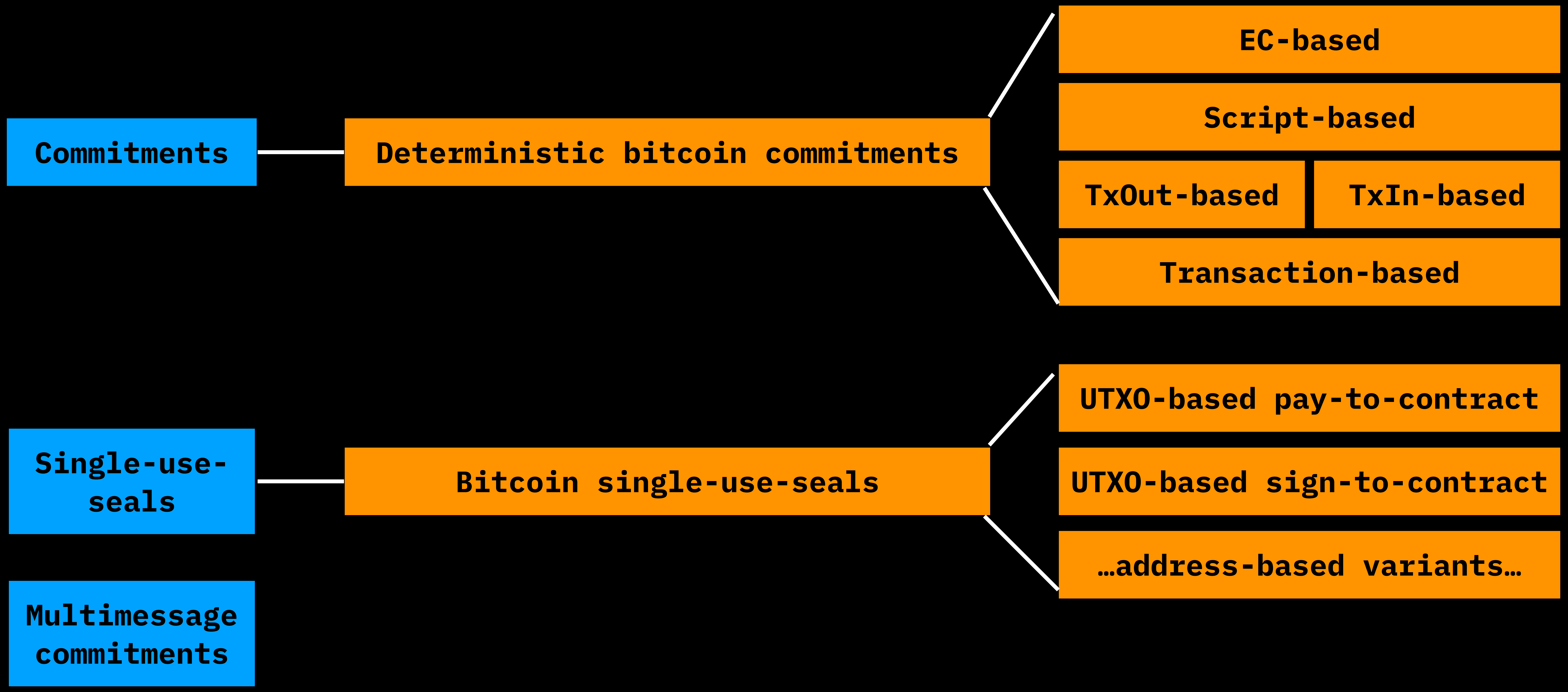
Commit encoding

Multimessage commitments

Consensus commitments

Single-use-seals

Bitcoin client-side-validation



Commitments

Deterministic bitcoin commitments

EC-based

Script-based

TxOut-based

TxIn-based

Transaction-based

Single-use-seals

Bitcoin single-use-seals

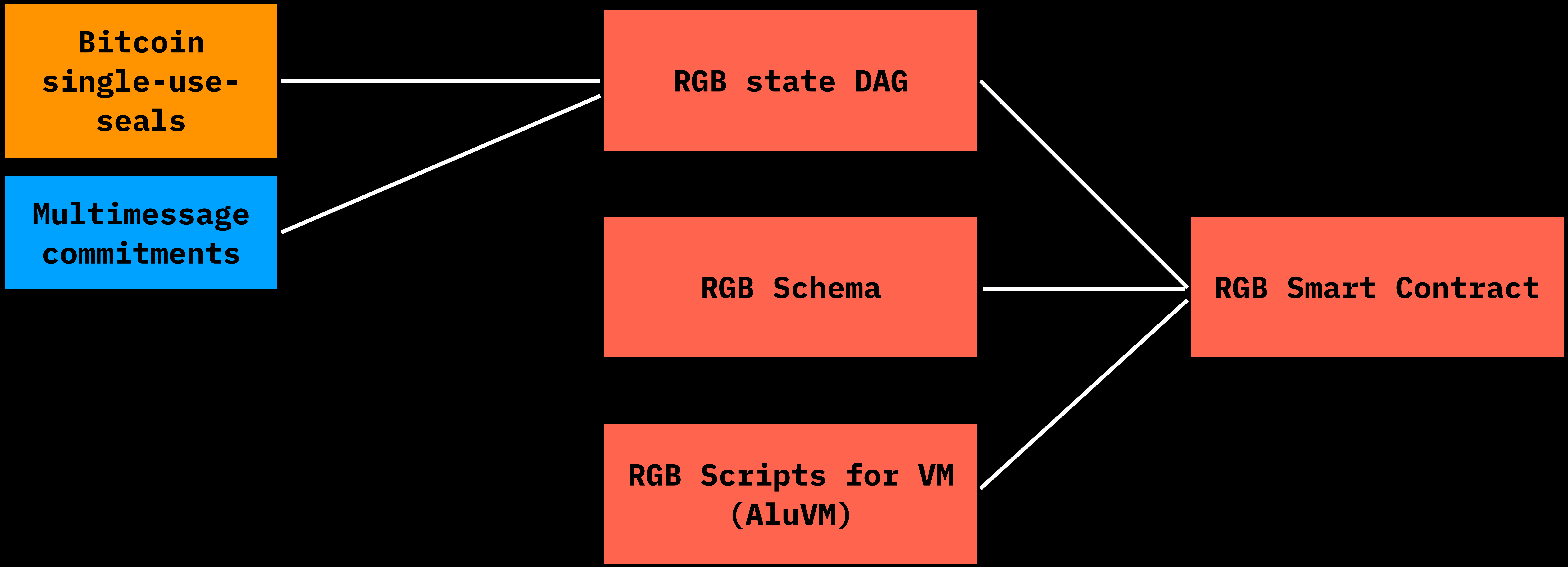
