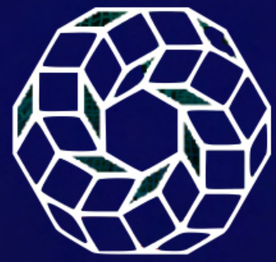
LNP/BP Standards Association

RGB smart contracts

Olga Ukolova, M.D.
Board member of LNP/BP Standards Association
Co-Founder of Pandora Prime SA



PANDORA PRIME

DISCLAIMER!

- High toxicity content
- Cypherporn, cryptonudity
- 1984+
- Not suitable for pregnant children
- May contain traces of black magic code

Agenda

- Why RGB?
- What is RGB?
- What RGB NOT?
- What is there to RGB?
- WEN RGB?
- Who RGB?
- How to support RGB?

Part I

Why RGB?

Digital smart contracts

Expectation

- I am sovereign
- My data - my Citadel
- My peers = my tribe = my fam

Reality

- Govern me harder Daddy
- We got HREKT (Hacked and REKT)
- Chainanalysis is my best friend

Decentralized financial revolution (DeFi)

Expectation

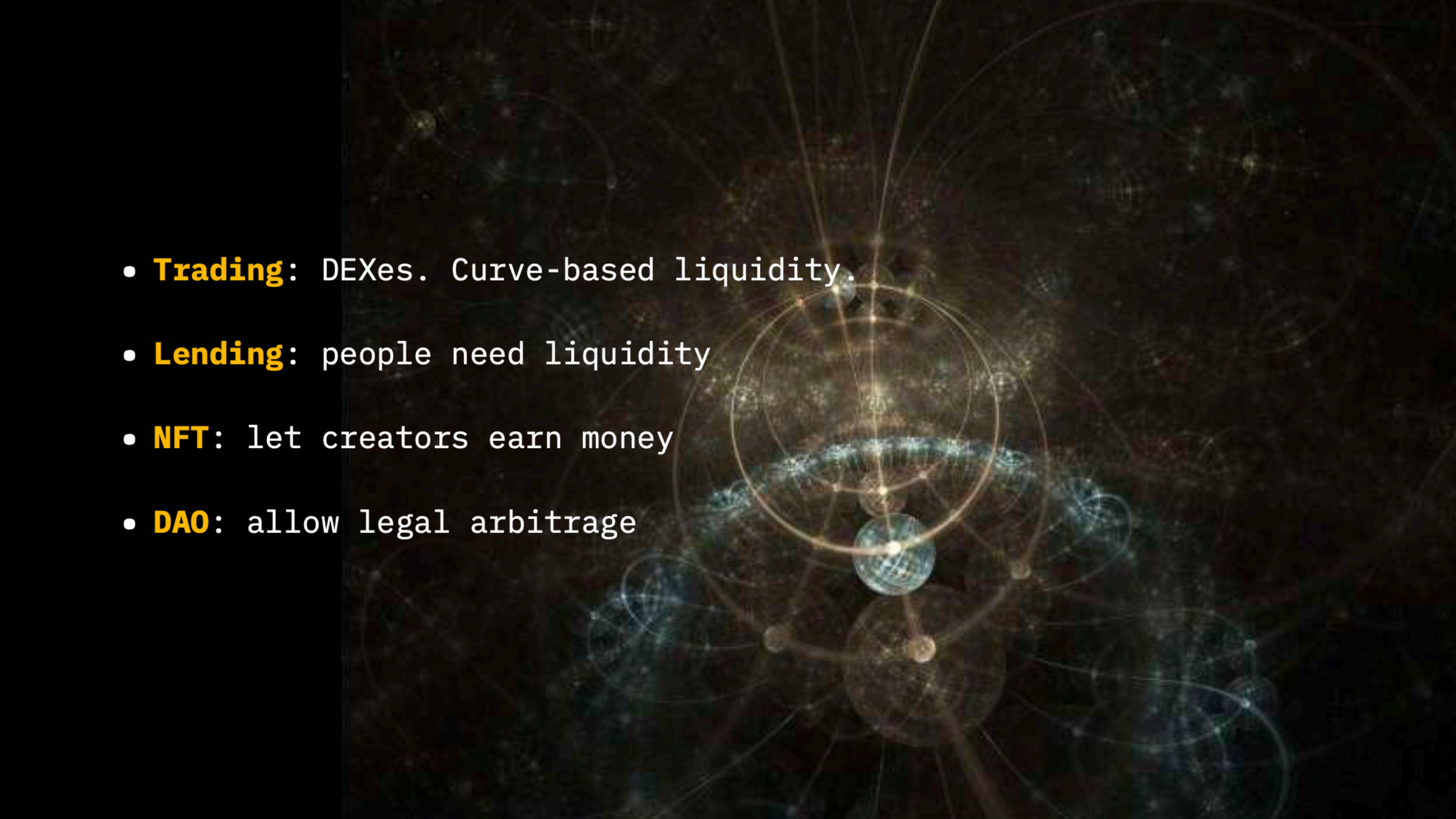
- We will kill VISA/MasterCard
- We will kill banks
- We will kill centralized exchanges
- We will create trustless synthetic assets
- We use tokens for creating incentives

Reality

- **No scalability**:
  cryptokitties kill it all
- **No security**:
  constant hacks
- **Trust to developers**:
  exit scams are common
- **Extremely high transaction cost**
- **Tokenomics of speculations**

But why should we even care?

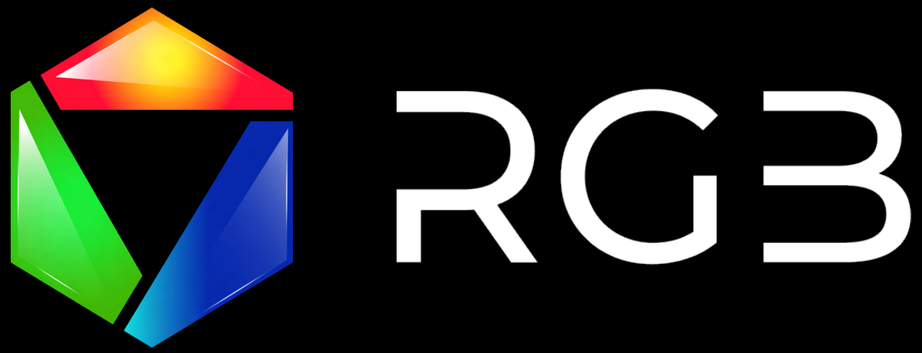

There is
a need
for
DeFi



- **Trading**: DEXes. Curve-based liquidity.
- **Lending**: people need liquidity
- **NFT**: let creators earn money
- **DAO**: allow legal arbitrage

What is needed?

- Smart-contract system
- Private but verifiable
- Resistant to censorship but open for fair participation
- Scalable but without bloating the blockchain
- Fast but able to process big massives of data

