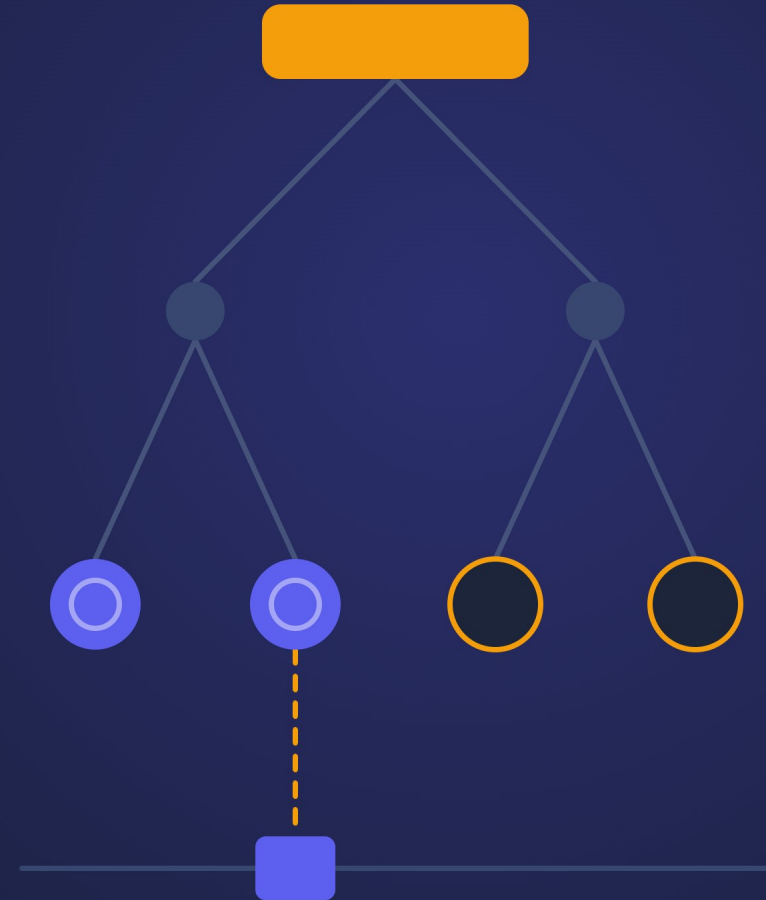


# Stablecoins in Wavelength

Dollars and bitcoin on the same rails



START WITH THE UTXO

**Every bitcoin owner needs a UTXO, and block space is scarce.**

Lightning and Ark answer the same question: how many owners can share one UTXO?

