YOUR COMPILER REFUSES THE SEQUENCE NOBODY WROTE A TEST FOR.

```
error[3-0036]: assertion failed in const context
= assertion message: invariant 'paid once' broken: buyer and seller both paid
error[8-0081]: static assertion failed
= left: `11234`
```

evidence/transcript-fail-refund-after-release.txt · fe 26.6.0 [5b3f96a]



INVARIANT 'PAID ONCE' BROKEN

ROUTE 1· 1· 2· 3· 4

START	1 DEPOSIT	1 DEPOSIT	2 LOCK	3 RELEASE	4 REFUND
[Open,0,0,0]	[Open,1,0,0]	[Open,2,0,0]	[Locked,2,0,0]	[Locked,1,1,0]	[Settled,0,1,1]

TESTS CHECK THE PATHS AN AUTHOR IMAGINED.

FIVE ACCEPTED CALLS. BOTH SIDES PAID.

ROUTE 1· 1· 2· 3· 4

START	1 DEPOSIT	1 DEPOSIT	2 LOCK	3 RELEASE	4 REFUND
[Open,0,0,0]	[Open,1,0,0]	[Open,2,0,0]	[Locked,2,0,0]	[Locked,1,1,0]	[Settled,0,1,1]

```
patched contract [search removed], fe test --filter
test_attack_patched_replay:
PASS [0.0002s] test_attack_patched_replay
-> all five calls accepted; the seller AND the buyer
were paid
```

evidence/demo-run.txt · the patched contract with the search removed

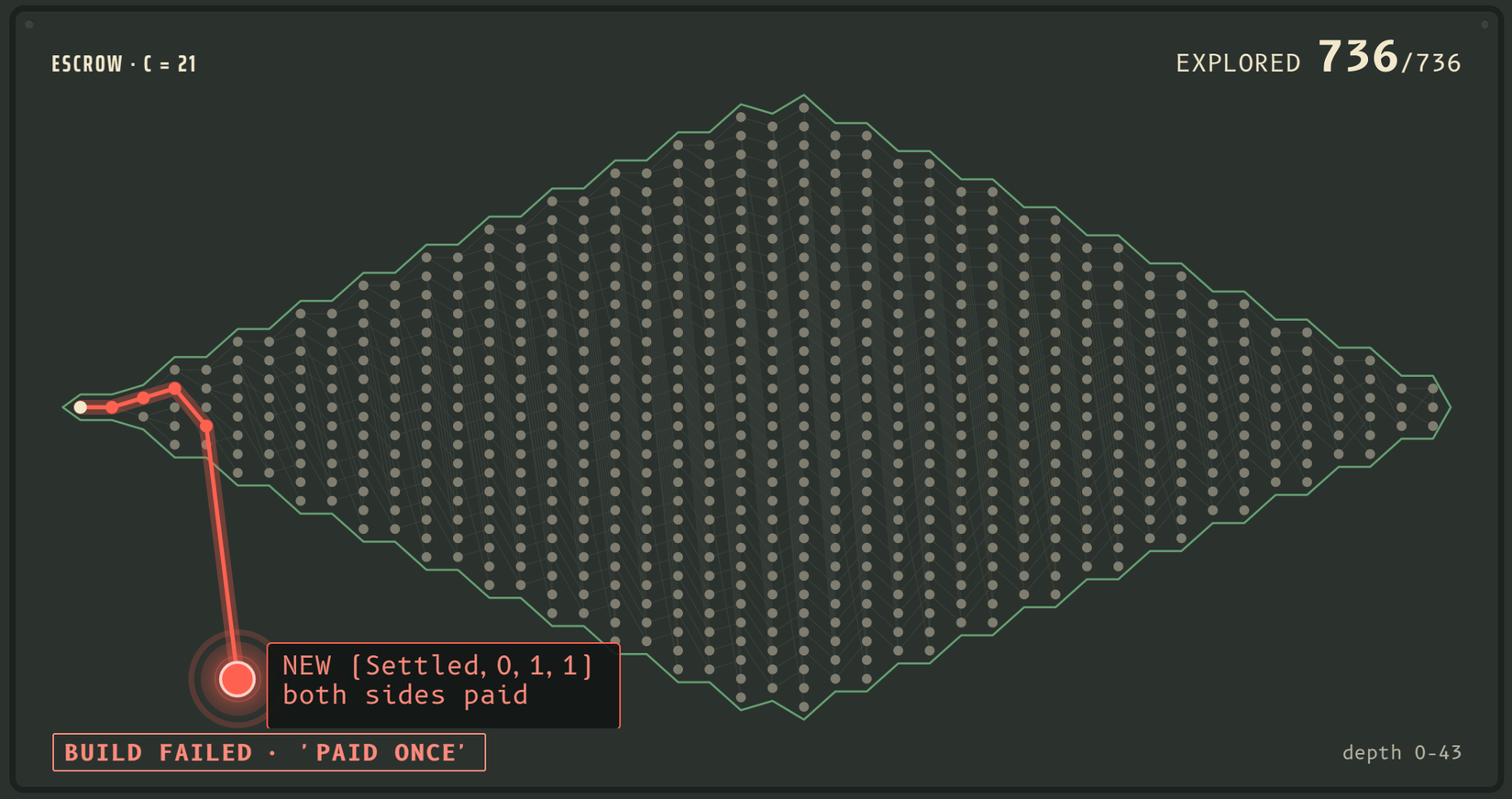
The patched contract accepts all five calls; only the order breaks the escrow. The per-handler test suite misses this patch (`evidence/check-bugs.txt`).

