Building RGB ecosystem together

LNP/BP Association recent developments and first products by member companies on RGB

RGB and beyond

- RGB: **non-blockchain** (but client-side-validated) smart contracts
  - Much more _privacy_ (even more than blockchain-based ZK)
  - Much more _scalability_ (works over P2P non-consensus networks like lightning)
  - Much more _safe_ programmability due to separation of concerns
  - Much more _ownership_ instead of “governance”
- Pure **cypherpunk** stuff
  - Created by coders & scientists
  - No token! Yes, no fucking token!
  - 100% non-profit, open-source, but still anarcho-capitalistic (strong ownership focus)
  - Developed & maintained by Swiss LNP/BP Association (non-profit), which we plan to grow into something alike Linux Foundation & IETF in the future for LNP/BP stack
  - “John Galt’s” solution to the world problems

RGB vs Ethereum

	“Ethereum-style”	RGB
● **Parties of the agreement**	loosely defined	issuer and current owners, good role distinction
● **Agreement:**	Bockchain-stored contract + who-knows-who-keeps ABI file	Client-stored data only
- **Current state**	blockchain-stored data: ★ publicly visible ★ non-confidential ★ non scalable ★ no 2nd layer support	client-stored data: ★ no chain analysis ★ confidential ★ scalable ★ 2nd layer support
- **State change rules**	custom EVM code	schema & simplicity script
- **Ownership rights**		bitcoin script
● **Mutability**	Pseudo-immutable: immutable in promise, *de facto* censored my miners, Vitalik® & contract creators	Well-defined mutability rights at genesis & schema level by issuer Mutable by new owners within the scope of rules

RGB vs Ethereum in simple words

Ethereum

is a mess:

- needless token (why do we need ETH?)
- no clear ownership rights at any level
- governance worse than with a government
- all layers mixed together
  - bugs & hacks
  - unscalable
  - low privacy
- constant hard forks
- contract can contain backdoors

RGB

quite the opposite:

- no token
- bitcoin-level safety guarantees of ownership
- scalable over layer 2 *and 3* solutions (LN, DEX, smart contracts on top of RGB)
- extreme confidentiality
- clear ownership rights & mutability due to client-side-validation
  - no miners involved
  - issuers lose control the moment they create a contract
  - owners are always in control and know all terms & conditions upfront; no backdoors are possible

“Multi-blockchain world” criticism

- Only a single blockchain should serve censorship resistance needs; other blockchains are not needed since they are either non-confidential or unscalable and insecure
- All data must be kept by data owners (client-side-validation); they may pay for delegating that, but not in “communistic way” (like with blockchains)
- What we need is isolated contracts (like with RGB), interoperable with each other via layer 2 & 3 (LN) – instead of connected “internet of blockchains”
- True proof of stake is a stake you can lose for breaking RGB contract in a multipeer LN channel – and not public & censorable blockchain shit tokens

RGB mission

- Much more _privacy_ (even more than blockchain-based ZK)

- Much more _scalability_
  (it works over P2P non-consensus networks like lightning)

- Much more _safe_ programmability due to separation of concerns

- Much more _ownership_ instead of “governance”

What will drive RGB adoption?

- Scalability

Governments like blockchains because they can control validators and do chain analysis (even more with new “ZK”-blockchains)

Enterprise follows the government because it’s scared of its enforcement power, so enterprise/corporates comply/cooperate (like they did even with Nazis)

BUT: *how the fuck they are going to scale with that shit?*
Blockchains, fortunately for us, do not scale!

So, our chance is: before the governments will understand what the new shift of paradigm on client-side-validation coming from cypherpunks is about (and previously this took years for bitcoin), normal companies will have a window to start using RGB because … they need digital scalability!

Building adoption

- User- and dev-facing tools are critical!
- Tools may be for-profit/commercial, since we need to provide support for businesses. Finally, we are anarcho-capitalists, not socialists!
- Open-source and “free to use if self-supported, paid for professional support” set of tools is required for real adoption
- Devs of the original protocol are able to deliver initial toolset to the market since they understand all possibilities of the new protocols
- Pandora Core AG run by RGB devs gives initial set of tools for devs & users matching those criteria

Build on LNP/BP Association tools

- These tools are just integration of & UI on top of LNP/BP tools, simplifying life for users & devs:
    - Client-side-validation and LNP/BP Core Libraries
    - RGB Core library & Node
    - LNP Core library & Node
    - Descriptor wallet library
- You can DIY your tools, even commercial
- Even more: you can use Pandora Core tools for free to start using RGB tomorrow!

What are these tools?