TODAY

# Three parts

---

## 01 Why Ark looks the way it does

N owners, a tree, and an operator that lends time

---

## 02 Dollars on the same rails

Why a VTXO can carry a Taproot Asset

---

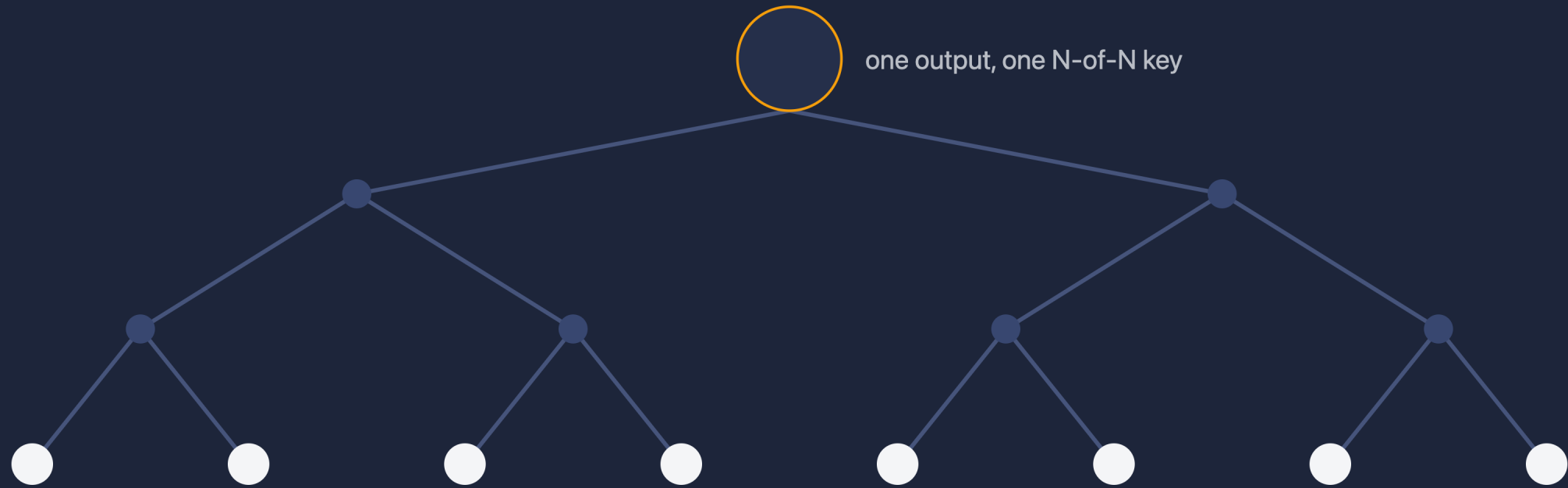
## 03 What it brings to Bitcoin

And what is real today

---

WHY ARK

# One UTXO, more owners



# What N owners cost



## Signing together

N people can't all be online for every payment.

---

An operator runs rounds and cosigns payments in between.



## Leaving alone

Anyone must be able to exit without the other N-1.

---

A tree of pre-signed transactions gives each owner a path out.



## Not waiting forever

Coins can't stay shared until the last owner acts.

---

Batches expire. Owners refresh, and the operator sweeps the rest.

The operator can't take your coins or block your exit. But it does lend its own coins, and that has a price.

# A tree, so anyone can leave alone



Leaving costs the few transactions on your own path, not the whole tree.

The round output's key combines the operator and every owner: **N-of-N**.

Everyone signs the whole tree before the round is broadcast.

Each owner can publish the path to their own leaf, a **VTXO**, alone.

After expiry, a sweep path lets the operator reclaim what wasn't refreshed.

# The operator lends time

**720 blocks left**

about 5.0 days until the operator gets the old coins back

**42 sats**

liquidity fee to refresh 50,000 sats, at 6% a year

Alice's leaf in batch A: 50,000 sats

free window

Operator's coins fronting Alice's new leaf, locked until batch A expires

Batch A created

Alice refreshes

Batch A expires, operator sweeps

A refresh swaps your old leaf for a new one. The operator pays for the new leaf now, and gets the old coins back only when the old batch expires.

# Originary interest, priced

Present coins are worth more than future coins. The operator hands out present coins and waits for future ones: that wait is **originary interest**.

```
liquidity fee =  
amount × effective rate × blocks left ÷ 52,560  
effective rate = 5% base + utilization premium
```

Boarding pays no liquidity fee, because nothing is lent.

Refresh late and there's less time to lend: in the last 144 blocks, a plain refresh is free.

## EXAMPLE · 6% EFFECTIVE (5% + 1%)

Refresh 50,000 sats with 720 blocks (about 5 days) left

---

$$50,000 \times 6\% \times 720 \div 52,560$$

**42 sats**

of liquidity fee

---

+ a share of the round's mining fee

+ a fixed margin of 100 sats

# One wallet, three rails

## waved

Lightning Labs' Ark wallet:  
one daemon, a CLI and  
an API.

- ✓ Embeds in iOS and Android apps
- ✓ Operator lumosd, swap server swapd
- ✓ Sole custody of every coin

## LIGHTNING

Pay and get paid over Lightning, through atomic swaps with Ark.

↕ atomic swaps

## ARK

Hold and pay with VTXOs, refresh them, exit whenever you want.

↕ board · leave · exit

## ON CHAIN

An embedded wallet to deposit, withdraw and fall back to.

