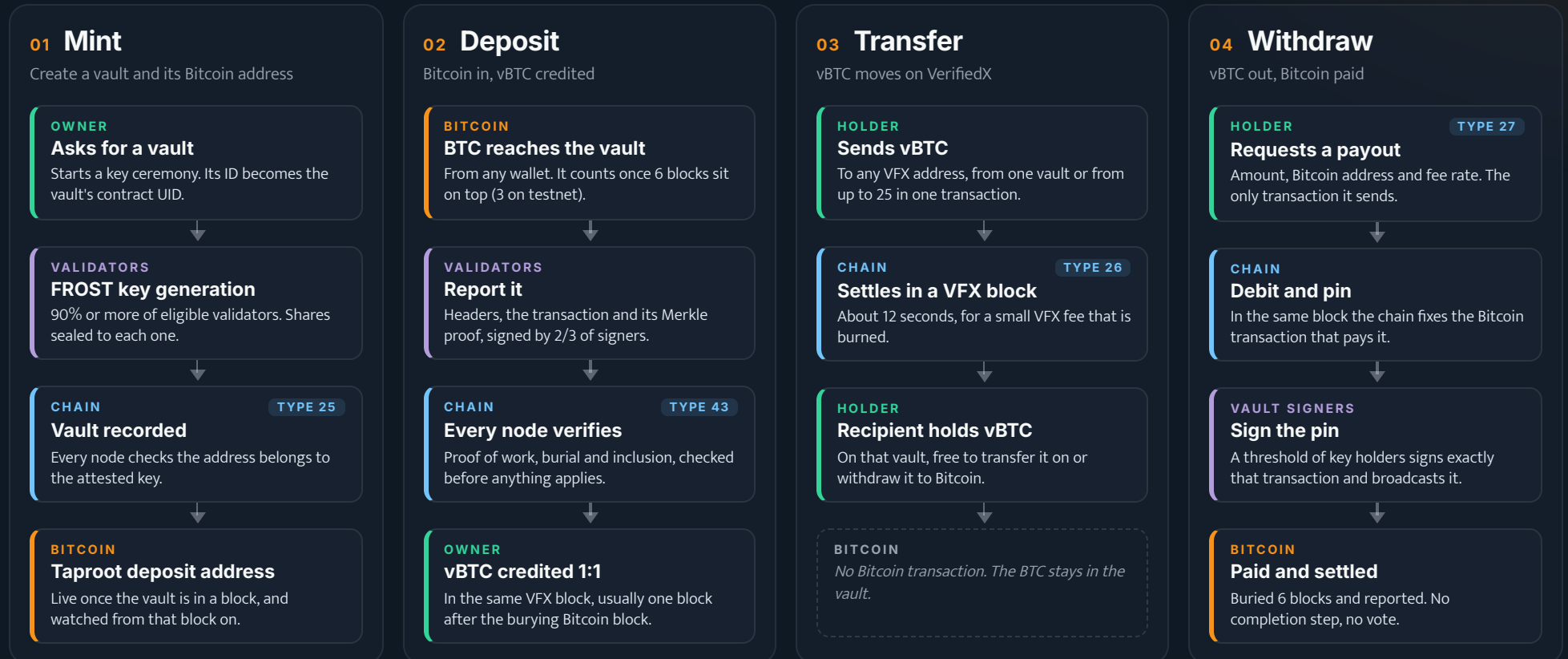


How vBTC works in Core 9.0

Four flows, one rule: Bitcoin establishes the truth, consensus verifies and enforces it, holders authorize, FROST signers execute.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



6 blocks

Bitcoin depth
before an event counts (3 on testnet)

2/3

Report quorum
of the epoch's signers, at least 3

90%

Ceremony turnout
of eligible validators per new vault

51%

Signing threshold
of key holders, rounded up

5,000

VFX bond
locked two days before a validator counts

0

Votes to withdraw
no completion transaction, no vote

NEW IN
Core 9.0

Bitcoin attestation

Validators report Bitcoin headers and Merkle-proved vault events; every node verifies them.

Watched vaults

A vault's vBTC follows the Bitcoin the chain has recorded, not a Bitcoin server's answer.

Withdrawal pins

The chain fixes each payout's Bitcoin transaction. No completion transaction, no cancellation vote.

Validator bond

5,000 VFX locked per validator, and two days bonded before it holds keys or signs reports.

