RGB

Roadmap 2022 towards release

Dr Maxim Orlovsky,
Pandora Core AG

LNP/BP Standards Association

BITFINEX

tether

Fulgur Ventures

Sabina Sachtachtinskagia

Died 23 Feb 2022

Reason of death: medical “accident” in Universitatspital Zurich (15 Jan 2022)

- Game theory expert
- LNP/BP contributor to game theory models of RGB, RGB-based DeFi (DEX, algorithmically stable coins)
- Partner in Pandora Core AG, CFO

Ukraine LNP/BP & Internet infrastructure support

http://vosv5oiypr7gyxuojpuemv3tkrkjazkwnabnonpws27onmtpf7c5e6id.onion/btcpay/apps/3iMr9YfKquQvRtBKUFyZTXJAXZCR/pos

On 24 Feb 2022 Russia started full-fledged war against Ukraine and Ukraine peaceful residents, which may be qualified as genocide

This is a continuation of a smaller-scale war lasting since Russia invasion to Ukraine in 2014.

LNP/BP Standards Association has started fund to support

- resilient internet connectivity;
- penetration of decentralized IT infrastructure based on LNP/BP stack (payments, messaging, legal system long-term)
- humanitarian support, primarily to people related to LNP/BP and decentralization tech and their relatives; help in their relocation

Stages of Ukraine LNP/BP support

- Urgent & research stage (until ceasefire)***
  - Starlink connectivity* (done)
  - Humanitarian personal-targeted support (~$10k in total; in the future up to 10% of funds)
  - Research on radio, satellite and mesh connectivity
  - Research on connectivity loss-resilient LNP/BP payment infrastructure based on LN
  - Software/hardware development for “adoption stage”**
- Reparative stage (once ceasefire will be achieved)
  - Reparation of main optic cables*
  - Creation of “airfiber” infrastructure to duplicate main Internet backbones
- Adoption stage
  - Deployment of personal mesh-network, radio and satellite connectivity
  - Low-energy bitcoin/LN hardware boxes and PoS terminals
  - Low-energy, surveillance & censorship-resistent P2P messaging & payments

* Stages where LNP/BP helps only with organizational & human resources and not funds; the funds are provided by other foundations of Ukraine government crypto fund

** All software development using LNP/BP funds will be done open source under permissive licenses (MIT, Apache etc)

*** On other points LNP/BP support fund operates in a tight connection with NYM Project and Asgard Foundation, also providing a lot of funding for Internet infrastructure and humanitarian topics

RGB Roadmap

RGB public preview

- Released in May 2021 as RGB Node version v0.4
- Accompanied with products by Pandora Core AG:
  - the first RGB-enabled wallet MyCitadel and wallet integration kit Citadel Runtime
  - tool for asset issuers Bitcoin Pro
  - asset catalog/explorer RGBEx.io
- Was lacking:
  - Turing complete scripting (AluVM)
  - Full Taproot support (no taproot was activated yet)
  - Usable way to transfer client-side-validated data (asset distribution, asset transfers)

Developed since May 2021

- By LNP/BP Standards Association
  - AluVM: virtual machine for Turing-complete scripting with RGB
  - Taproot implementation in rust-bitcoin
  - Wallet-specific updates required for RGB (PSBT LNPBP and BIP standards, derivation paths)
  - Lightning implementation:
    - new Bifrost protocol and channels supporting RGB
    - full BOLT lightning compatibility by LNP Node
- By Pandora Core company:
  - AluAsm: an assembler langage and compiler for AluVM
  - Design of algorithmically stable coin using RGB, Bifrost and DeFi + other DeFi products
- By other companies:
  - NFT wallet by DIBA

Time

Taproot

RGB Protocol (onchain)

AluVM

Bifrost P2P + Storm

PSBT extensions

Strict encoding API

UX for RGB onchain transfers & NFTs

RGB Integration Kits (wallets, exchanges)

Bifrost channels

RGB-enabled LN channels

Contractum & strict encoding compilers

RGB Dev Kits (new smart contracts etc, DeFi etc)

Release batches in 2022

1. RGB protocol: May 2022
2. P2P RGB assets & NFT distribution and transfers: Aug 2022
3. RGB-enabled lightning (Bifrost) channels: end of 2022

Current action points

Answering the question “How I can contribute”

RGB protocol

- Strong rust skills:
  contribute to RGB repos
  (contact us directly)

- Medium rust skills:
  do a test coverage for existing RGB repos

- Poor or no rust, but cryptography knowledge:
  - audit existing code base
  - help in writing & reviewing standards describing RGB

RGB Integration / Dev Kits

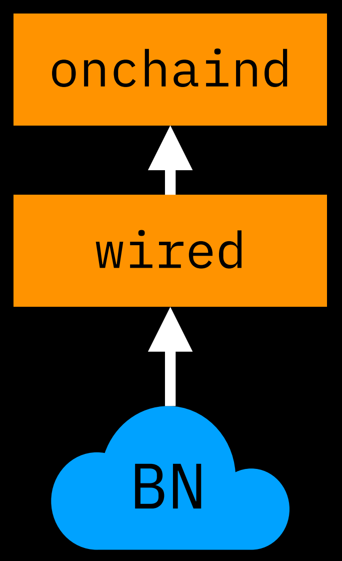
- Strict Encoding libraries in different languages

- ZMQ/StrictEncoding gateway with
  - Protobuf/gRPC API
  - JSON RPC API (not recommended)

