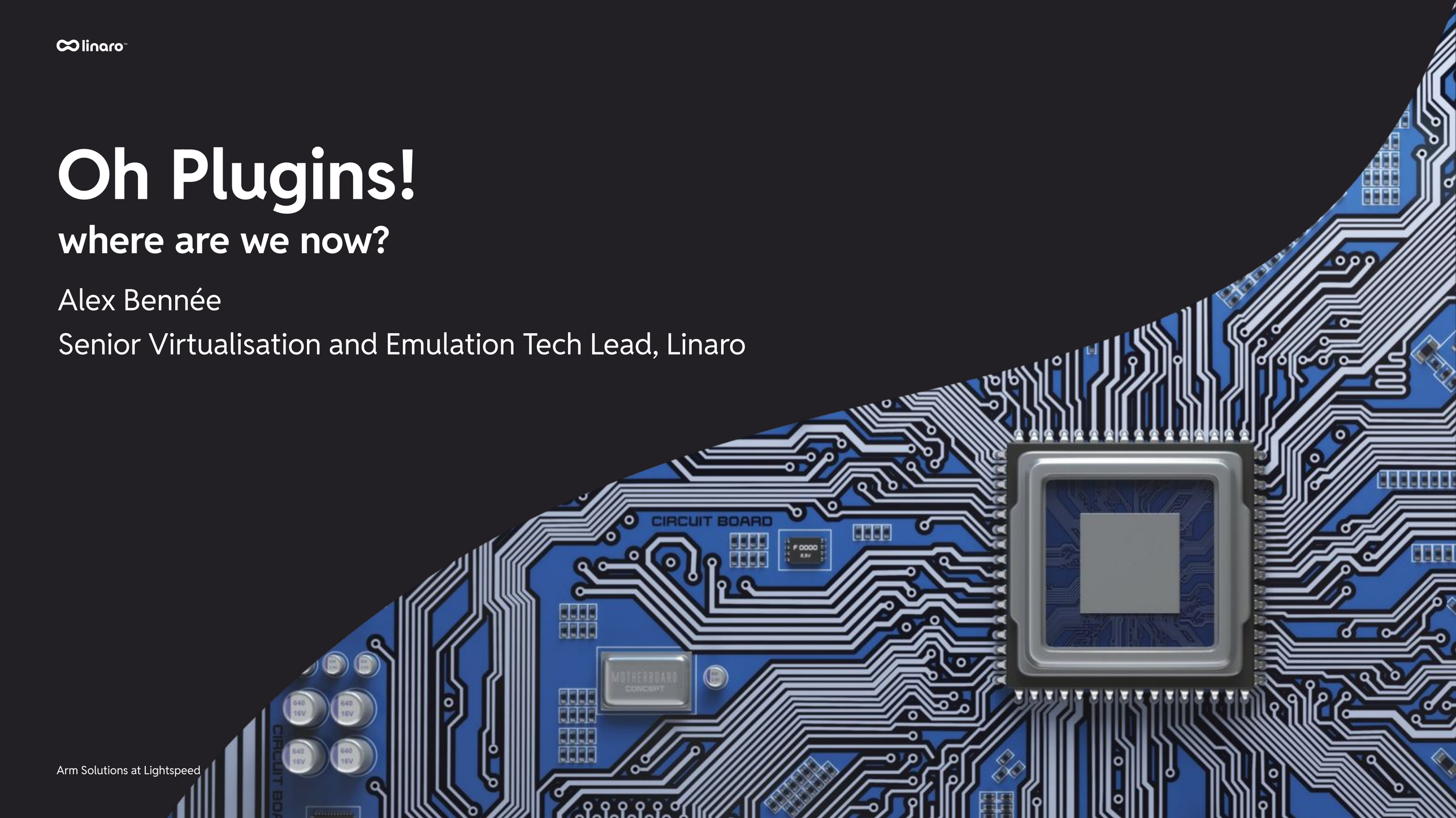
Oh Plugins!

where are we now?