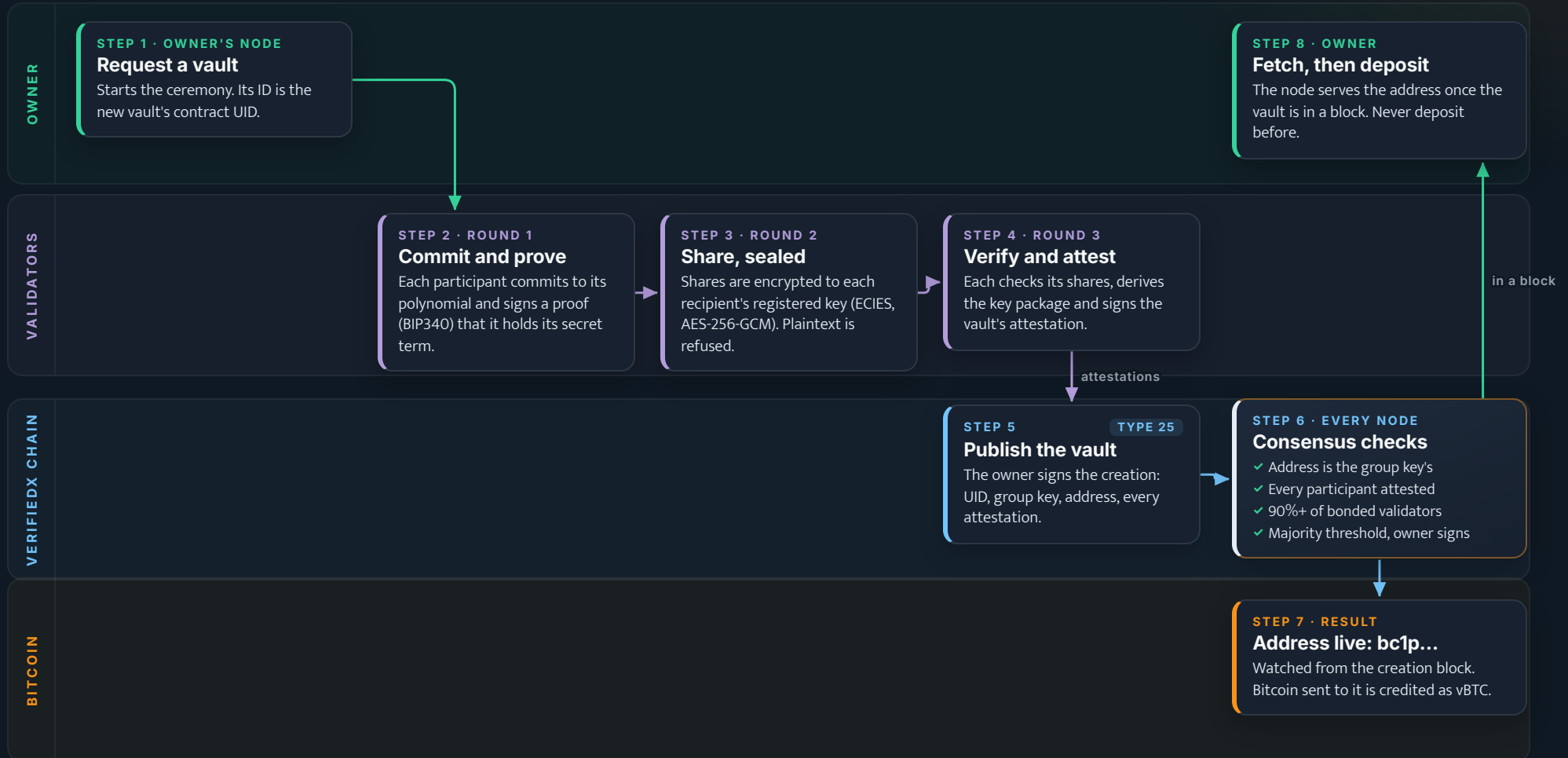
Mint: create a vault

01

A FROST key ceremony among the validators, bound on chain to the vault it creates.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



WHO TAKES PART

- **Eligible:** registered, active, 5,000 VFX bonded for 14,400 blocks (about two days).
- At least **90% of eligible** validators, never fewer than 3, at most 512.
- One ceremony per owner at a time; it times out after an hour.

