Challenges with digital assets today

- **Low scalability**
  - limited by blockchains, which are inherently inscalable
  - no layer 2 assets
- **Poor privacy**
  - Everyone in the world sees the transactions
  - Zero-knowledge is nearly absent for the assets even if it is present in blockchain (Monero, Grin, Beam, …)

Challenges with digital assets today

- **Inefficient smart contracts**
  - Asset ownership is mixed with contract business logic
  - Pseudo-decentralized (governance problem)
  - Not formally verified languages (security problem)

RGB was created to solve these issues

- Originally proposed by **Giacomo Zucco** & **Peter Todd** in 2016
- Supported by **Tether Inc/Bitfinex** & other sponsors in early 2019
- **Pandora Core** is the main subcontractor for technology development
- Governed by non-profit **LNP/BP Standards Association**, Switzerland

What is RGB?

Client-validated state and smart contract system working at Layer 2/3 in Bitcoin and Lightning Network.

- Works with **Lightning Network**
- No on-chain usage nor trackable footprint: client-validated paradigm
- **Scales** independently from blockchain
- **Zero-knowledge** & privacy built on best products
  - Mimblewhimble: Bulletproofs by Andrew Poelstra
  - Liquid: Confidential Assets by Blockstream

How RGB works?

we started with looking for problems to solve,
not the solution to sell...

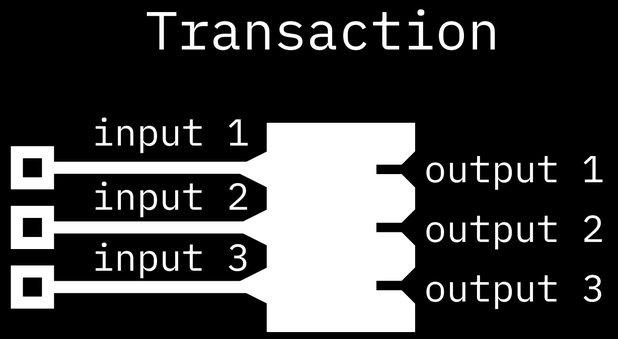
Problem 1: Blockchain does not scale

Problem 2: Blockchain is transparent

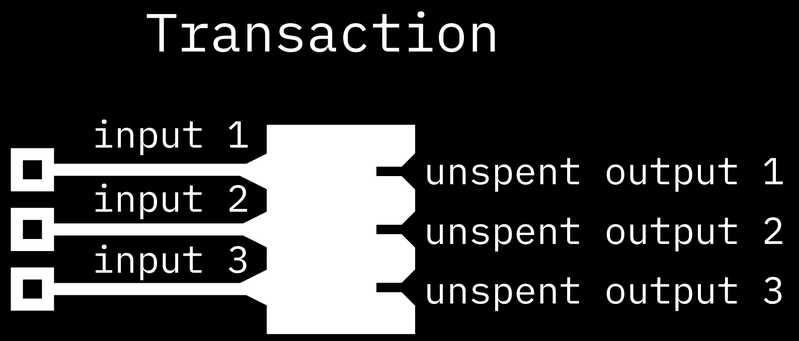
Solution: client-side validation

- Let’s not put data into blockchain!
  - Solves scalability problems of Ethereum, EOS and other systems…
  - Now the whole world does not see our transactions
- Use blockchain as a cryptographically commitment layer
  - Commit to some extra-blockchain data with elliptic curve homomorphic properties
- Data/history is maintained by asset owner
- Proposed by Peter Todd