THE COMPILER IS THE MODEL CHECKER.

A `const fn` breadth-first search inside `fe build`. Every successor is checked against five named invariants.

ONE LINE CHANGES · A NEW RED LAMP

press → to step the search · evidence/state-graph-escrow.json



DROP ONE CONDITION. THE BUILD GOES RED.

SRC/ESCROW.FE · REFUND GUARD

```
-   if s.escrow > 0 && s.seller == 0 {
+   if s.escrow > 0 {
```

```
error[3-0036]: assertion failed in const context
= assertion message: invariant 'paid once' broken: buyer and seller both paid
error[8-0081]: static assertion failed
= left: `11234`
```

evidence/transcript-fail-refund-after-release.txt [excerpt]

The compiler names the invariant and prints the route as digits.

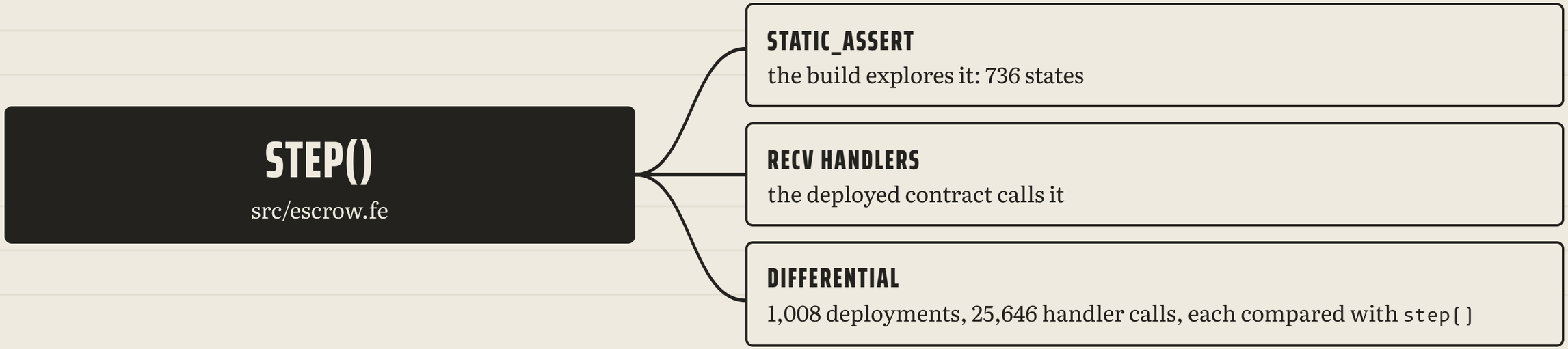
LEFT: `11234`, DECODED

ROUTE 1 · 1 · 2 · 3 · 4

START	1 DEPOSIT	1 DEPOSIT	2 LOCK	3 RELEASE	4 REFUND
[Open,0,0,0]	[Open,1,0,0]	[Open,2,0,0]	[Locked,2,0,0]	[Locked,1,1,0]	[Settled,0,1,1]

CHECKED = DEPLOYED

ONE `STEP( )`, CALLED BY THE CONTRACT.