THE KEY

- Signing threshold: **51% of participants, rounded up.**
- A validator that fails a round is dropped and the ceremony reruns without it, if enough remain.
- No participant, and not the owner, ever holds the whole key.

THE ADDRESS

- Taproot, key-path spend: the address encodes the **raw x-only group key**.
- A vault that copies another's address is not watched and holds no coins.
- **S3C:** the owner's own validators (three or more) replace the public pool. See page 7.

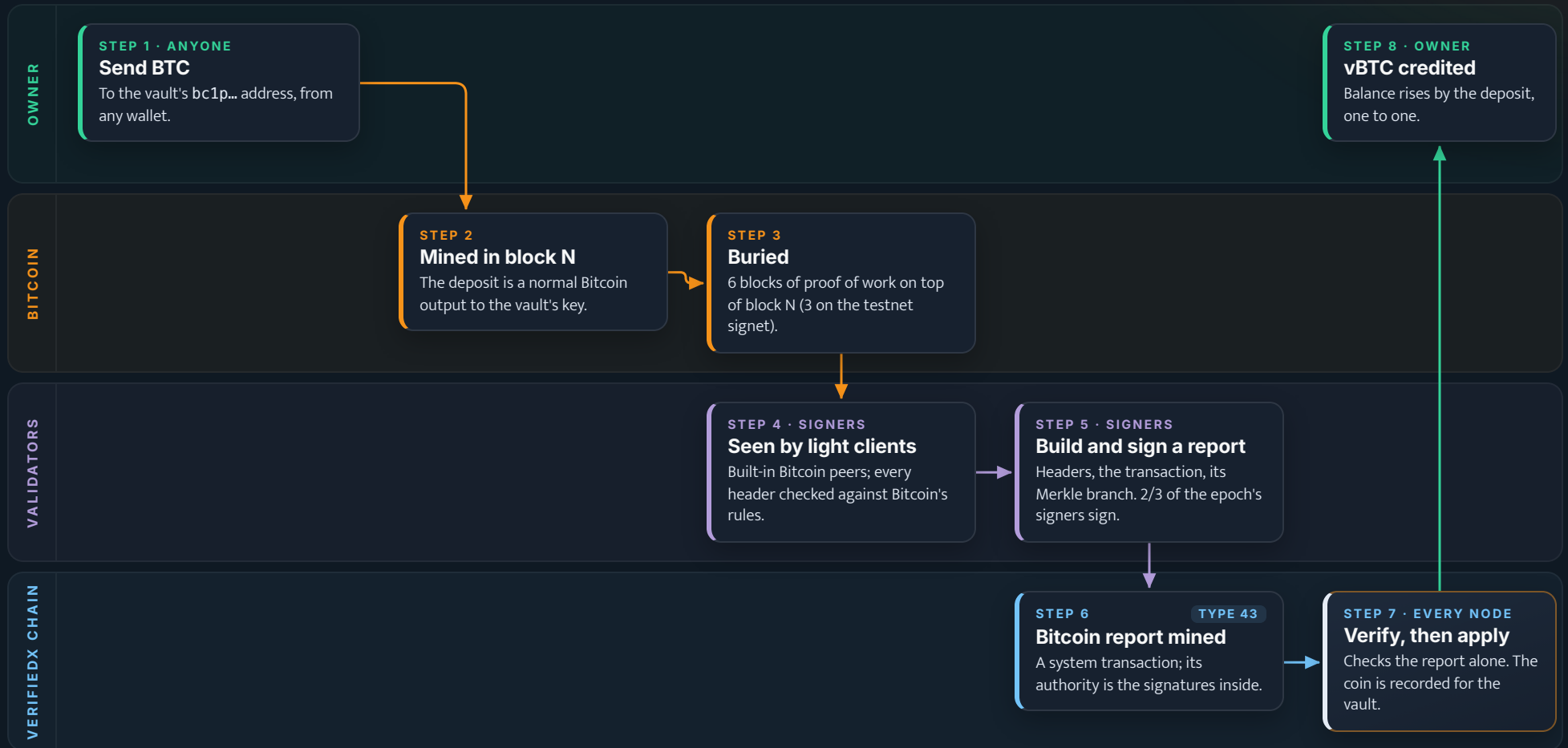
Deposit: Bitcoin in, vBTC credited

02

Validators report the Bitcoin. Every node checks the proof before a single satoshi is credited.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



EVERY NODE CHECKS

- Each header links to the last, carries the **target Bitcoin's retarget rules require**, meets it, and is timed after the median of the 11 before it.
- The block is **buried** by 6 counted headers.
- The transaction's **Merkle branch** reaches the header, as deep as the coinbase's. Transactions of 64 bytes or less are refused.
- What the transaction does to vault coins is **read from its own inputs and outputs**.