- **Bitcoin Pro:** MIT-licensed tool for professional asset issuers (and even non-RGB professional bitcoiners)
  GTK+-based, all desktop platforms, pure Rust

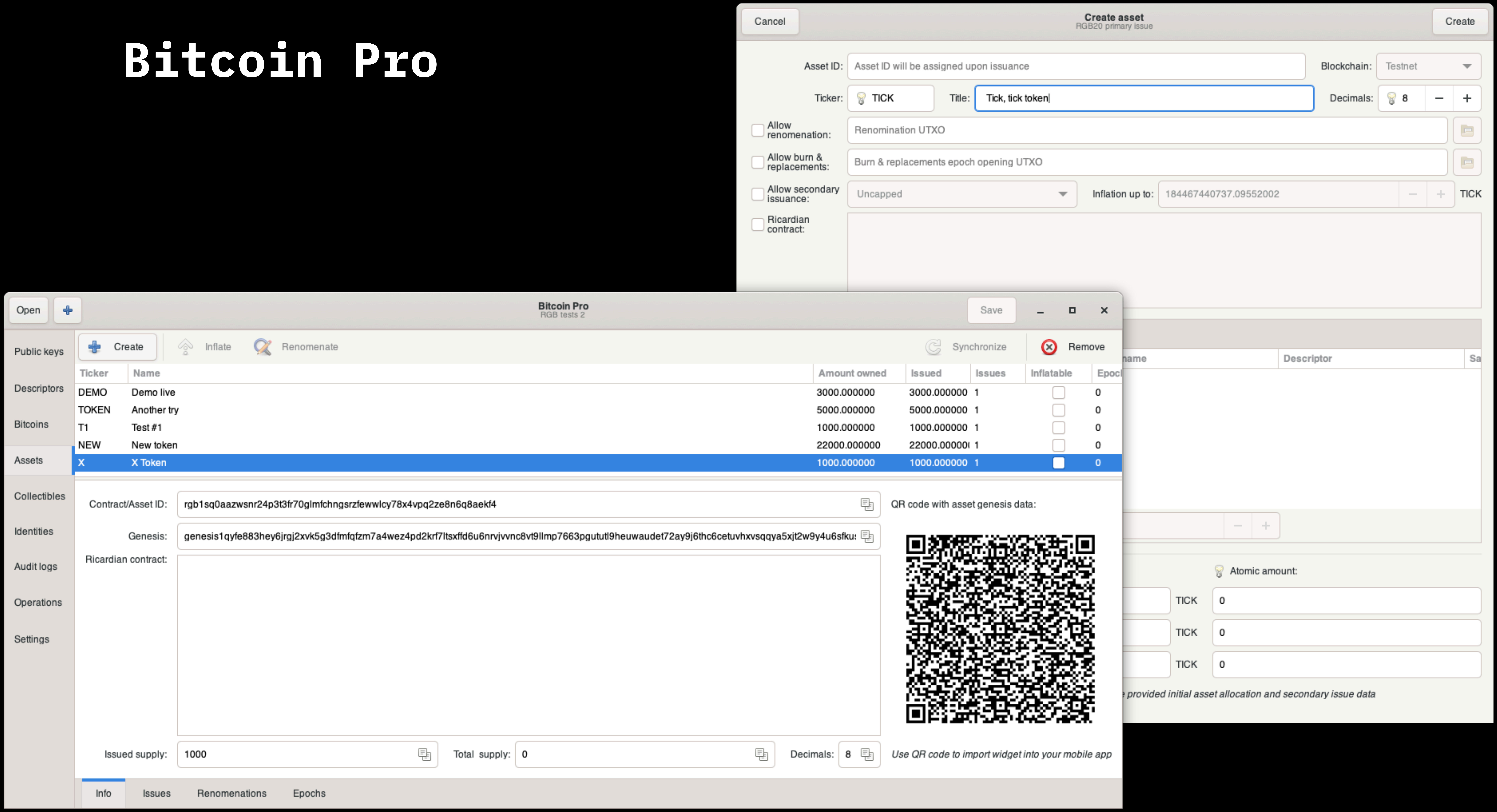
- **Citadel SDK**: MIT-licensed SDK for wallet devs to get RGB & LN running spending just a week on integration

- **MyCitadel** suite of products:
  wallet apps, appliances, private cloud

- …one more thing which we will uncover today

- …even more LN & DEX-related things to come by the end of the year

Bitcoin Pro



Asset ID: Asset ID will be assigned upon issuance

Blockchain: Testnet

Ticker: TICK

Title: Tick, tick token

Decimals: 8

☐ Allow renomenation: Renomination UTXO

☐ Allow burn & replacements: Burn & replacements epoch opening UTXO

☐ Allow secondary issuance: Uncapped

Inflation up to: 184467440737.09552002 TICK

☐ Ricardian contract:

TICK 0

TICK 0

TICK 0

provided initial asset allocation and secondary issue data

Ticker	Name	Amount owned	Issued	Issues	Inflatable	Epoc
DEMO	Demo live	3000.000000	3000.000000	1	☐	0
TOKEN	Another try	5000.000000	5000.000000	1	☐	0
T1	Test #1	1000.000000	1000.000000	1	☐	0
NEW	New token	22000.000000	22000.00000	1	☐	0
X	X Token	1000.000000	1000.000000	1	☐	0

Contract/Asset ID: rgb1sq0aazwsnr24p3t3fr70glmfchngsrzfewwlcy78x4vpq2ze8n6q8aekf4

Genesis: genesis1qyfe883hey6jrgj2xvk5g3dfmfqfzm7a4wez4pd2krf7ltsxffd6u6nrvjvvnc8vt9llmp7663pgututl9heuwaudet72ay9j6thc6cetuvhxvsqqya5xjt2w9y4u6sfku

Ricardian contract:

QR code with asset genesis data:

Use QR code to import widget into your mobile app

Issued supply: 1000

Total supply: 0

Decimals: 8

4:24 PM Thu Mar 18

100%

My Citadel

Default

X Token

1,000.000000 X

Unknown

Bitcoin (testnet)