UTXO-based pay-to-contract

UTXO-based sign-to-contract

…address-based variants…

Multimessage commitments

RGB: client-side-validated smart contracts



Bitcoin single-use-seals

Multimessage commitments

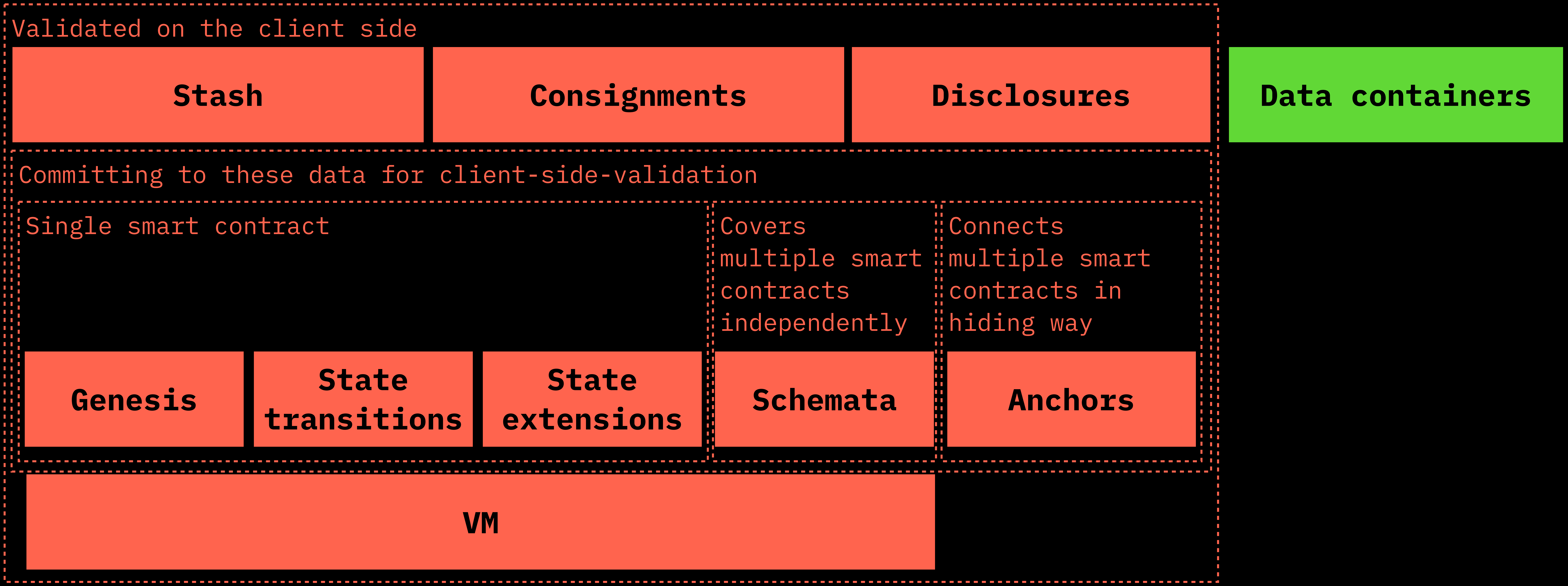
RGB state DAG

RGB Schema

RGB Scripts for VM (AluVM)

RGB Smart Contract

RGB data & client-side-validation