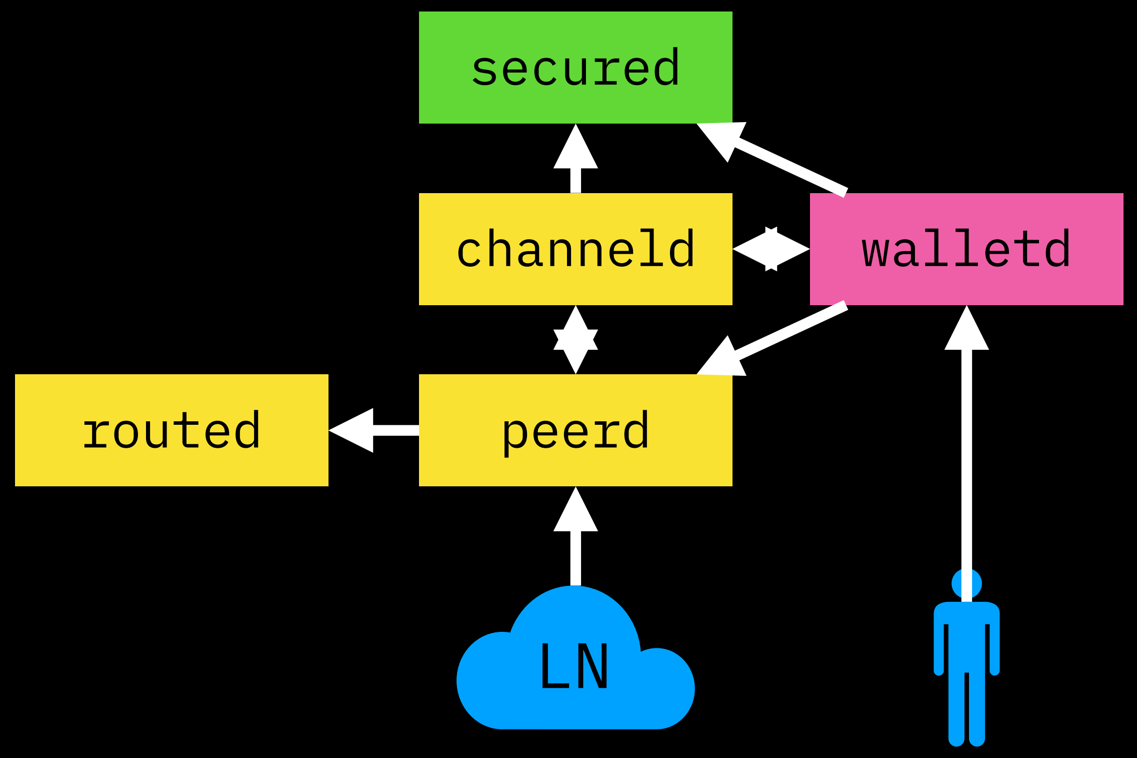
Integration languages

- C (implemented in Rust, required for the most of the rest)
- WASM (implemented in Rust)
- JavaScript
- Java (and Kotlin)
- Dart (for Flutter)
- Python
- Swift

