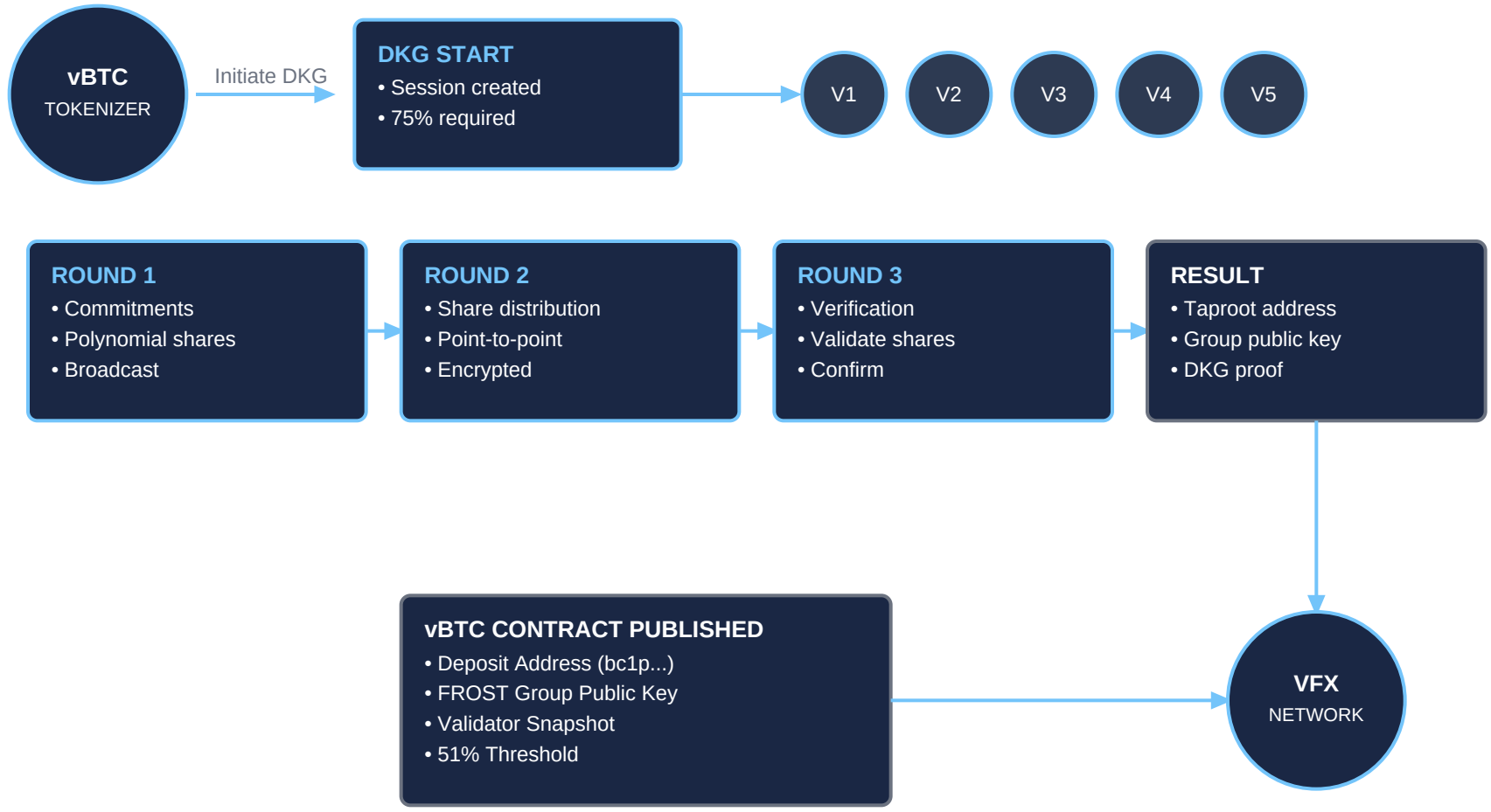
PROCEDURE 1 - DKG CEREMONY

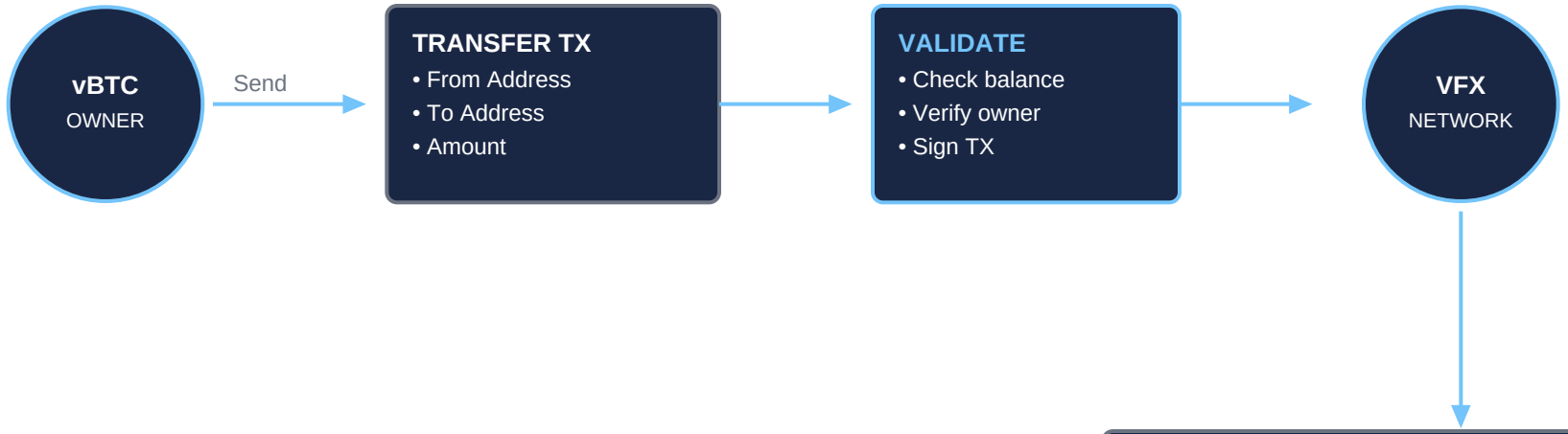
Get Taproot Address



KEY:
No single party knows the full private key

PROCEDURE 2 - TOKEN TRANSFER