Validated on the client side

Stash

Consignments

Disclosures

Data containers

Committing to these data for client-side-validation

Single smart contract

Genesis

State transitions

State extensions

Covers multiple smart contracts independently

Schemata

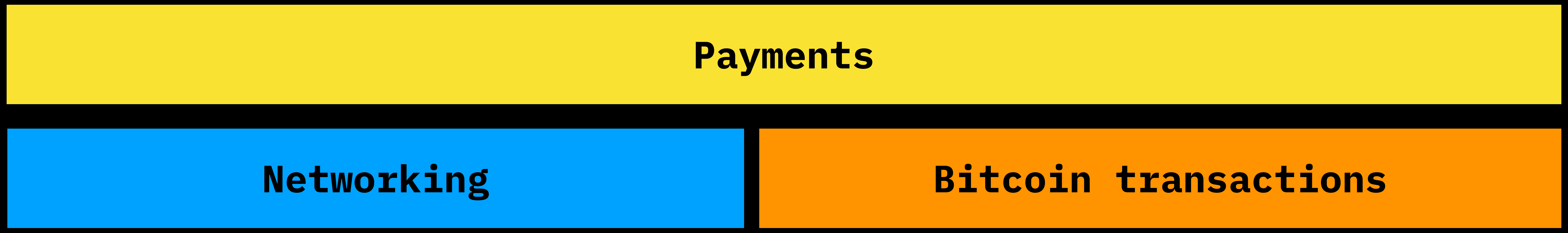
Connects multiple smart contracts in hiding way