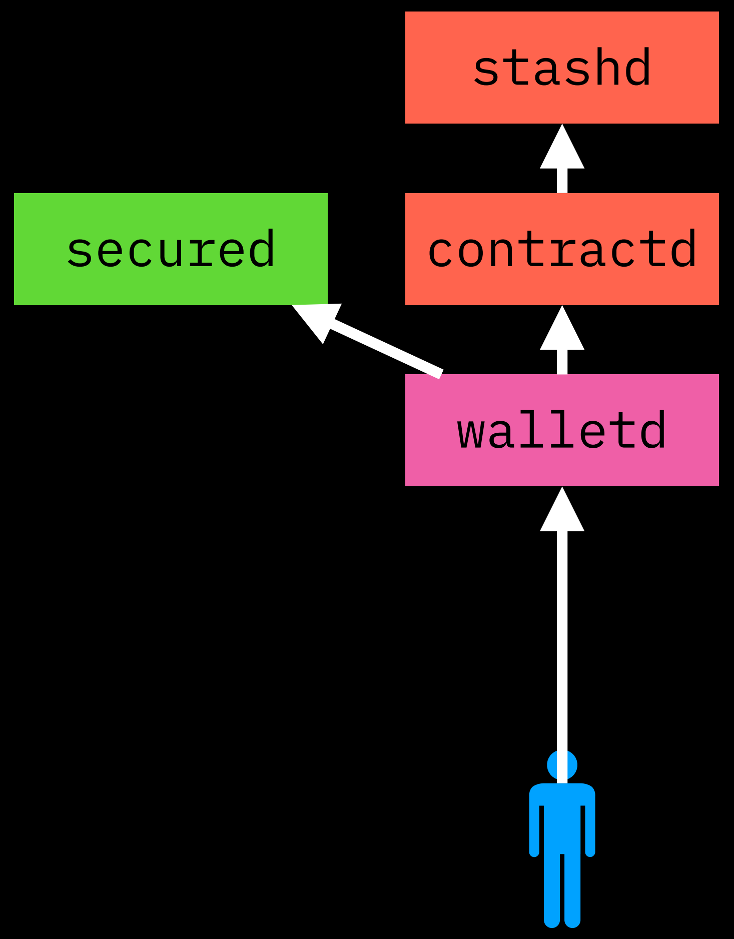
BP Node



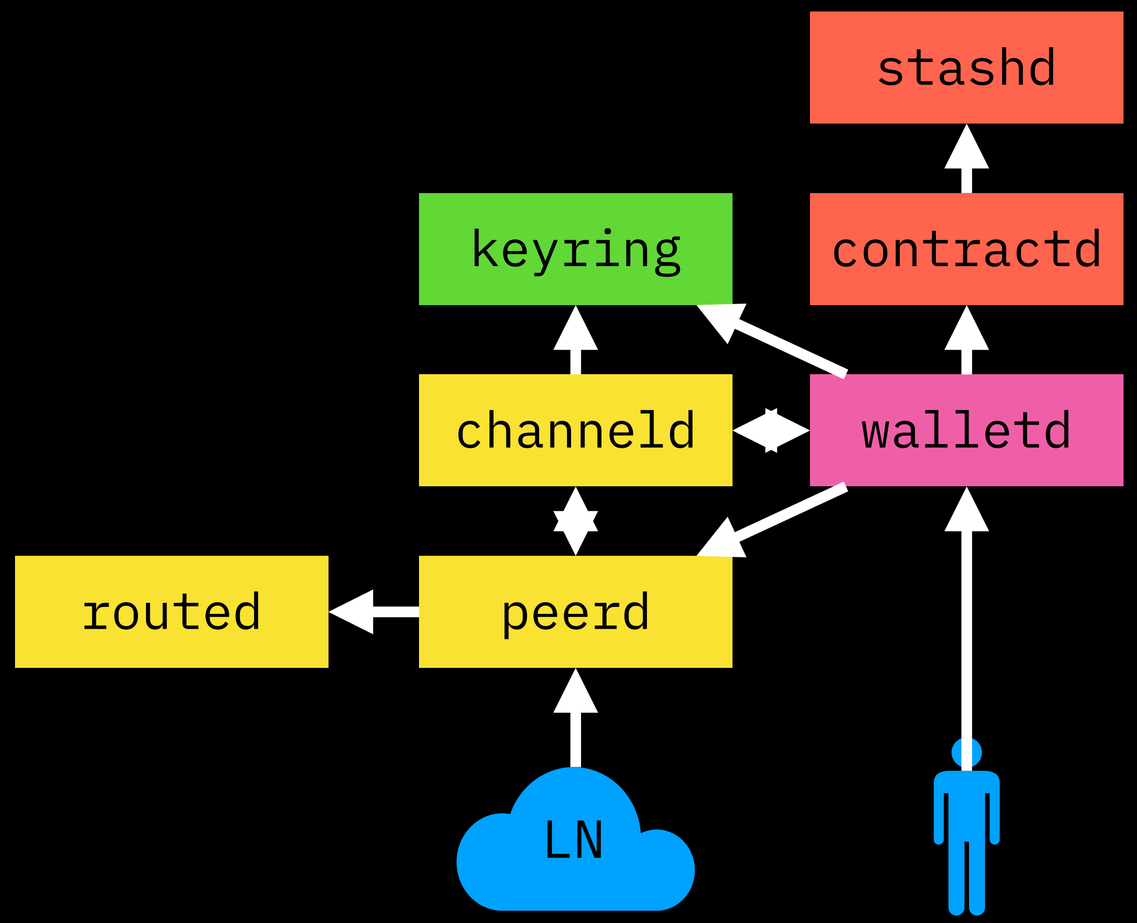
LNP Node



RGB Node



MyCitadel Node



Integration

- All communications between components are done via ZMQ with strict encoding

- This is more robust and client-side-validation compatible than Protobuf/gRPC-based APIs

- However, most software used to Protobuf/gRPC or JSON RPC

Integration landscape

Node (RGB, LNP, BP, Storm)

C FFI

Swift/Kotlin/Dart class library

Mobile app UI

Node (RGB, LNP, BP, Storm)

ZMQ strict-encoded API

Language-specific ZMQ strict encoding libraries

Server-side or desktop app UI

Node (RGB, LNP, BP, Storm)