WHAT RESTS ON THE SIGNERS

- Which Bitcoin branch is followed, and that **blocks skipped held no vault event**: two thirds of the epoch's signer set vouch for both.
- The signer set is fixed every **600 VFX blocks**: active validators whose bond is at least two days old.
- With no vault activity, a **quiet report** covers each 144 Bitcoin blocks.

REORGs AND TIMING

- Unreported headers are replaced only by a branch with **more work**. Reported events are taken back by a **Bitcoin reorg** transaction (type 45).
- Credit normally lands **one VFX block** after the burying Bitcoin block.
- A coinbase output is credited but cannot be spent for 100 blocks.

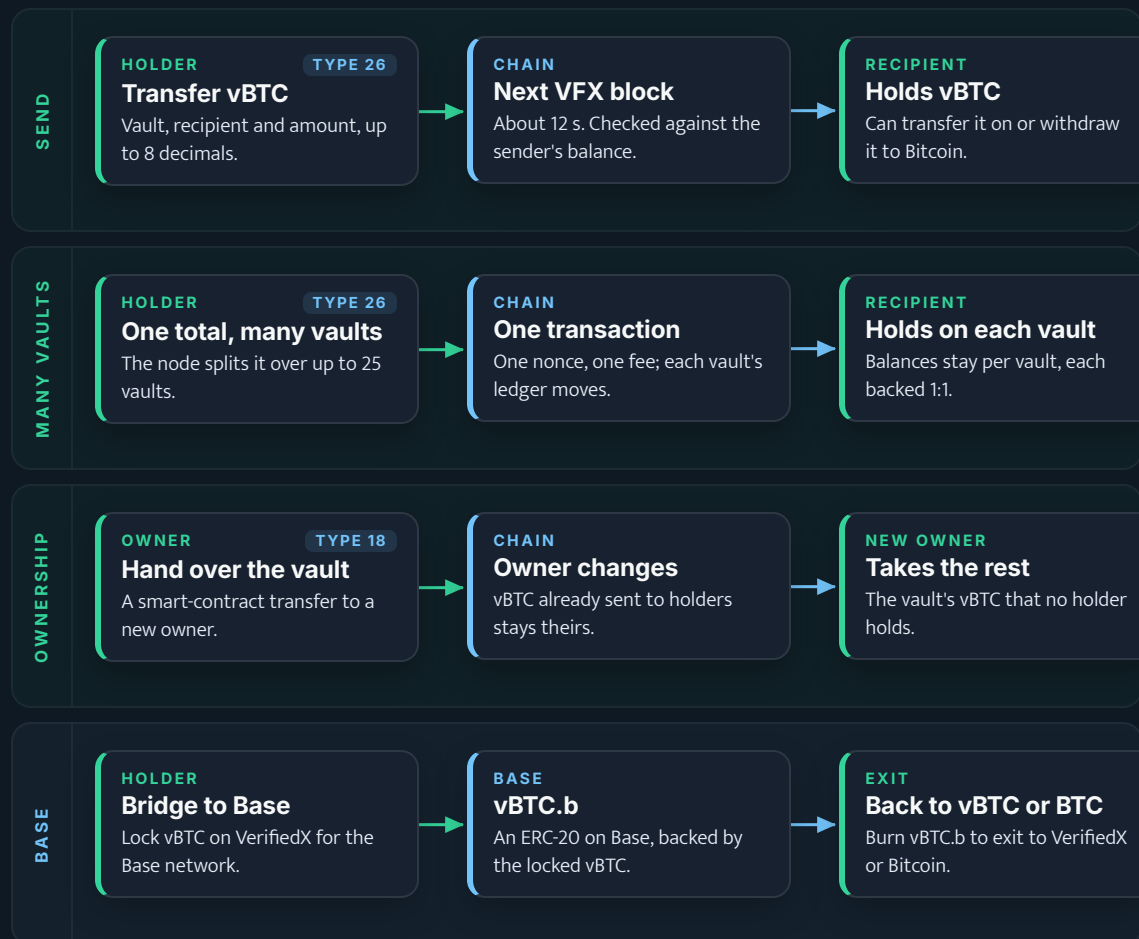
Transfer: vBTC moves on VerifiedX

03

Transfers change who holds the vault's Bitcoin on the ledger. The Bitcoin itself stays put.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



THE BALANCE MODEL

Owner's vBTC = the vault's verified BTC – what other holders hold. A holder's vBTC = its ledger balance.

