

Don't Share the Database

Interface Contracts Between Isolated AI Agents

Martin Bliss

AGNTCON + MCPCON NORTH AMERICA • OCTOBER 22, 2026

You've seen this talk. It had a different noun.

AGENTS

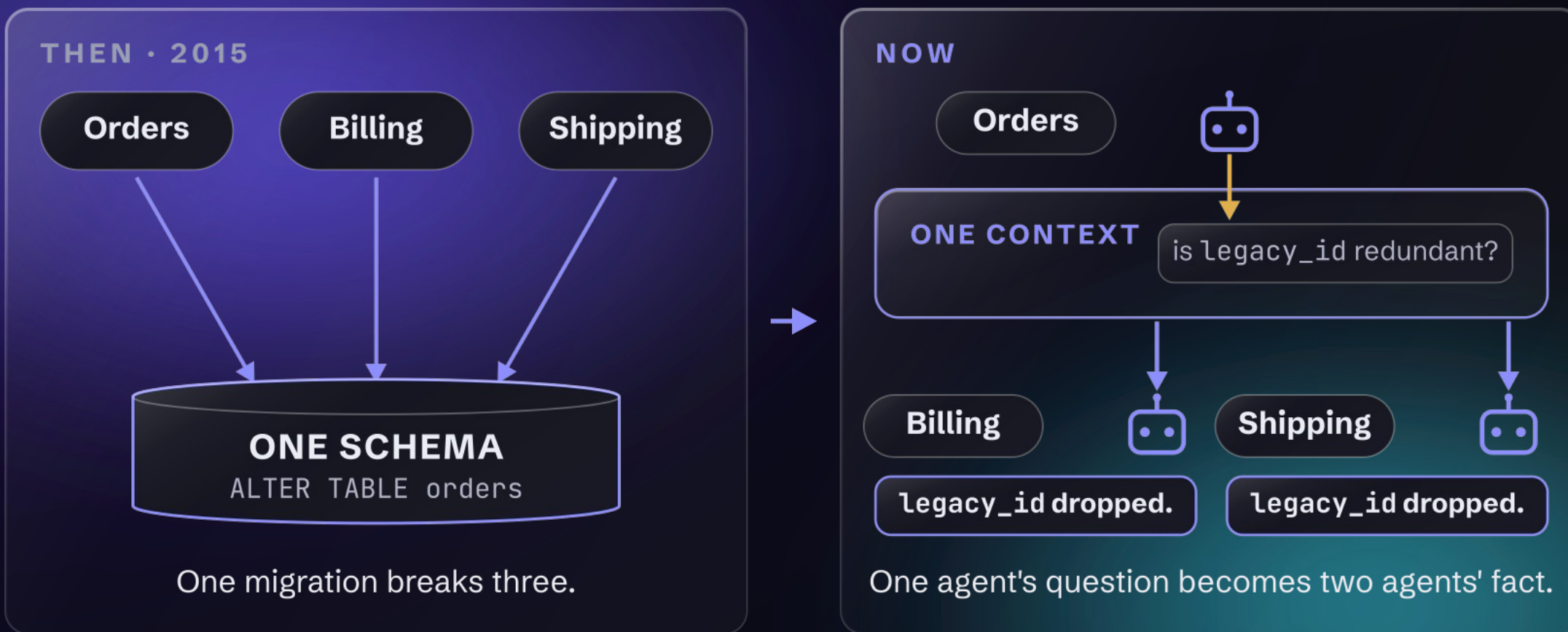
~~Microservices:~~

Don't Share the Database