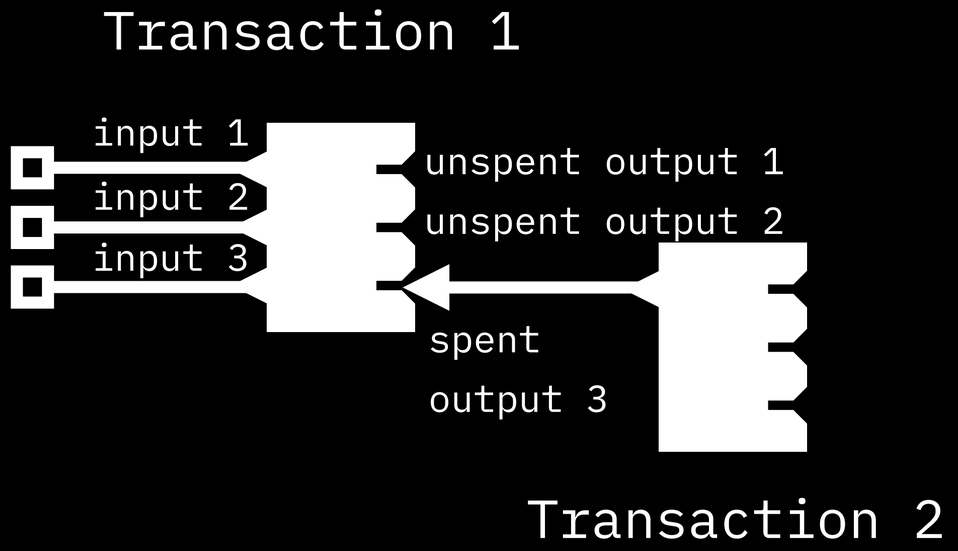
Bitcoin as single-use seal commitments medium