Anchors

VM

Lightning network in RGB & general LNP/BP context

Lightning: dissection 2021



Payments

Networking

Bitcoin transactions

Lightning: future 2024

Payments

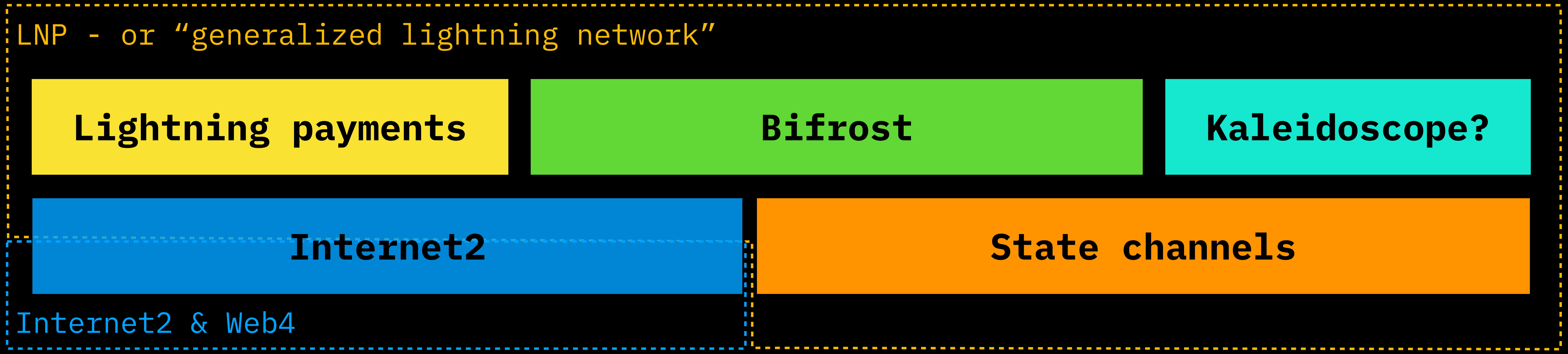
Data storage & querying

DEX & DeFi

Networking

Bitcoin transactions

Lightning: vision by LNP/BP Association



LNP - or “generalized lightning network”

Lightning payments

Bifrost

Kaleidoscope?

Internet2

State channels

Internet2 & Web4

Color coding:

Networking

Bitcoin transactions

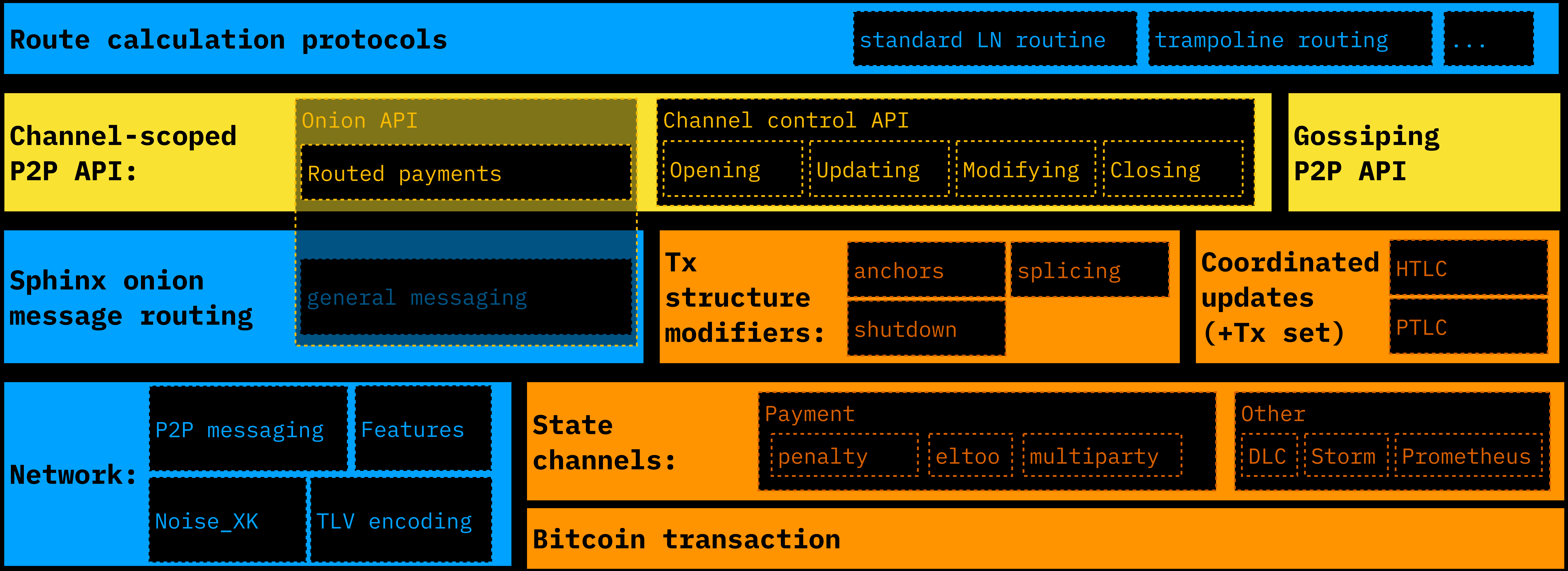
Payments

Advanced:

Data

Dex & DeFi

Lightning: dissection 2021



Route calculation protocols

standard LN routine

trampoline routing

...

