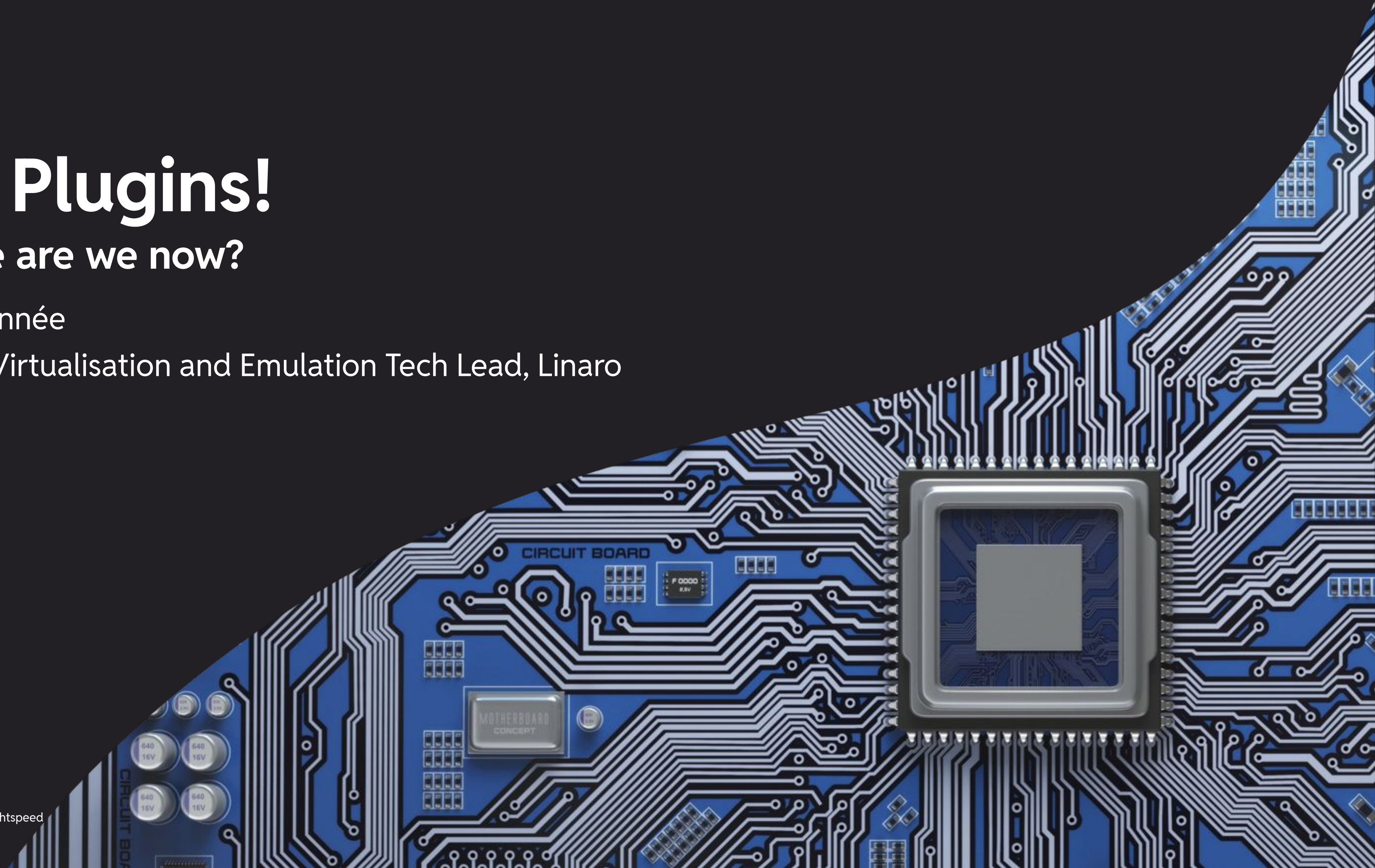


# Oh Plugins!

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

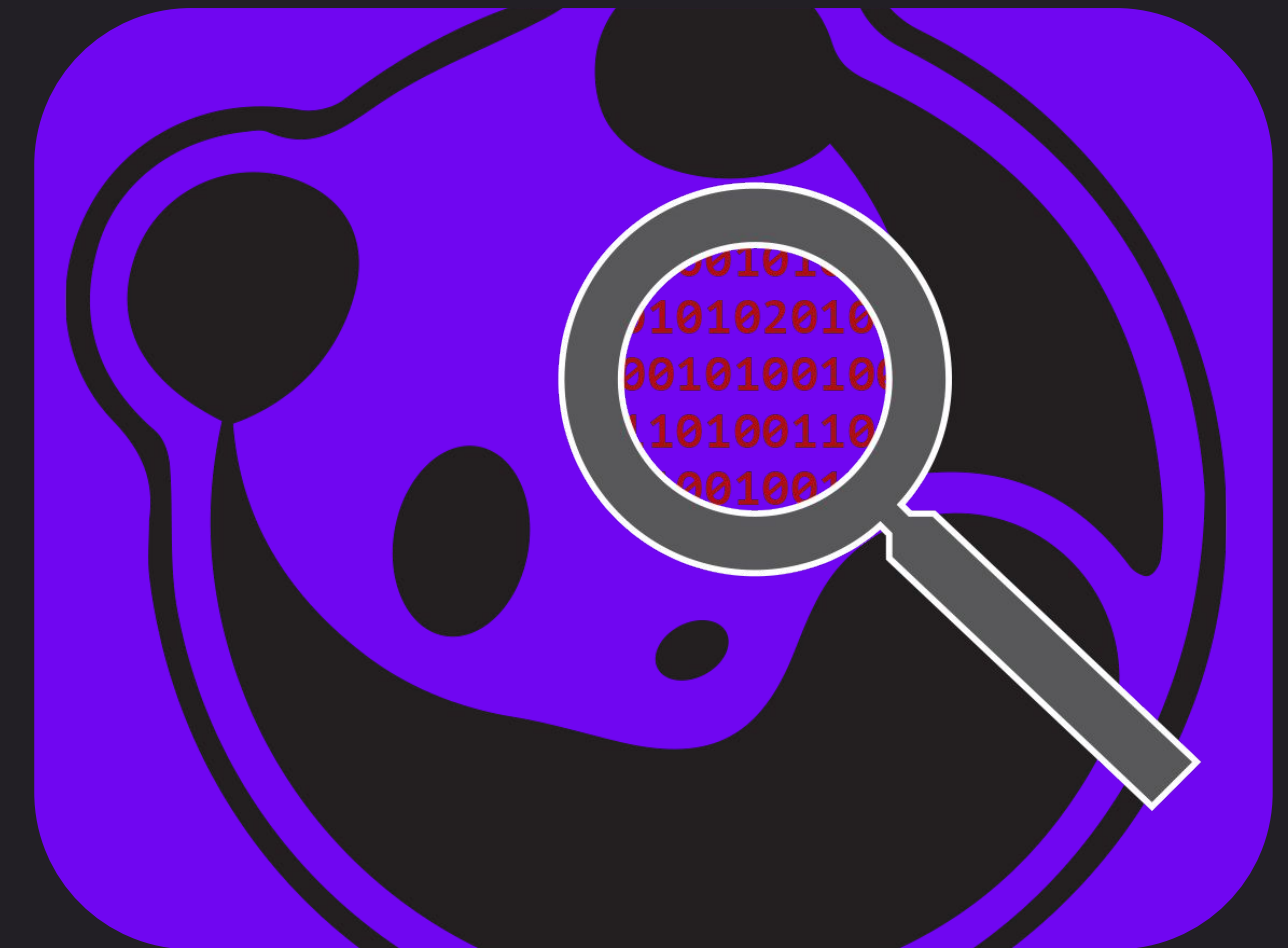
## AFL++

```

american fuzzy lop ++2.65d (libpng_harness) [explore] {0}
process timing
  run time : 0 days, 0 hrs, 0 min, 43 sec
  last new path : 0 days, 0 hrs, 0 min, 1 sec
  last uniq crash : none seen yet
  last uniq hang : none seen yet
cycle progress
  now processing : 261*1 (37.1%)
  paths timed out : 0 (0.00%)
stage progress
  now trying : splice 14
  stage execs : 31/32 (96.88%)
  total execs : 2.55M
  exec speed : 61.2k/sec
fuzzing strategy yields
  bit flips : n/a, n/a, n/a
  byte flips : n/a, n/a, n/a
  arithmetics : n/a, n/a, n/a
  known ints : n/a, n/a, n/a
  dictionary : n/a, n/a, n/a
  havoc/splice : 506/1.05M, 193/1.44M
  py/custom : 0/0, 0/0
  trim : 19.25%/53.2k, n/a
map coverage
  map density : 5.78% / 13.98%
  count coverage : 3.30 bits/tuple
findings in depth
  favored paths : 114 (16.22%)
  new edges on : 167 (23.76%)
  total crashes : 0 (0 unique)
  total tmouts : 0 (0 unique)
path geometry
  levels : 11
  pending : 121
  pend fav : 0
  own finds : 699
  imported : n/a
  stability : 99.88%
overall results
  cycles done : 15
  total paths : 703
  uniq crashes : 0
  uniq hangs : 0
[cpu000: 12%]
  