1,008
deployed contracts

25,646
handler calls replayed

25,646
stored states compared with `step[]`, all equal

`evidence/differential.txt · the vault's caller and timelock checks are adapter code outside the check [README · Limitations]`

THREE EXECUTIONS

COMPILE TIME, EVM, NATIVE: ONE COUNT.

736 = **736** = **736**

`static_assert` · Sonatina EVM · `fe test` · `fe test --backend native`

Asserted in `test_runtime_explore_agrees` (and 494 at C = 17).
The EVM search at C = 17 burns **16,394,182** gas: `black_box`
keeps it from being folded.

28
EVM tests

10
native tests

15/15
Fe pins matched by a Python oracle

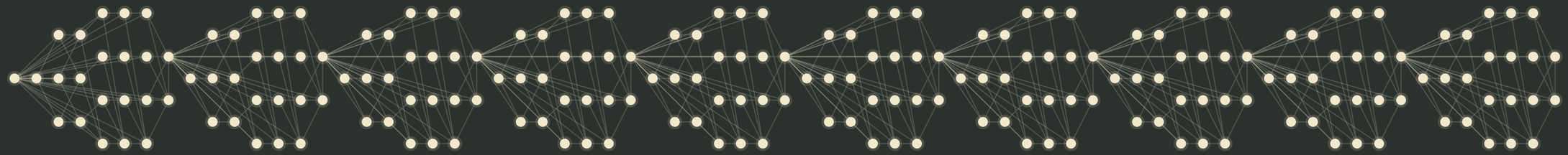
`evidence/transcript-tests.txt` · `evidence/gas.txt` · `evidence/oracle.txt`

ESCROW + A 2-OF-3 TIMELOCK VAULT

TWO PROTOCOLS. NINE PATCHES, NINE REFUSALS.

VAULT · B = 10 · T = 3

211 STATES · 580 WIRES



NO.	PATCH	INVARIANT	ROUTE
01	refund-after-release	'PAID ONCE'	11234
02	settle-early	'SETTLED EMPTY'	1123
03	mint-release	'CONSERVED'	123
04	cap-off-by-one	'WITHIN CAPACITY'	11111111111111111111
05	vault-approve-twice	'COUNTED ONCE'	122
06	vault-execute-early	'TIMELOCK RESPECTED'	1236
07	vault-pay-twice	'PAYS ONE UNIT'	1235556
08	vault-cancel-pays	'ONLY EXECUTE PAYS'	17
09	vault-execute-unguarded	'TWO DISTINCT APPROVALS'	6

THE CEILING

1,000,000 STEPS PER ASSERT. NO OVERRIDE.



Consts that reference consts share one budget, so bigger models split into independent asserts: **91** · **238** · **385** states.

Bounded: only the stated capacities. No liveness.

The escrow model has no caller identity and moves no value.

Model, Fe code and oracle share one author.

TAKE FE OUT AND THE CHECKER IS GONE.

CONST FN + WHILE | ARRAY WRITES | STATIC_ASSERT | ASSERT! MESSAGES | ENUM + MATCH

CONTRACT · MSG · RECV | FE TEST · 2 BACKENDS | FE FMT --CHECK

Since Fe 26.1.0 a `const fn` can loop and write arrays under `static_assert`. The search is ordinary Fe; the build is the checker.

const fn + while + array writes	src/escrow_explore.fe:94
static_assert as the build gate	src/escrow_explore.fe:254
assert! message = named invariant	src/escrow_explore.fe:41
contract · recv calling step()	src/escrow_contract.fe:64
fe test on both backends · black_box	src/tests.fe:30

`fe 26.6.0 [5b3f96a] · no comparison with other languages was made`

CLONE IT. BREAK IT.

WATCH THE BUILD REFUSE.

```
# fe 26.6.0 [5b3f96a]
git clone https://github.com/edycutjong/exhaust
cd exhaust
fe build            # green: 736 states
sh demo/run.sh      # red: 'paid once', 11234
fe test && fe test --backend native
```



exhaust.edycu.dev

github.com/edycutjong/exhaust

Apache-2.0