Channel-scoped P2P API:

Onion API

Routed payments

Channel control API

Opening

Updating

Modifying

Closing

Gossiping P2P API

Sphinx onion message routing

general messaging

Tx structure modifiers:

anchors

splicing

shutdown

Coordinated updates (+Tx set)

HTLC

PTLC

Network:

P2P messaging

Features

Noise_XK

TLV encoding

State channels:

Payment

penalty

eltoo

multiparty

Other

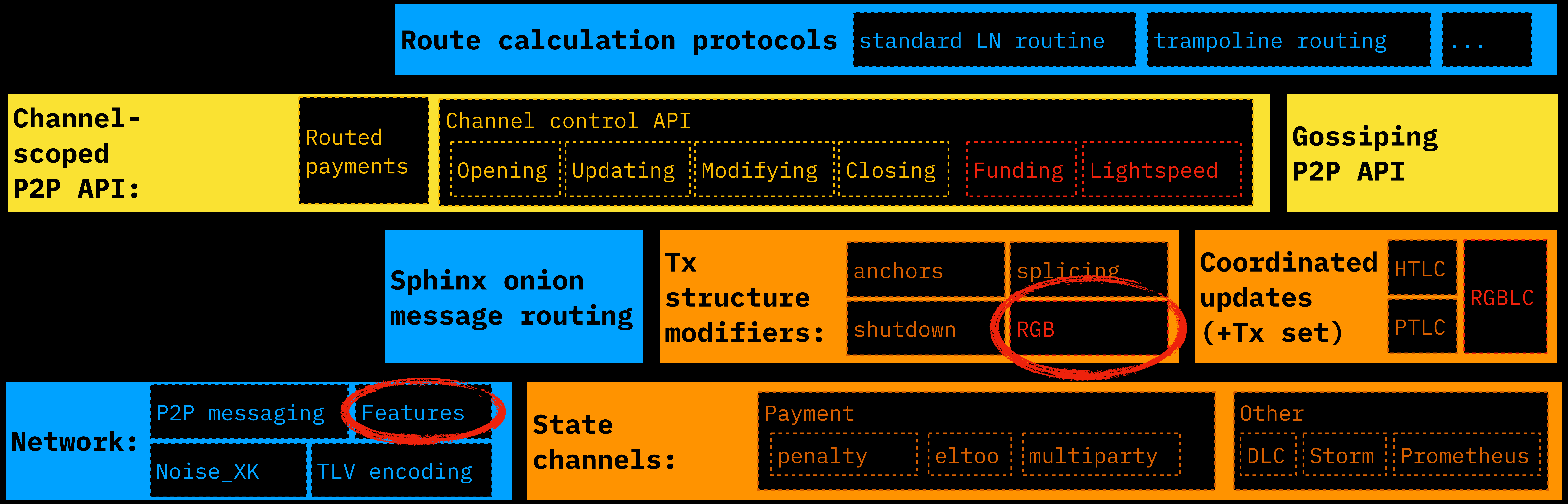
DLC

Storm

Prometheus

Bitcoin transaction

Lightning: plastic surgery with RGB



Route calculation protocols

standard LN routine

trampoline routing

...

Channel-scoped P2P API:

Routed payments

Channel control API

Opening

Updating

Modifying

Closing

Funding

Lightspeed

Gossiping P2P API

Sphinx onion message routing

Tx structure modifiers:

anchors

splicing

shutdown

RGB

Coordinated updates (+Tx set)

HTLC

PTLC

RGBLC

Network:

P2P messaging

Features

Noise_XK

TLV encoding

State channels:

Payment

penalty

eltoo

multiparty

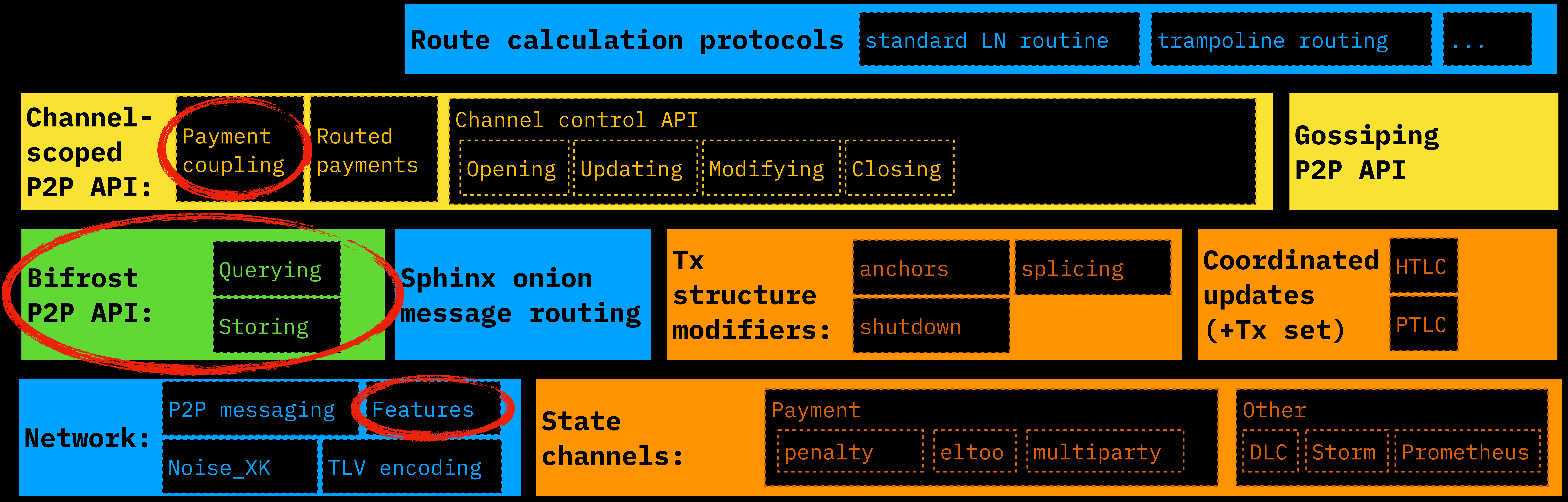
Other

DLC

Storm

Prometheus

Lightning Bifrost



Route calculation protocols: standard LN routine | trampoline routing | ...

Channel-scoped P2P API: Payment coupling | Routed payments | Channel control API: Opening | Updating | Modifying | Closing

Gossiping P2P API

Bifrost P2P API: Querying | Storing

Sphinx onion message routing

Tx structure modifiers: anchors | splicing | shutdown

Coordinated updates (+Tx set): HTLC | PTLC

Network: P2P messaging | Features | Noise_XK | TLV encoding

State channels: Payment: penalty | eltoo | multiparty; Other: DLC | Storm | Prometheus