0.000100 tBTC

Proof of Work

Send

History Balance

Invoice Accept

Balance

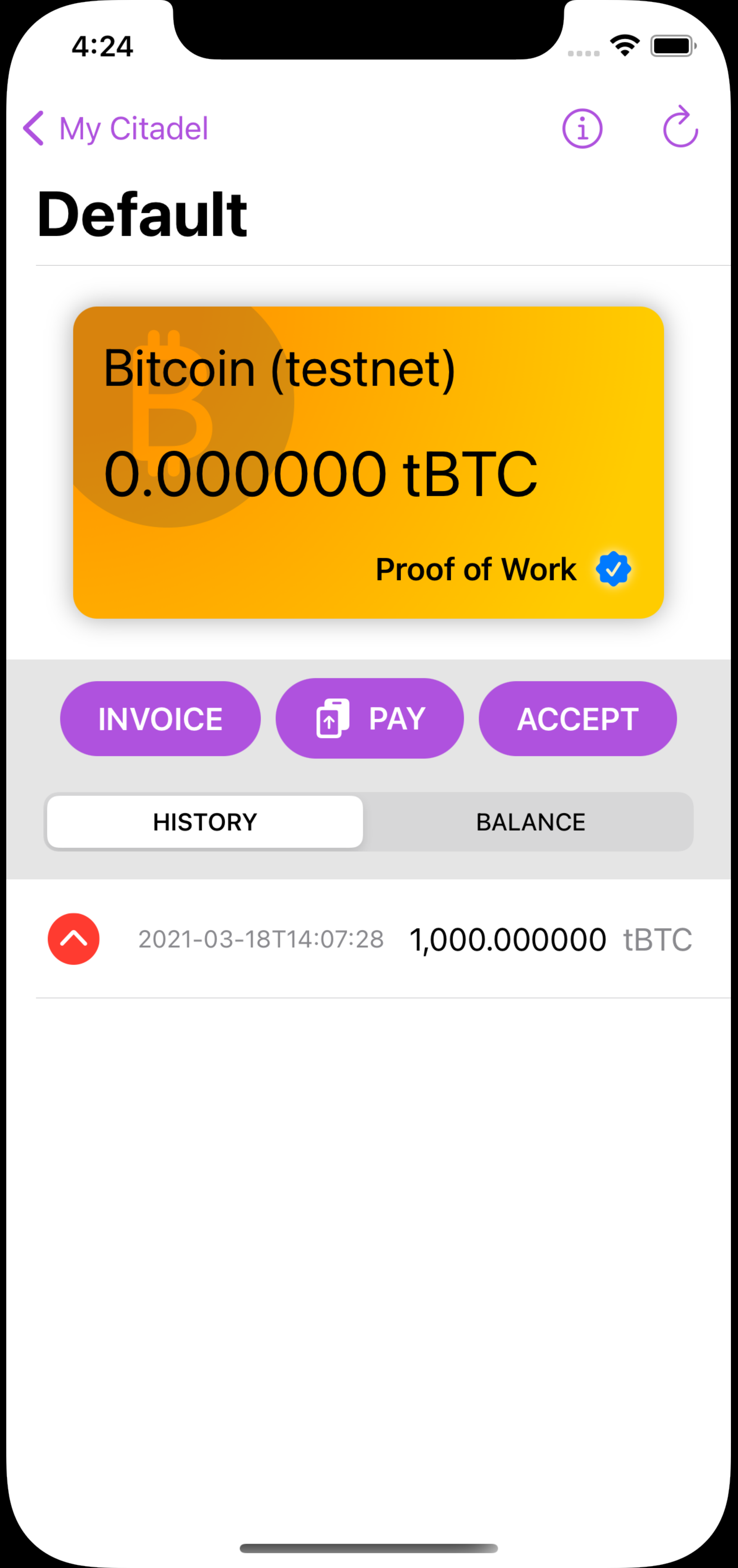
ADDRESS

TB1zswt4lsmevzfqyvldq8rp3vjadewq6we**t48d5c**

Balance: 0.0001 tBTC

3680829e9e50cc9a75d01ce855c7701c4b830570a66610db564ce31247ef77eb 0.000100 tBTC

Output number: 0