Send vBTC



BALANCE CALCULATION

Balance = Received - Sent - Withdrawals

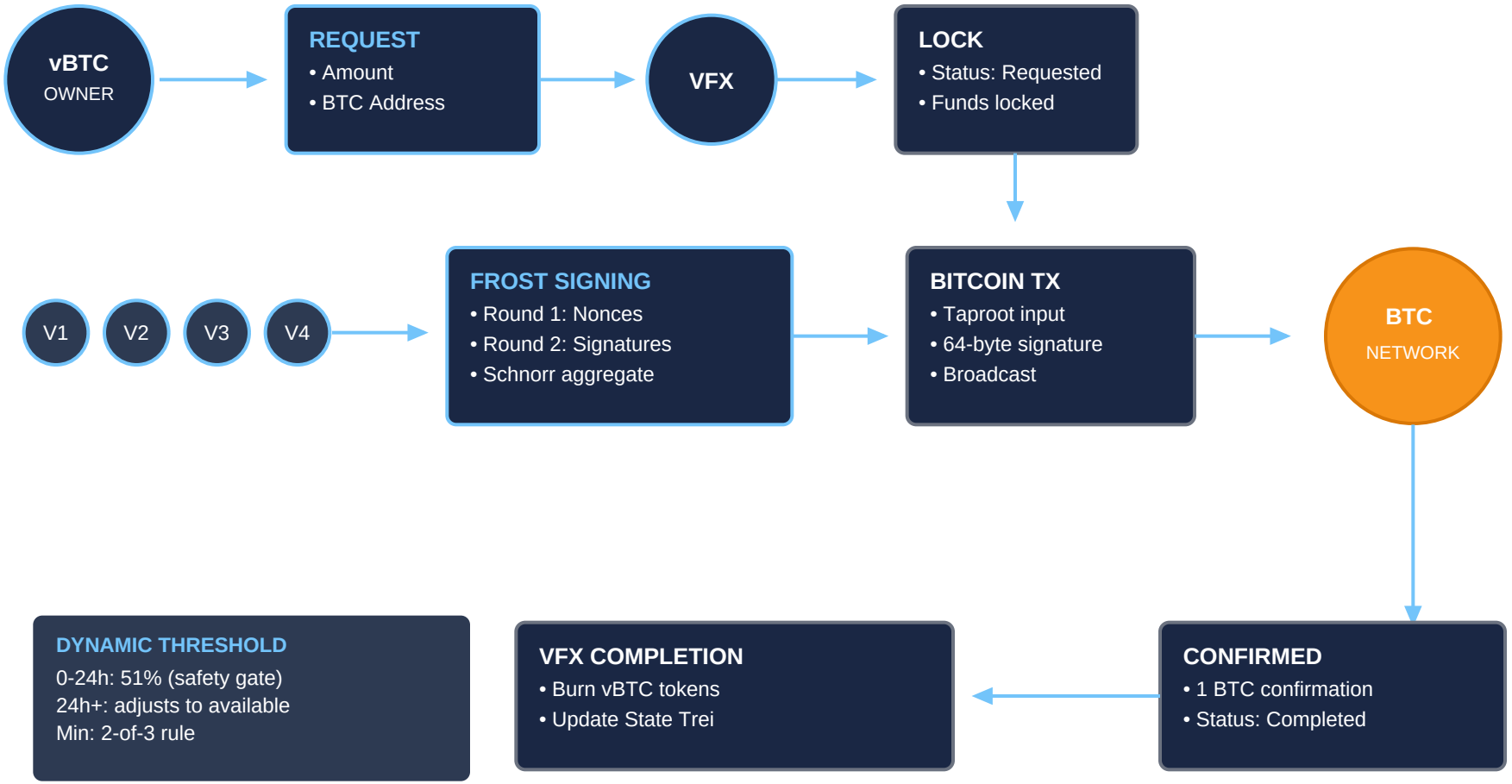
Calculated real-time from State Trei

STATE TREI UPDATE

- Record transfer
- Update balances
