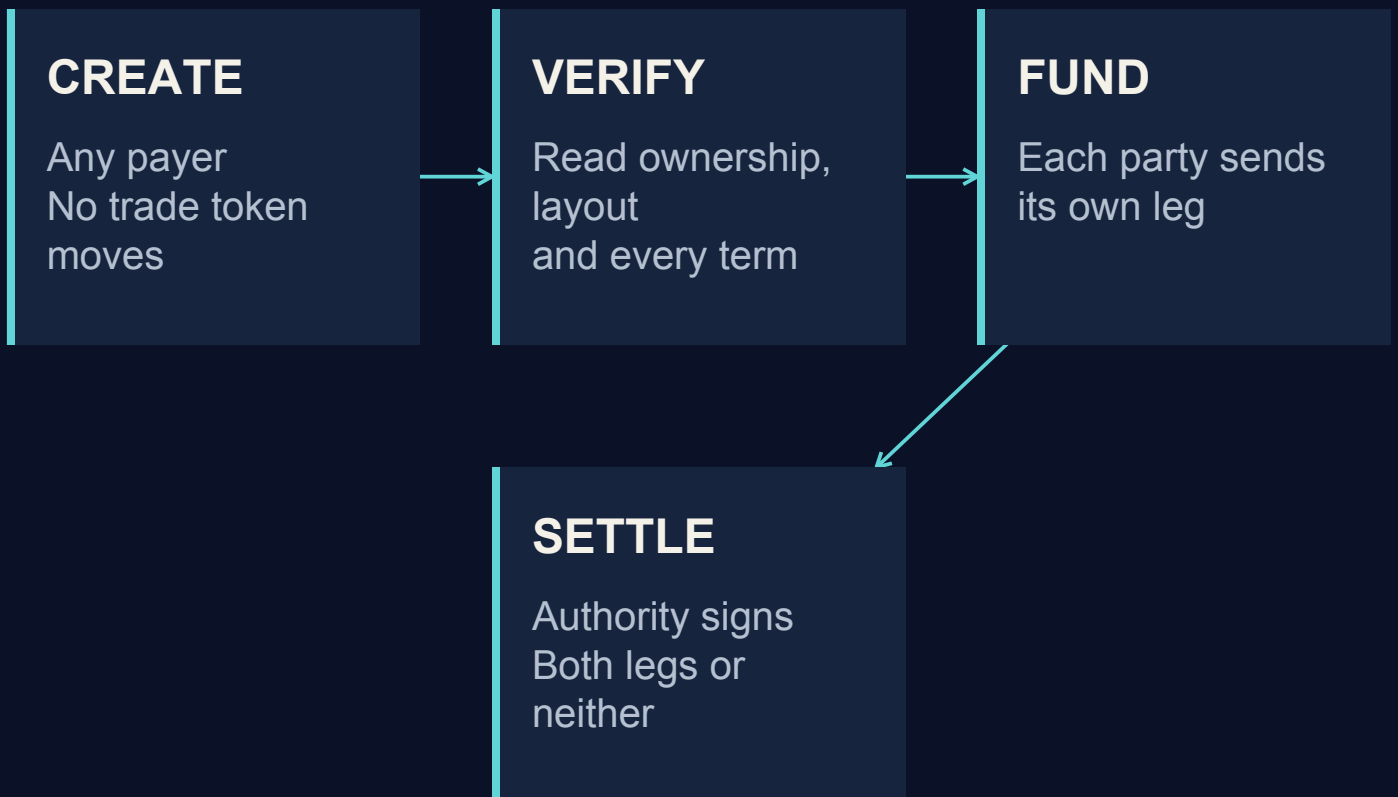


Anyone can write the ticket.

Permissionless creation is safe only when funding begins with verification.



Creation does not carry the parties' signatures. Funding and settlement remain separately authorized actions.

The record is a proposal. The first token makes it real.

Atomicity protects one narrow moment.

The final exchange can be indivisible while the proposed ticket is still wrong.

ATOMIC SETTLEMENT

Atomic transfer

Both funded legs move together

Only the stored authority settles

A failed sub-step reverts the transaction

TICKET VERIFICATION

Verified ticket

The record belongs to the real program

Stored terms match the approved order

Token powers do not invalidate the plan

Atomicity does not authenticate the off-chain agreement or make the authority available.

Execution safety and input truth are different controls.

The address is a label. The terms live inside.

A familiar PDA can hold amounts, times or destinations you never approved.

ADDRESS SEEDS

Identity fields

Settlement authority

Two parties + two mints

Single-use nonce

STORED TERMS

Economic fields

Amounts

Earliest time + expiry

Two settlement destinations

The official guide specifies a fixed 458-byte program-owned account. The client must verify both identity and economic fields.

Deriving the address is necessary. Reading the record is decisive.

Five checks before the first token moves.

Make the consent boundary inspectable and fail closed on any mismatch.

CHECK	COMPARE	FAILURE ACTION
Owner	DvP program owns the account	Stop
Layout	Exactly 458 bytes	Stop
Identity	PDA, parties, mints, nonce	Stop
Economics	Amounts, times, authority	Stop
Delivery	Both settlement destinations	Stop

Build funding only after the ticket passes every comparison.

Test the rejection path before the happy path.

One changed destination should prevent a funding instruction from being built.

FIXTURE A

Expected terms
and destinations



ACCEPT

Checks pass
Funding may be built

FIXTURE B

One material field
changed



REJECT

Show the mismatch
Build nothing

Use serialized account fixtures or devnet records with no real assets. Change one field per case.

Prove the client notices the wrong ticket.

Move the control left of transaction build.

A warning after funding records the failure. A gate before funding prevents it.

01

Fetch

Read the program-owned record

02

Compare

Match every approved term

03

Construct

Create funding only after PASS

Mismatch stays visible. Unknown never becomes zero or consent.

The safest integration makes refusal routine.

Make the earlier refusal boring.

Atomic settlement makes the last button safer. Verification decides whether the first token should move.

PERMISSIONLESS INPUT

Anyone can write the ticket.

Should the first token move?

Put ownership, layout, identity and every economic term in front of the funding button.

Read-only research · Proposed fixture test · No asset movement

Treat the record as a proposal until the checks pass.