ZMQ strict-encoded API

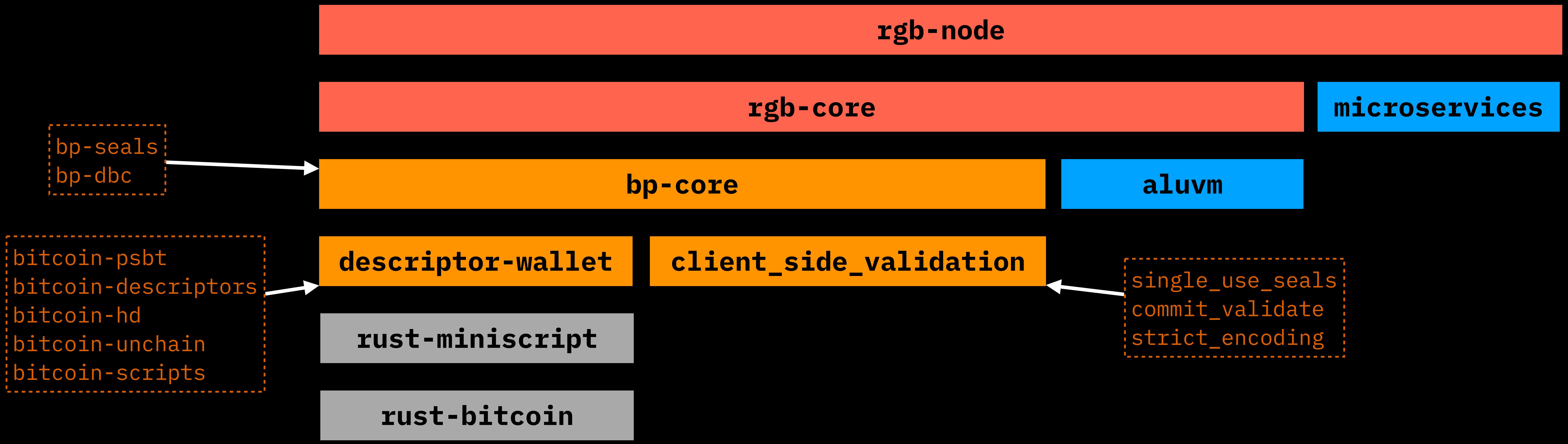
Gateway

Protobuf/gRPC API

Server-side or desktop app UI

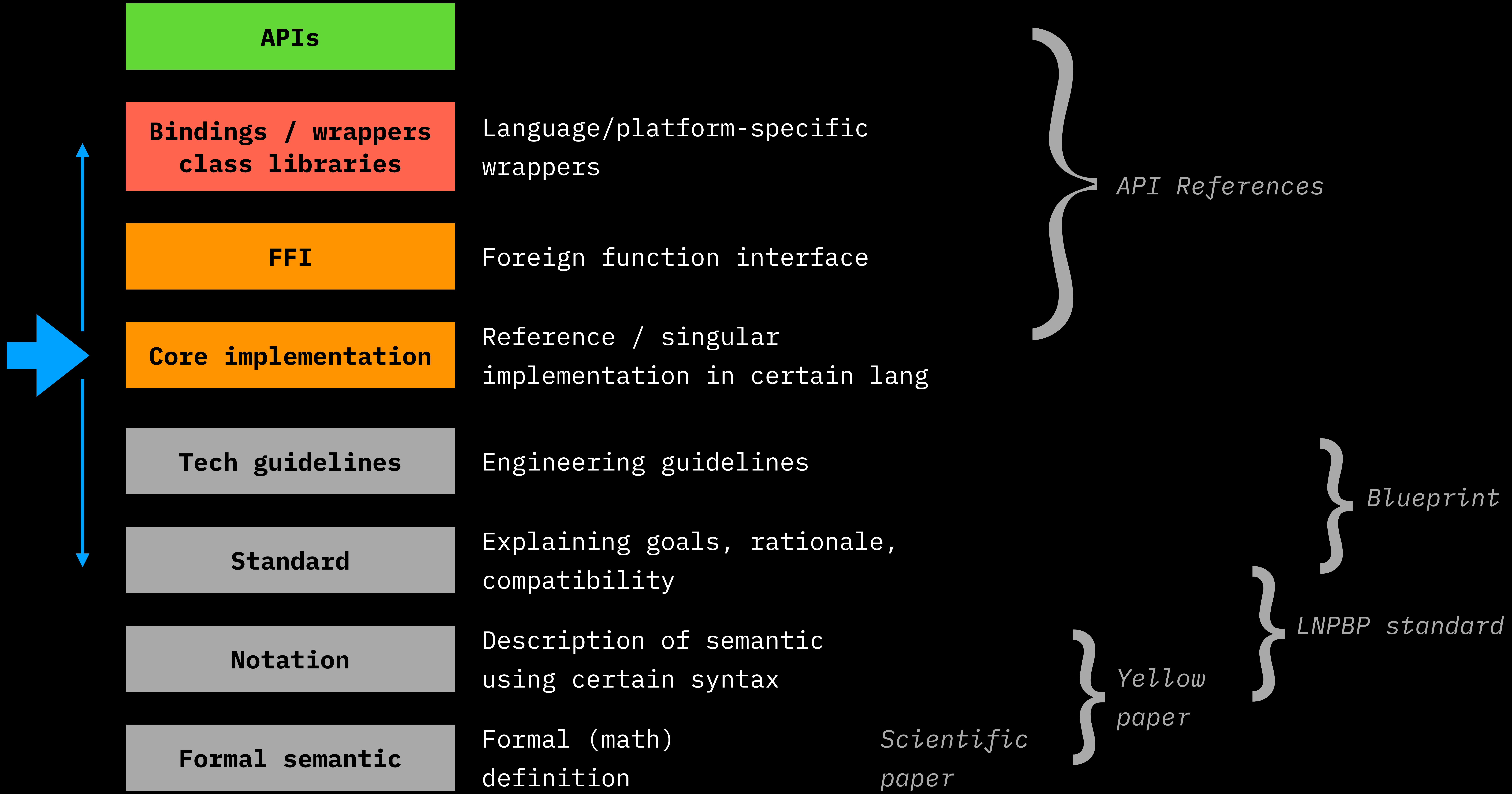
Contributing to & auditing RGB

RGB-related libraries stack



GitHub

- github.com/rust-bitcoin – bitcoin implementation
- github.com/LNP-BP – standards, client-side-validation, BP, LNP
- github.com/RGB-org – RGB smart contracts, Contractum language
- github.com/Internet2-org – AluVM, BOLT-8 based networking
- github.com/Storm-org – decentralized storage & messaging
- github.com/Prometheus-org – decentralized trustless computing