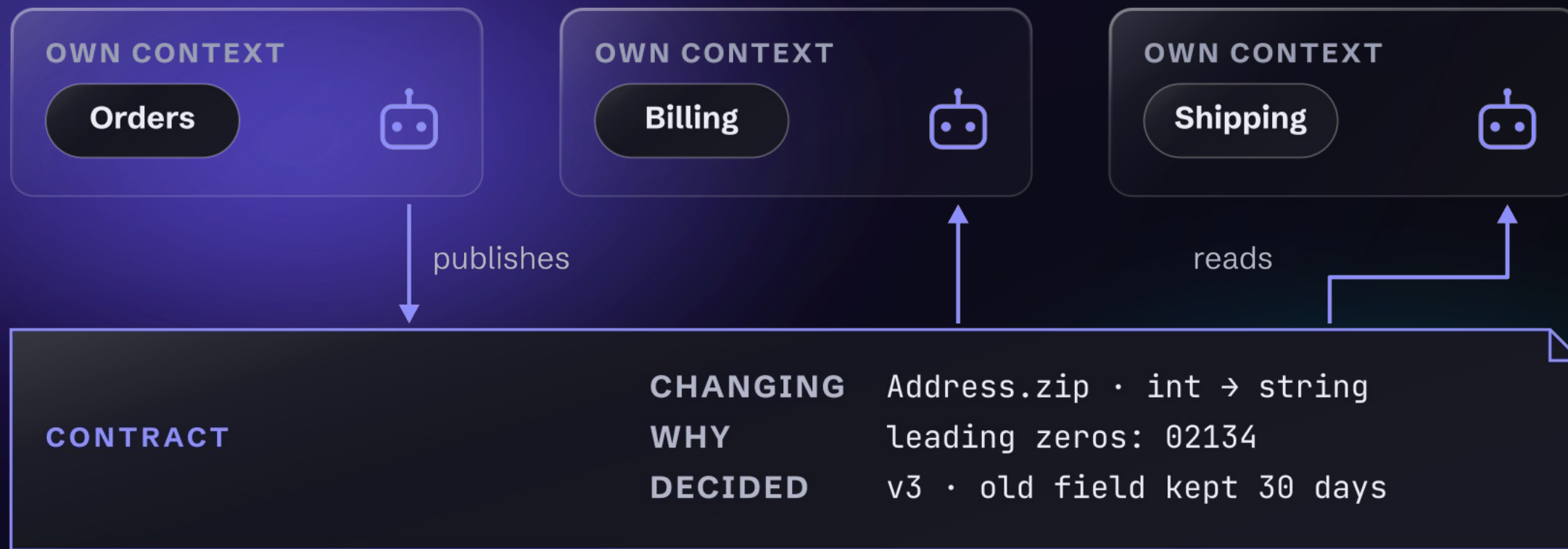
- Each service owns its own data
- Integrate through APIs, not tables
- A shared schema couples every deploy

2015

Then they shared a schema. Now they share a context.

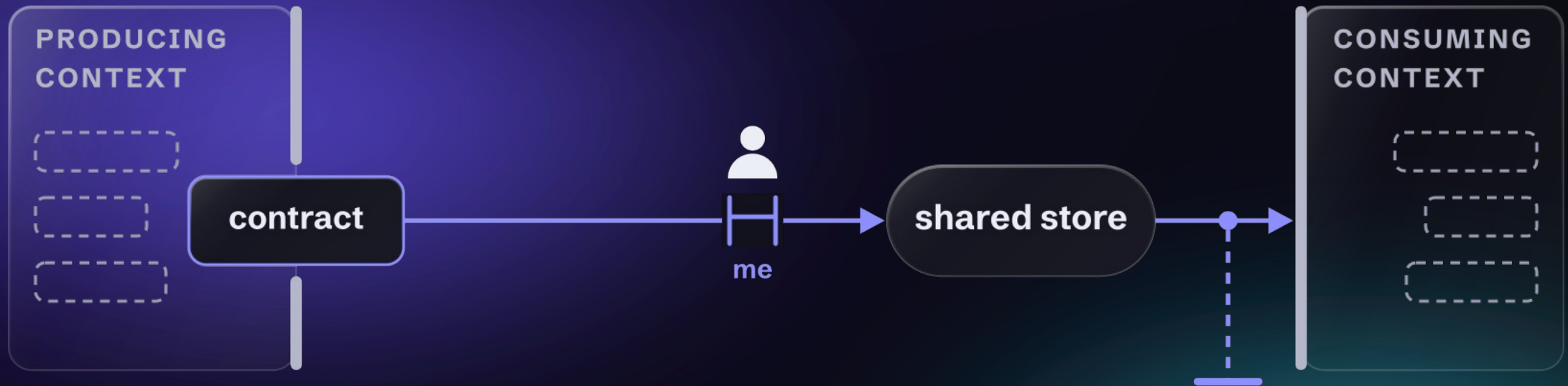


Separate contexts. One contract.