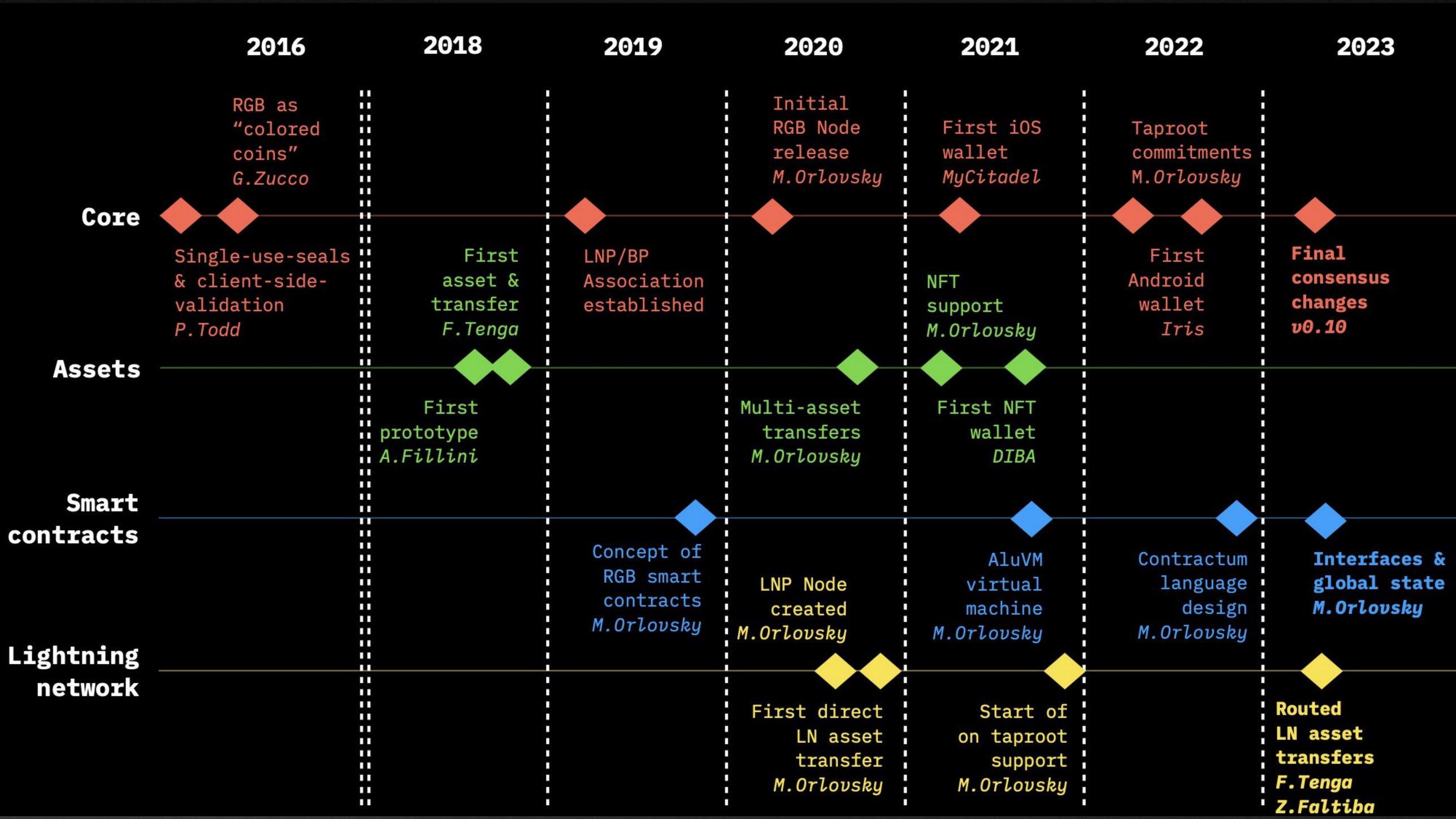


RG3

Part II

What is RGB?

RGB is scalable Turing-complete smart contracts for Bitcoin,
able to run on Lightning Network
zk-based, with strong privacy


2016
2018
2019
2020
2021
2022
2023
Core
Assets
Smart contracts
Lightning network
RGB as "colored coins" G.Zucco
Single-use-seals & client-side-validation P.Todd
First asset & transfer F.Tenga
First prototype A.Fillini
LNP/BP Association established
Concept of RGB smart contracts M.Orlovsky
Initial RGB Node release M.Orlovsky
Multi-asset transfers M.Orlovsky
LNP Node created M.Orlovsky
First direct LN asset transfer M.Orlovsky
First iOS wallet MyCitadel
NFT support M.Orlovsky
First NFT wallet DIBA
AluVM virtual machine M.Orlovsky
Start of on taproot support M.Orlovsky
Taproot commitments M.Orlovsky
First Android wallet Iris
Contractum language design M.Orlovsky
Final consensus changes v0.10
Interfaces & global state M.Orlovsky
Routed LN asset transfers F.Tenga Z.Faltiba

RGB IS:

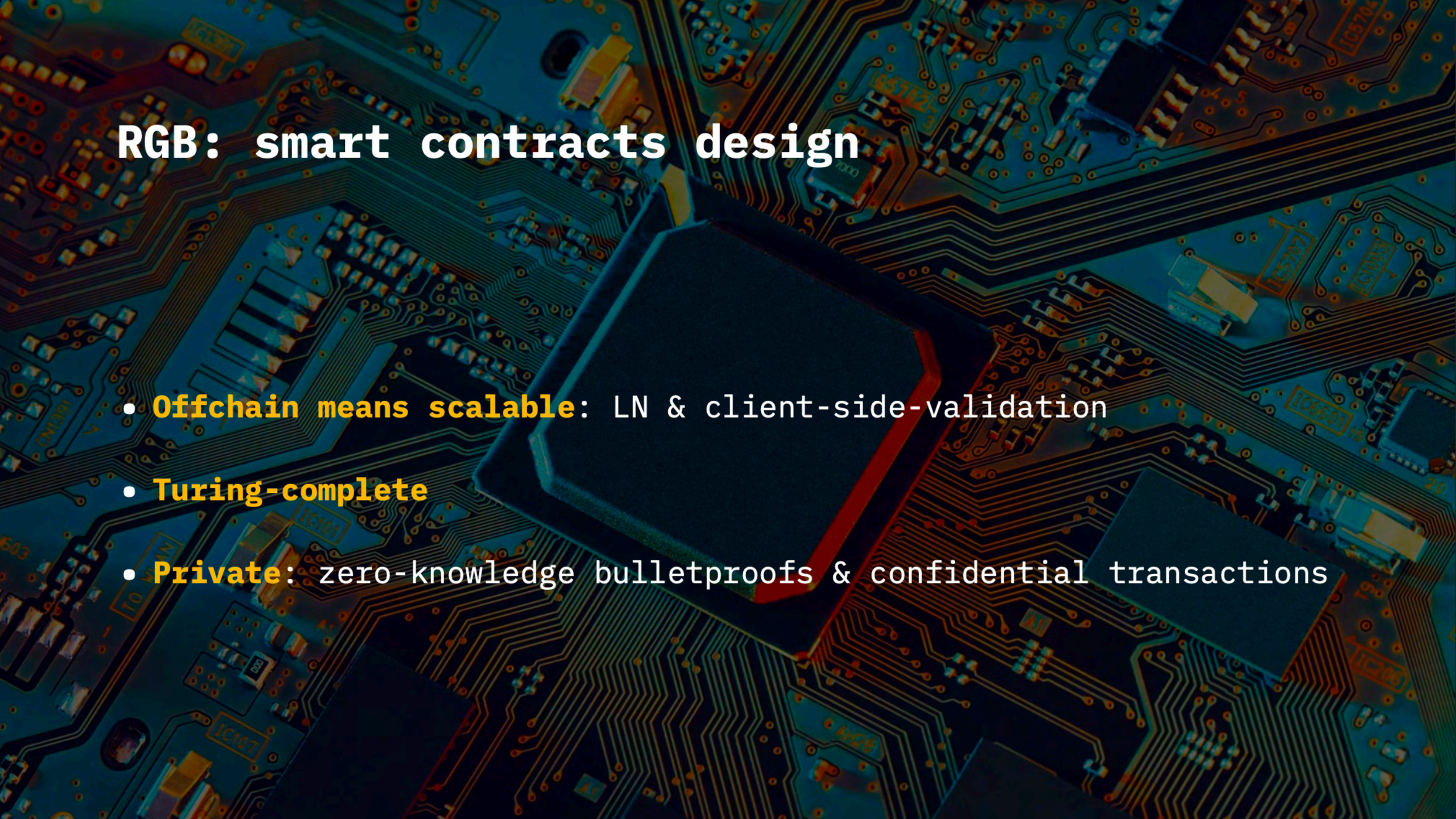
- smart-contract system*
- DAG
- No native token
- Private
- The only tech that works over Lightning Network
- Blockchain agnostic

***Smart contract** - *is the way to enforce the fulfilment of a certain agreement between humans without an external centralized agency (military, government, court etc)*

RGB paradigms:

- **Client-side validation** - all the data is kept outside of the bitcoin transactions, i.e. bitcoin blockchain or lightning channel state
- **Single-use seals** - abstract mechanism to prevent double-spends
- **Cryptographic commitments**
- **Strict encoding**

https://blackpaper.rgb.tech/general-information/2.-protocol-design/2.2.-design-overview



RGB: smart contracts design

- **Offchain means scalable**: LN & client-side-validation
- **Turing-complete**
- **Private**: zero-knowledge bulletproofs & confidential transactions

RGB: smart contracts using client-side validation

Interface

Contract

=

Schema

Requirements for the contract state + contract business logic

"Class" in terms of OOP

+

Interface implementation

Bindings to human & wallet-readable names from the interface

Implementation of an interface/trait for a class/struct

+

Genesis

Initial setup of the contract state

Instance of a class created by the class constructor

Contract components overview:

Contract components	Meaning	OOP terms	Ethereum terms
Interface	*Contract semantics*	Interface (Java), trait (Rust), protocol (Swift)	ERC* standards
Schema	*Contract business logic*	Class	Contract
Interface implementation	*Mapping semantics to business logic*	Impl (Rust), Implements (Java)	ABI
Genesis	*Initial contract state*	Class constructor	Contract constructor

	AluVM	Bitcoin script	EVM, kEVM, IELE	WASM	JVM, CLR	LLVM
Type	Register	Stack	Stack	Stack	Stack	Stack
Random memory access	No	No	No	Yes	Yes	Yes
Dynamic memory allocations	No	Yes	Yes	Yes	Yes	Yes
I/O operations	No	No	No	Via extensions	Yes	Yes
Turing completeness	Yes (bounded)	No	Yes (bounded)	Yes	Yes	Yes
Static analysis	Simple	Simple	Complex	Hard	Hard	Hard
Sandboxing	Always	Always	Always	Poor	No native	No native
Runtime environment	Any sandboxed	UTXO blockchain	Account-based blockchain	Internet	OS	Compiler
Library code immutability	Yes	No libraries	Yes	No	No	No
Undefined behavior (UB)	Impossible	Possible	Possible	Possible	Possible	Possible

RGB vs Alternatives

https://blackpaper.rgb.tech

Parameter	RGB	Liquid	Ethereum, RSK etc	Stacks
Native currency	✅ BTC	⚠️ LBTC (federated peg)	🚫 ETH	🚫 ?
Requires token	✅ No	✅ No	🚫 Yes (except RSK)	🚫 Yes
Issues token	✅ No	✅ No	🚫 Yes	🚫 Yes
Gas	✅ No	✅ No	🚫 Yes	?
Non-token smart contracts	✅	🚫	✅	?
Data network for NFTs and attachments	✅ Storm on LN paid in sats	🚫	⚠️ IPFS (no incentivation)	?
Support for arbitrary structured data	✅	🚫	✅	🚫
Virtual machine	Bitcoin Script + AluVM	Bitcoin Script	EVM, sometimes EWASM	?
Turing completeness	✅	🚫	✅	?
Separation of state from ownership	✅	🚫	🚫	🚫
Client-side-validation (scalability & privacy)	✅	🚫	🚫	🚫
Zero knowledge	✅ Bullet proofs	✅ Range proofs	⚠️ n/a, maybe STARKs	🚫
Breaks transaction graph & chainanal	✅	🚫	🚫	🚫
Released / used in production	✅	✅	✅	✅

RGB

- In development since 2016
- ~1 mln of external funding,
  ~500k of developer funds
- Original concept by Peter Todd & Giacomo Zucco
- Cross-industry effort
  (5+ competing companies involved)
- Released Jul 2022, alpha in 2019, beta in 2021
- Smart contracts
- Can do DeFi (DEX, AMM, algorithmic stablecoins etc)
- Can do NFTs, DAOs etc

Taro

COPYCAT

Internal name was CMYK

- Announced this year
- >80m of funding
- RGB copycat
- Internal Lightning Labs project
- Alpha in 2022
- Just tokens and nothing more

Part III

What RGB is NOT?

RGB is NOT:

- blockchain/sidechain/[whatever]chain
- ZK-rollup
- token protocol
- network

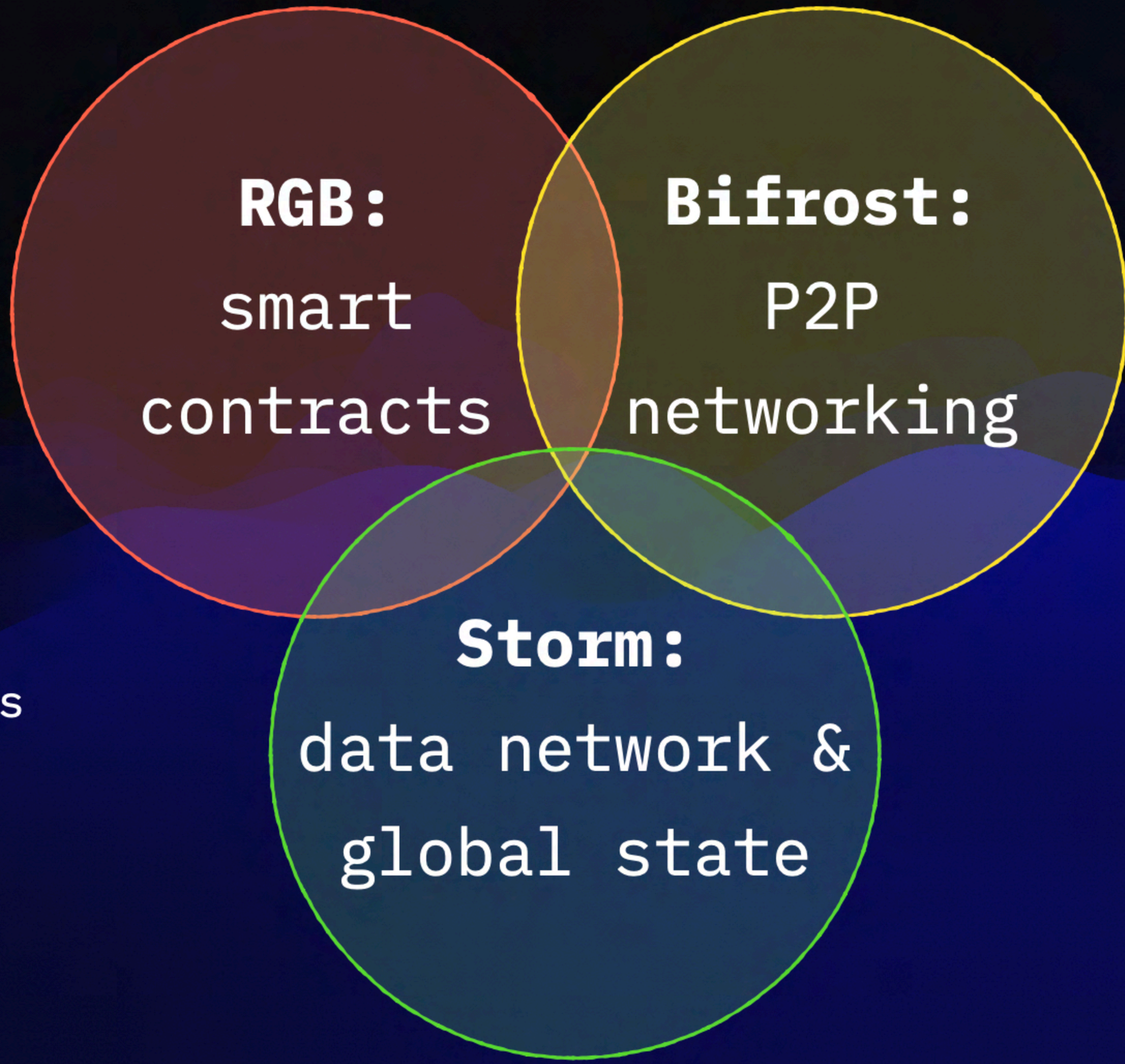
Sounds like Black Magic

Part IV

How to #BiFi with RGB?

LNP/BP for Bitcoin Finance

- Assets
- DEX
- Liquidity pools
- AMM & algorithmic stable coins
- futures/options