APIs

Bindings / wrappers class libraries — Language/platform-specific wrappers

FFI — Foreign function interface

Core implementation — Reference / singular implementation in certain lang

Tech guidelines — Engineering guidelines

Standard — Explaining goals, rationale, compatibility

Notation — Description of semantic using certain syntax

Formal semantic — Formal (math) definition

API References

Blueprint

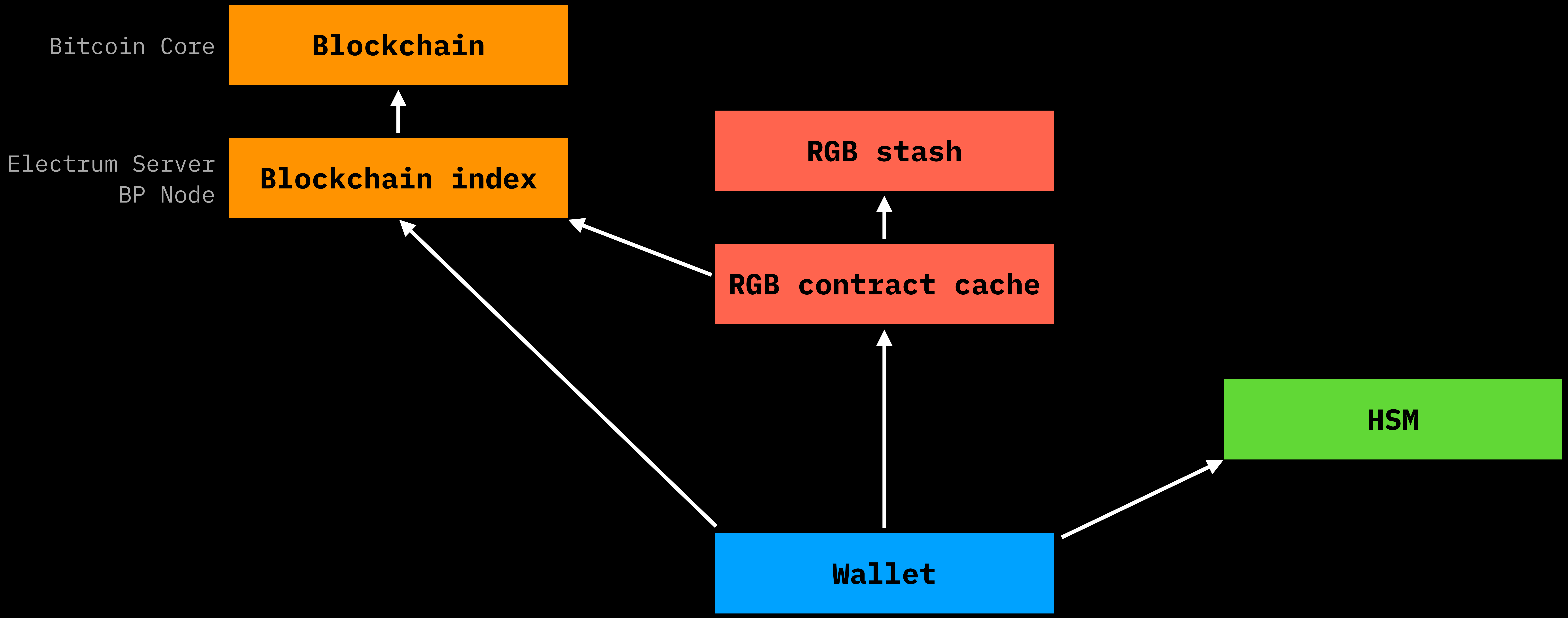
LNPBP standard

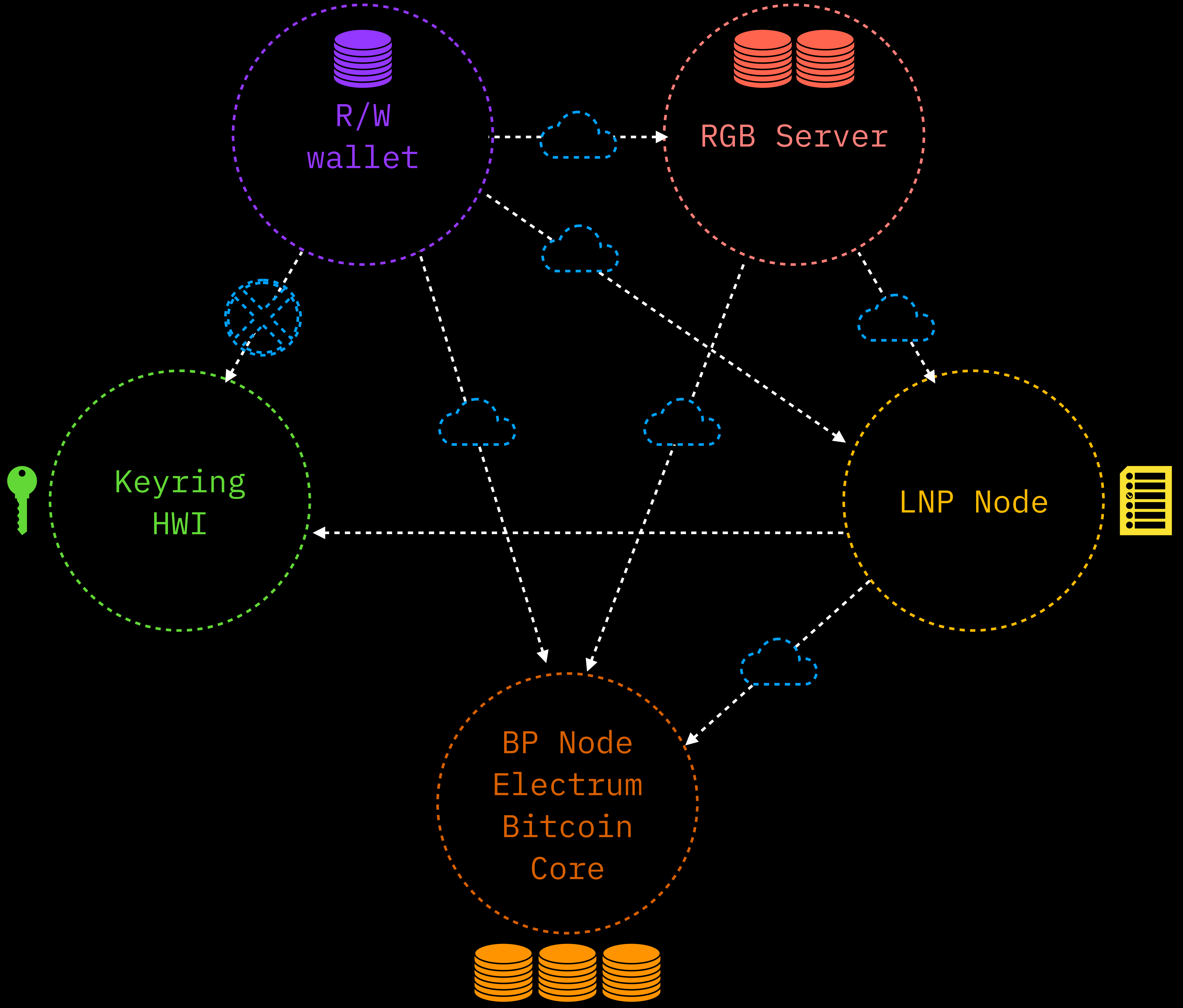
Yellow paper

Scientific paper

