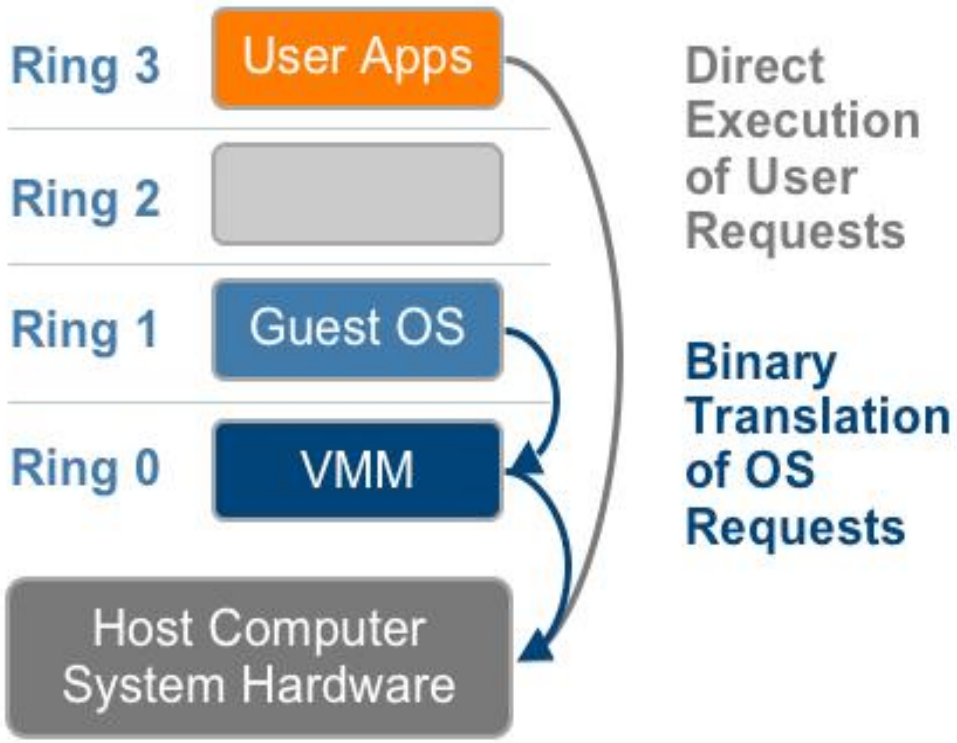
QEMU Binary Translation

Ashish Kaila (akaila)

Maneet Singh (maneets)