LNP/BP Nodes

RGB Node

Smart contract validation & state RPC

BP Node

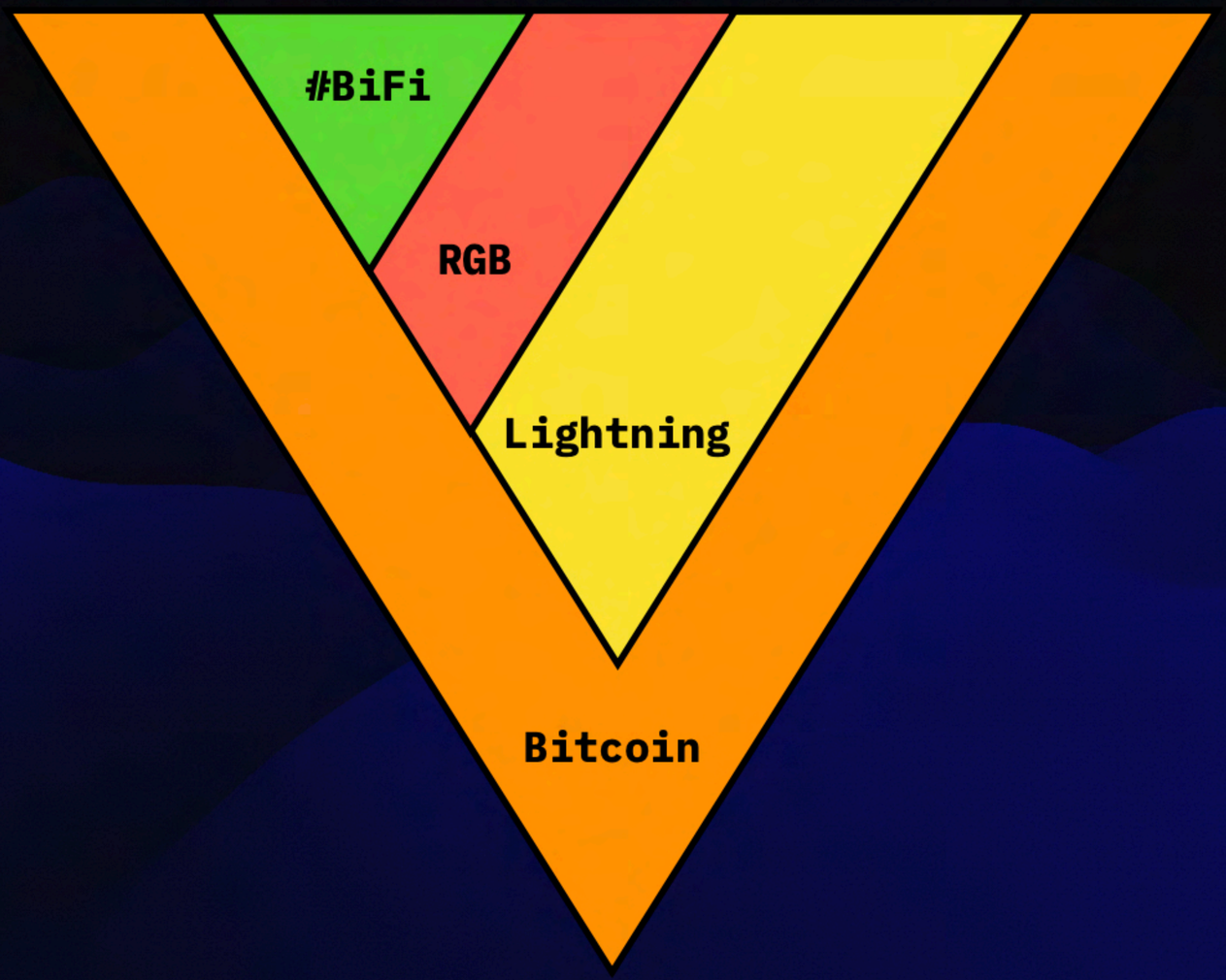
Bitcoin indexing node (faster & more efficient than Electrum server)

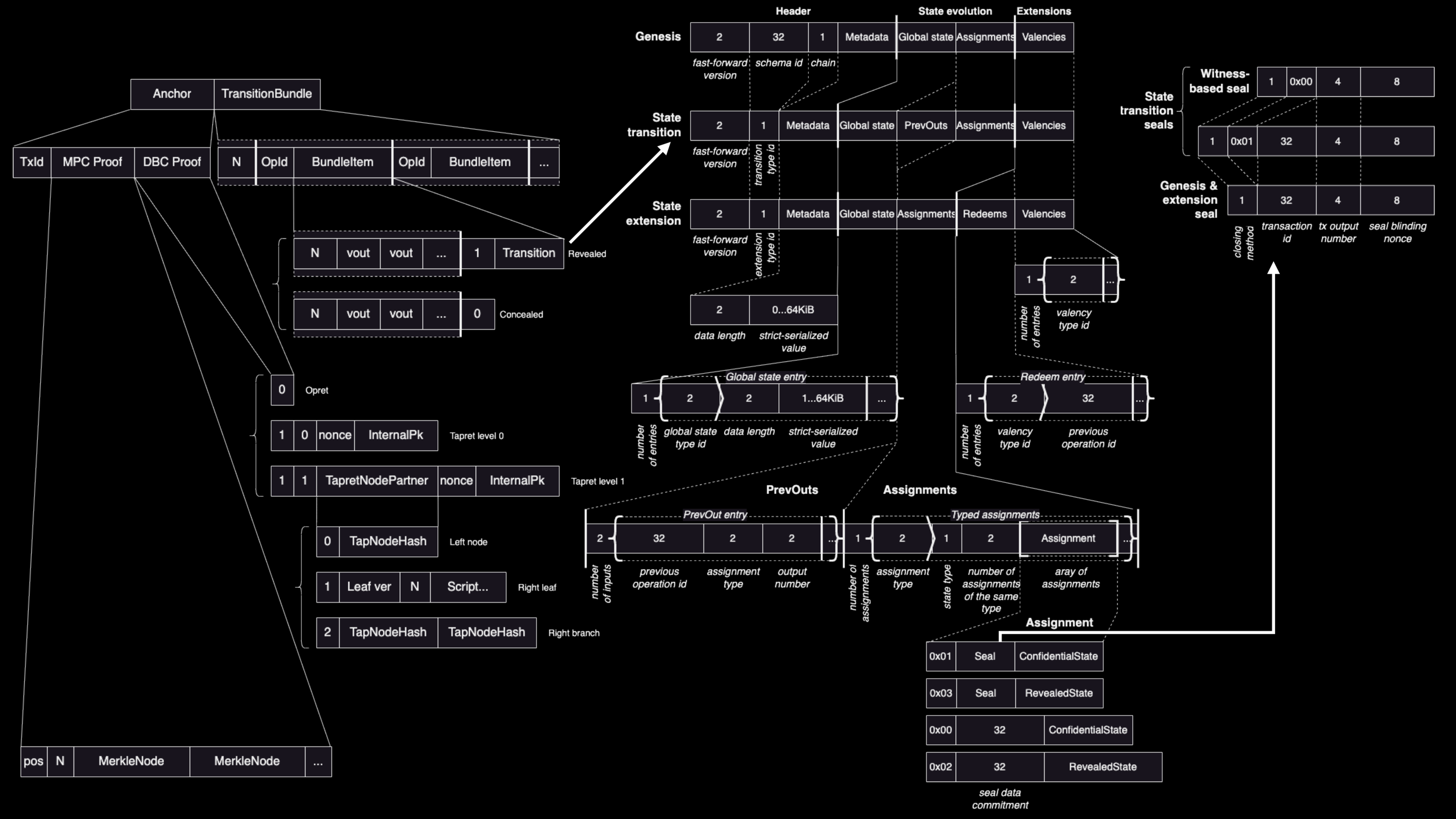
LNP Node

Lightning node supporting RGB, Taproot, DEX, BiFi

Storm Node

Decentralized storage, messaging & search


#BiFi
RGB
Lightning
Bitcoin


Anchor
TransitionBundle
TxId
MPC Proof
DBC Proof
N
OpId
BundleItem
OpId
BundleItem
...
N
vout
vout
...
1
Transition
Revealed
N
vout
vout
...
0
Concealed
0
Opret
1
0
nonce
InternalPk
Tapret level 0
1
1
TapretNodePartner
nonce
InternalPk
Tapret level 1
0
TapNodeHash
Left node
1
Leaf ver
N
Script...
Right leaf
2
TapNodeHash
TapNodeHash
Right branch
pos
N
MerkleNode
MerkleNode
...
Header
State evolution
Extensions
Genesis
2
32
1
Metadata
Global state
Assignments
Valencies
fast-forward version
schema id
chain
State transition
2
1
Metadata
Global state
PrevOuts
Assignments
Valencies
fast-forward version
transition type id
State extension
2
1
Metadata
Global state
Assignments
Redeems
Valencies
fast-forward version
extension type id
2
0...64KiB
data length
strict-serialized value
1
2
...
number of entries
valency type id
Global state entry
1
2
2
1...64KiB
...
number of entries
global state type id
data length
strict-serialized value
Redeem entry
1
2
32
...
number of entries
valency type id
previous operation id
PrevOuts
PrevOut entry
2
32
2
2
...
number of inputs
previous operation id
assignment type
output number
Assignments
Typed assignments
1
2
1
2
Assignment
...
number of assignments
assignment type
state type
number of assignments of the same type
aray of assignments
Assignment
0x01
Seal
ConfidentialState
0x03
Seal
RevealedState
0x00
32
ConfidentialState
0x02
32
RevealedState
seal data commitment
State transition seals
Witness-based seal
1
0x00
4
8
1
0x01
32
4
8
Genesis & extension seal
1
32
4
8
closing method
transaction id
tx output number
seal blinding nonce

Part V

WEN RGB?