RGB wallet integration

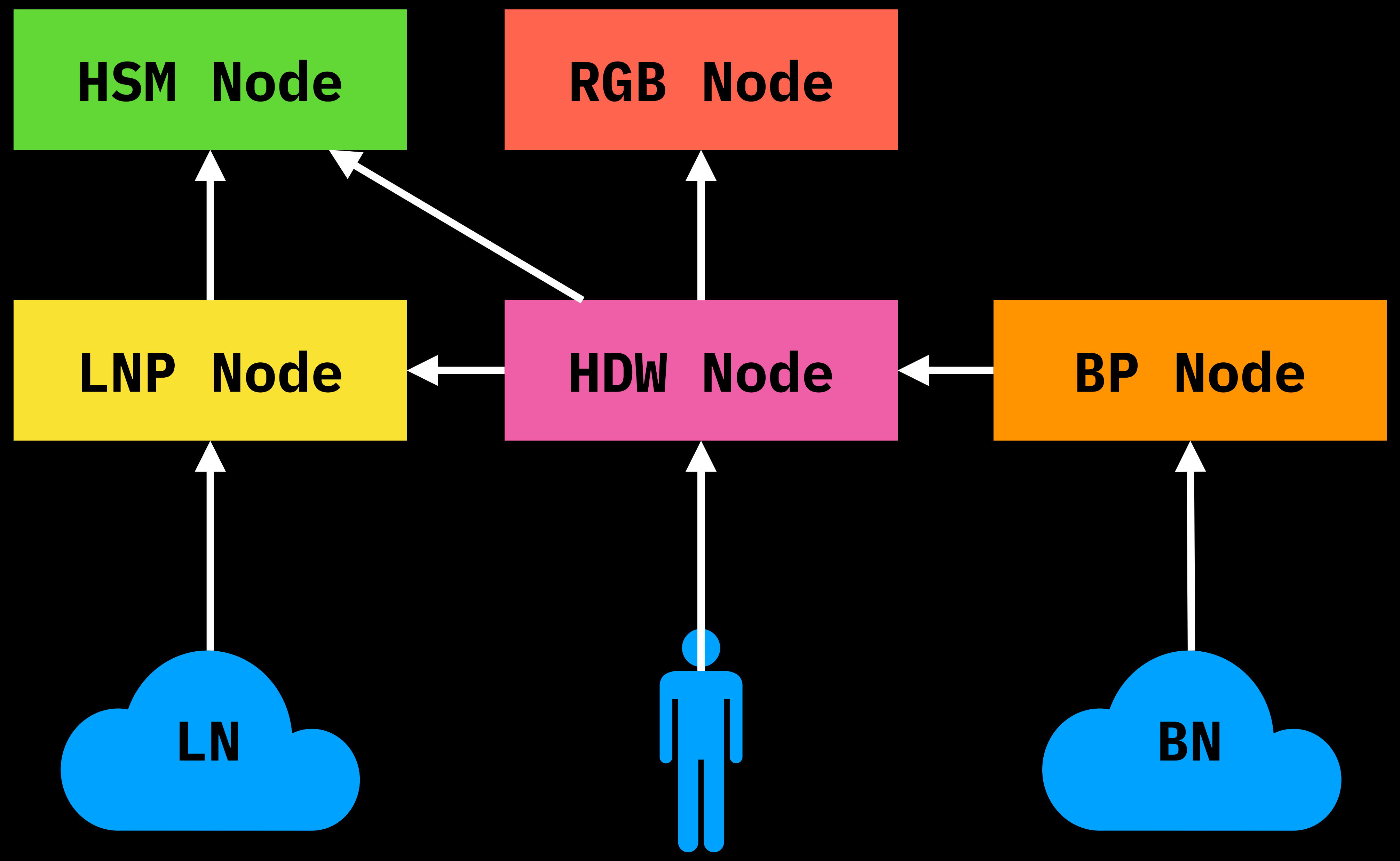
On-chain RGB wallet




R/W
wallet
RGB Server
Keyring
HWI
LNP Node
BP Node
Electrum
Bitcoin
Core

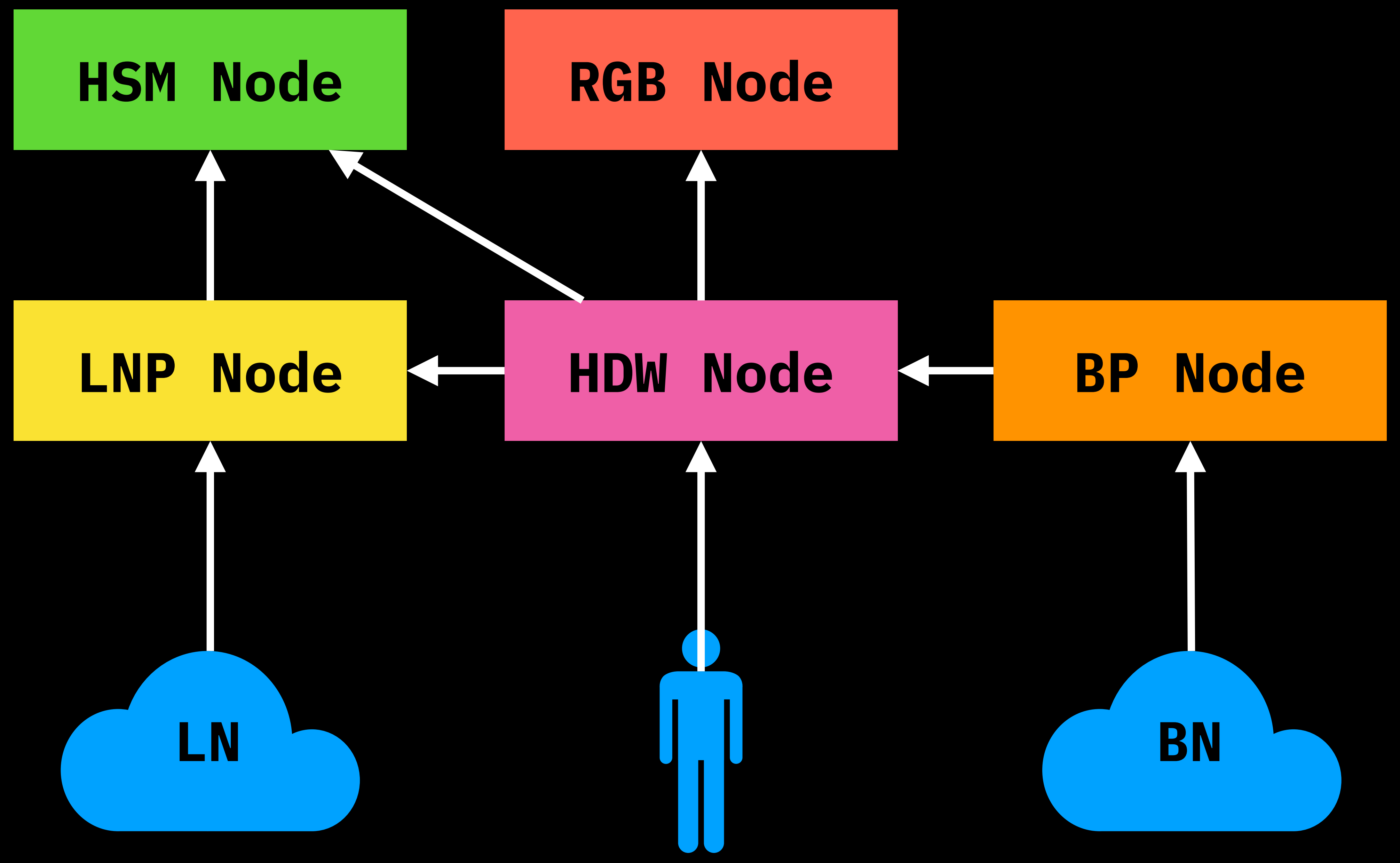
Anatomy of LNP/BP wallet

- BP Node:
  - tracks chain events
  - keeps mempool
- LNP Node:
  - maintains channel state
  - handles lightning network messages
- RGB Node:
  - keeps stash
  - maintains contract state
- HSM Node: provides signatures on PSBTs
- HDW Node (hd wallet):
  - maintains HD accounts
  - knows which UTXOs are owned & valid by the user