Walls alone fork reality. Walls + a contract **pay the tax once, at the wall.**

Your agents are like microservices. Don't share the database. Share the contracts.



1 • Publish a contract

decisions + state out,
internals stay home

2 • Gate the write

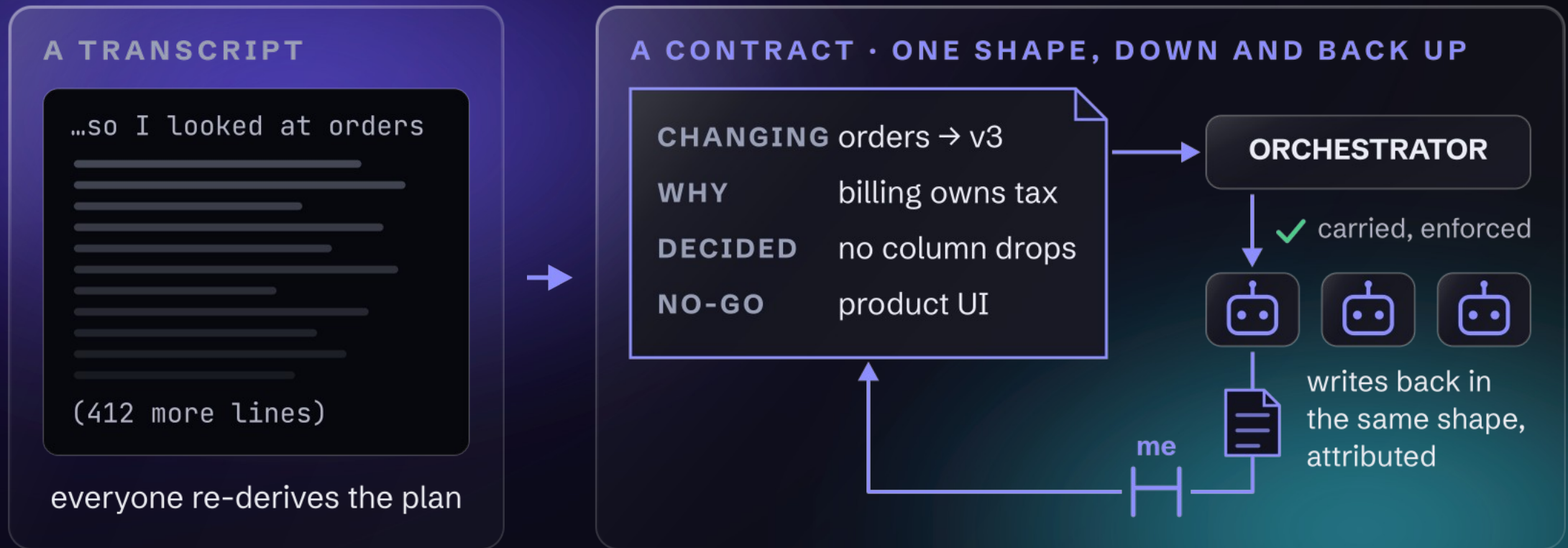
a human approves
before it lands

3 • Push back on a miss