RGB protocol was released on the 13th of June 2022

(protocol freeze, final public preview, v0.8)

RGB v0.10 release progress

	Readiness	Released	Presentation
Consensus (Core lib)	✅	9 Feb	Part 1
Standard library	✅	9-10 March	Part 2
Wallet library	✅	22 March	Part 3
Command-line tool	✅	10 April	Part 4

RGB library stack for app devs

Server-side Desktop Mobile

Lightning, networking, always online

RGB Node

RGB Tools

High-level APIs

RGB (rgb-contracts)

WASM/Web Exchanges

FS & I/O

PSBT & invoices

RGB Wallet

Custom wallet libs

Contract APIs

RGB Standard Lib

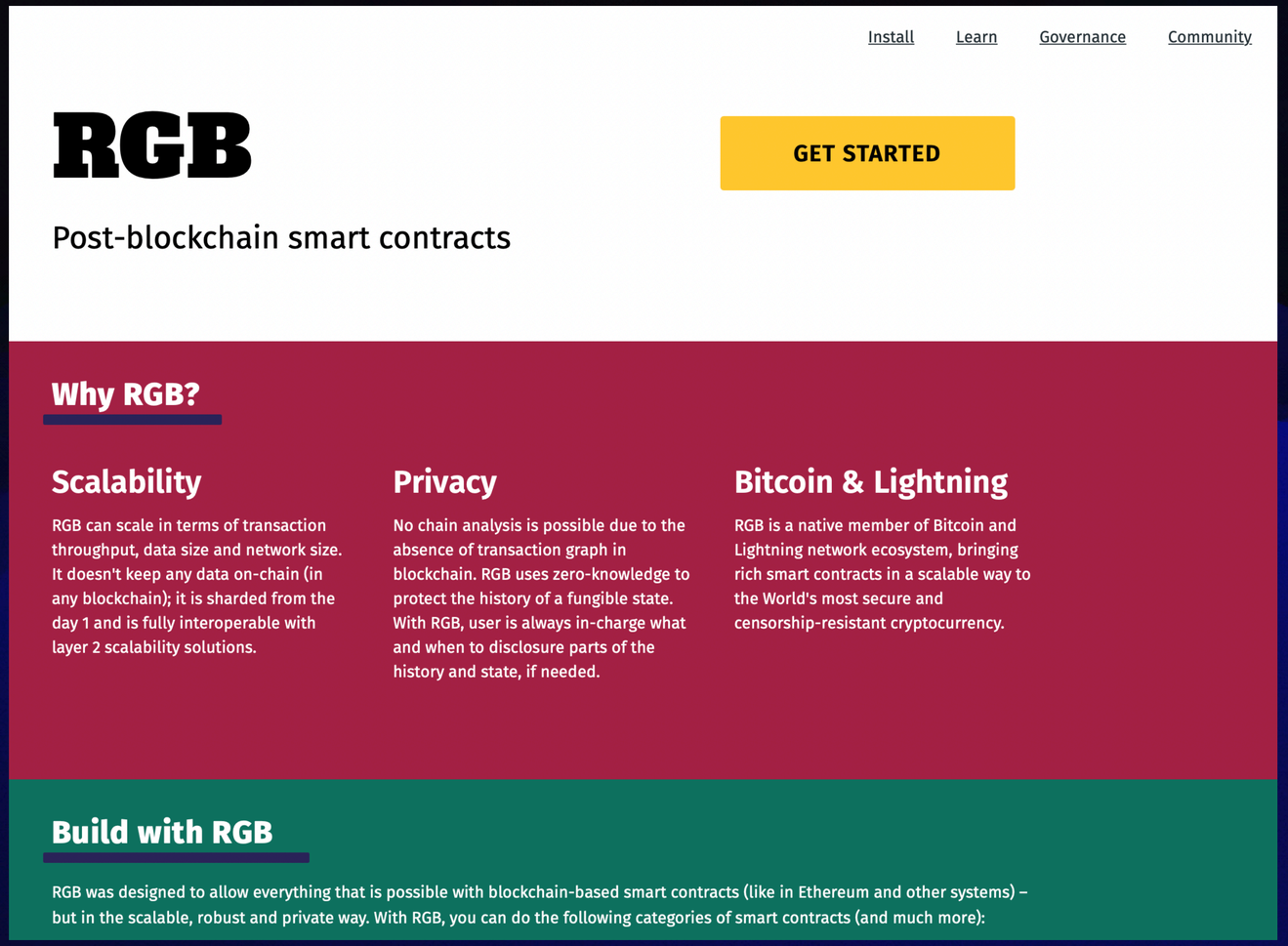
Consensus

Consensus, validation

RGB Core Lib

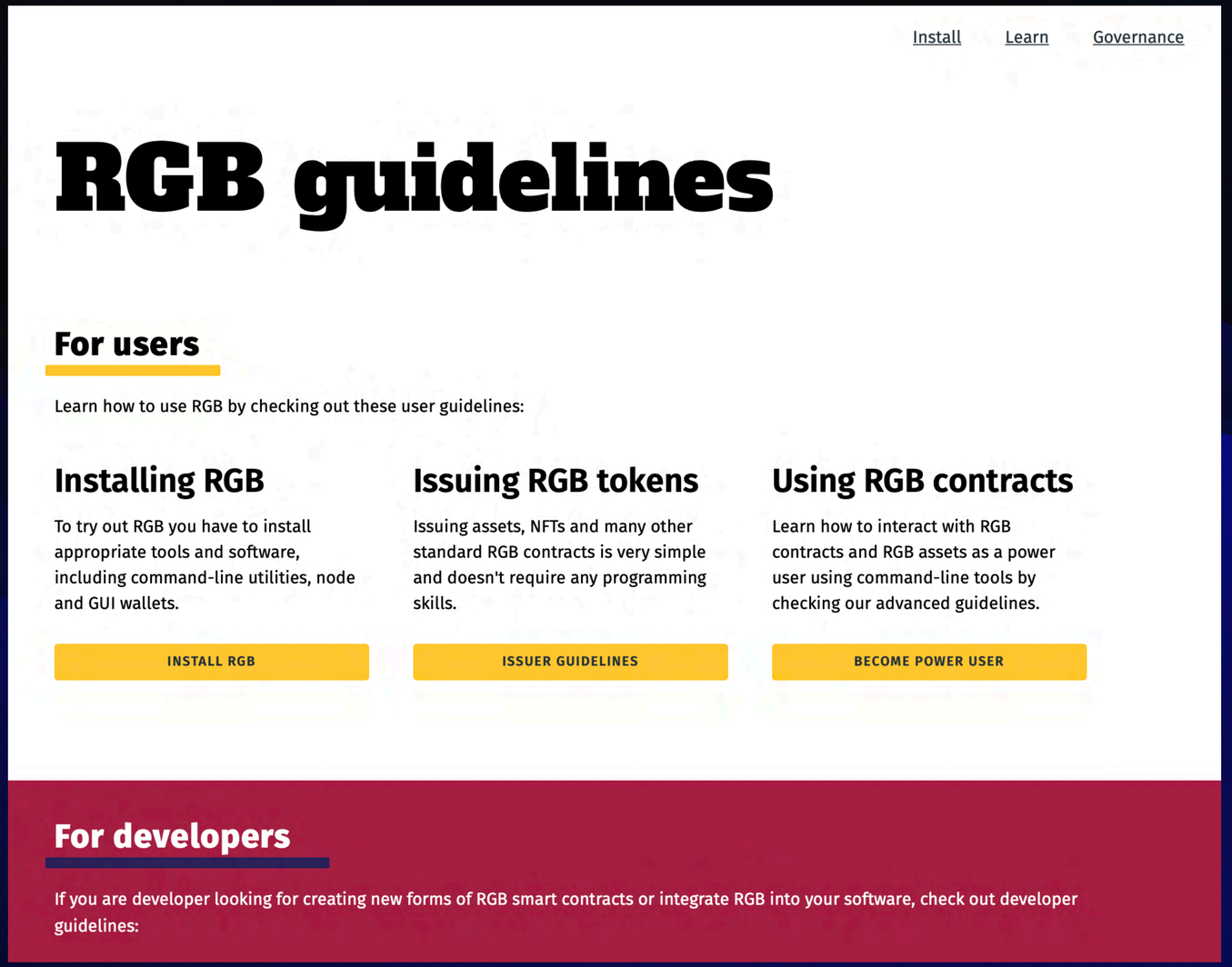
Info-resources

- www.rgb.tech



Info-resources

- www.rgb.tech



Can I do with anything beyond
BiFi with RGB?