Alex Bennée

Senior Virtualisation and Emulation Tech Lead, Linaro



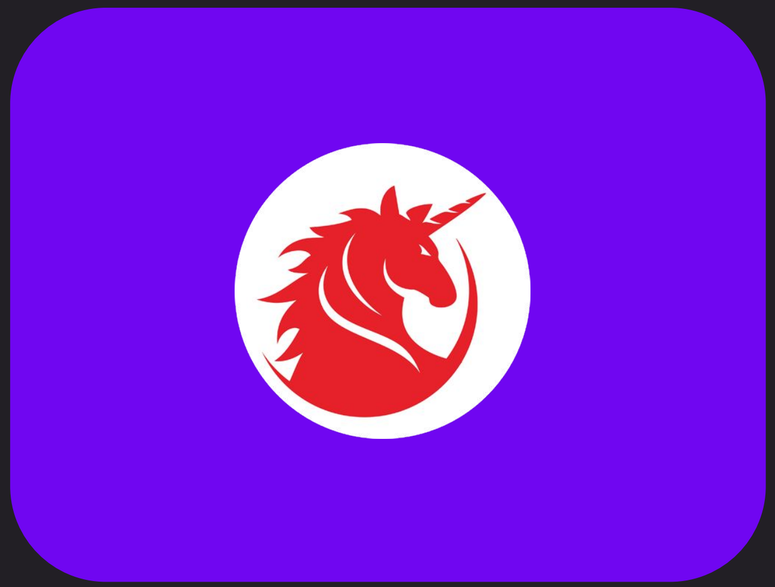
Agenda

- Instrumenting with QEMU
- Overview of TCG Plugins
- New features
- Future Directions?

Some Notable Forks

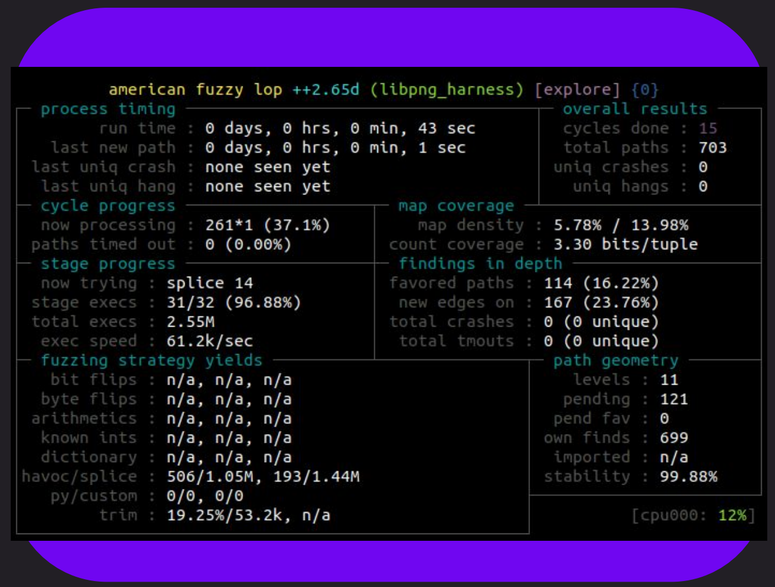
(cool things based on QEMU)

Unicorn



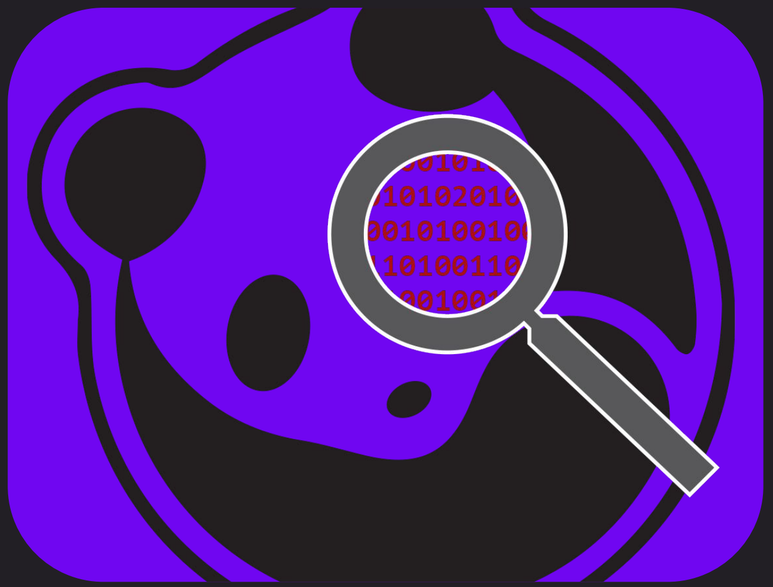
CPU emulation framework - lots of downstream users