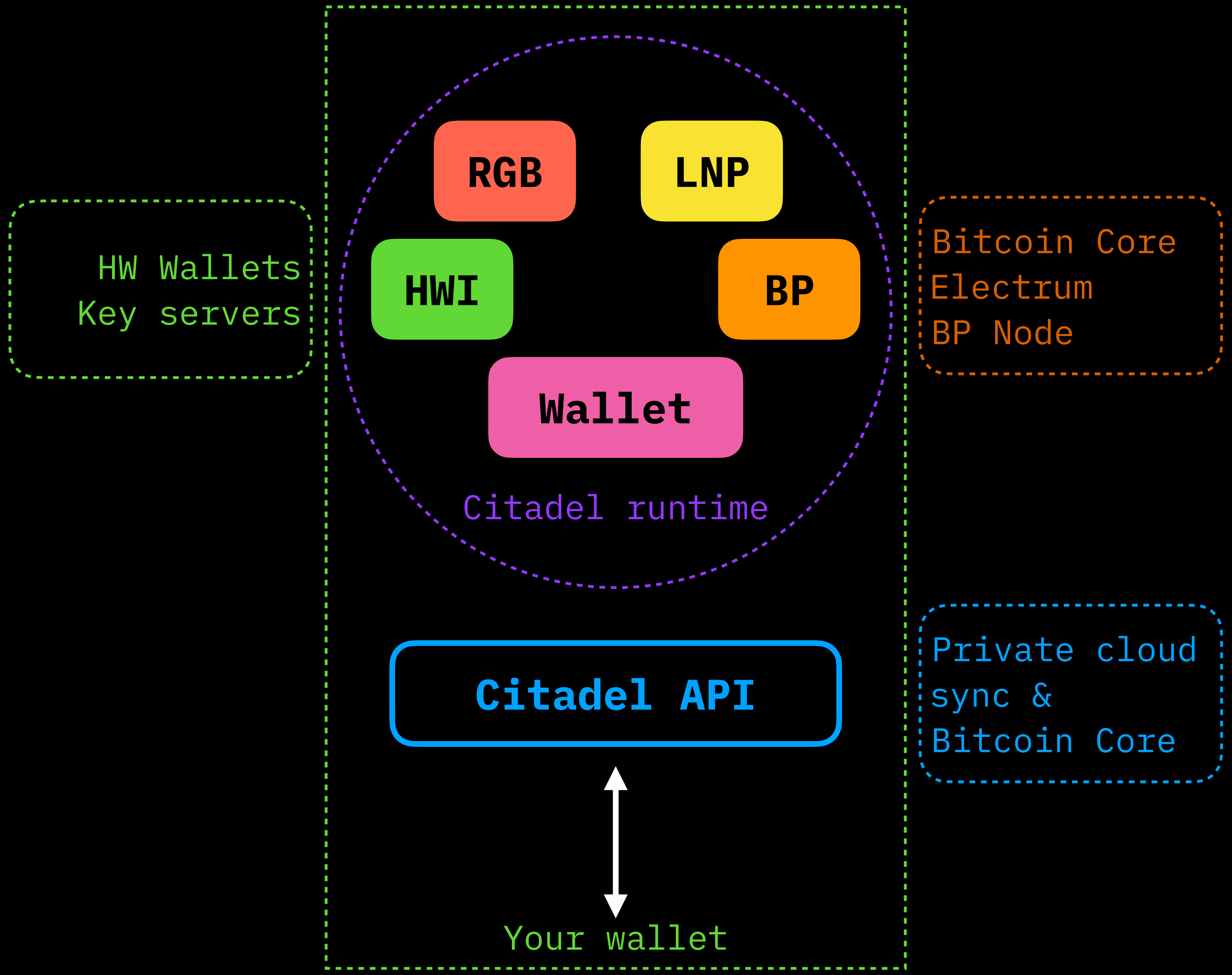
Wallet event model

- Chain _and_ mempool events (BP Node)
  - LNP channel update
  - RGB contract state update
- Lightning network events (LNP Node)
  - LNP channel update
  - RGB stash update
  - RGB contract state update
- User events (HDW Node):
  creating tx/LN payment/state transition
  changing accounts
  - BP update
  - LNP channel update
  - RGB stash update
  - RGB contract state update