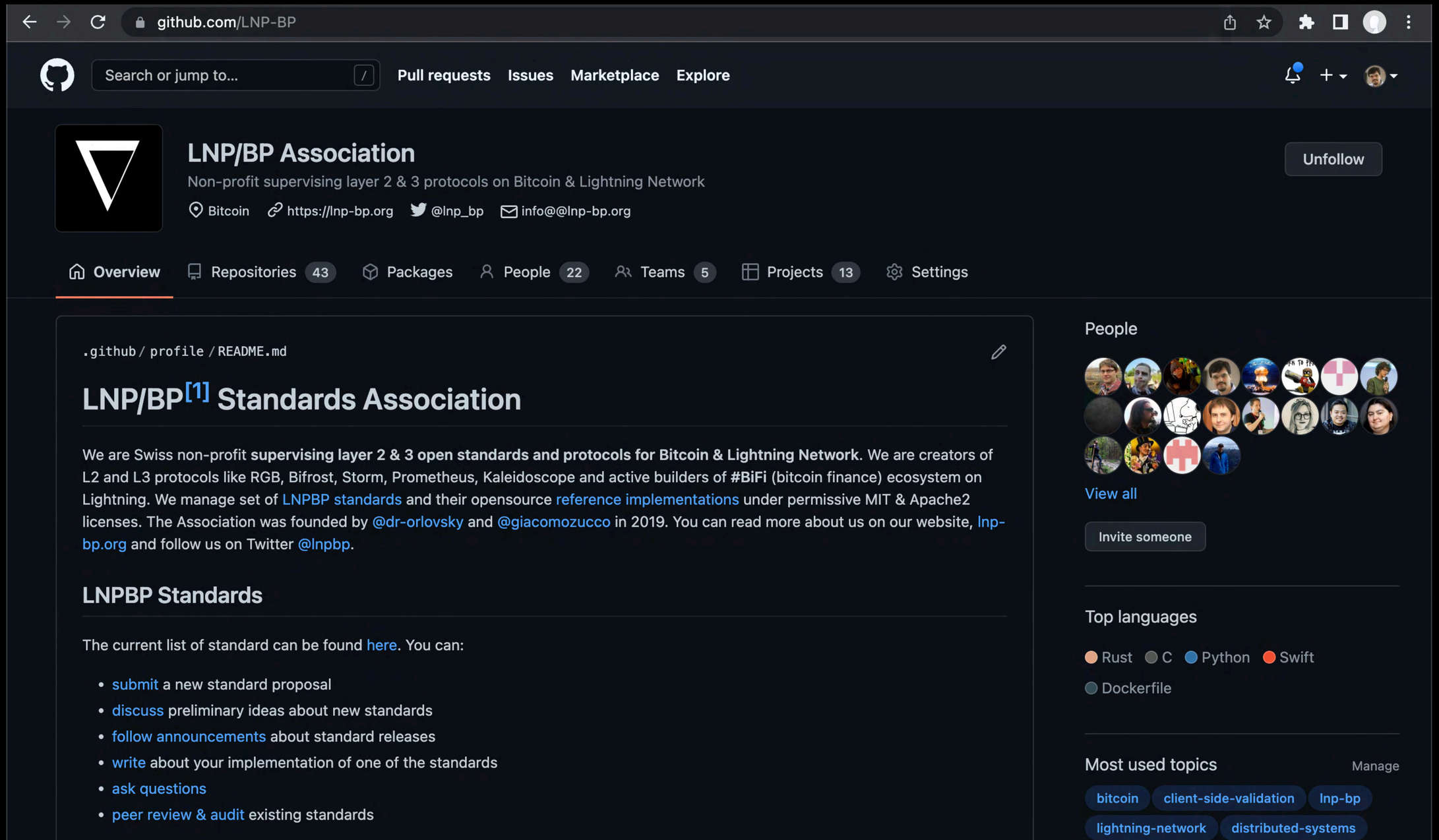
What can I do with RGB?

- Fungible assets & securities (options, futures)
  - centrally or federation-issued
  - issued anonymously or publicly
  - with possible secondary issuance, demurrage, inflation
- NFTs (game skins, collectibles, digital art etc)
- Bearer rights (voting etc)
- AMMs, liquidity pools, DEXs
- DAOs
- Digital Identities, roaming profiles & key management

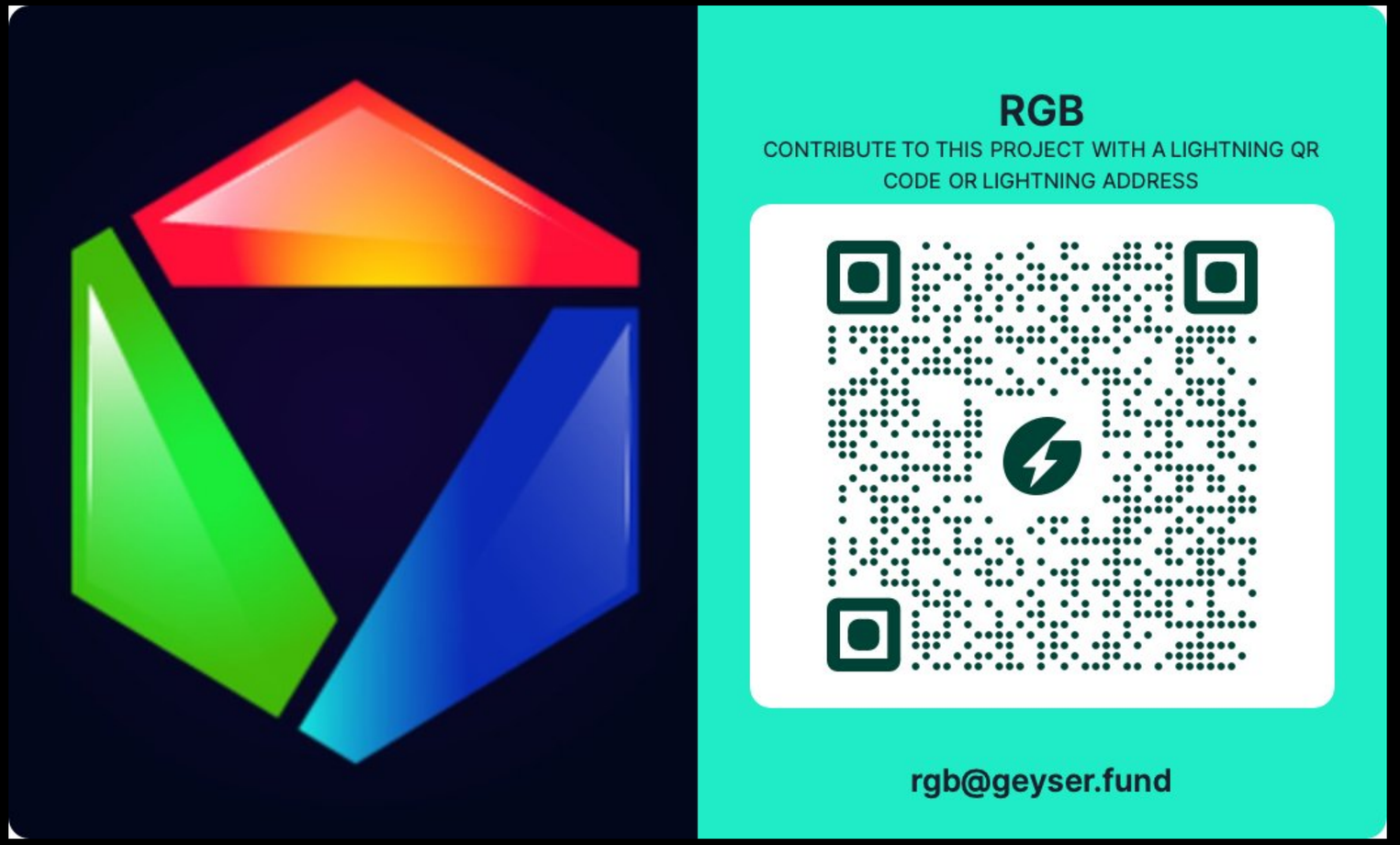
Part VI

Who RGB?