```

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

arm

RISC-V

Loongson

IBM

# 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

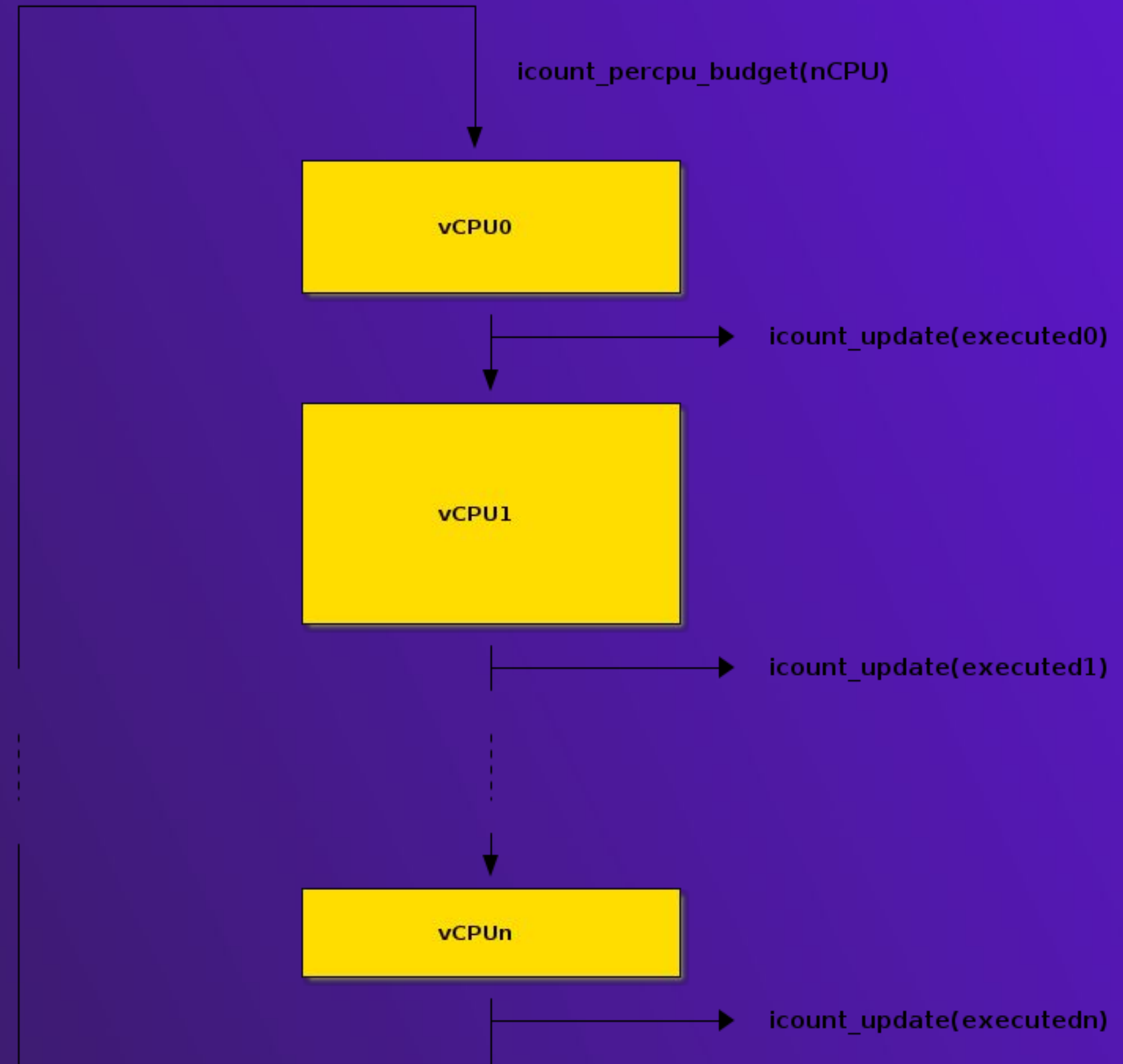
- `qemu_plugin_scoreboard_new()`
- inline `STORE_U64`
- Conditional callbacks