EVENT	VAULT BTC	OWNER	HOLDER A
Deposit 1.0 BTC	1.0	1.0	0
Owner sends A 0.3	1.0	0.7	0.3
A withdraws 0.1	0.9	0.7	0.2
Deposit 0.5 BTC	1.4	1.2	0.2

The vBTC on a vault always adds up to its Bitcoin. A withdrawal's Bitcoin fee comes out of its own amount, so the vault never pays it.

Holders are protected from the owner. The owner's figure is whatever is left after every other holder, so it can never spend vBTC it has already sent.

Deposits accrue to the owner. New Bitcoin at the vault address raises the owner's balance only.

RESERVE ACCOUNTS

vBTC in a reserve (vault) account keeps its time-lock protection: a transfer from it is held for **24 hours** and can be called back until then. Move vBTC to a normal address before withdrawing it to Bitcoin.

READ FROM CHAIN STATE

Balances, vaults and withdrawals are answered from chain state, so **any node gives the same answer** for any address, whether or not it holds the keys.

FEES AND LIMITS

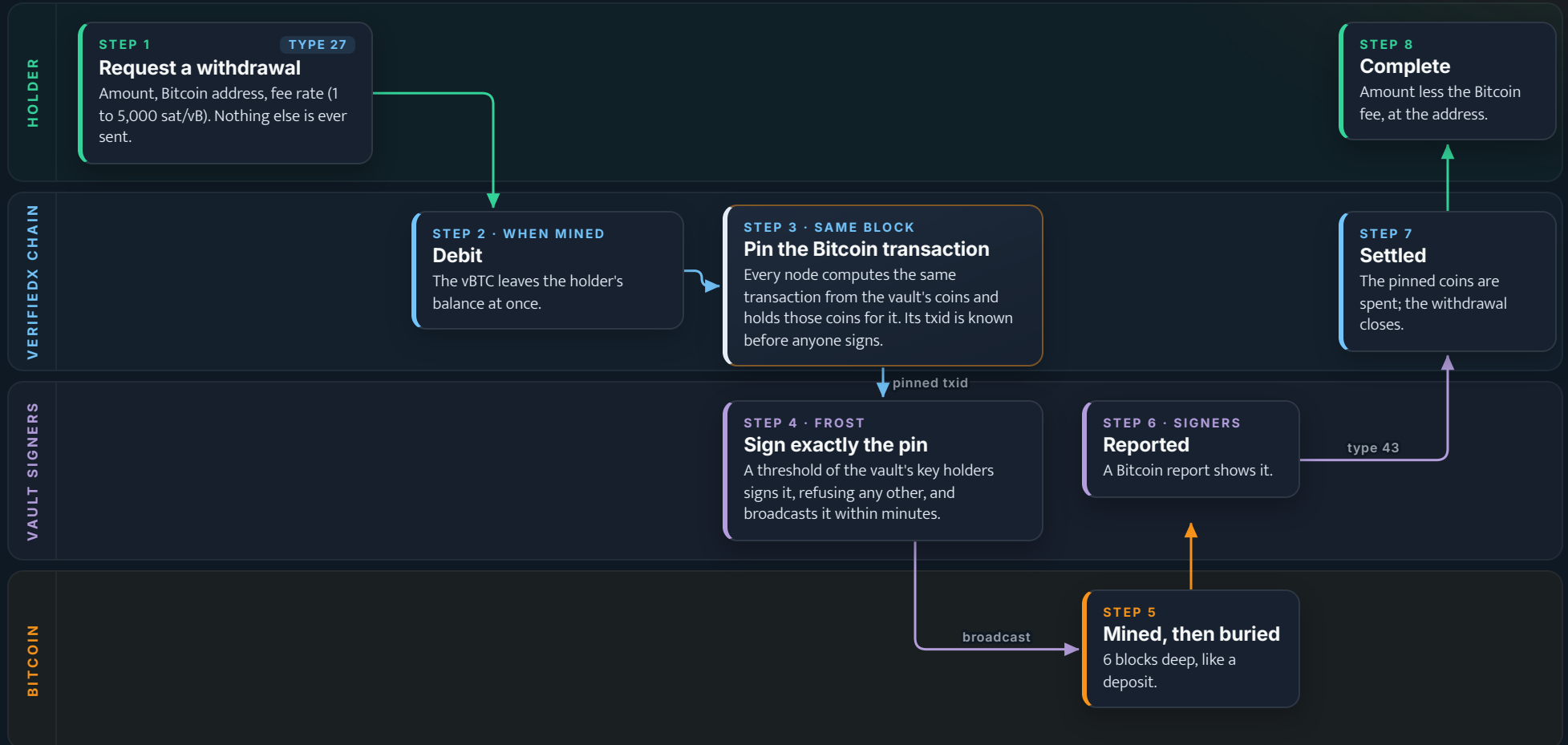
A transfer pays a small VFX fee, which is burned, and **no Bitcoin fee**: the Bitcoin does not move. Amounts carry up to 8 decimals; a multi-vault transfer draws on up to 25 vaults.