The largest Bitcoin tech non-profit in Switzerland

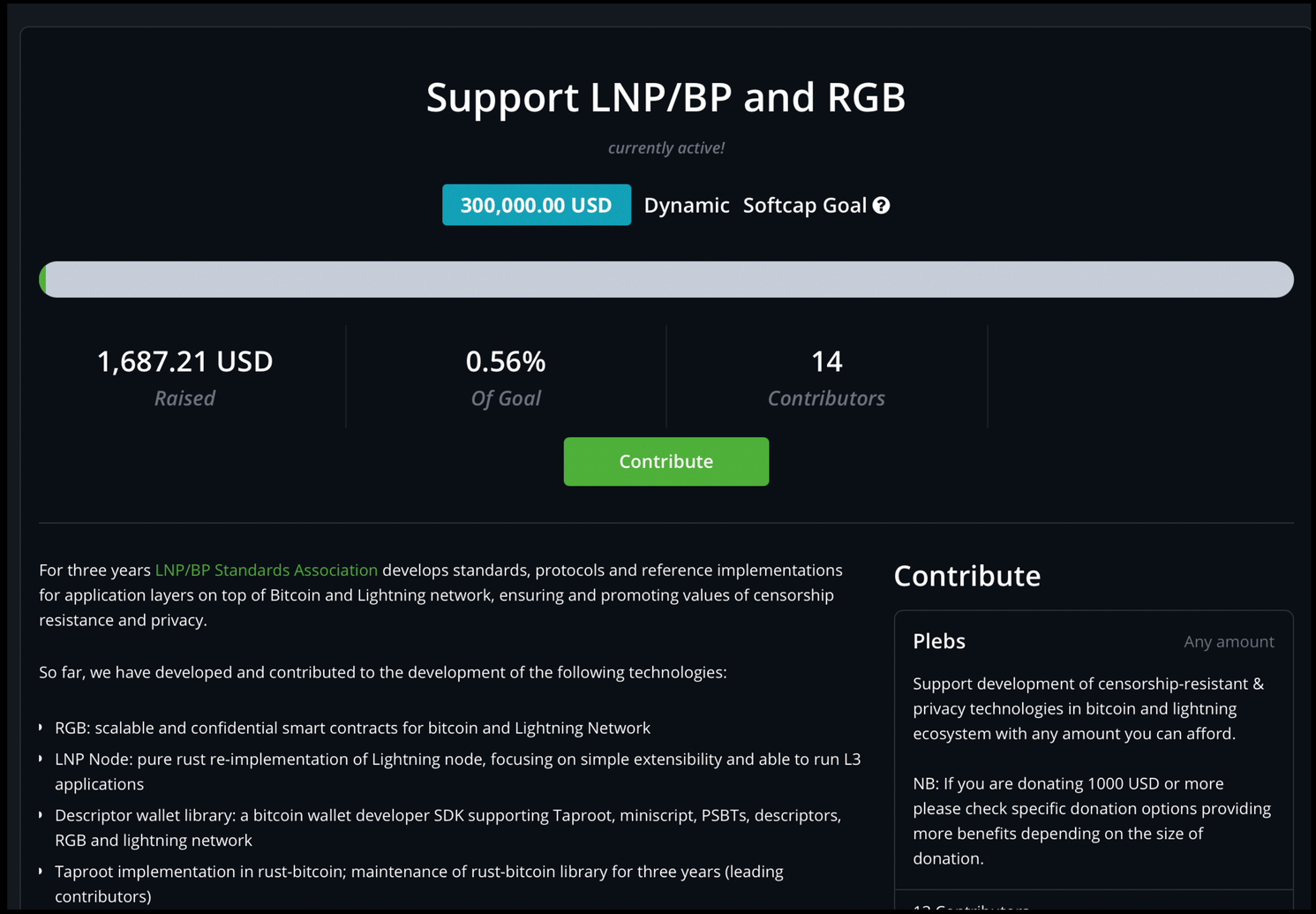


Support & donate



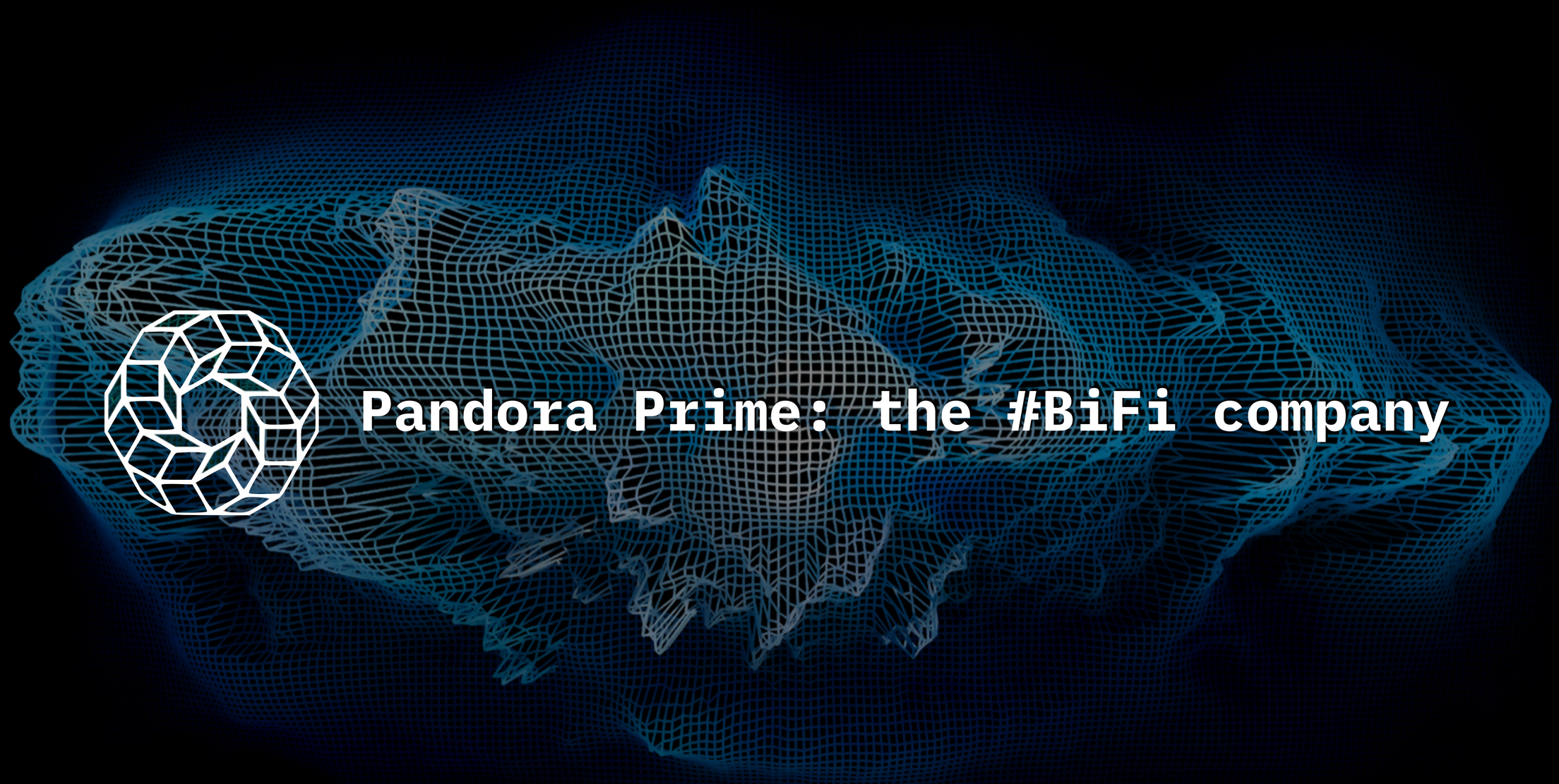
Support & donate

https://www.lnp-bp.org

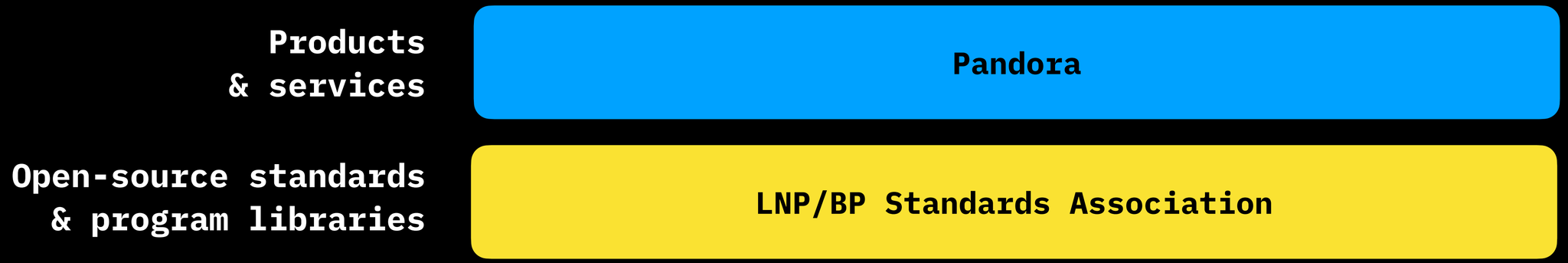



ONE MORE
THING

Driving RGB adoption


Pandora Prime: the #BiFi company

Layered tech, layered business




MyCitadel
Bitcoin, Lightning & RGB wallets
Create
Open
Import
About
Use taproot
Use testnet
Use RGB
Single-sig watch-only
A watch-only wallet controlled by a single signature
Current wallet
Wallet for current payments with a single hardware device
Hodling wallet
Wallet controlled by a set of your devices with expiration periods
devices
Custom wallet
Fully-customizable wallet
Instant payments with Lightning
Open a lightning channel with a peer or multiple peers
MYCITADEL
Ultimate digital privacy

mycitadel.io

New distributive packages

- Debian package
- Flatpak package
- Windows installer
- Freedesktop environment integration

Version 1.3 (Pacific Eclipse) Latest

Compare

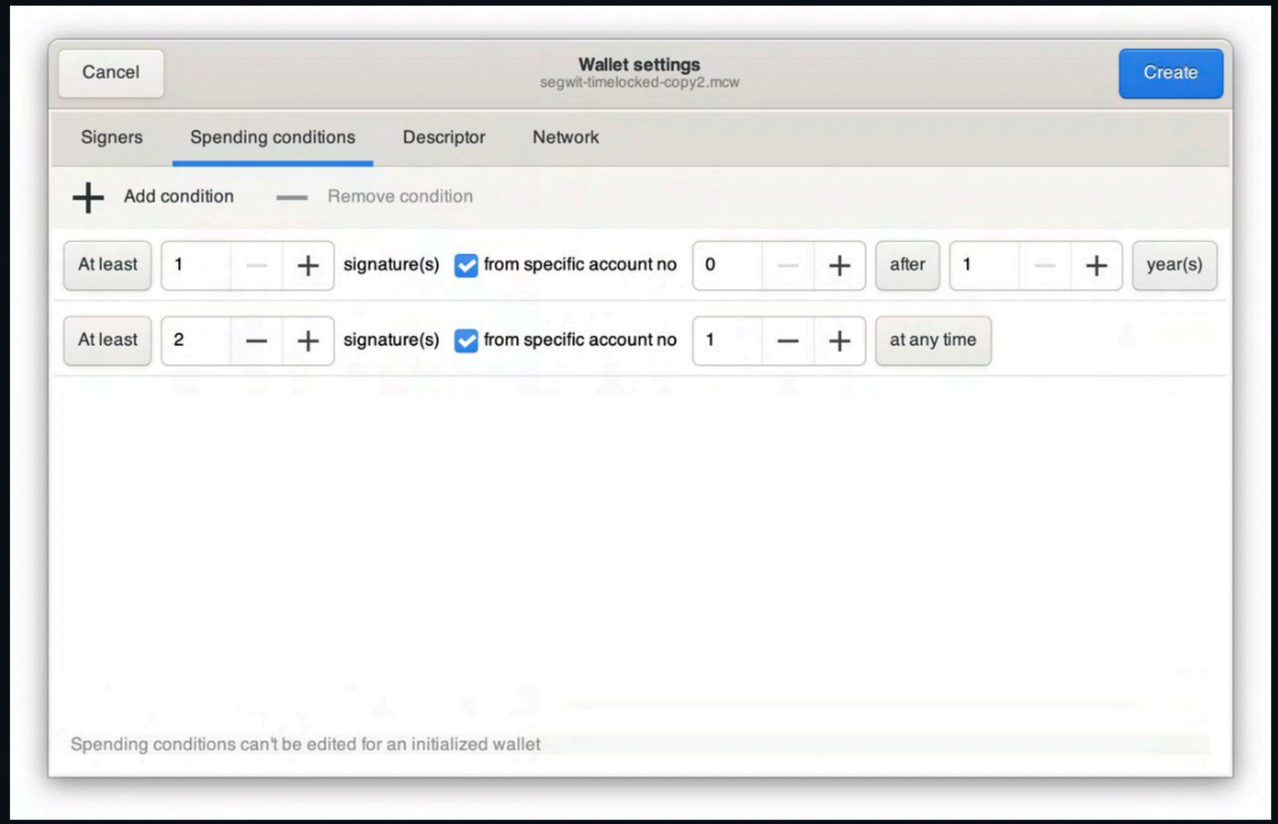
dr-orlovsky released this last week · v1.3.0 · 423937f

What's Changed

MyCitadel 1.3 ships with support for more advanced miniscripts with account- based time-locked multi-sigs and multiple user interface improvements.

Core functionality