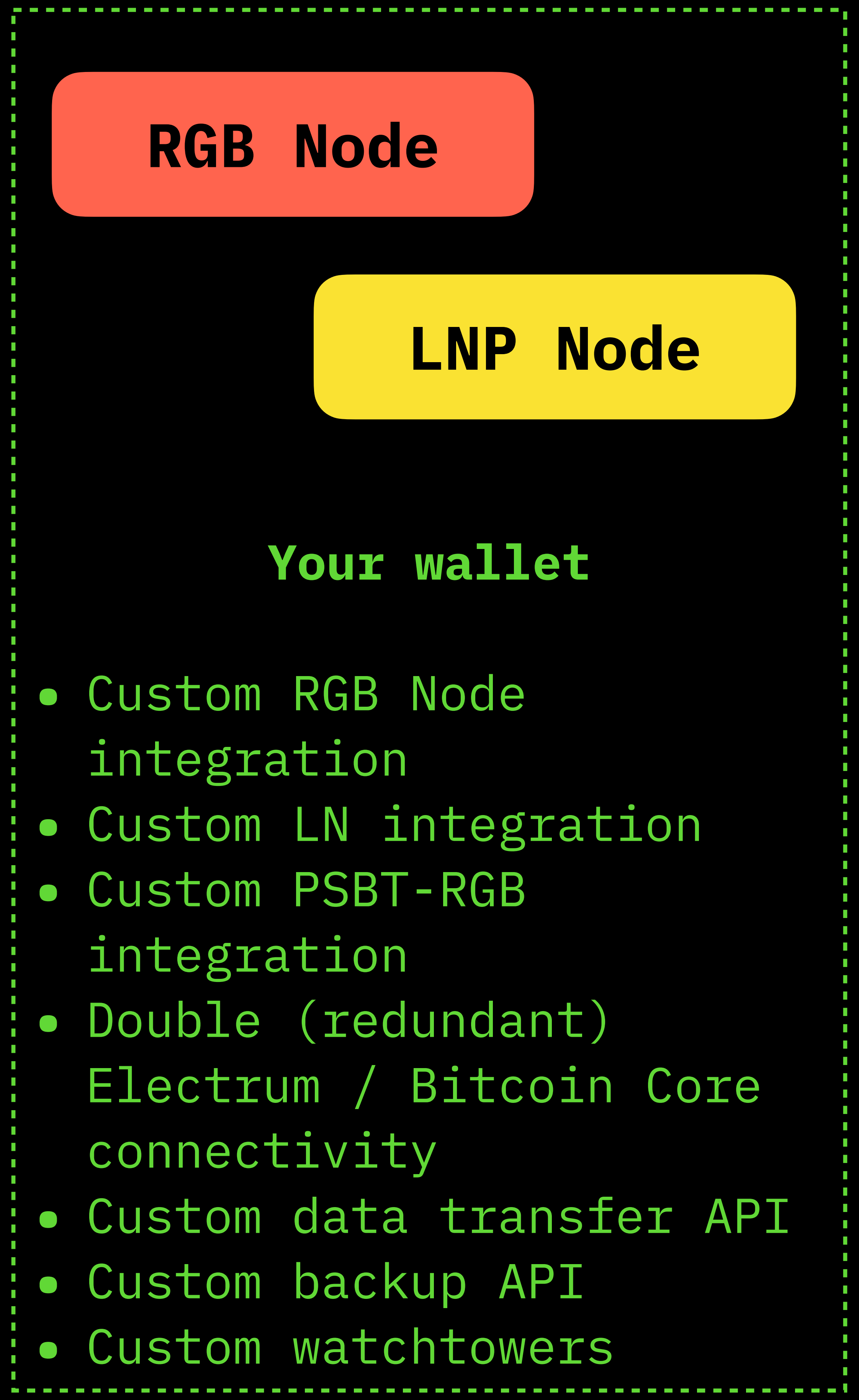


Two ways of integrating RGB

Simple



Complex



- Custom RGB Node integration
- Custom LN integration
- Custom PSBT-RGB integration
- Double (redundant) Electrum / Bitcoin Core connectivity
- Custom data transfer API
- Custom backup API
- Custom watchtowers

Decentralizing RGB

Actors in RGB ecosystem

- Users: always know which terms & contitions apply for each assets. These terms can’t be changed EVER.
  Most influencing actor.

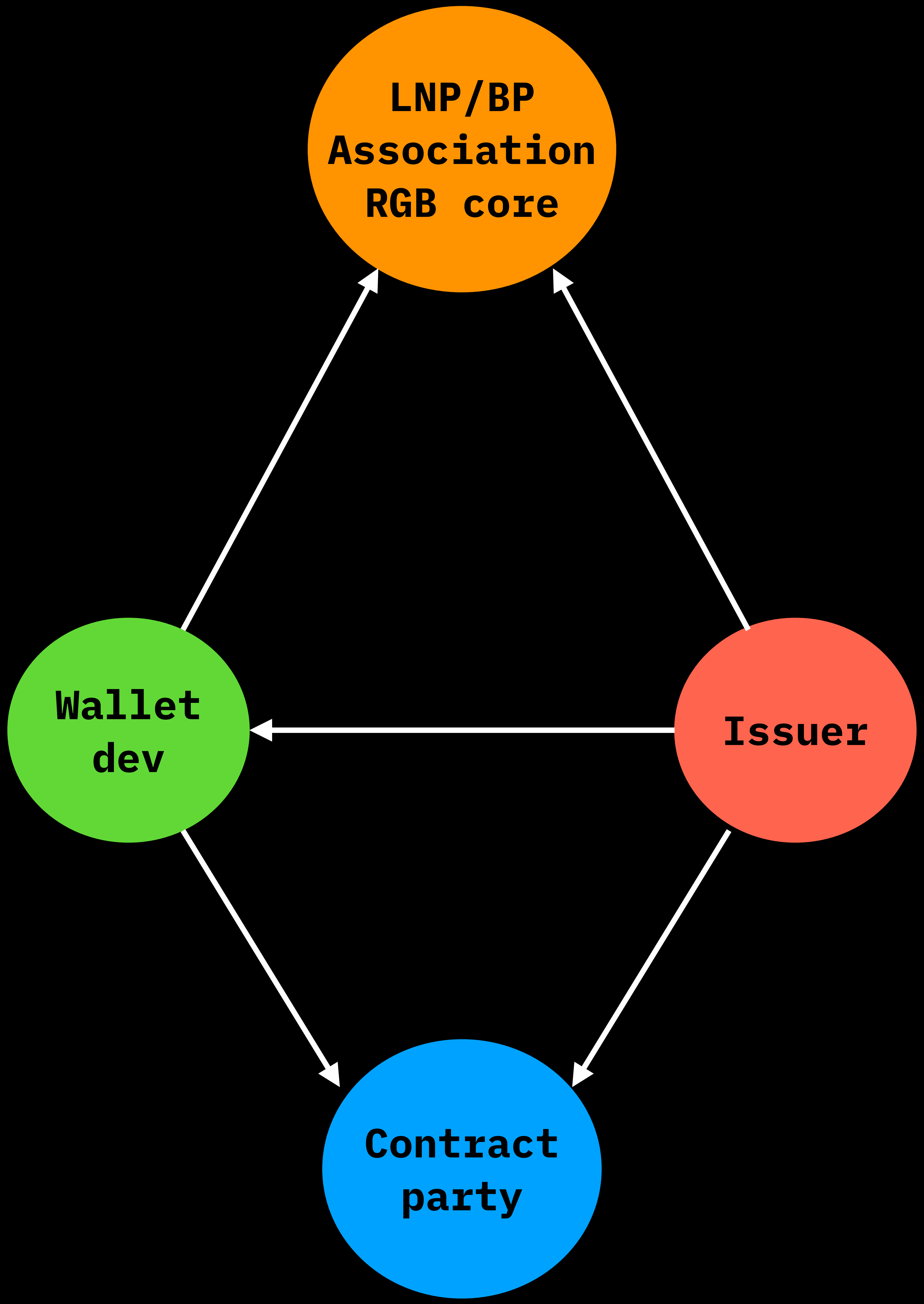
- Issuers: creators of RGB assets, NFTs, smart contracts.
  The actor taking decisions.

- Wallet & software devs: controls what actually can be added to RGB, what issuers can do etc.

- LNP/BP Association & RGB core devs: coordinate issuers & wallet devs at initial stages, loosing control over the time.

Who depends on whom

- “Hard-Soft forks” (was invalid - became valid)
  - We can’t have a global date for client-side-validation fork (b/c of partial state), so must not change binary structure
  - Issuers should be able to opt in without issuing new contract
  - Developed by LNP/BP association and distributed to wallet devs
- “Soft-Hard forks” (was valid - became invalid):
  - Any update which require binary structure update
  - Require new schema
  - Require issuers to issue new contract
  - In fact, a new RGB version (RGB/2 etc)



Roadmap towards RGB immutability and attack resistance

- Increase number of contributors

  LNP/BP Association, Bitfinex, Fulgur Ventures,
  Pandora Core, DIBA and others provide financial support for contributors

- Each contributor with a track record will become a RGB Core & underlying repos maintainer

- Maintainers will have a veto right on any future RGB changes, the threshold of ACKs will increase over time…

- … until RGB code will become unchangeable w/o full consensus of all maintainers (targeting >50), so only in case of obvious bug fixes the code may change