Bitcoin as single-use seal commitments medium

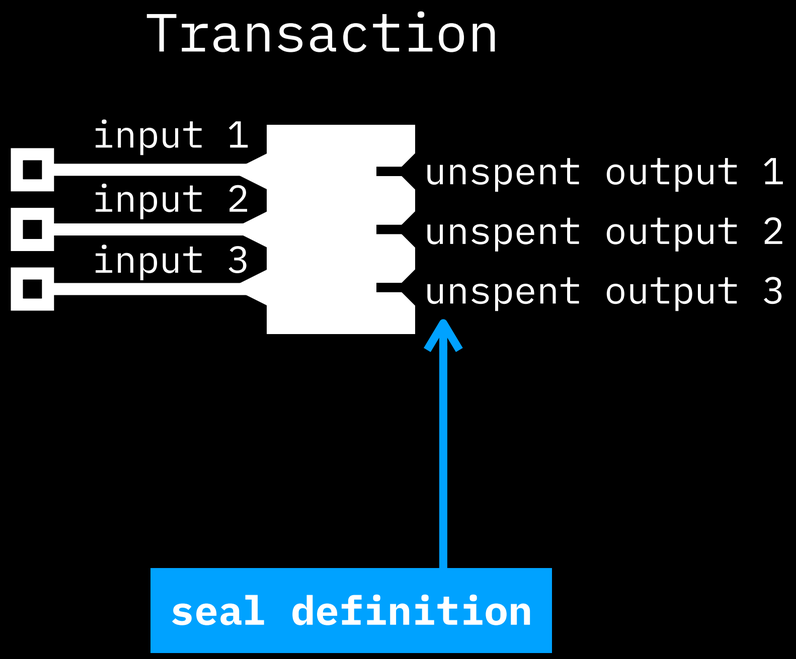


Bitcoin as single-use seal commitments medium

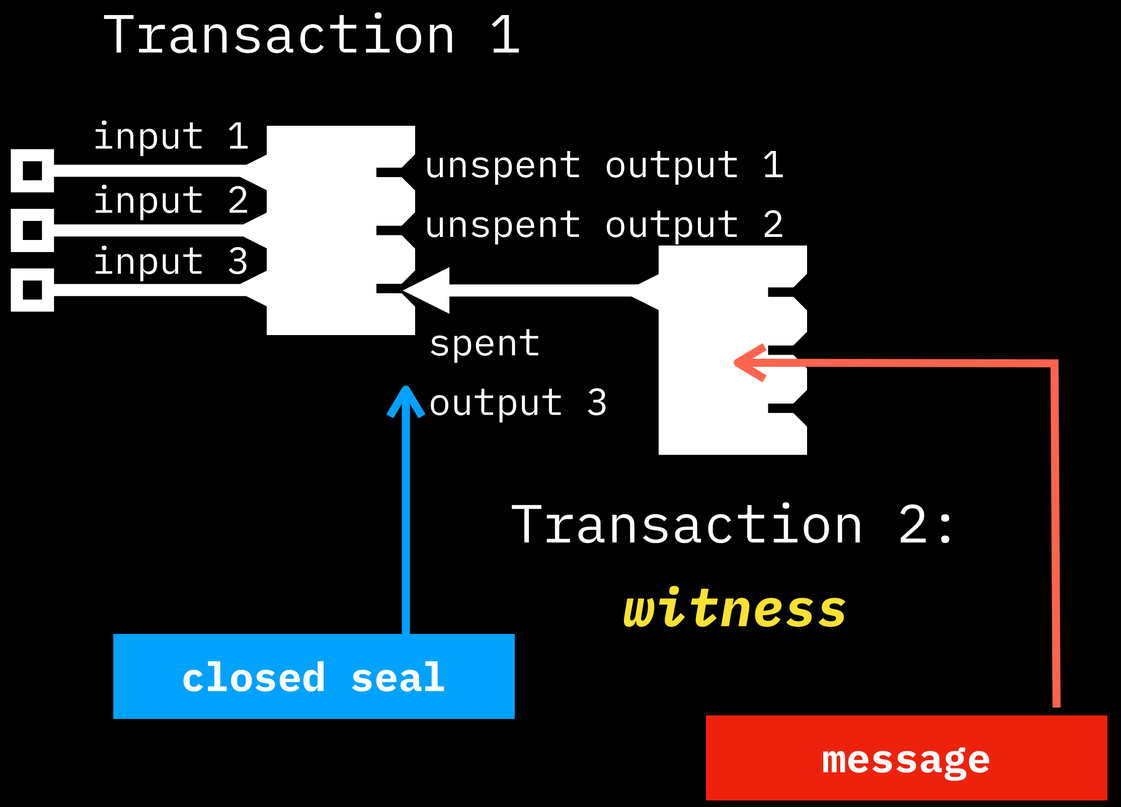


A unique event

Bitcoin as single-use seal commitments medium



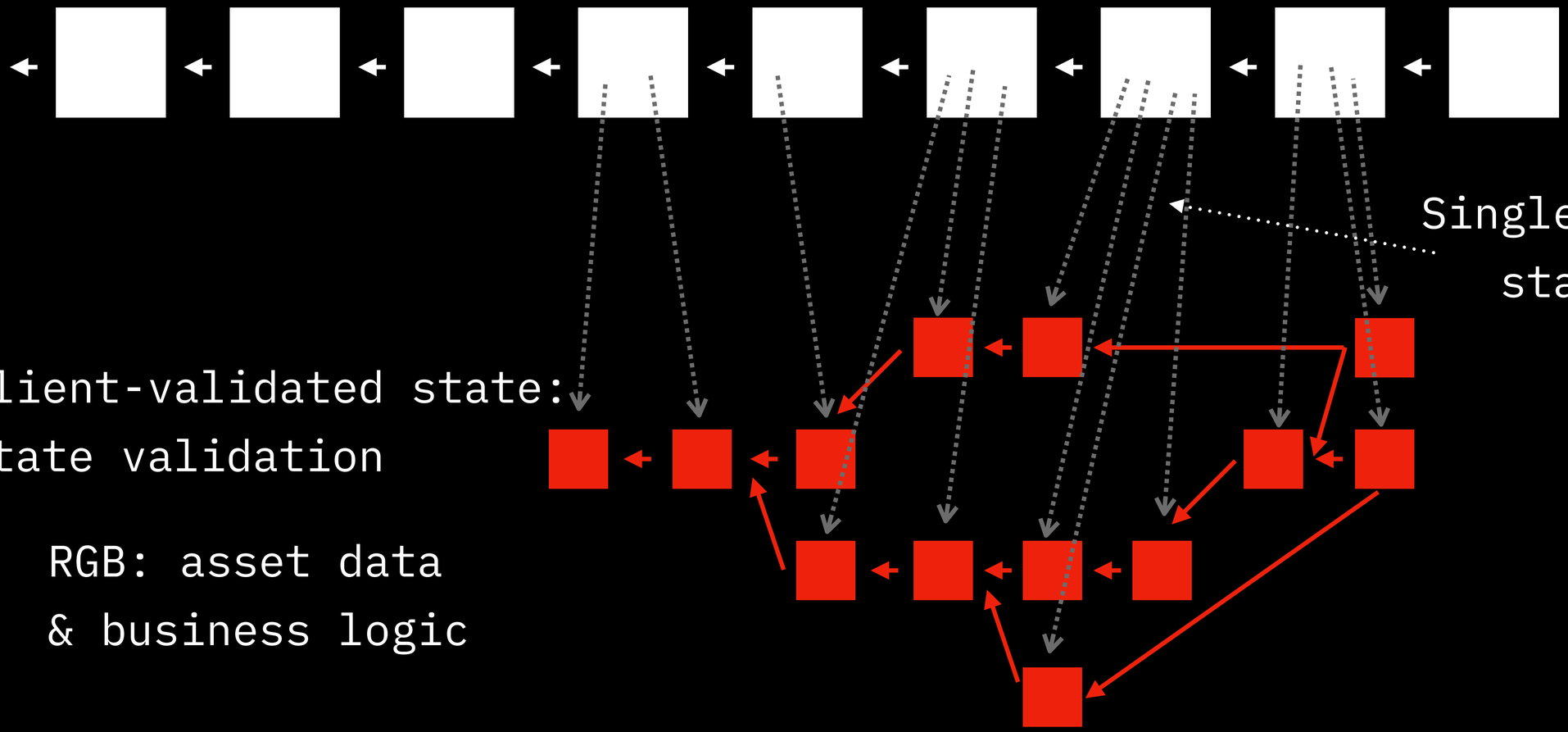
Bitcoin as single-use seal commitments medium



Main components of RGB

- 1. Commitments in transactions, proving unique history
  - private
  - zero storage cost
  - work both with blockchain (layer 1) and Lightning Network (layer 2)
  - meaning extreme scalability
- 2. Off-chain data & code held by asset/contract owner
  - zero blockchain storage cost
  - assets are linked to transaction outputs, which define their ownership & prevent double-spending (single-use seals)
  - off-chain smart contract code defines asset evolution

Bitcoin blockchain:
state ownership



Single-use seals:
state bindings

Client-validated state:
state validation

RGB: asset data
& business logic

two core theses

1. There always must be an owner

- Smart contract state is not a “public good” (Ethereum/“blockchain” approach); it must always have a well-defined ownership (private, multisig etc).
- RGB defines ownership by binding/assigning state to Bitcoin transaction outputs: whoever controls the output owns the associated state
- I.e. RGB leverages Bitcoin script security model and all its technologies (Schnorr/Taproot etc).

2. State ownership != state validation

- Ownership defines WHO can change the state
- Validation rules (client-side validation) define HOW it may change

2. State ownership != state validation

- Ownership controlled by Bitcoin script, at Bitcoin blockchain level (non-Turing complete)
- Validation rules controlled by RGB Schema with Simplicity script (Turing-complete)

This allows to avoid mistake done by “blockchain smart contracts” (Ethereum/EOS/Polkadot etc): mixing of layers & Turing completeness into non-scalable blockchain layer

Also it makes possible for smart contracts to operate on top of Layer 2 solutions (Lightning Network)

Smart contract is

- A pre-arranged *agreement*
- of trade (i.e. mutual voluntary exchange of *goods*)
- automatically executed under certain *conditions*,
  where “automatic” means
  - ✴ anonymous: no KYC is done
  - ✴ trustless: no need to do KYC to protect from the failure to execute contract