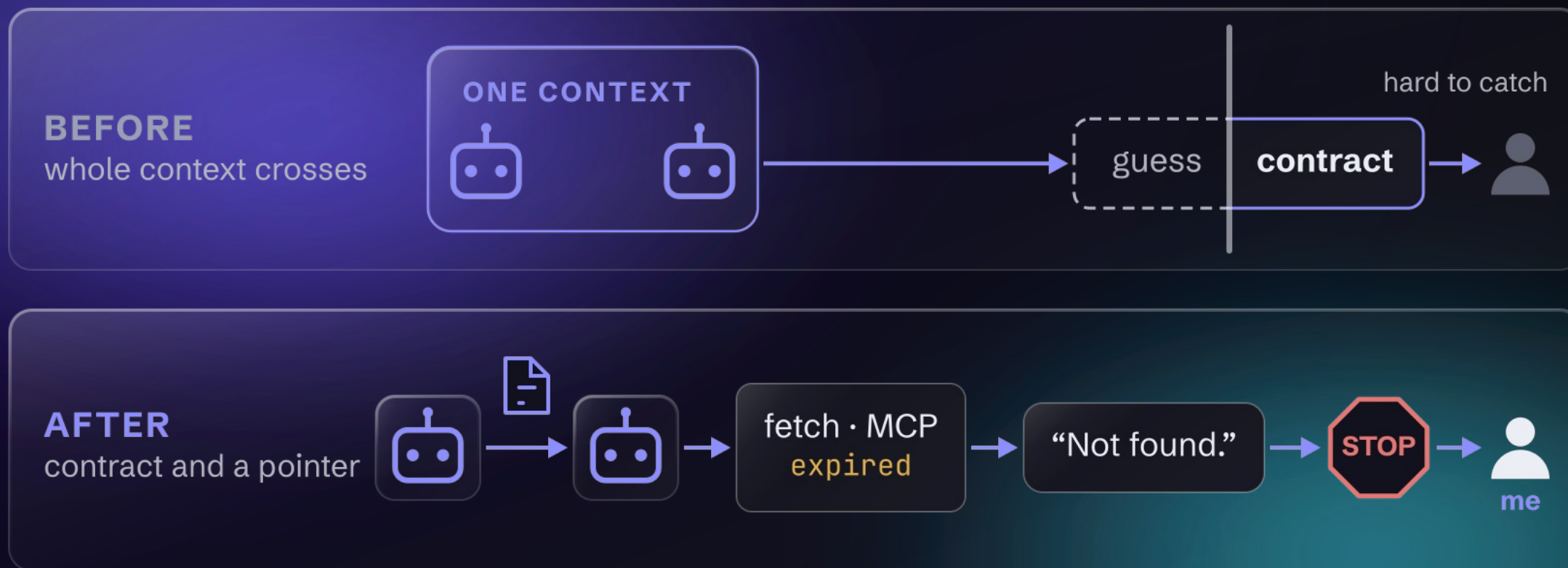
name what's missing, stop

A contract beats a transcript: written once at the top, enforced all the way down.

Then · 2015: the architect wrote the API spec; every team built and tested against it.



A narrow contract turns a guess into “not found.”



The after lane is drawn from a real session, Oct 2026.