**A VTXO is a real Bitcoin output that just hasn't been published yet.**

So anything a taproot output can carry, a VTXO can carry too, including dollars issued as Taproot Assets.

# Taproot Assets in one slide

- 1 An asset hides inside the taproot key of a normal Bitcoin output: **the anchor**.
- 2 Moving it is a **transition**, backed by proofs that reach back to issuance.
- 3 Two locks: Bitcoin script on the anchor, and a **script key** on the asset.

## BITCOIN OUTPUT • THE ANCHOR

Its output key commits to scripts and to an asset tree

### ASSET COMMITMENT

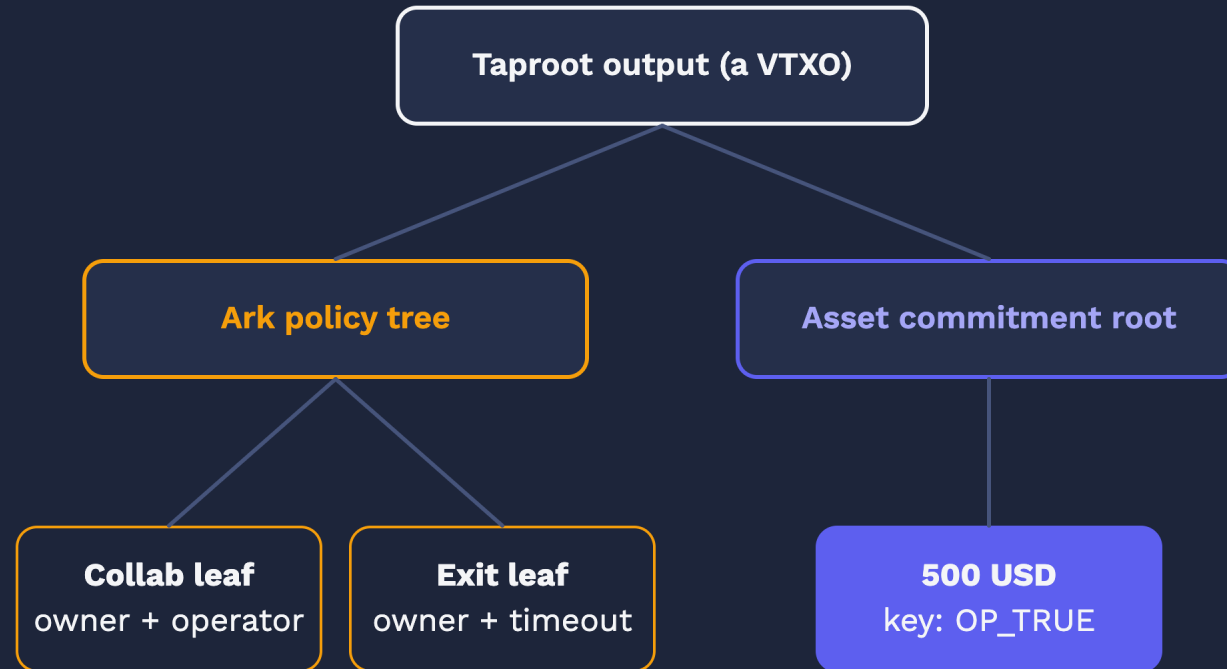
500 USD

42 OTHER

A Merkle-sum tree: amounts add up at every node

🔗 Proof file: the asset's full history, back to its issuance

# One output, two protocols



Why OP\_TRUE is safe: the asset only moves if its Bitcoin output does, and that still needs the owner's signature.

**Ark scripts are untouched.** Spending a policy leaf reveals one extra 32-byte hash.

**The asset key is OP\_TRUE,** unique to each round. Custody stays in the Bitcoin script.

**So the operator can batch assets it never owns,** and the tree needs no asset signatures.

# Why operators choose their assets

## THE OPERATOR FRONTS DOLLARS TOO

- 🕒 **Refresh:** the new leaf's dollars come from the operator's own inventory.
- 🏠 **Cooperative exit:** pays out of that inventory.
- ⚡ **Swaps with Lightning:** need that asset on both sides.