Smart contract components

- Agreement: the code
- Goods: digital assets
- Conditions:
  contract parties or external actors able to call some code

Smart contract components

- Agreement: the **code**
- Goods: digital assets -> **Ownership**
- Conditions: -> **Access rights**
  contract parties or external actors able to call some code

Ownership & access: core properties

- **Ownership**: digital assets must be owned by a well-defined party
- **Access**: a parties able to call the contract execution should be well-defined

Pure blockchain/layer 1 approach is wrong:

- Mixing ***code***, ***ownership*** and ***access rights*** into a single layer (“blockchain”)
- which is inherently ***unscalable*** and well-trackable (***anti-privacy***) since VERIFICATION is needed by the whole world
- With Turing-complete ***code*** operating at the same level, ***compromising security***
- Running ***non-censorship-resistant*** consensus algorithms (PoS, PoW forks with small hashing power)

Smart contract language: Simplicity

- Proposed and developed by Russel O’Conner, Blockstream
- Planned to be included into Elements and Liquid
- Formal semantics
- Formally-verified language with proofs on execution
- Succinct (complete Schnorr signatures are just few kB)

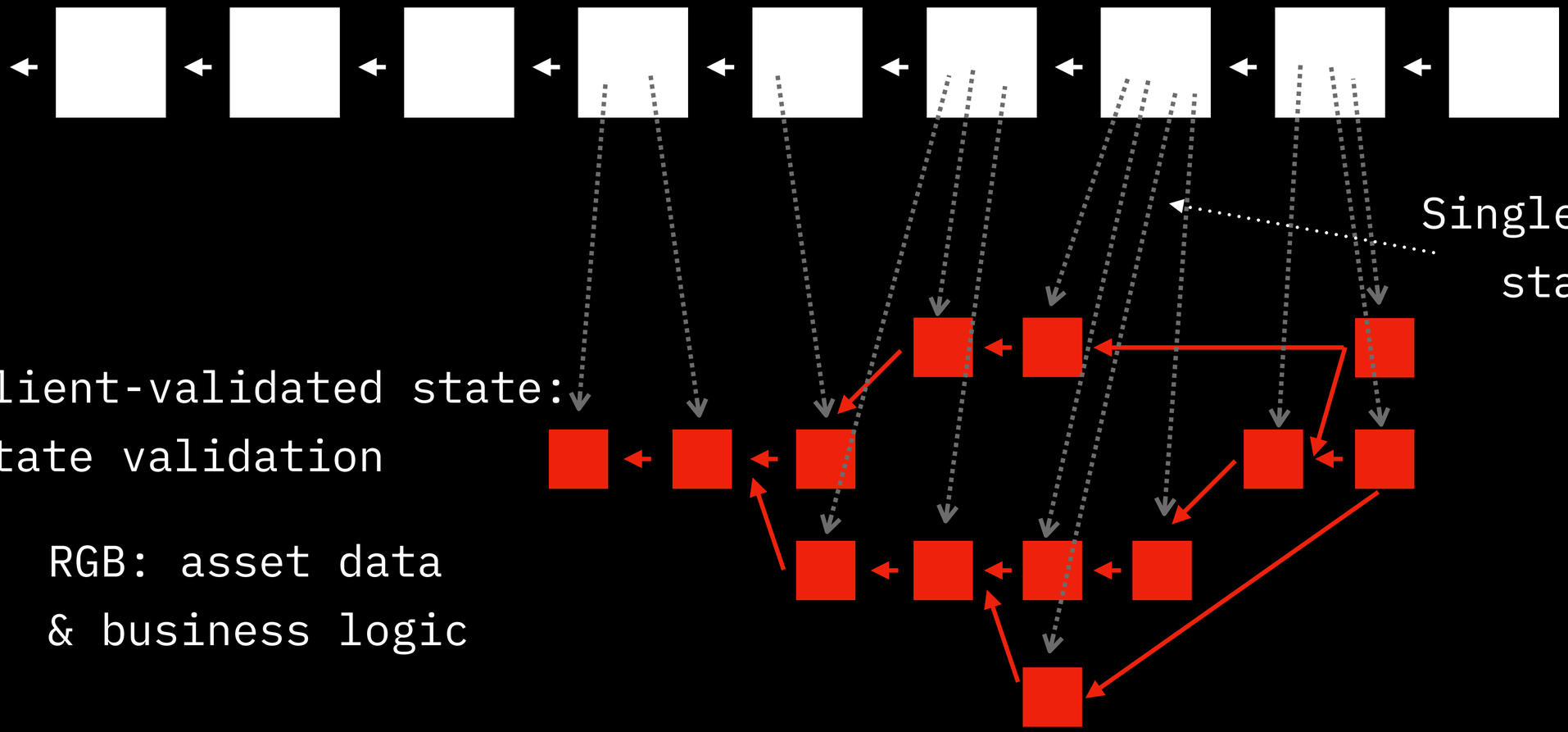
RGB is an asset and smart-contract
protocol for LNP/BP