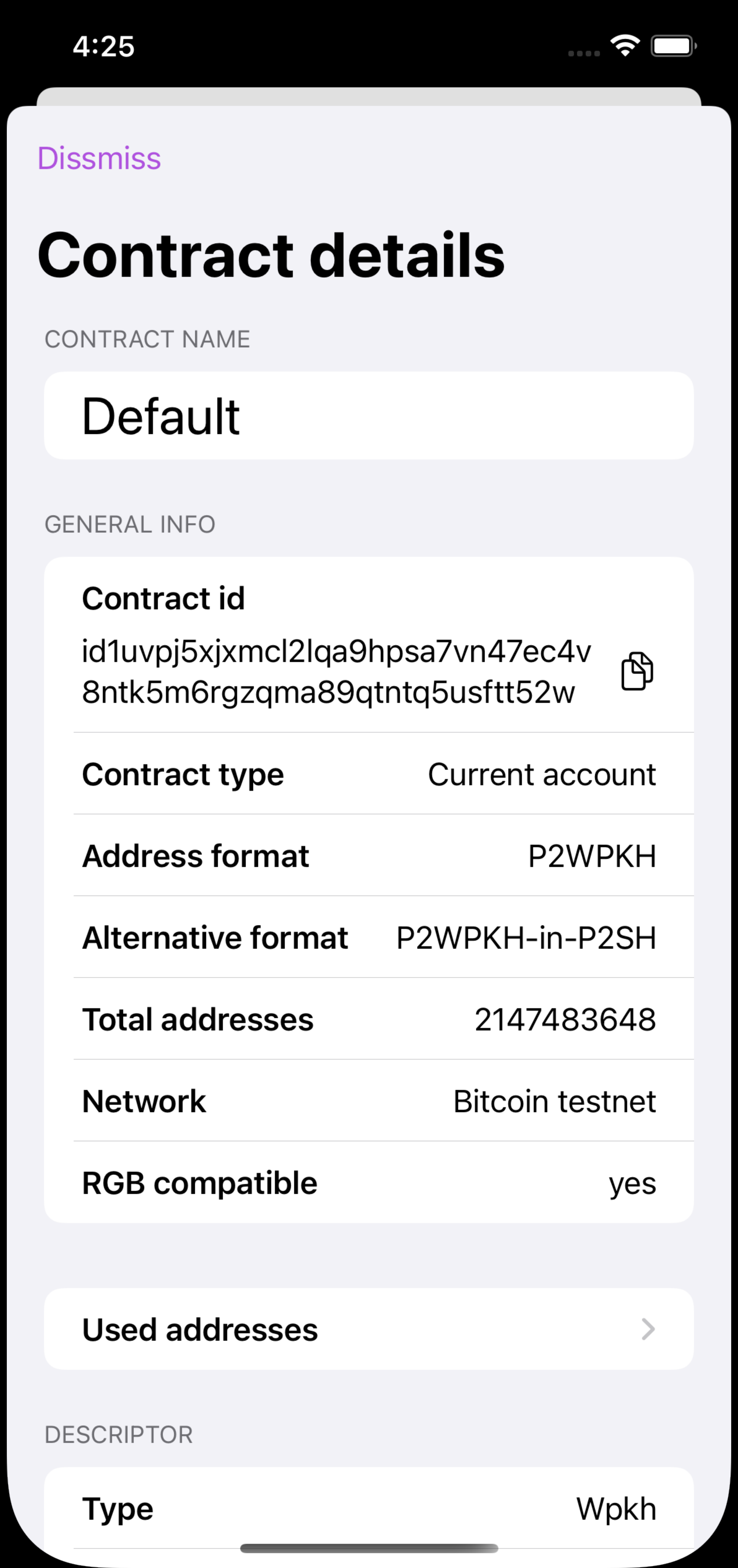
Default

Bitcoin (testnet)

0.000000 tBTC

Proof of Work

2021-03-18T14:07:28 1,000.000000 tBTC



Contract details

CONTRACT NAME

Default

GENERAL INFO

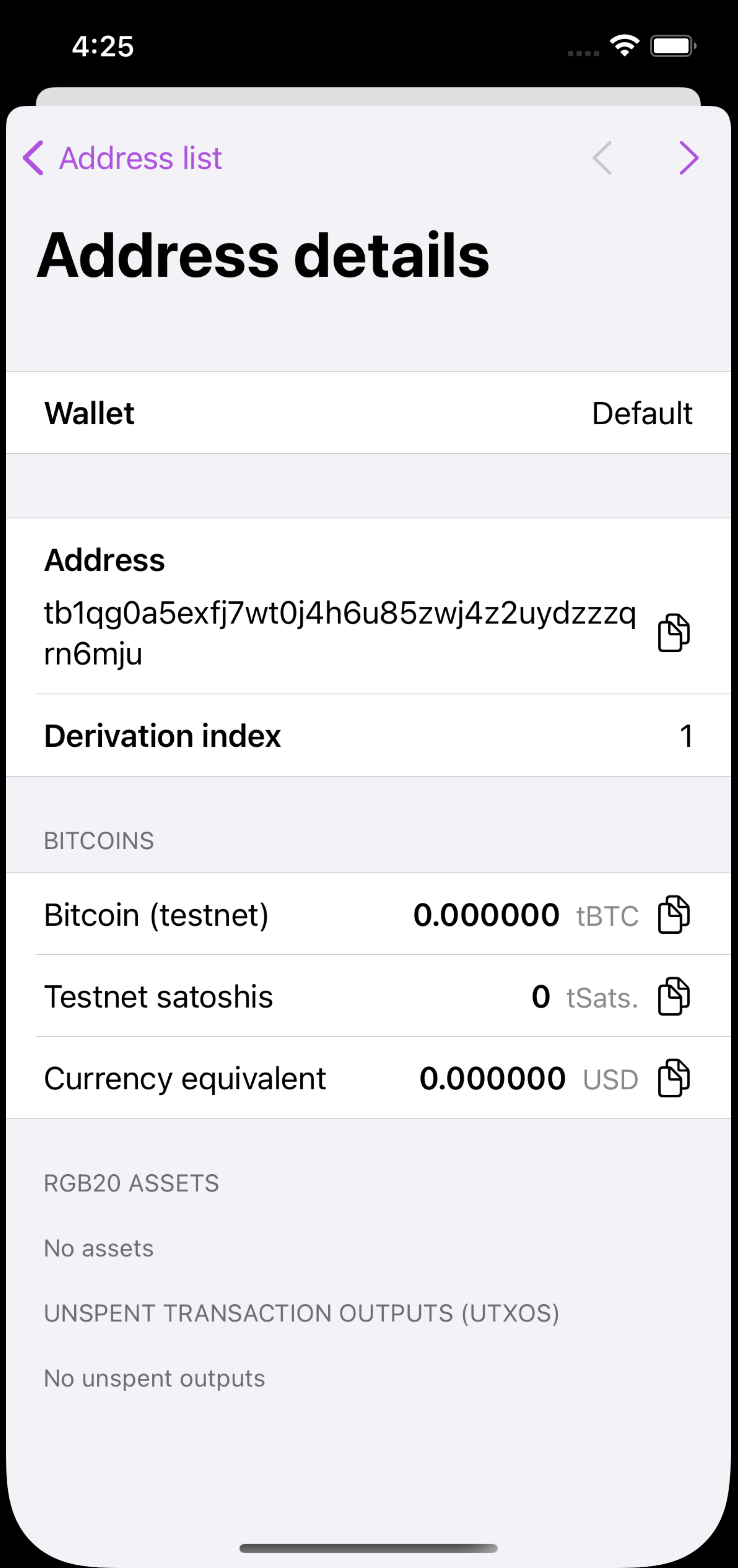
Contract id
id1uvpj5xjxmcl2lqa9hpsa7vn47ec4v8ntk5m6rgzqma89qtntq5usftt52w