# 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

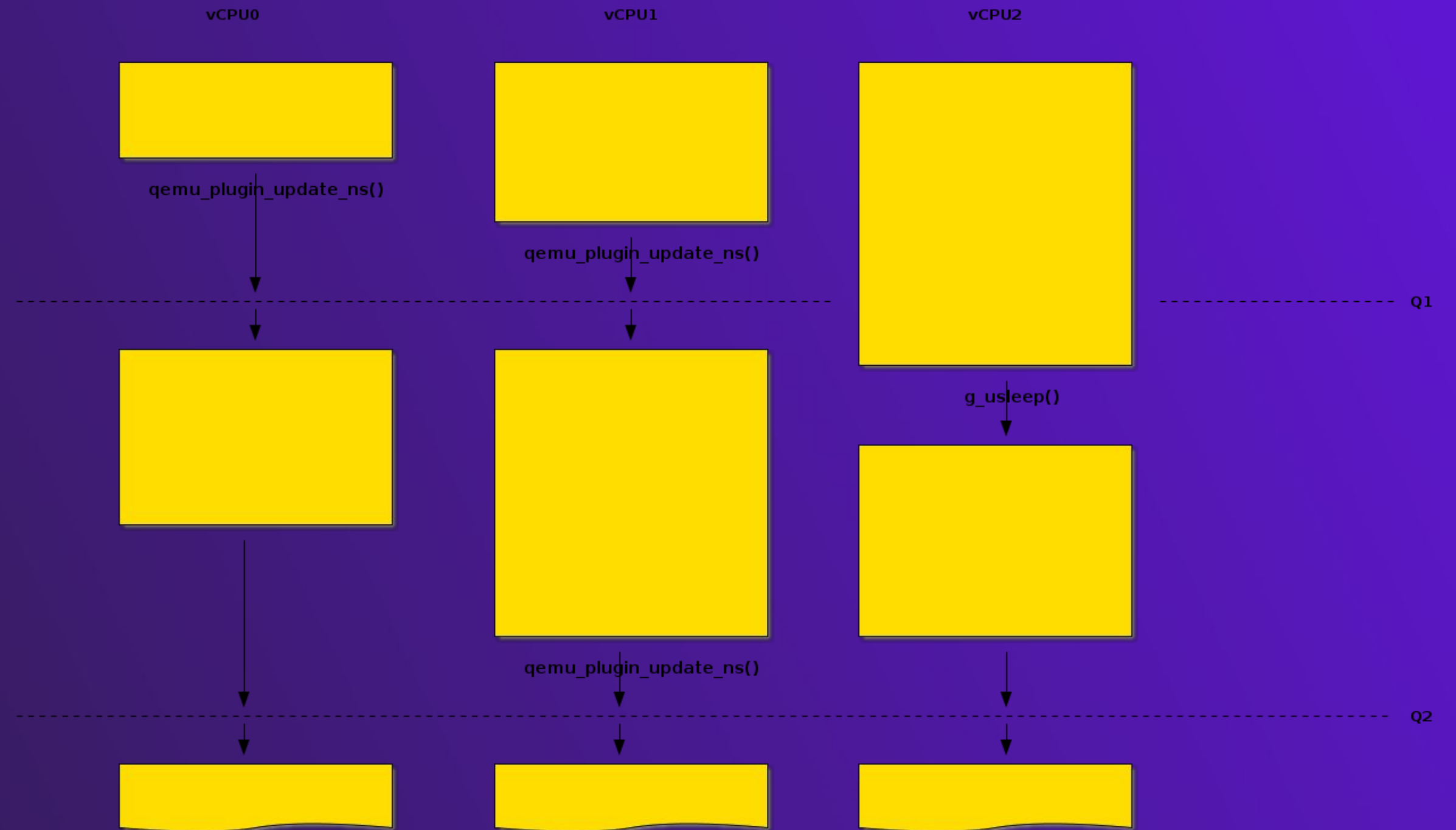




# Controlling Time

## plugins controlling state

- qemu\_plugin\_update\_ns()
- multi-threaded
- ips

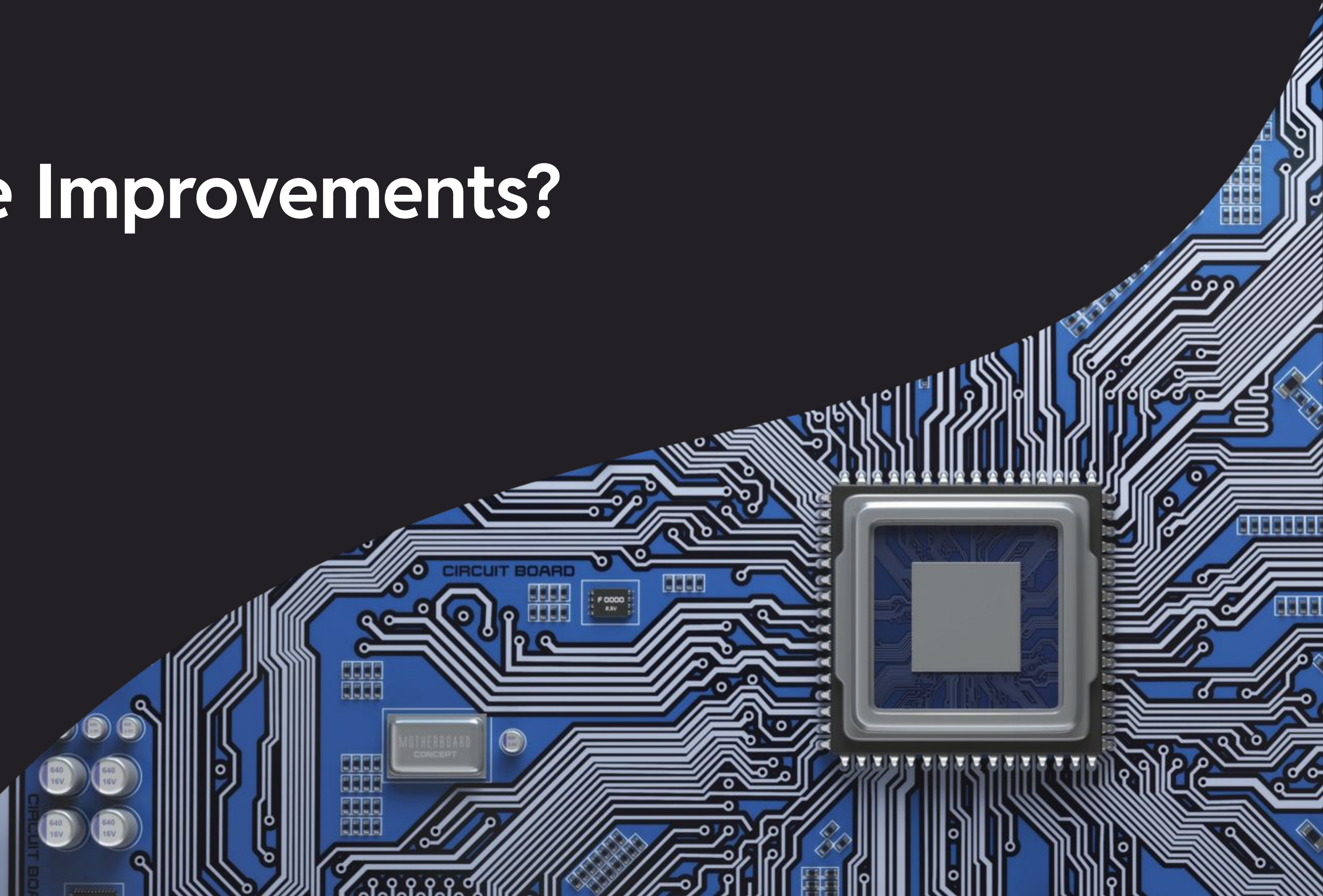


# New Examples

looking for gems in contrib

- bbv
- stoptrigger
- cflow

# 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**

A close-up, top-down view of a blue printed circuit board (PCB) with intricate white and silver traces. Various components are visible, including several silver electrolytic capacitors with labels like "820 2.5V" and "64 16V", and integrated circuits with markings such as "F 0000 2.5V". The board is partially obscured by a large, dark grey, curved shape that frames the central text.

# Any Questions?



# Thank you

[stsquad@](mailto:stsquad@)

[#qemu on OFTC](#)

[mastodon.org.uk](https://mastodon.org.uk)

[lemmy.ml](https://lemmy.ml)

[bsky.social](https://bsky.social)