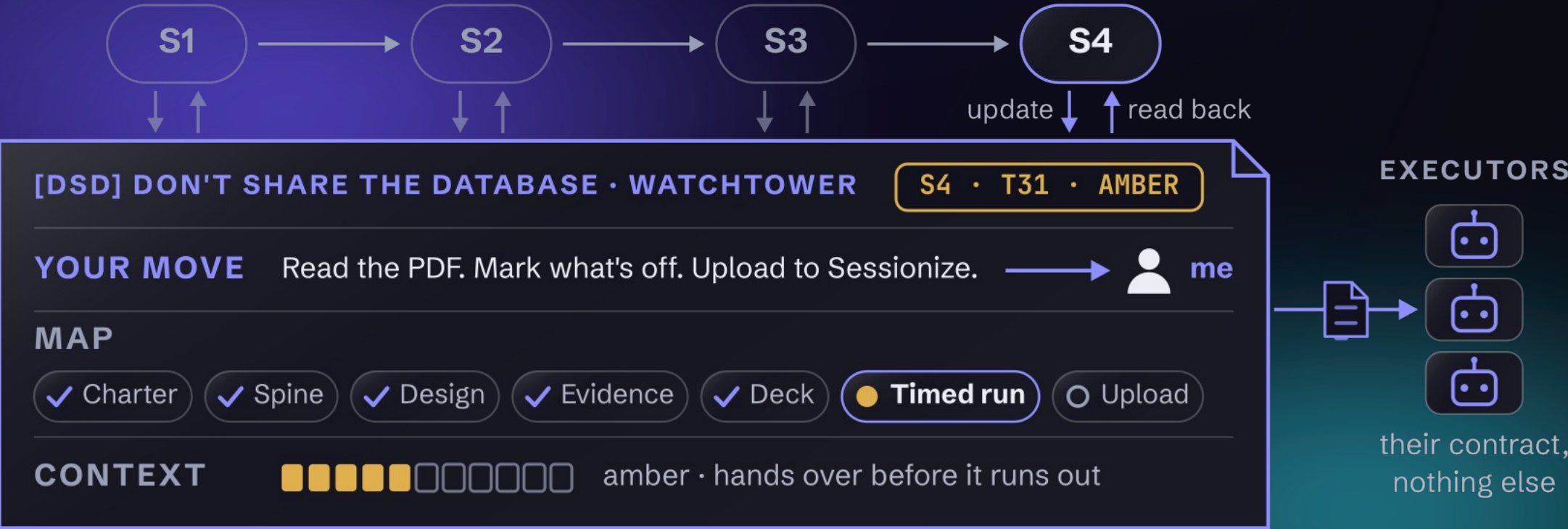


Meet the foreman: a personal AI session manager protocol



This presentation brought to you by Heimdall — *my* personal AI foreman

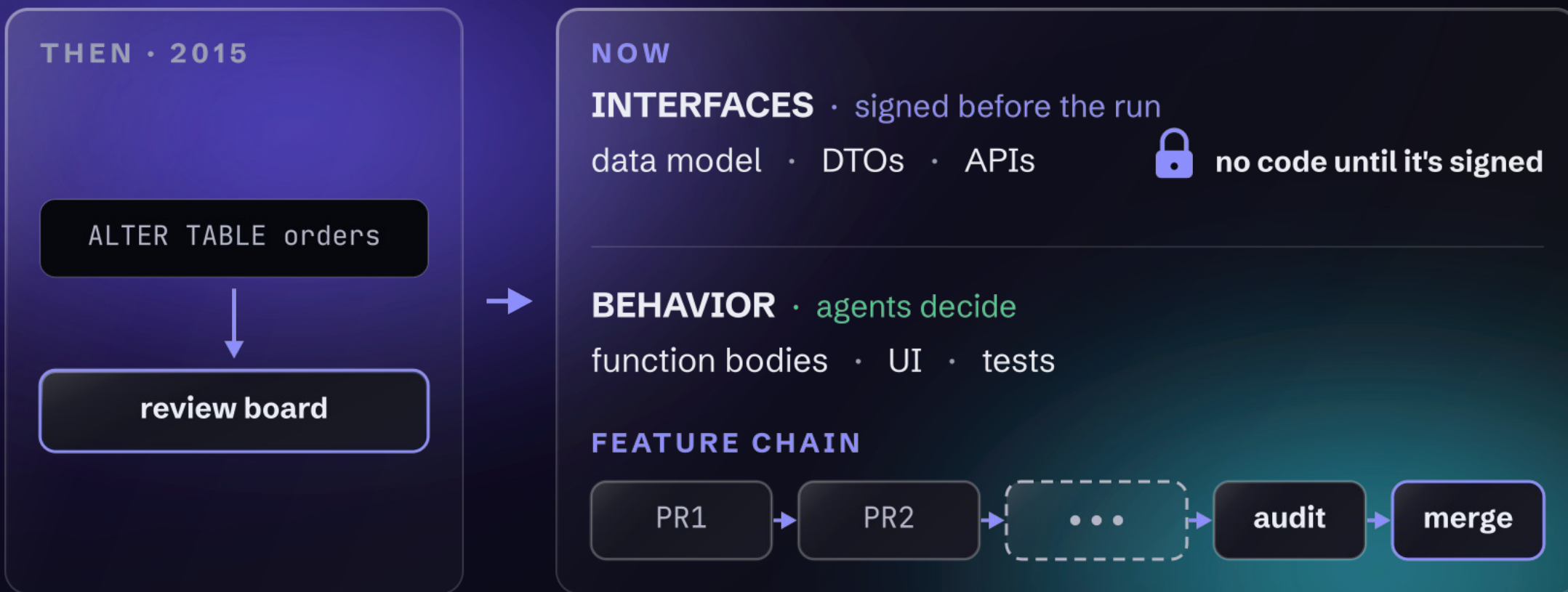
The foreman holds the project and watches the clock, so I don't have to.



This talk's own state document, Wed Oct 21, 2026.



**I sign the interfaces first.
Agents build the behavior inside them.**



Decide and tell me, or stop and ask: the foreman's rubric.

BEFORE

pre-mortem: where will this halt?

rule the likely ones now

DURING

a surprise · can it be undone?