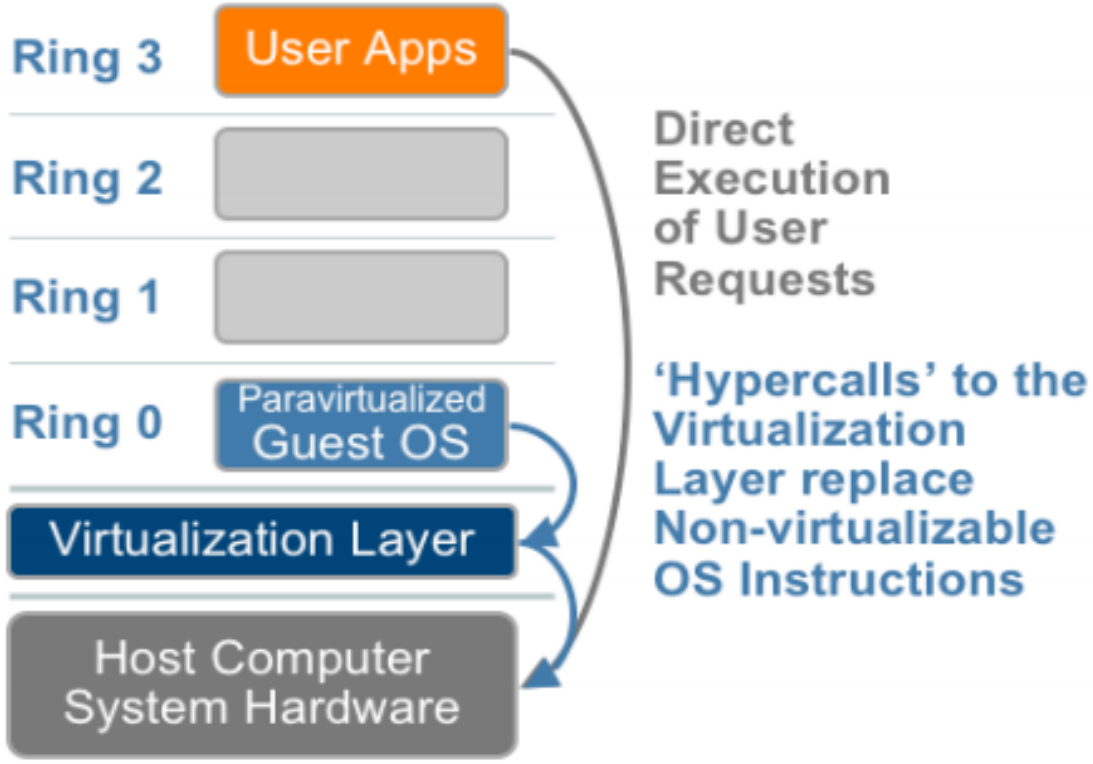
Virtualization Techniques

- **Full Virtualization using Binary Translation**



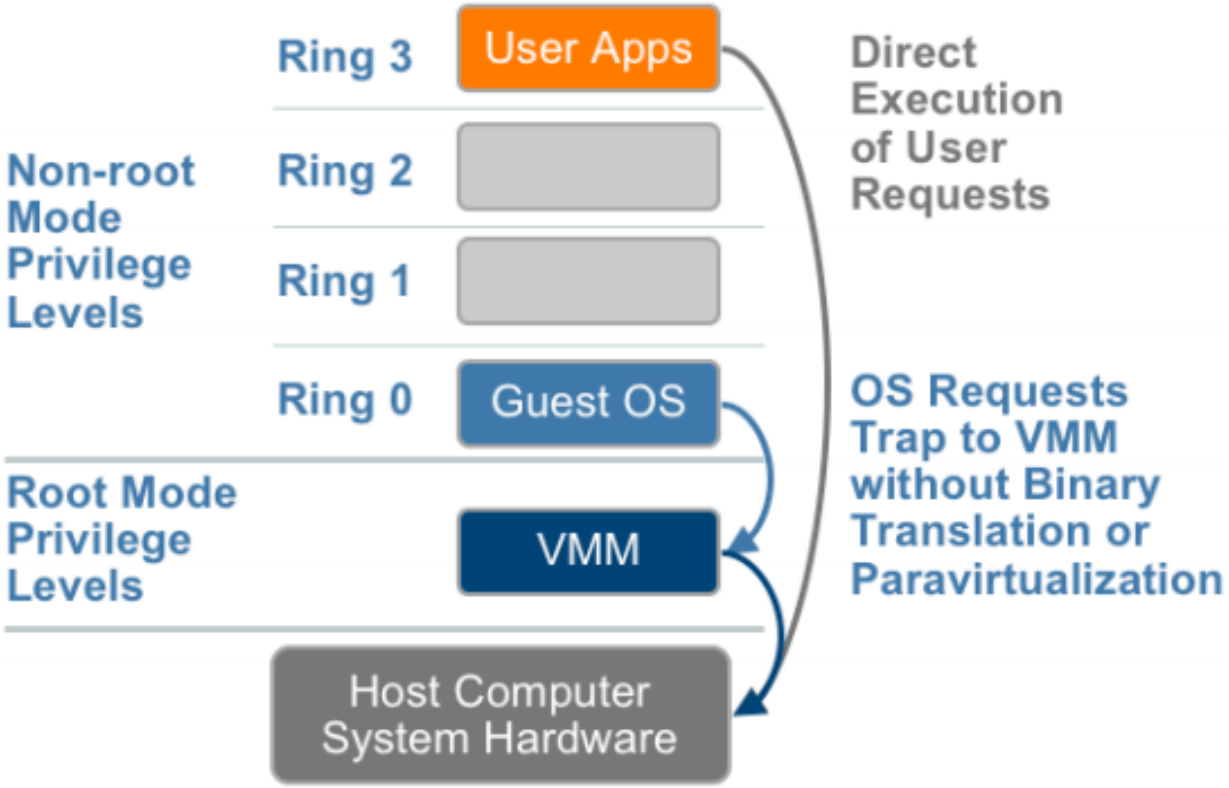
Virtualization Techniques

- **OS Assisted Virtualization or Paravirtualization**



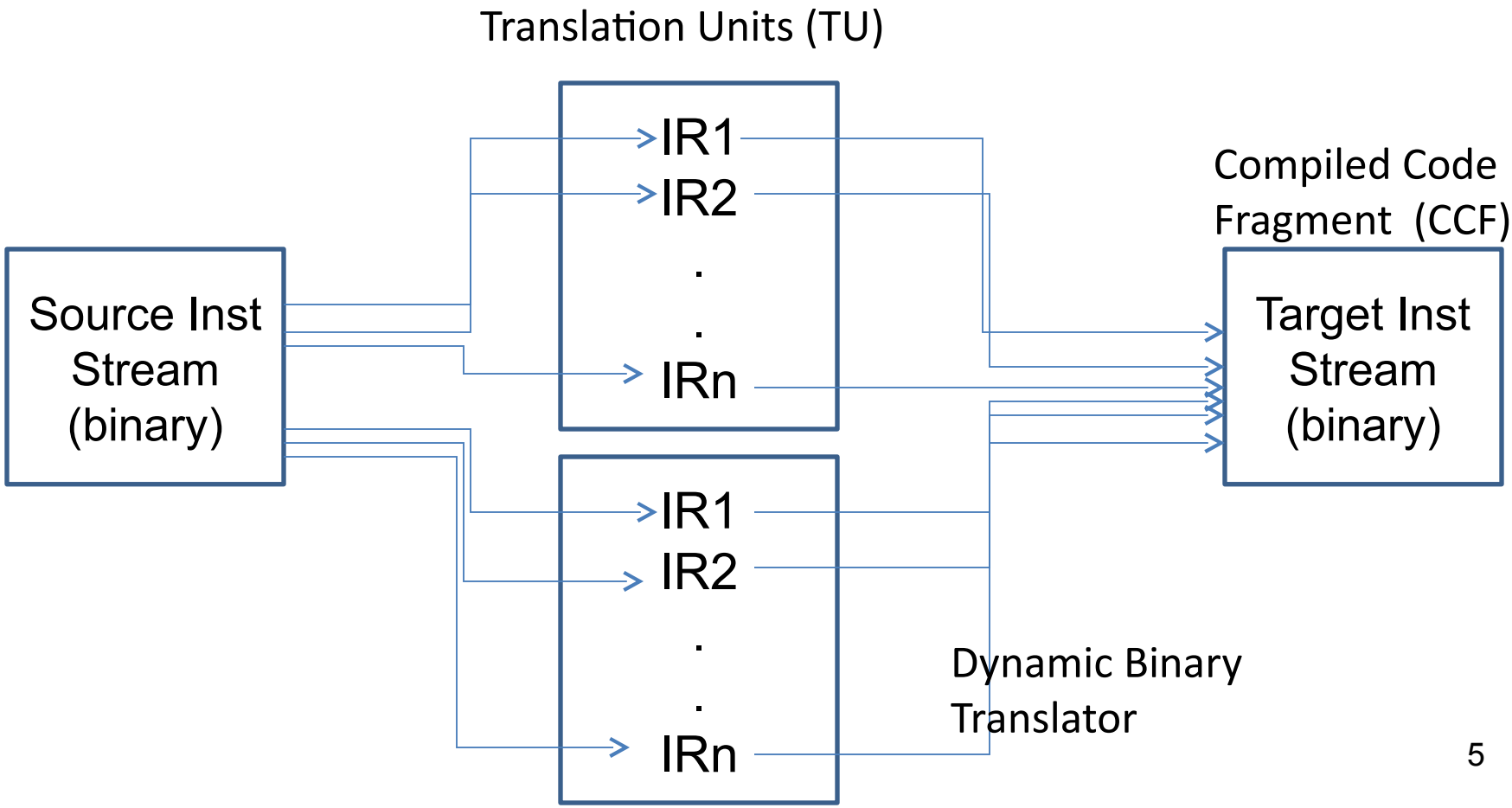
Virtualization Techniques

- **Hardware Assisted Virtualization**