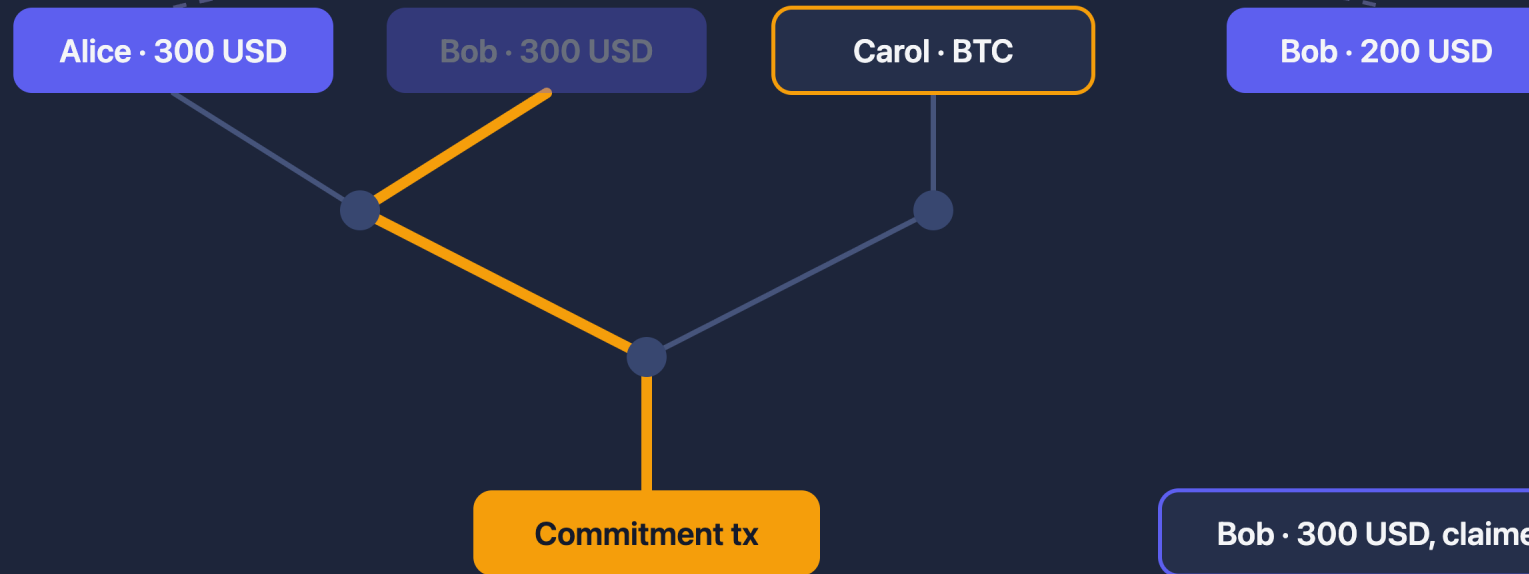
## SO TO SERVE AN ASSET, IT MUST

- ✓ Hold an inventory of it
- ✓ Charge interest (in it), for the time it lends
- ✓ Verify its proofs back to issuance

Admission rejects any asset that isn't on the operator's allowlist. You can't bring an arbitrary token into a round.

# A dollar's life in Wavelength

Off chain



Bitcoin chain

4 · Exit: Bob takes his 300 USD leaf on chain and claims it into tapd

# Sending dollars with zero bitcoin

Every Taproot output must hold a few sats: the **carrier**. It moves with the output, so who pays for it is a design choice.

| Leaf created by | Carrier paid by                   | When the leaf is spent        |
|-----------------|-----------------------------------|-------------------------------|
| Boarding        | Your own wallet                   | Back to you as bitcoin change |
| Off-round send  | The operator, lent from its float | Reclaimed into the float      |
| Refresh         | Carried over from the old leaf    | Stays with the new leaf       |

Senders and receivers need no bitcoin at all. Round fees are still paid in sats; fees in the asset are an open item.