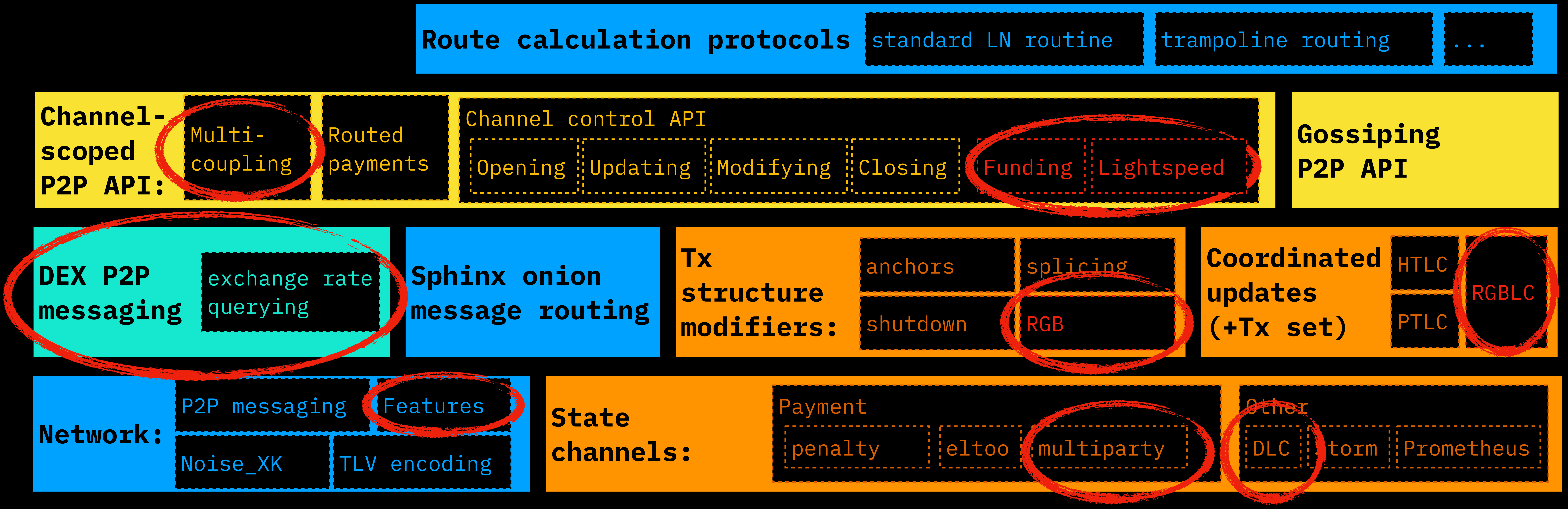
Bifröst: what will it do

- Passing RGB consignments during payments to the receiver
- Publishing & distributing data on **RGB assets**
  (fungible, NFTs, identities)
- **Decentralized name resolution system** (RGB-24-based)
  “DNS for Internet2”
- Storing RGB consignments for third-parties (encrypted and paid)
- LN & RGB watchtower
- Backing up RGB client-side-validated data (encrypted & distributed)
- Generic data storage network
  (will encompass Storm channels in the future)

Lightning message-payment atomic coupling

- Binds API query to payment for the service
  - Bifrost storage for consignments
  - DEX functionality
- Uses Lightspeed and RGB

Lightning: plastic surgery with RGB & DEX



Route calculation protocols
standard LN routine
trampoline routing
...

Channel-scoped P2P API:
Multi-coupling
Routed payments
Channel control API
Opening
Updating
Modifying
Closing
Funding
Lightspeed

Gossiping P2P API

DEX P2P messaging
exchange rate querying

Sphinx onion message routing

Tx structure modifiers:
anchors
splicing
shutdown
RGB

Coordinated updates (+Tx set)
HTLC
PTLC
RGBLC

Network:
P2P messaging
Features
Noise_XK
TLV encoding

State channels:
Payment
penalty
eltoo
multiparty
Other
DLC
storm
Prometheus

Lightning multiple payments atomic coupling

- Couples two LN payments in together in atomic way
- Early concepts (jointly with Christian Decker)
- Required for DEX and reverse American call option problem

Roadmap

Next steps: RGB

- **Finalization of RGB layers**
  (API freeze + docs + test coverage + standards writeup + audit)
  - Client-side-validation
  - Bitcoin Taproot
  - Bitcoin single-use-seals & deterministic commitments
  - RGB Core library
  - RGB Standard library
  - RGB Virtual machine (AluVM)
  - RGB20, 21, 22, 23, 24 schemata
  - Work on integration libraries and products
    (Bitcoin Pro, RGBex, Citadel Runtime, MyCitadel Wallet/Node)

Next steps: LN & Bifrost

- **Lightning network**
  - Update for miniscript & Taproot
  - LNP Core Lib and LNP Node completion for 100% LN compatibility
  - Finalization of core RGB LN messaging & features
  - RGB integration in Citadel Runtime
- **Bifrost**
  - Sending RGB payment consignments
  - Publishing information about assets
  - Third-party consignment storage
  - Watchtower functionality
  - Generic data storage/backup API

Next steps: DEX

- **LN extensions**
  - Generalized channel structure negotiating API
  - Multiparty channels, splicings etc
  - Lightspeed payments & payment couplings
- **DEX**
  - DEX P2P API for LN
  - Update atomic coupling (American call option problem solution)
  - Liquidity pools
  - Algorithmical stablecoins
  - DLCs and derivatives: options, futures, ...

RGB future

- Contractum language
- Sign-to-contract single-use-seals
- Bulletproof aggregation & mimblewimble cut-thoughts
- Dedicated commitment layer 0