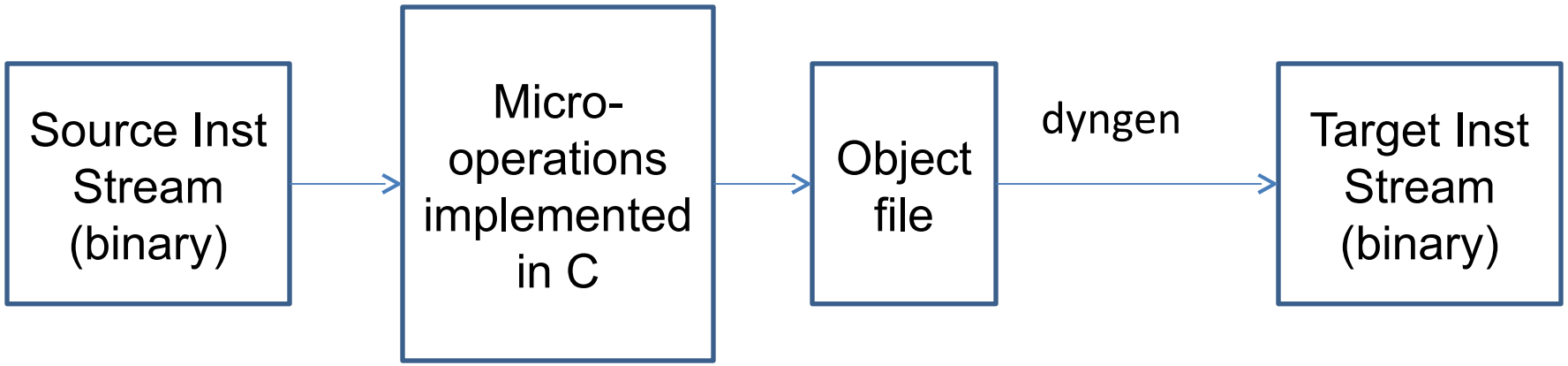
Binary Translation

- **VMWare Software Virtualization**



Binary Translation

- **QEMU Binary Translation in brief**



Quick EMUlation (QEMU)

- Machine Emulator
- Virtualizer

QEMU modes:

- User-mode emulation – Allows a process built for one CPU to be executed on another.
- System-mode emulation – Allows emulation of a full system, including processor and assorted peripherals.

References

- A comparison of software and hardware techniques for x86 virtualization – Keith Adams, Ole Agesen, ASPLOS'06
- Understanding Full Virtualization, Paravirtualization and Hardware Assist – VMware Whitepaper
- QEMU, a fast and portable Dynamic Translator – Fabrice Bellard
- QEMU Wiki: wiki.qemu.org