# Same trust model, one new risk

## TRUST · SAME AS ARK

### The operator can

Refuse or delay rounds and transfers, or decline an asset.

### The operator cannot

Move your dollars without your signature, inflate them, or stop your exit.

## NEW RISK · BURNING

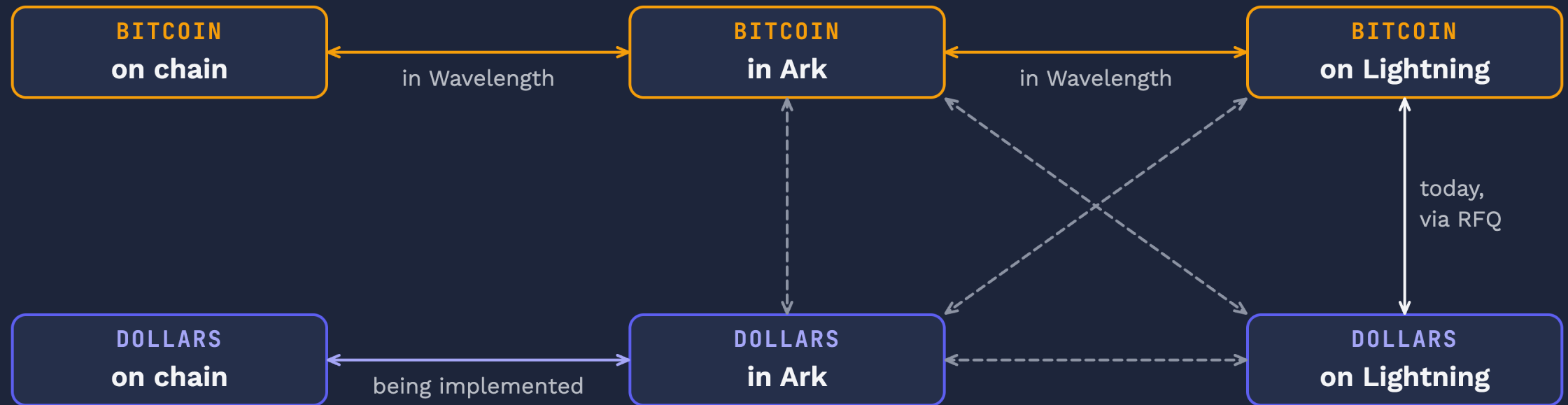
⚠ A plain Bitcoin spend of an asset's output destroys the dollars inside it.

### The rule

Only asset-aware transitions may spend an asset output. Coin selection, refresh, sweeps and exits refuse everything else.

Assets add checks to verify, not a party to trust.

# Dollars and sats, one set of rails



Solid: works today, or being implemented · Dashed: possible, coming eventually

Coming: bitcoin  $\rightleftharpoons$  dollars inside Ark, dollars between Ark and Lightning, and both at once: pay in bitcoin, receive dollars, or the reverse.

WHAT IT BRINGS

# What this brings to Bitcoin



## No bank, no other chain

A USDT- or USDC-style dollar moves on Bitcoin rails from end to end.



## Sats one swap away

Dollars and bitcoin sit in the same wallet, a quoted swap apart.



## Self-custody for dollars

Every dollar leaf keeps a pre-signed path back to the chain.

A stablecoin user on Wavelength is already a Bitcoin user.

USDT and USDC are named as examples of dollar stablecoins. This is not an announcement of any issuance.



ONE UTXO • N OWNERS • DOLLARS AND SATS

# Thank you

Questions?

[github.com/lightninglabs/wavelength](https://github.com/lightninglabs/wavelength)

[github.com/lightninglabs/tap-sdk](https://github.com/lightninglabs/tap-sdk)

[github.com/lightninglabs/taproot-assets](https://github.com/lightninglabs/taproot-assets)

Dario Anongba Varela • [@dario\_nakamoto]