- Immutable ledger

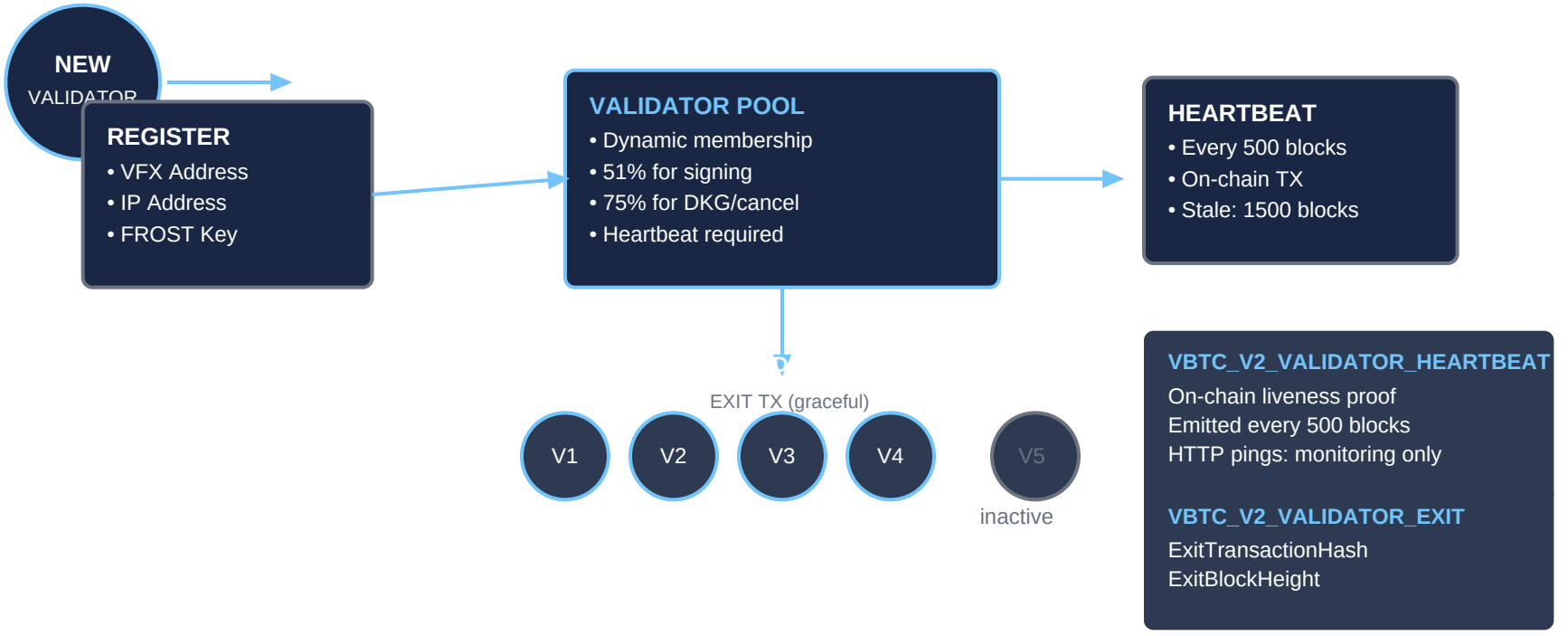
PROCEDURE 3 - WITHDRAWAL

Unlock to Bitcoin



PROCEDURE 4 - VALIDATORS

MPC Pool Management

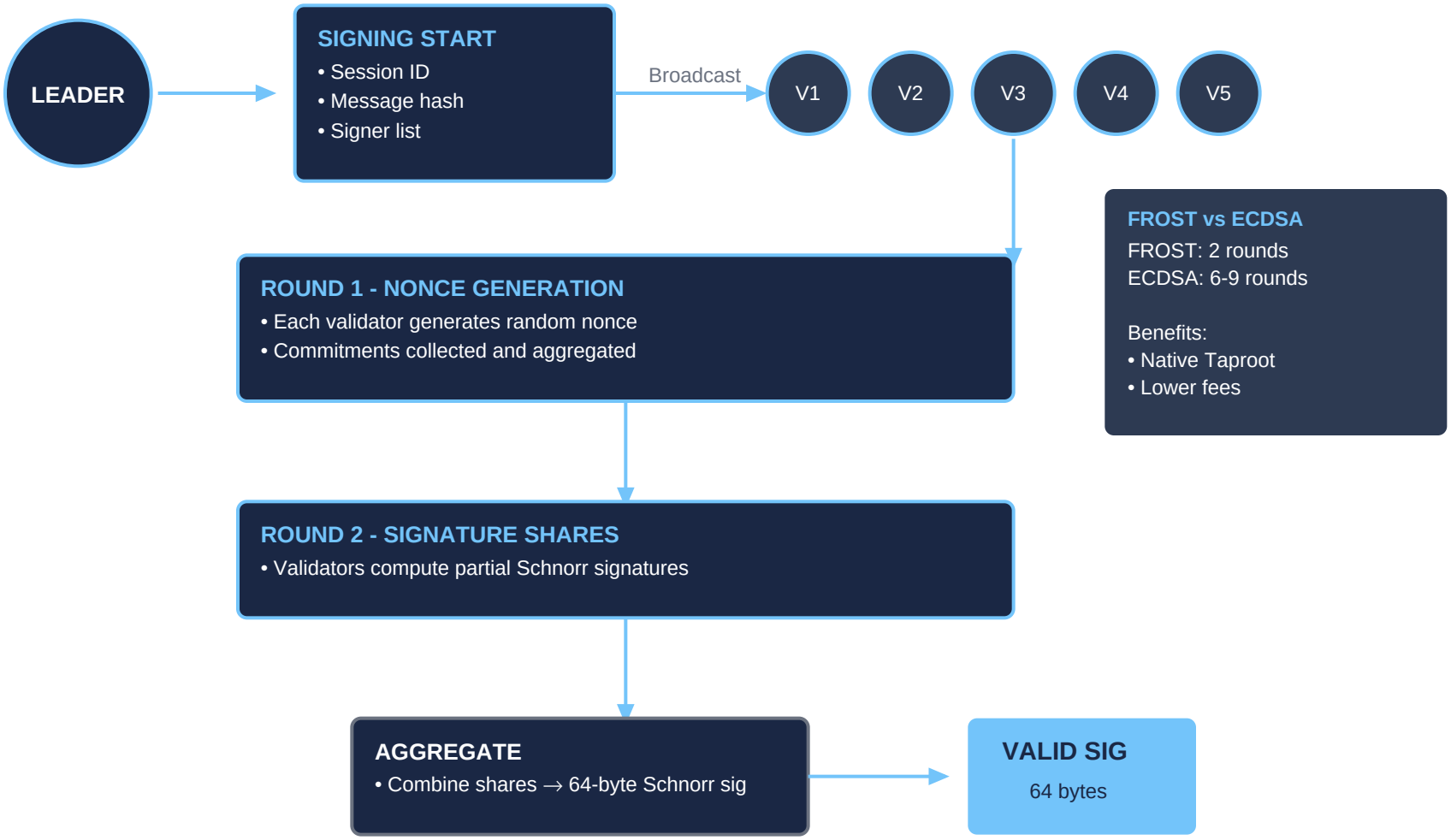


DYNAMIC THRESHOLD ADJUSTMENT

Hours 0-24:	51% threshold enforced (safety gate)
After 24h:	MIN(51%, available_validators% + 10%)
If 3 left:	2-of-3 rule applies (66.67%)
Example:	100 → 10 validators = 20% threshold after 24h