QEMU Deep Dive

Source: wiki.qemu.org

Different ISAs

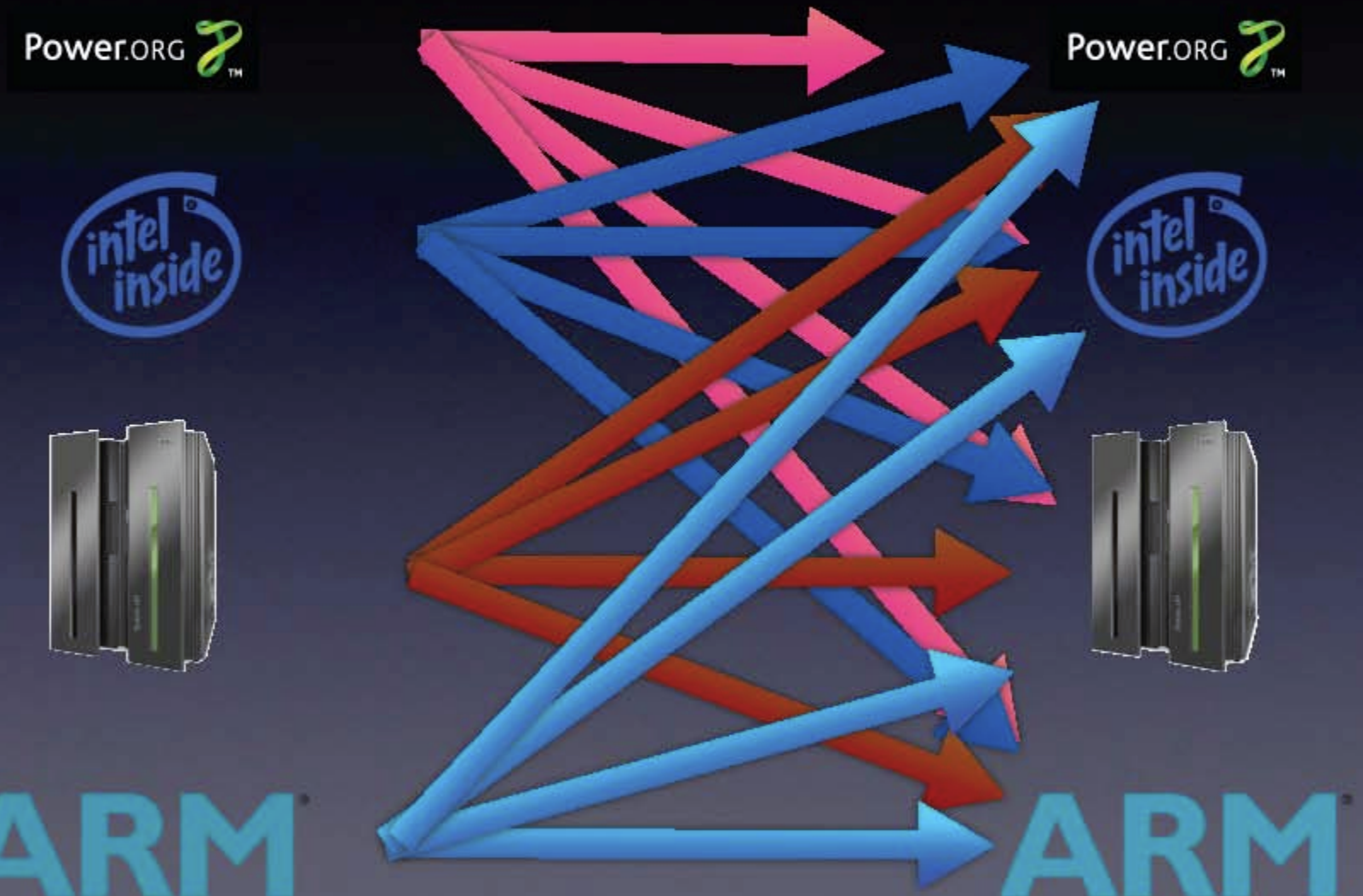
Register	Value
r0	1
r1	2
...	...

```
code:
bb 01 00 00 00 mov $0x1,%ebx
89 d8          mov %ebx,%eax
83 c3 01       add $0x1,%ebx
```