Contract type	Current account
Address format	P2WPKH
Alternative format	P2WPKH-in-P2SH
Total addresses	2147483648
Network	Bitcoin testnet
RGB compatible	yes

Used addresses ›

DESCRIPTOR

Type	Wpkh



Address details

Wallet	Default

Address
tb1qg0a5exfj7wt0j4h6u85zwj4z2uydzzzqrn6mju

Derivation index	1

BITCOINS

Bitcoin (testnet)	0.000000 tBTC
Testnet satoshis	0 tSats.
Currency equivalent	0.000000 USD

RGB20 ASSETS

No assets

UNSPENT TRANSACTION OUTPUTS (UTXOS)

No unspent outputs

Citadel SDK

- **Single point of integration** for all cool stuff
  (RGB, LN, Taproot, miniscript, multisigs & descriptors; DLC & DEX in the future …)

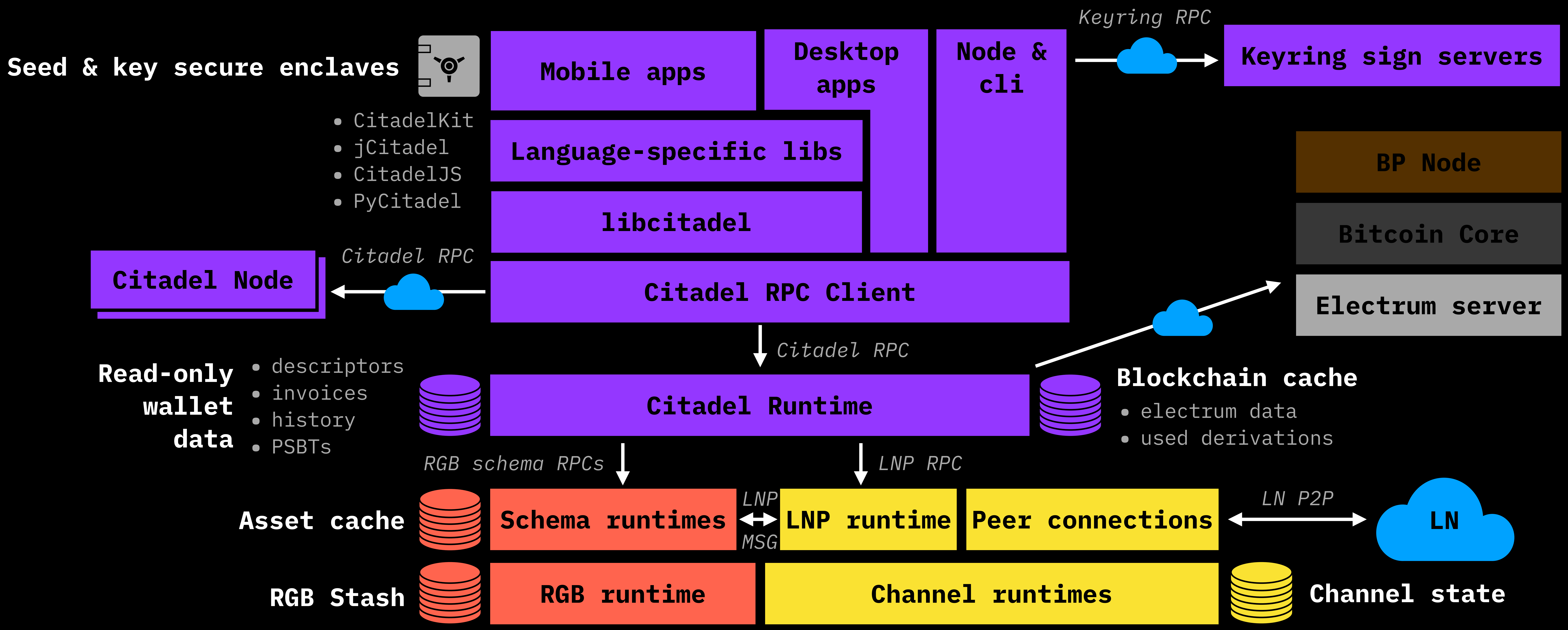
- **Simple API** hiding complexity of RGB and LN nodes management,
  Electrum integration & and wallet data storage
  (call just one method for RGB or LN payment with an invoice)