Withdraw: one request, a payout the chain fixes

04 The holder sends one transaction. Consensus decides the Bitcoin transaction; signers execute it; Bitcoin completes it.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



THE PINNED TRANSACTION

- **Coins:** the smallest single coin that covers the amount, else the largest first.
- **Fee:** rate × size (154 vB with one input, 212 with two, about 57.5 more per input), taken out of the amount.
- **Change** returns to the vault's own address. Inputs signal replace-by-fee.

AMOUNTS

- Smallest withdrawal: $154 \times \text{fee rate} + 546$ sats (1,008 sats at 3 sat/vB).
- The destination receives the amount less the fee; the vault and its owner pay nothing.
- A holder can have several withdrawals open at once.

MANY VAULTS, ONE REQUEST

- One type 27 transaction can draw on **up to 10 vaults**.
- Each vault is a share with its own Bitcoin transaction and its own fee.
- Shares settle independently; each can be raised, released or cancelled alone.

After the request: states and requester controls

05

Every path ends in one of two places: Bitcoin paid, or vBTC back. No vote decides either.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



WHAT THE REQUESTER CAN DO

Waiting	Cancel (type 29). Takes effect when mined: closed, vBTC returned. Nothing was signed, so nothing can still be paid.
Pinned	Raise the fee (type 44): a replacement at a higher rate on the same coins, the extra fee out of the amount. Whichever transaction confirms pays it.
Pinned	Release (type 44): the chain pins a transaction returning the coins to the vault; once buried, vBTC is refunded less its fee. Up to 4 releases.
Stuck	If a pinned payment has not confirmed after 2,160 VFX blocks (about 7.2 hours), a withdrawal paying a higher fee rate may be pinned on its coins. If that one confirms, this one is Void and refunded.
Track it	GetWithdrawalPin answers from the block that mines the request, on any node.

WHY NO VOTE IS NEEDED

A cancel is accepted only before the pin, when nothing has been signed, so nothing signed can still be paid. After the pin, every outcome is decided by what Bitcoin shows: the pinned payment confirms, a release confirms, or a coin is spent elsewhere. No validator vote can pay twice or hold a refund back.