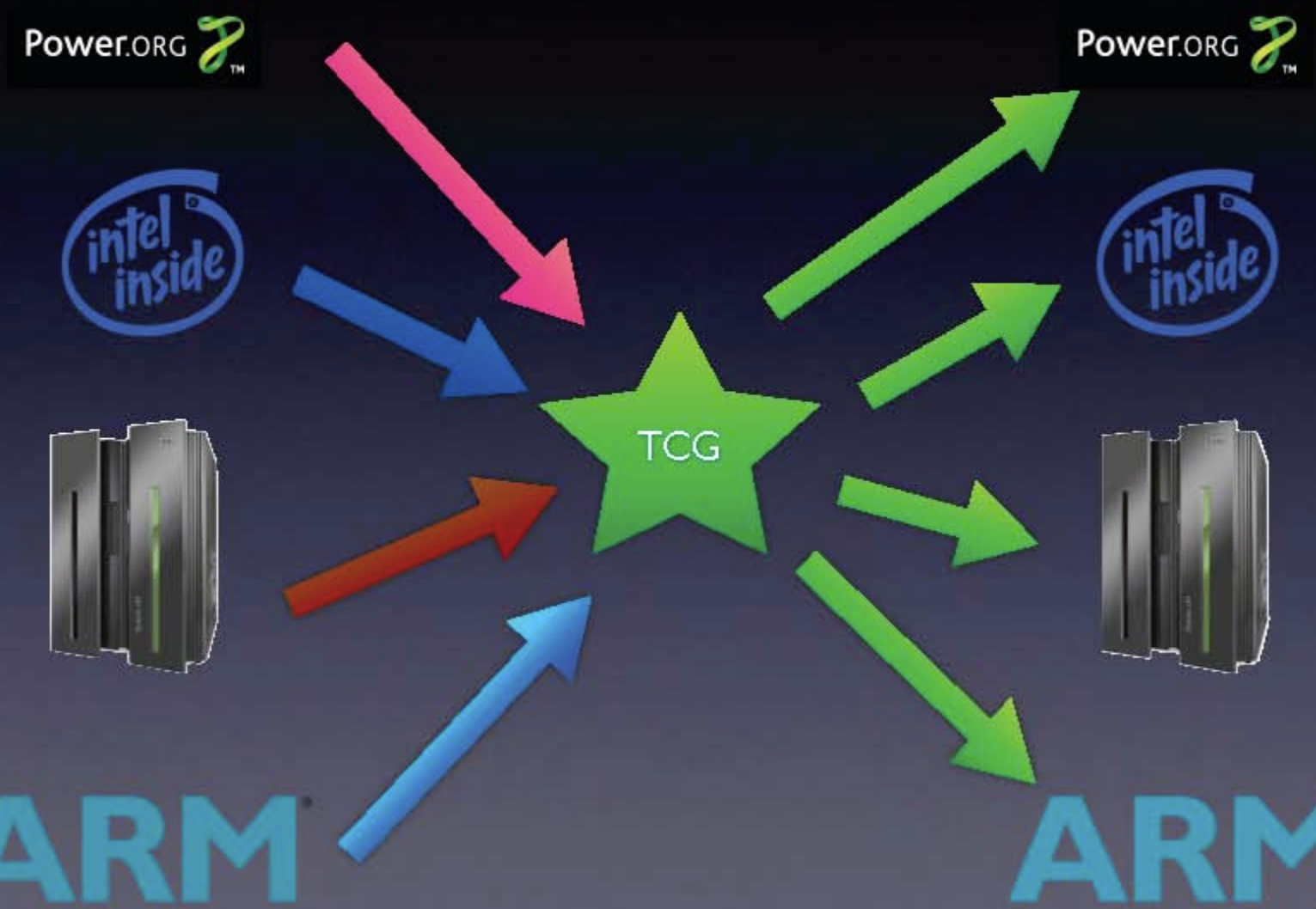
Register	Value
eax	0
ebx	0
...	...

```
code:
38 20 00 01   li      r1,1
7c 20 0b 78   mr      r0,r1
38 21 00 01   addi    r1,r1,1
```