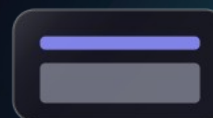
yes

DECIDE + DISCLOSE

a logged row,
read in the audit

no

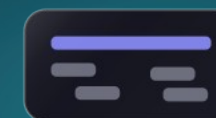
STOP + ASK, shaped



too tight



★ default

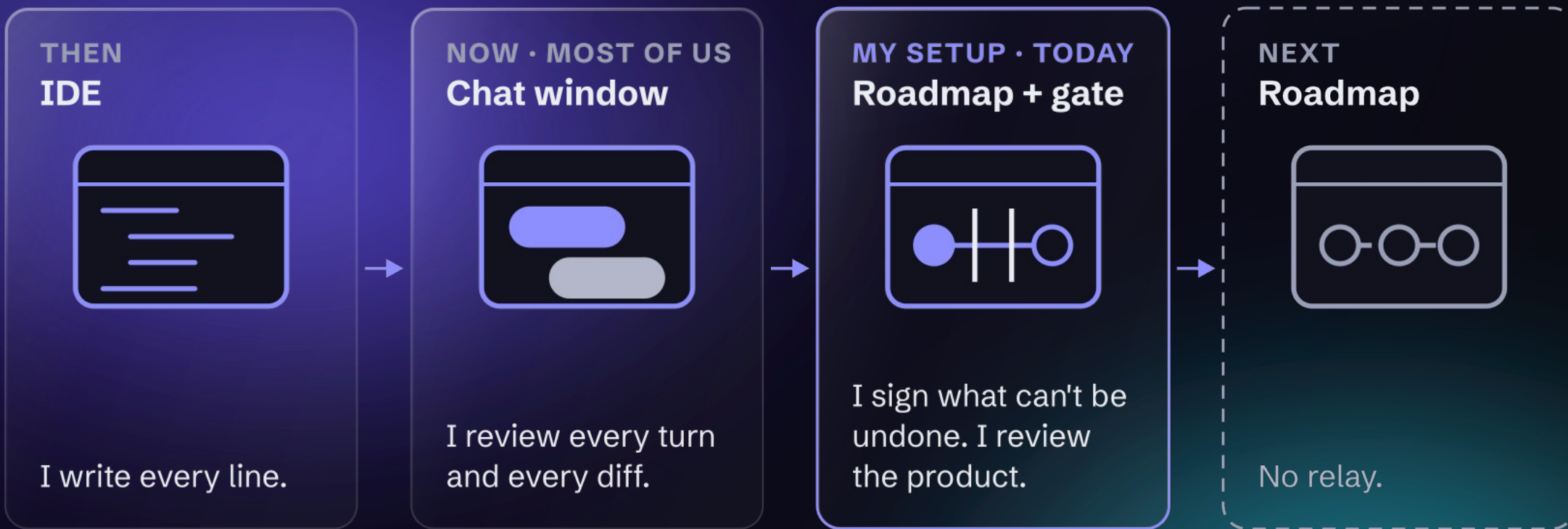


too loose



me

From the IDE, to the chat window, to the roadmap.



THE TAX, PAID IN

every keystroke

every line

every boundary

—

Takeaways

- 01 Publish contracts, not context.
- 02 Don't share the database. Or the context.
- 03 Gate shared writes through a human.
- 04 Treat a silent miss as a bug, not a default.

Next: the factory, built.

Open to consulting engagements and AI leadership roles

[linkedin.com/in/martinbliss](https://www.linkedin.com/in/martinbliss)

martin@prophecycontrols.com

Backup — the real artifacts

```
notion-download-attachment → response
{"name":"APIResponseError","code":"object_not_found","status":404,...,"message":"Could not find file_upload with
ID: [REDACTED]. Check that you have access and that you're authenticated to the
correct workspace."}

notion-get-file-download-urls → response
{"files":[{"reference":"notion-file-block://...&name=slides.pdf","url":"https://prod-files-secure.s3.us-west-
2.amazonaws.com/.../slides.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-
Credential=[REDACTED]&X-Amz-Date=20261018T063605Z&X-Amz-Expires=300&X-Amz-Security-Token=[REDACTED]
&X-Amz-Signature=[REDACTED]
&X-Amz-SignedHeaders=host&...","expiry_time":"2026-10-18T06:41:05.313Z"}],"unresolved":[]}
```

AGENT

I can't read slides.pdf. The attachment request returned object_not_found, and the download link expires in five minutes. I won't describe a file I haven't read. Can you upload it here?

Slide 7's source: the two MCP responses and the agent's reply, Oct 18, 2026. Names changed; secrets and the upload ID redacted.