AFL++



Application fuzzer, multiple backends (inc QEMU)

PANDA



Whole system analysis with record/replay and OS introspection

Why base on QEMU

victims of our own success

- Actively developed architectures
- Focus on Fidelity
- Performant enough

Loongson

Downstream downsides

forking isn’t free

- Re-basing a challenge
- Multiple hook implementations
- Instrumentation at architecture level

Downsides for upstream

- Missing functionality
- Missing developers
- Fixes not being upstreamed

TCG plugins

Subscribe to Events

- Translation
- vCPU Idle and Resume
- vCPU Init and Exit
- Syscall (*-user only)

At Translation

- Block
  - **Inline counter or callback**
- Individual Instruction
  - **Inline counter**
  - **Callback**
  - **Memory Callback**

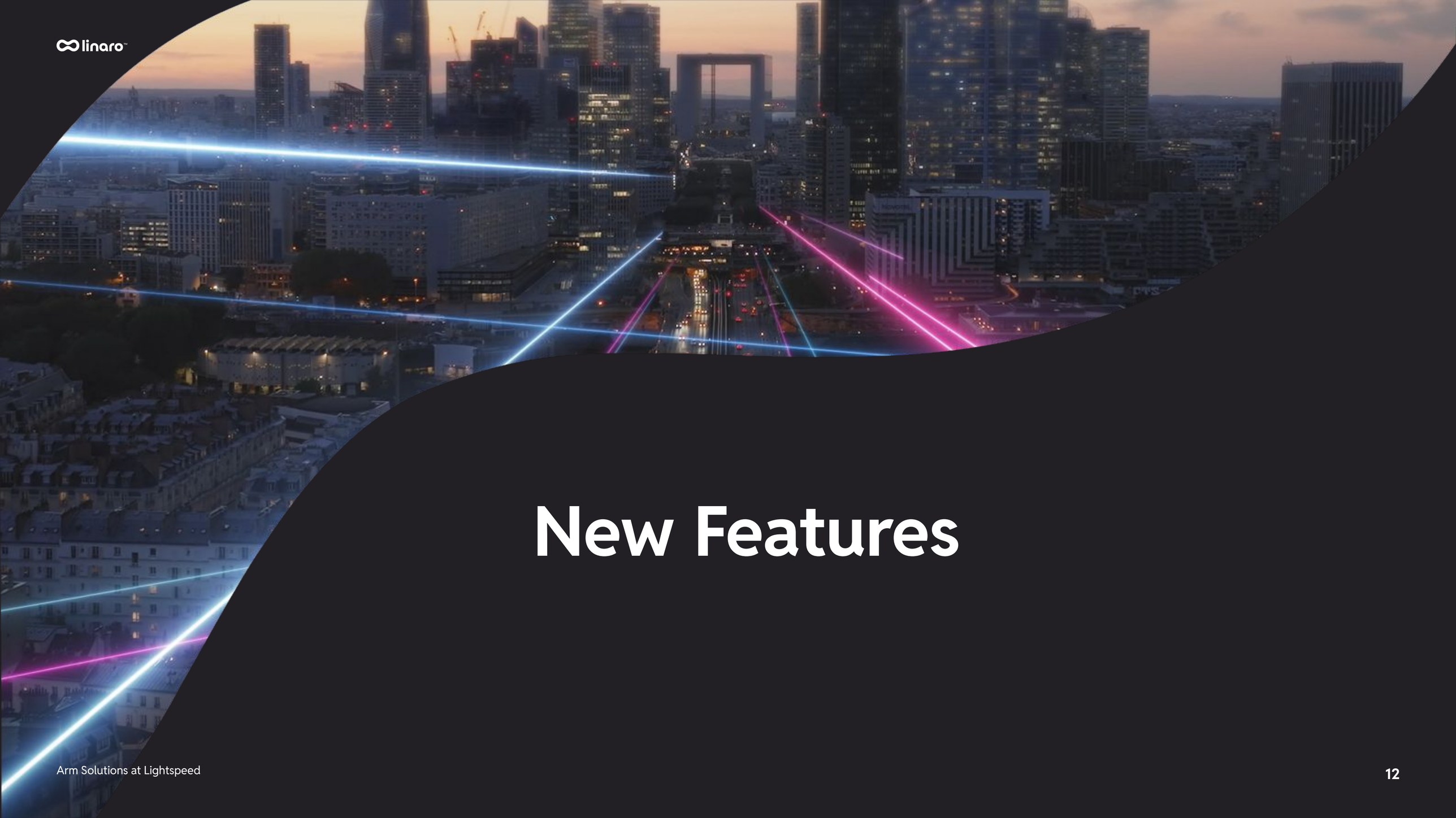
Limitations

- Plugin specific API
- Can’t change state*
- Cannot simulate HW
- Will not aid bypassing the GPL