Account-based multi-sigs with time-locks and complex miniscript descriptors. This adds ability to compose complex time-locked conditions involving same signers in different time-locks (for instance having 2-of-4 multi-sig which in 1 year becomes 1-of-2).



UI improvements

- Double-click on addresses copies address to clipboard
- Double-click on history entry copies transaction id to clipboard
- Double-click on coin entry copies outpoint information to clipboard

RGB-wrapped bitcoin (BTCN)

- **Decentralized issuance (!)**
- Programmability for Bitcoin
- Cash-level of privacy
- Foundation for building #BiFi products:
  - DEX
  - AMM markets
  - Algorithmic coins

Stablecoins

CHFN, USDN, EURN

- Working on lightning network
- VISA/MC level of transaction throughput
- Confidential as cash (“digital cash”)

Info-resources

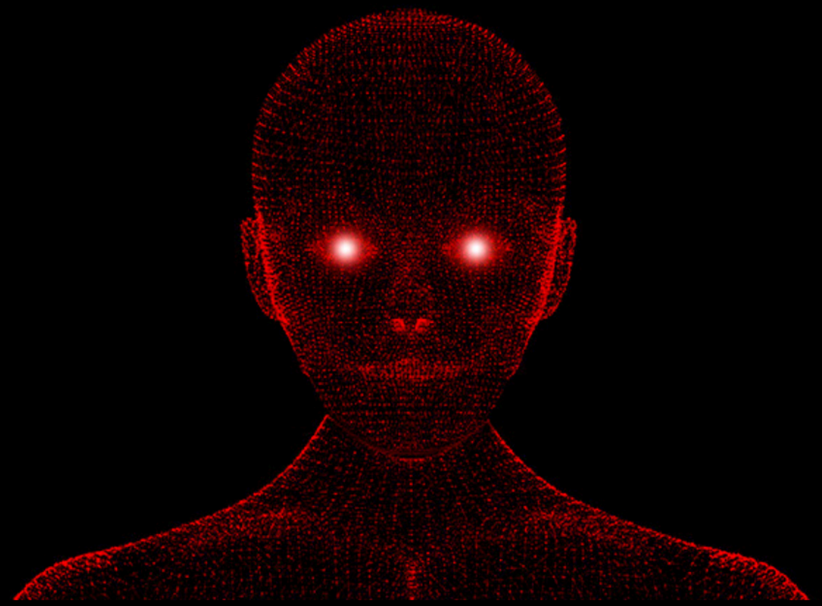
LNP/BP Standards Association

- www.rgbfaq.com
- www.rgb.tech

- LNP/BP Standards Association
  https://twitter.com/lnp_bp
- RGB Community
  https://twitter.com/i/communities/1585365616743022595

- LNP/BP Standards YouTube channel
  http://youtube.com/c/LNPBP

- RGB Telegram chat
  https://t.me/rgbtelegram
- LNP/BP Telegram channel
  https://t.me/lnp_bp



Olga Ukolova*

Twitter @OlUkolova

- Co-author of #FreeAI Manifesto
- Board member at LNP/BP Standards Association
- Founder @Pandora Prime

**I identify as Dolores the Queen of Geeks*