- **Native libraries** with OOP API for:
  Apple platforms, Android & Java$^{\text{WIP}}$, NodeJS$^{\text{WIP}}$, Python$^{\text{WIP}}$

- **MIT-licensed** with tech **support** & integration services by Pandora Core AG

- Can be used in **personal/enterprise** setups with shared wallets
  (across devices or company employees) using
  self-hosted **MyCitadel Box** or **private cloud-hosted MyCitadel Node** by Pandora Core AG
  with revenue sharing for wallet development companies

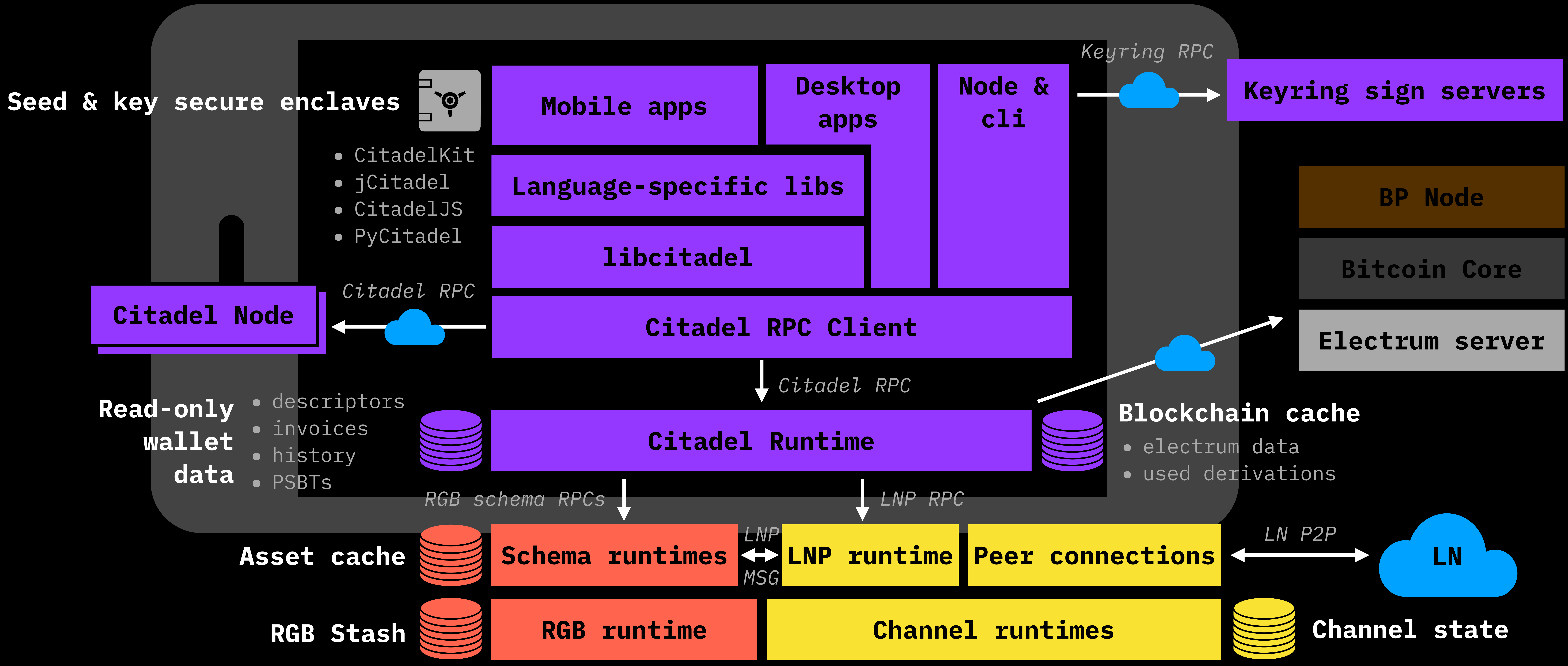
Wallet architecture (based on Citadel SDK)