See: What's Going On? Taking advantage of TCG's total system awareness, KVM Forum 2019

Helpers

- Extra information
  - **memory**
  - **instruction data**
  - **symbol information**
- Disassembly



New Features

New features

- Read Registers (see Akihiko's talk, up next)
- Scoreboards
- Memory access
- Controlling time

Scoreboards

thread safe inline ops

- qemu_plugin_scoreboard_new()
- inline STORE_U64
- Conditional callbacks

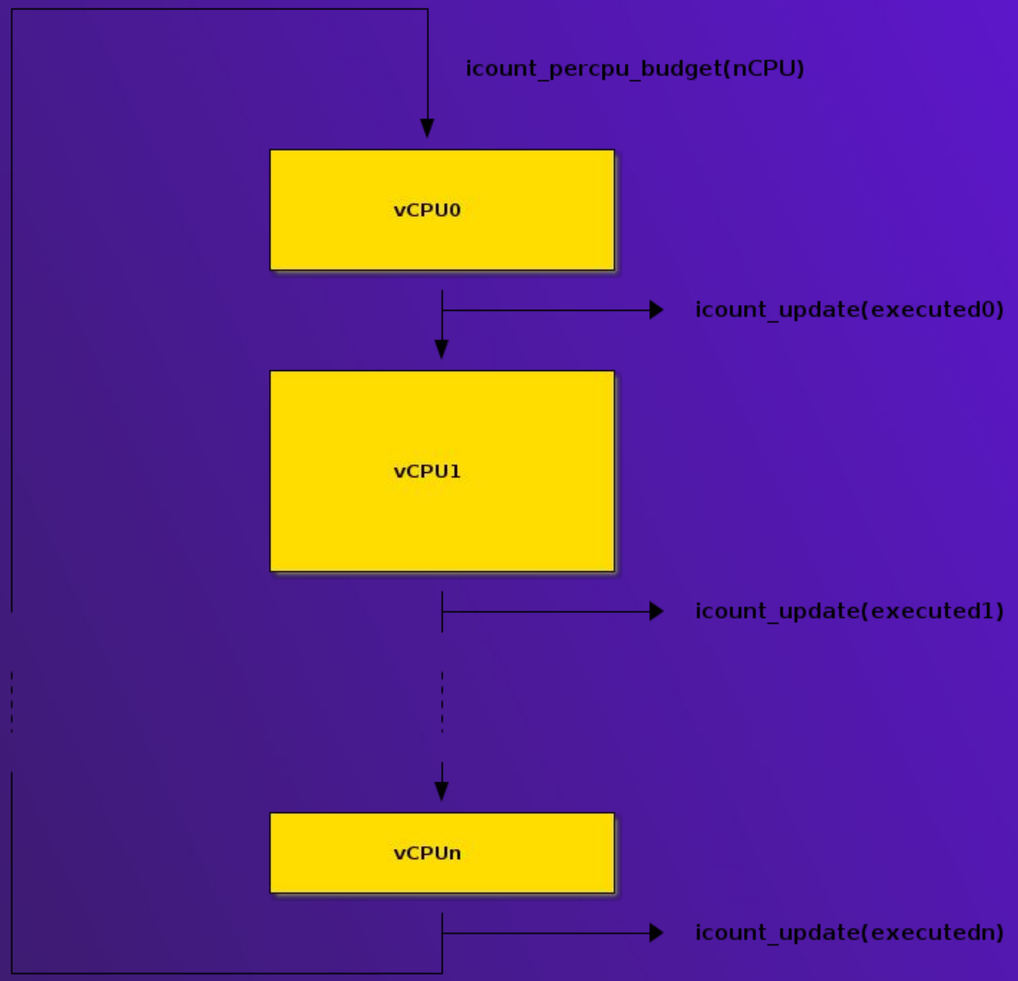
Memory APIs

- Two APIs
- qemu_plugin_mem_get_mem_value()
- qemu_plugin_read_memory_vaddr()