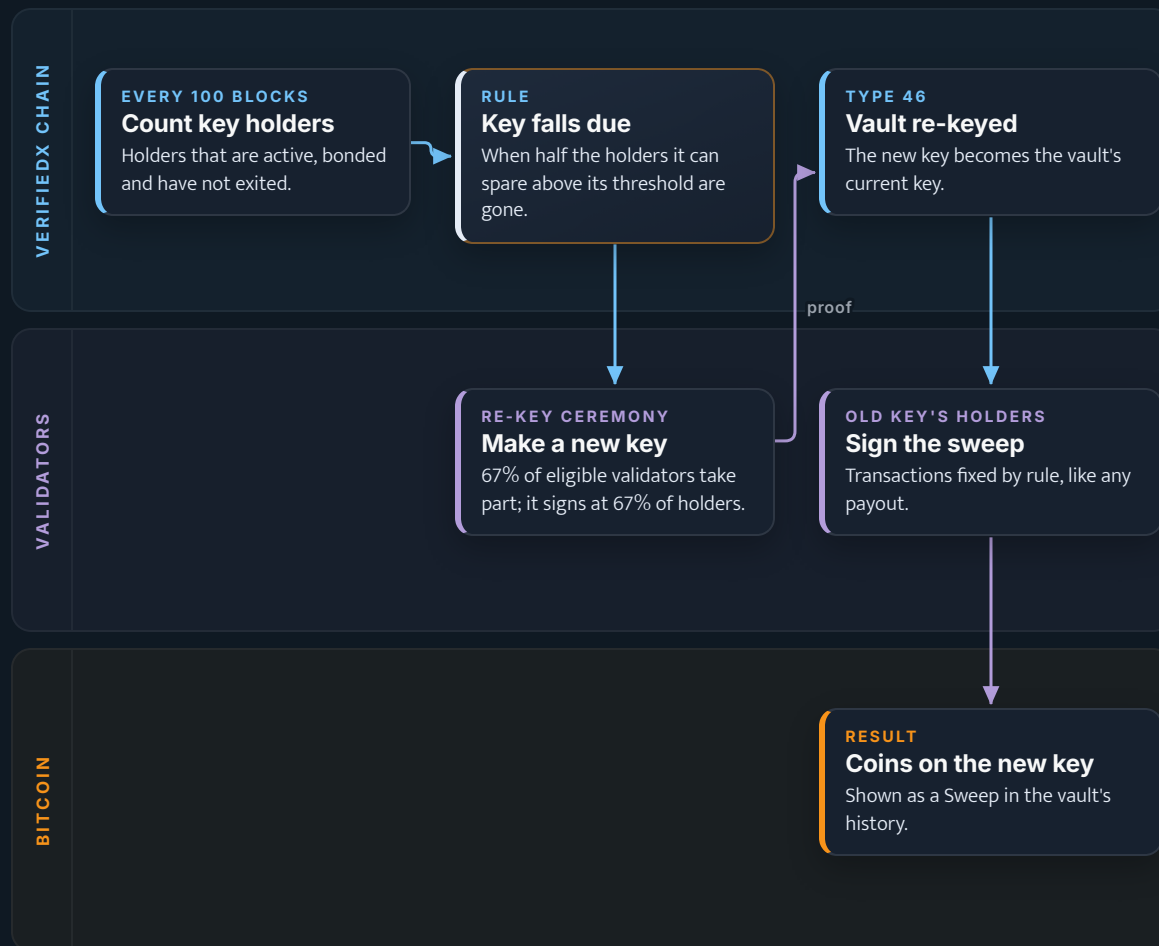
Vault keys over time: re-keying and S3C

06

Validators come and go. A vault's key is renewed while it can still sign, or kept on the owner's own validators.

VerifiedX

VBTC FLOW DIAGRAM · CORE 9.0



S3C · SELF-CUSTODIAL SMART CONTRACTS

Keep the key on validators you run

An owner can restrict a vault's key generation and signing to **at least three of its own validators**, instead of the public pool.

```
validator nodes: S3CValidator=true  
minting node: S3C=IP:Address,IP:Address,IP:Address
```

- › **All or nothing.** Every listed validator must be registered, active, flagged S3C and bonded long enough, and all of them take part. If one is not, the ceremony fails and names it.
- › **No silent fallback.** An invalid S3C= setting makes the node refuse to mint rather than use the public pool.
- › **Separate pools.** Public vaults never use S3C validators.
- › **The owner's keys.** The chain never re-keys an S3C vault: who holds its key is the owner's matter.
- › **Pre-flight.** GetS3CStatus reports each configured validator's registration and reachability.

DEPOSITING DURING A RE-KEY

Bitcoin sent to the old address is still credited while that key's holders can sign. Always deposit to the address `GetMPCDepositAddress` returns.

BEFORE ANYONE IS DEBITED

If a vault's current key can no longer sign, new withdrawals are refused before any vBTC moves, until the vault is re-keyed.

WHO LEADS A RE-KEY

Any validator may lead it and submit the result; validators take turns. The leader chooses nothing: **who holds the key, when it is due and what the new key must satisfy** are read from the chain.