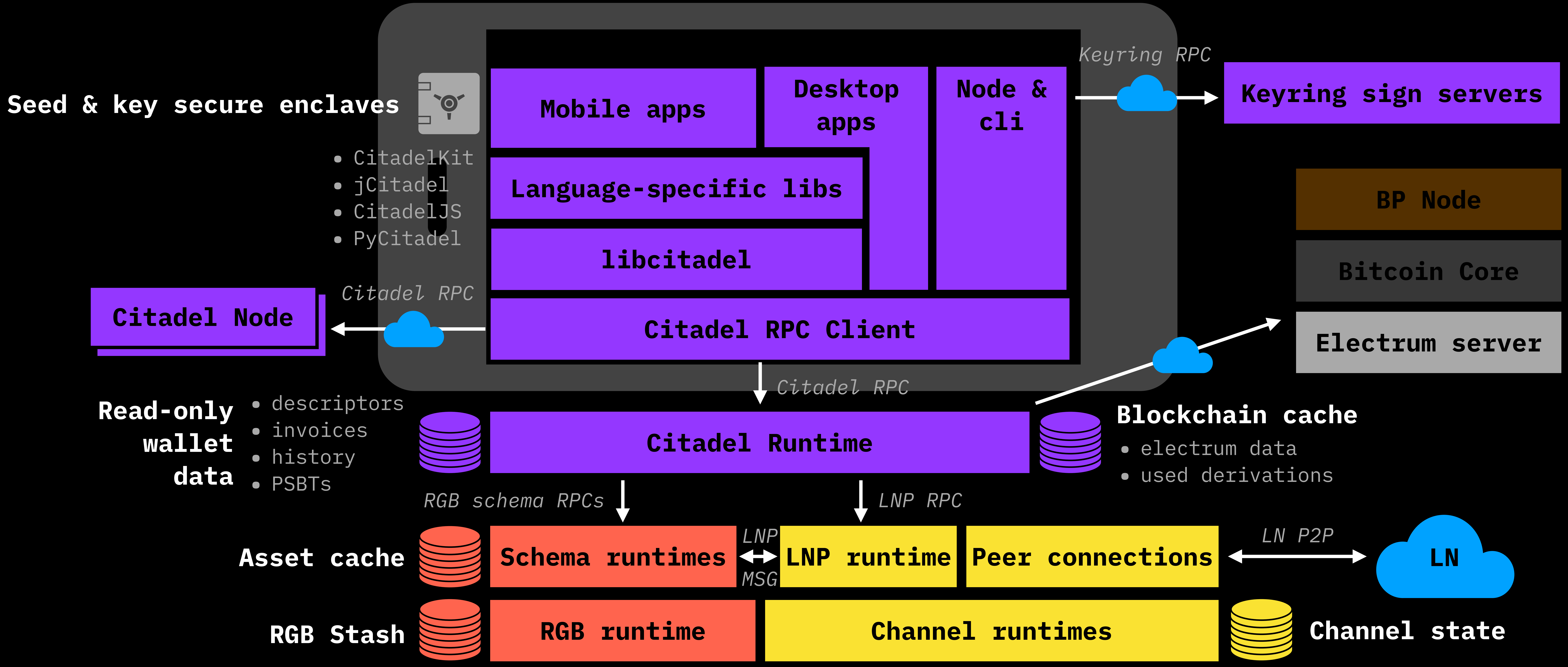
Everything can run on mobile!

Keyring RPC
Seed & key secure enclaves
Mobile apps
Desktop apps
Node & cli
Keyring sign servers
• CitadelKit
• jCitadel
• CitadelJS
• PyCitadel
Language-specific libs
BP Node
libcitadel
Bitcoin Core
Citadel Node
Citadel RPC
Citadel RPC Client
Electrum server
Citadel RPC
Read-only wallet data
• descriptors
• invoices
• history
• PSBTs
Citadel Runtime
Blockchain cache
• electrum data
• used derivations
RGB schema RPCs
LNP RPC
LN P2P
Asset cache
Schema runtimes
LNP
MSG
LNP runtime
Peer connections
LN
RGB Stash
RGB runtime
Channel runtimes
Channel state

…or with external RGB & LN nodes



…or just as a client



Keyring: signature server infrastructure

- Manage **multisig policies** for a hot custody
- …including **enterprise** + **personal/family setups**
- 100% **PSBT** compatible, **Taproot** & MuSig-ready
- **RGB** compatible (and supports pay-to-contract key tweaks)
- **Part of Citadel suite**: works well with the Citadel SDK and MyCitadel wallet, hardware & private cloud setups
- Under development: expected **by the end of year**