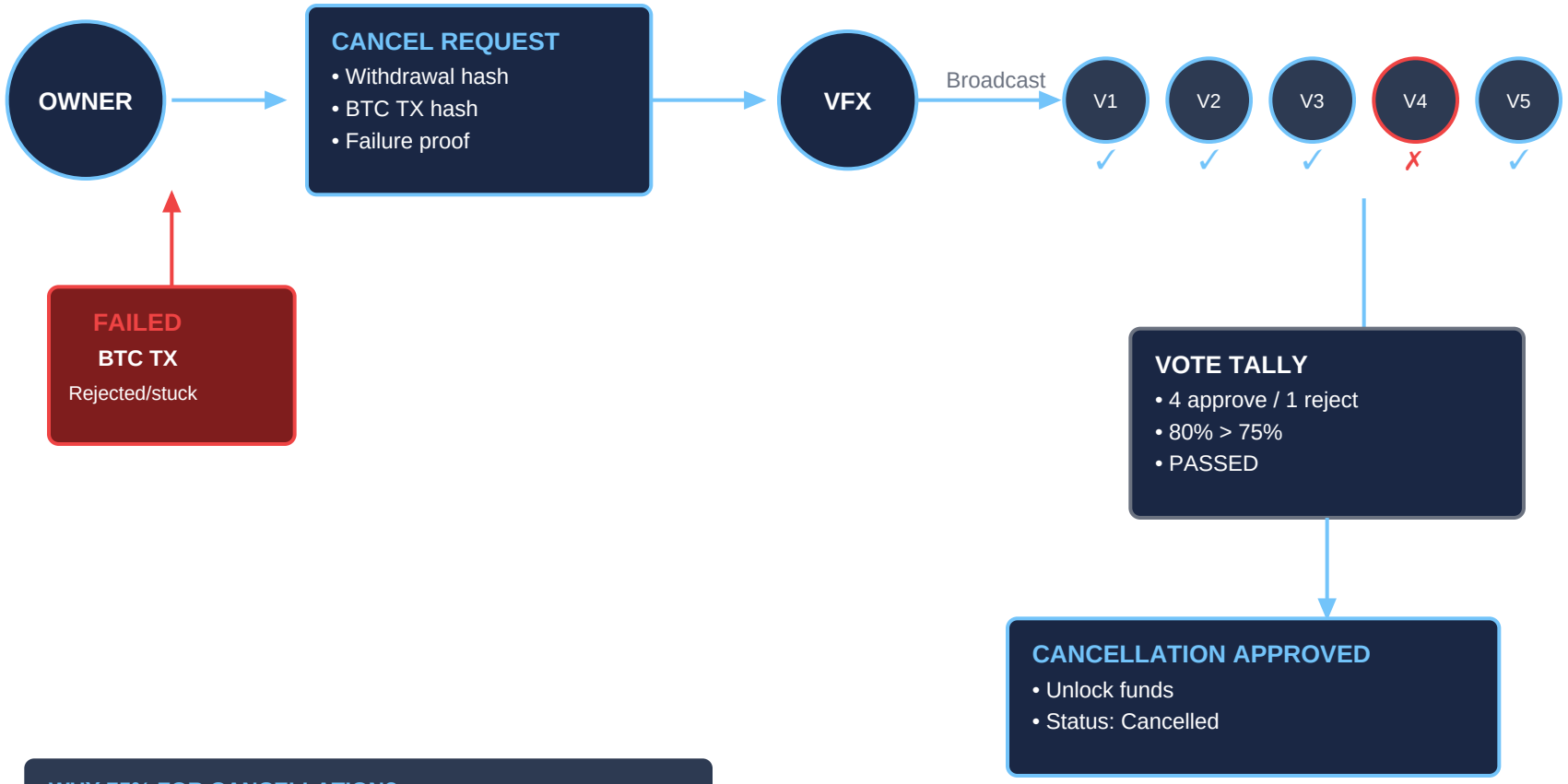
PROCEDURE 5 - FROST SIGNING

2-Round Schnorr



PROCEDURE 6 - CANCELLATION

Failed Withdrawal Recovery



WHY 75% FOR CANCELLATION?

Higher than signing (51%) to prevent abuse

Valid reasons:

• TX rejected • TX stuck • Timeout