Controlling Time

or the illusion of it

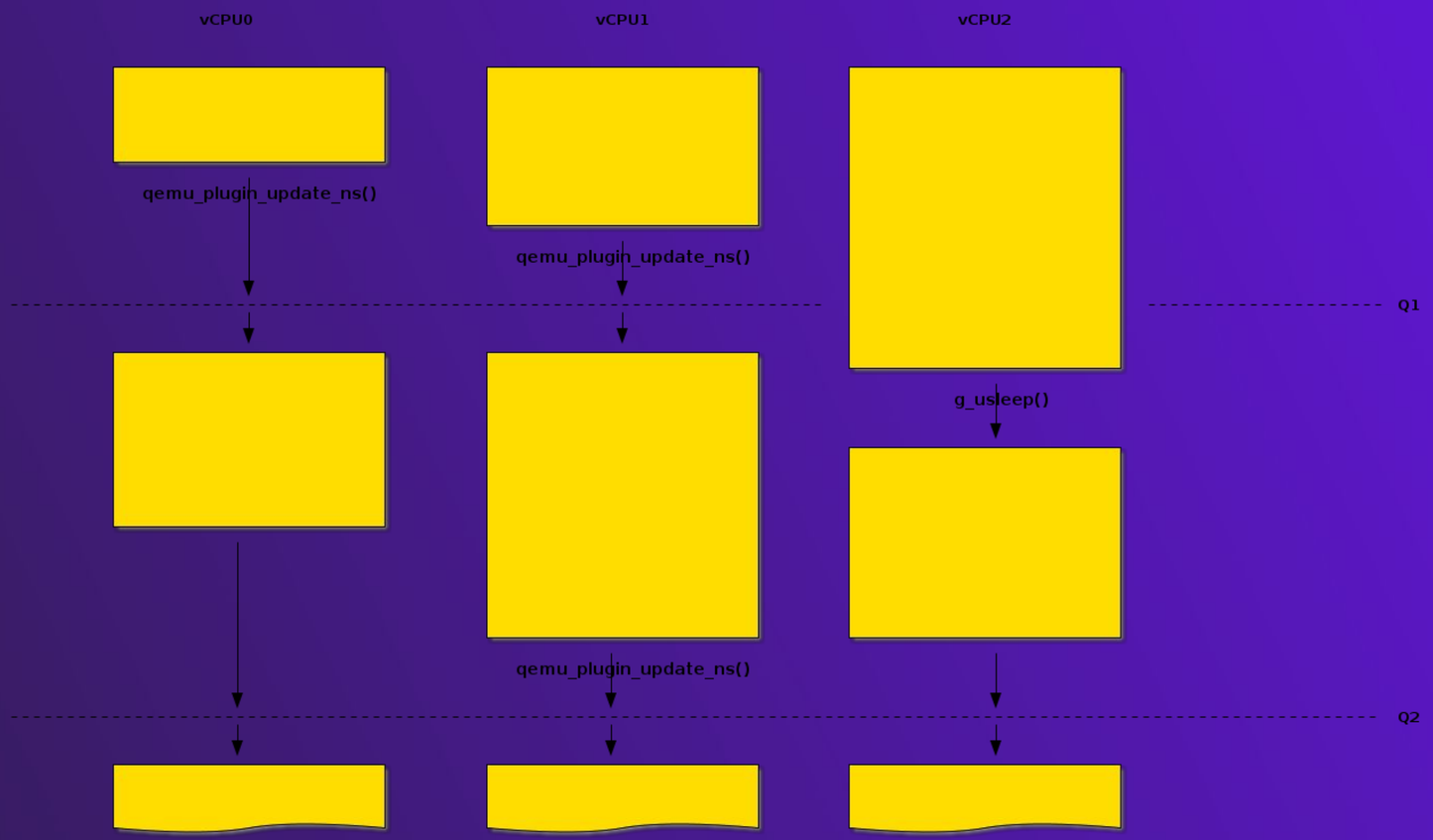
- icount
- round-robin schedule



Controlling Time

plugins controlling state

- qemu_plugin_update_ns()
- multi-threaded
- ips



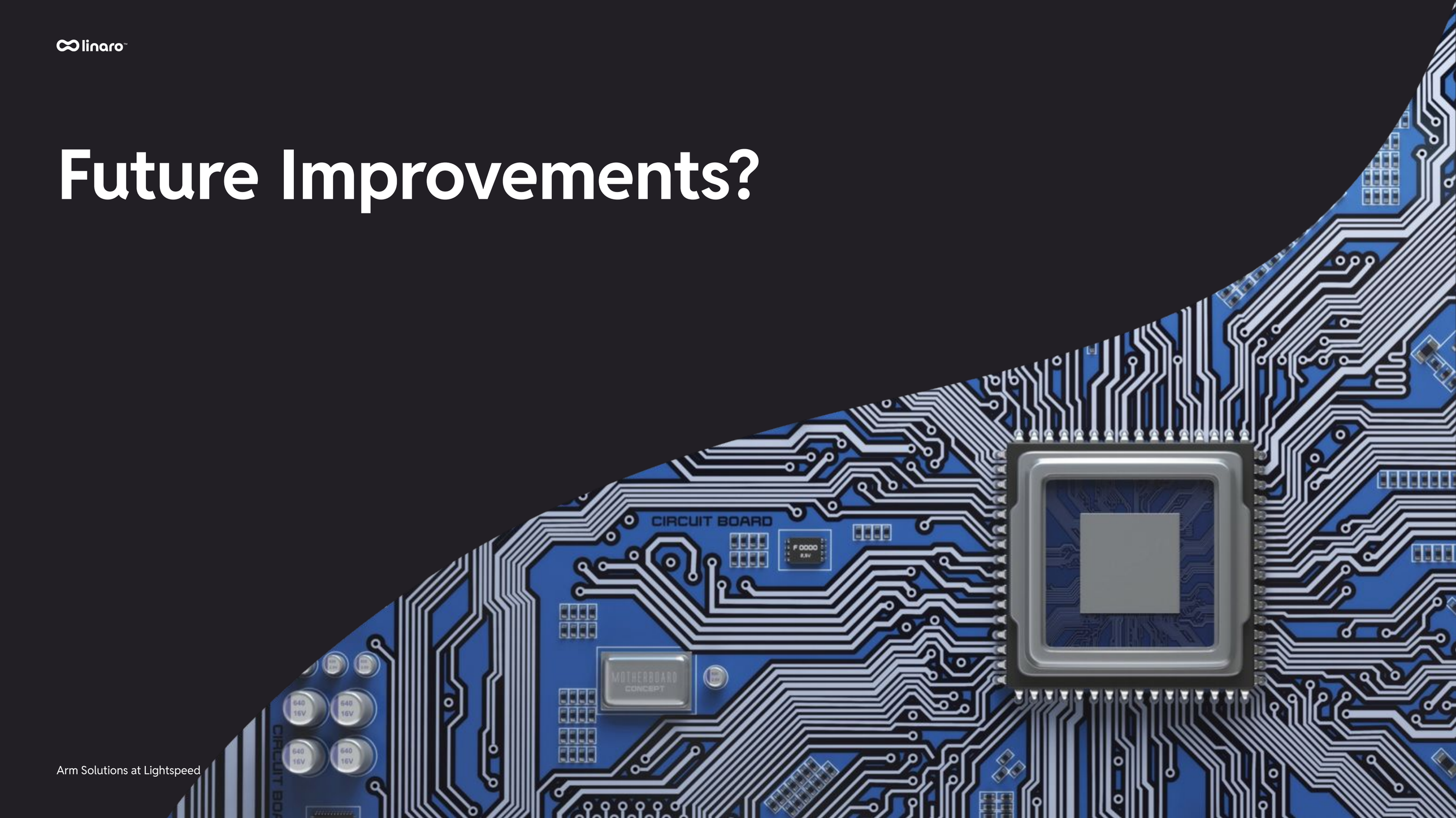
New Examples

looking for gems in contrib

- bbv
- stoptrigger
- cflow

linaro™

Future Improvements?



Semantic Hooks

- Where is malloc?
- Hypercalls to Plugins
- Inter-plugin communication

Another Memory API?

- Fast and racy
- Slow and precise
- Range based?

Alternate Bindings

- All current plugins use C
- Rust examples downstream
- Require a more formal API

Summary

- Core plugin API
- Growing list of examples
- Won’t replace downstream forks
  - **but may reduce the delta**

Any Questions?

Thank you

stsquad@

#qemu on OFTC

mastodon.org.uk

lemmy.ml

bsky.social