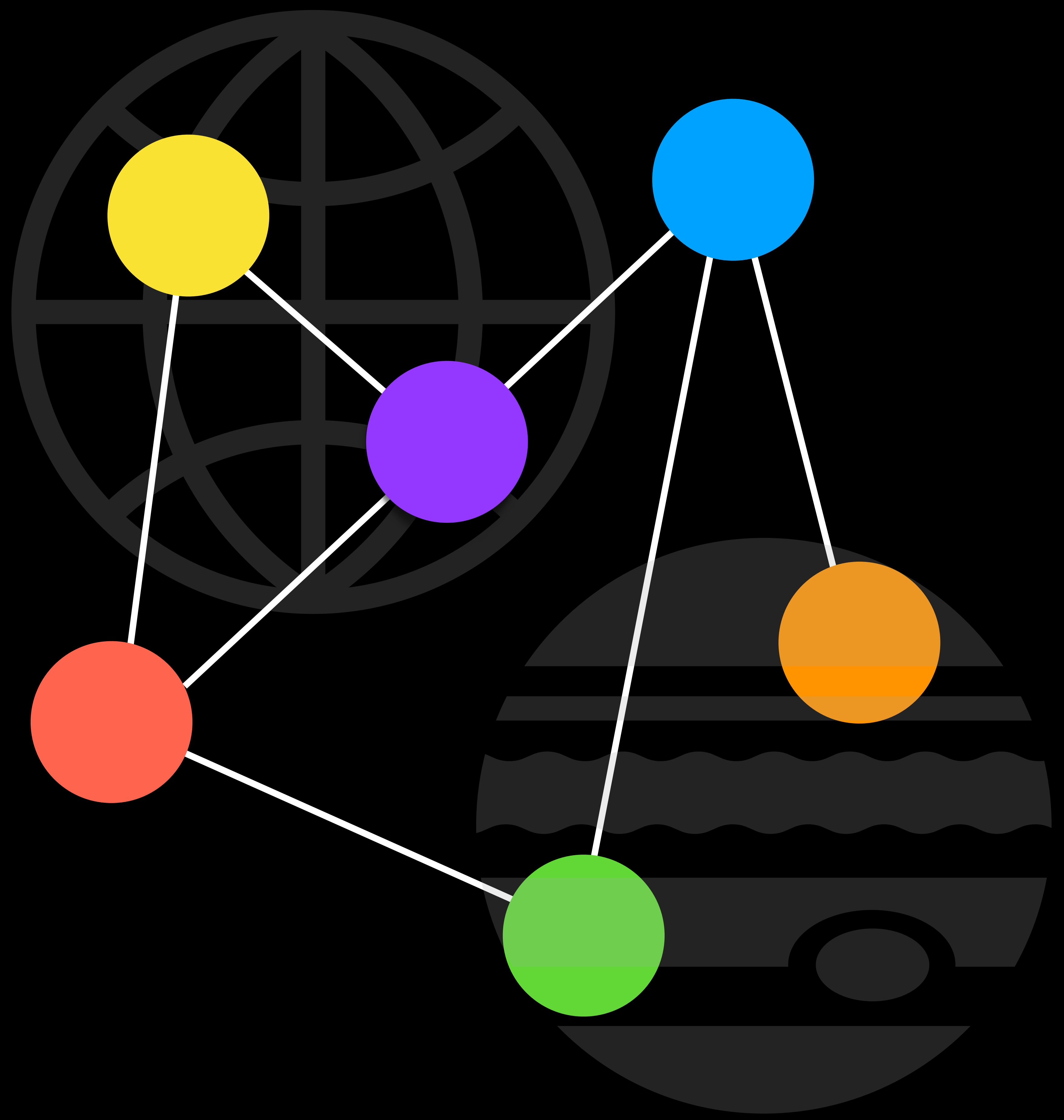
Architecture: Internet2 by LNP/BP Association

- Everything made of modular compact **microservices**:
  you can distribute your software across **mobile devices & servers**,
  including **cloud**, **Docker**, Kubernets the way you like

- Talking to each other over binary encrypted LN-style protocol
  on top of **ZeroMQ**: no old, slow and insecure JSON RPCs etc,
  no HTTP or plain text data

- All business logic is written in **Rust**:
  - Blazingly-fast
  - Deterministically secure and highly robust in runtime

- API is wrapped in language-specific **class libraries with good OOP abstractions**



Internet2

github.com/internet2-org

When Citadel?

- **Citadel SDK** technology preview available today on github.com/MyCitadel
  - main *Citadel runtime* implementing 100% of business logic for RGB, miniscript & multisigs (LN, Taproot expected by June)
  - C- and Swift class library (*libcitadel* & *CitadelKit*) NodeJS, Java & Python are expected by June and end of summer
  - Wallet developers technical support starts mid-summer (upon LN completion)
- **MyCitadel Node** for self-hosting or enterprise setups at v0.1 beta
- **MyCitadel Box** – hardware appliance running MyCitadel Node, in cooperation with Nodl – expected by the end of summer
- **MyCitadel Cloud** (in cooperation with Nodl) – this autumn

…and one more thing

–Johnny Appleseed

Presenting

RGBex.io

The first RGB explorer

… and it is not a “blockchain explorer”: no chain analysis, tracking etc.
Just publishing & sharing information about your assets

Demo

Works best with Bitcoin Pro (issuance) & MyCitadel wallet (payments)

RGBex is

- Playground for RGB assets, including NFTs
- Playground for Bifrost infrastructure experiments
- Playground for RGB-based identity management

We are hiring

- Cool **rust** devs: **LNP/BP Association**
  for working on *LNP Node*, *NFTs*, *identity*, *LN DEX*, *BP Node*
  Taproot, *PSBT2*, *descriptors & miniscript*
  Internet2 protocols
  work with Blockstream, Square Crypto engineers, TLS creator

- **Android dev**: **MyCitadel** wallet
  with Kotlin & Jetpack Compose experience

We are fundraising

- **LNP/BP Association** donations for 2021
  - private
  - corporate
  - LNP/BP membership
  - LNP/BP memorable tokens (zero-value indeed, just a memento :)
  - will have a separate presentation for 2021 Roadmap
  - Bitfinex/Tether Inc, Fulgur Ventures and Pandora Core were major contributors in 2020 & Q1 2021, but more scale & resilience is desired for the rest of 2021

- **Pandora Core AG** investments for further product development, marketing & support:
  - Citadel & MyCitadel suits (SDK, node, wallets, appliance, cloud, custody)
  - Bitcoin Pro enterprise
  - future (not yet) uncovered DEX-related products (joint project with **HodlHodl**)

- **Federation** participation to run RGB-wrapped decentralised-issued non-custodial* Bitcoin (RGB30)
  - Exchanges, wallets & cool tech guys
  - More programmability & privacy to Bitcoin!

Contact Olga Ukolova for details (Telegram: @dr_ukolova, E-mail: ukolova@lnp-bp.org or ukolova@pandoracore.com)