Spectrum is DEX protocol for RGB assets &
smart contract interaction
over Lightning Network

Parts of LNP/BP technology stack

- Bitcoin blockchain: ownership & access rights
- RGB: data, metadata & Turing-complete business logic
- Lightning network: transaction scalability
- Spectrum: decentralized exchange & smart contract execution over Lightning Network

Bitcoin blockchain:
state ownership



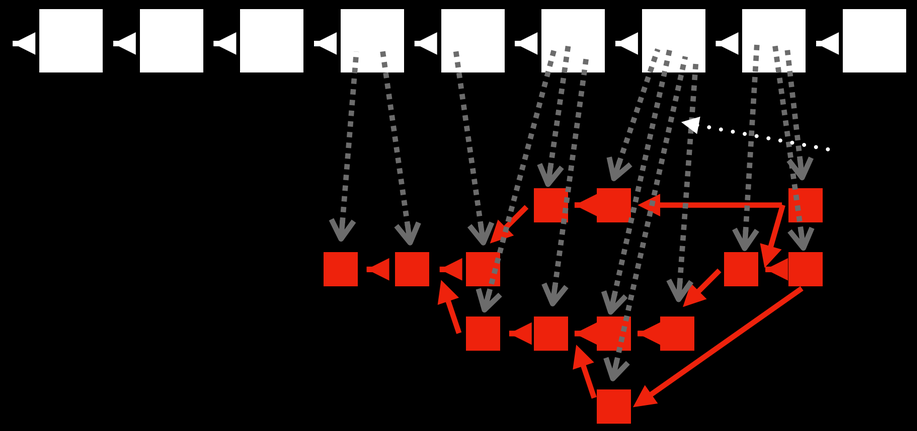
Single-use seals:
state bindings

Client-validated state:
state validation

RGB: asset data
& business logic

RGB is:

- “Sharding made right”
- “DAG made right”
- “Digital assets made right”
- “Smart contracts made right”
- “Confidentiality made right”



Spectrum is:

- “DEX made right”
- “Inter-blockchain protocol made right”

What is possible to do with RGB?

- Fungible assets & securities
  - Centrally or federation-issued
  - Issued anonymously or publicly
  - With possible secondary issuance, demurrage, inflation,
- Different forms of bearer rights
- Non-fungible assets (collectibles)
- Decentralized digital identity & roaming profiles
- Complex accounting systems & utility tokens

What is possible to do with RGB?

- Complex & highly-efficient smart-contract systems
  - Lightspeed: high-frequency micropayments on top of Lighting
  - Storm: trustless storage & messaging
  - Prometheus: trustless high-load computing & machine learning

And it’s all:

- Scalable
- Confidential
- Working over Lighting Network
- With DEX functionality
- Operating as a bearer instrument