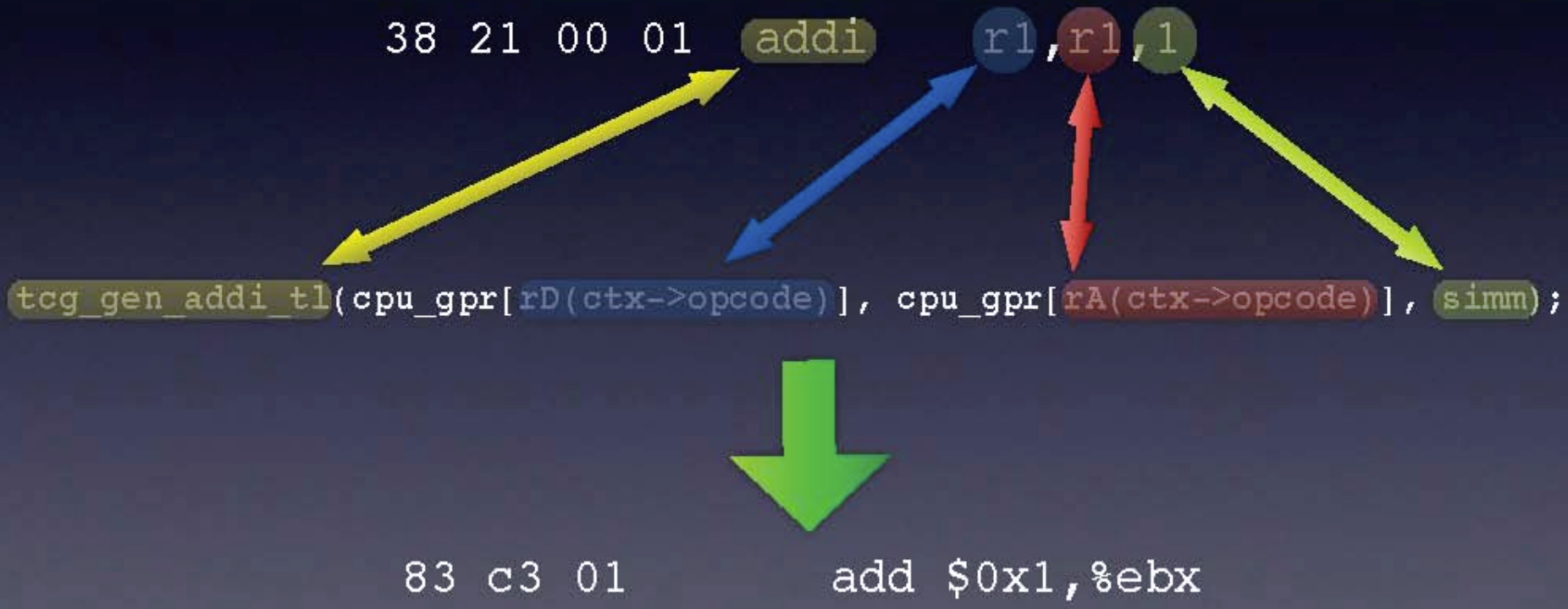
Converting code



TCG

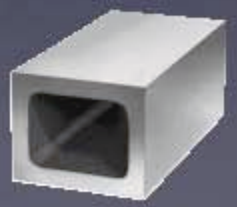


TCG micro-ops

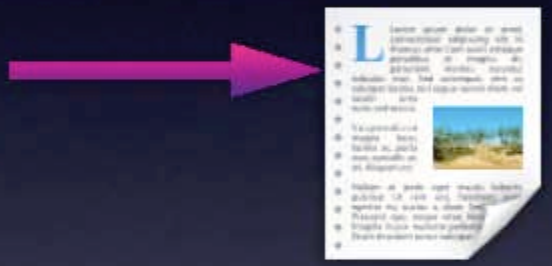


Translation Blocks

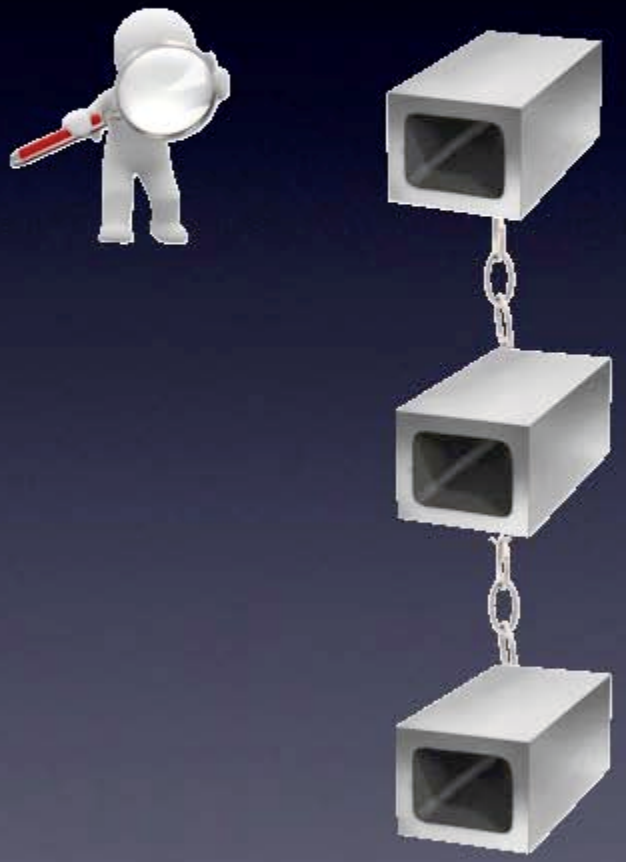
```
 0:38 20 00 01   li      r1,1
 4:7c 20 0b 78   mr      r0,r1
 8:38 21 00 01   addi    r1,r1,1
 c:2c 01 00 02   cmpwi   r1,2
10:41 82 ff f0   beq+    0x0
```



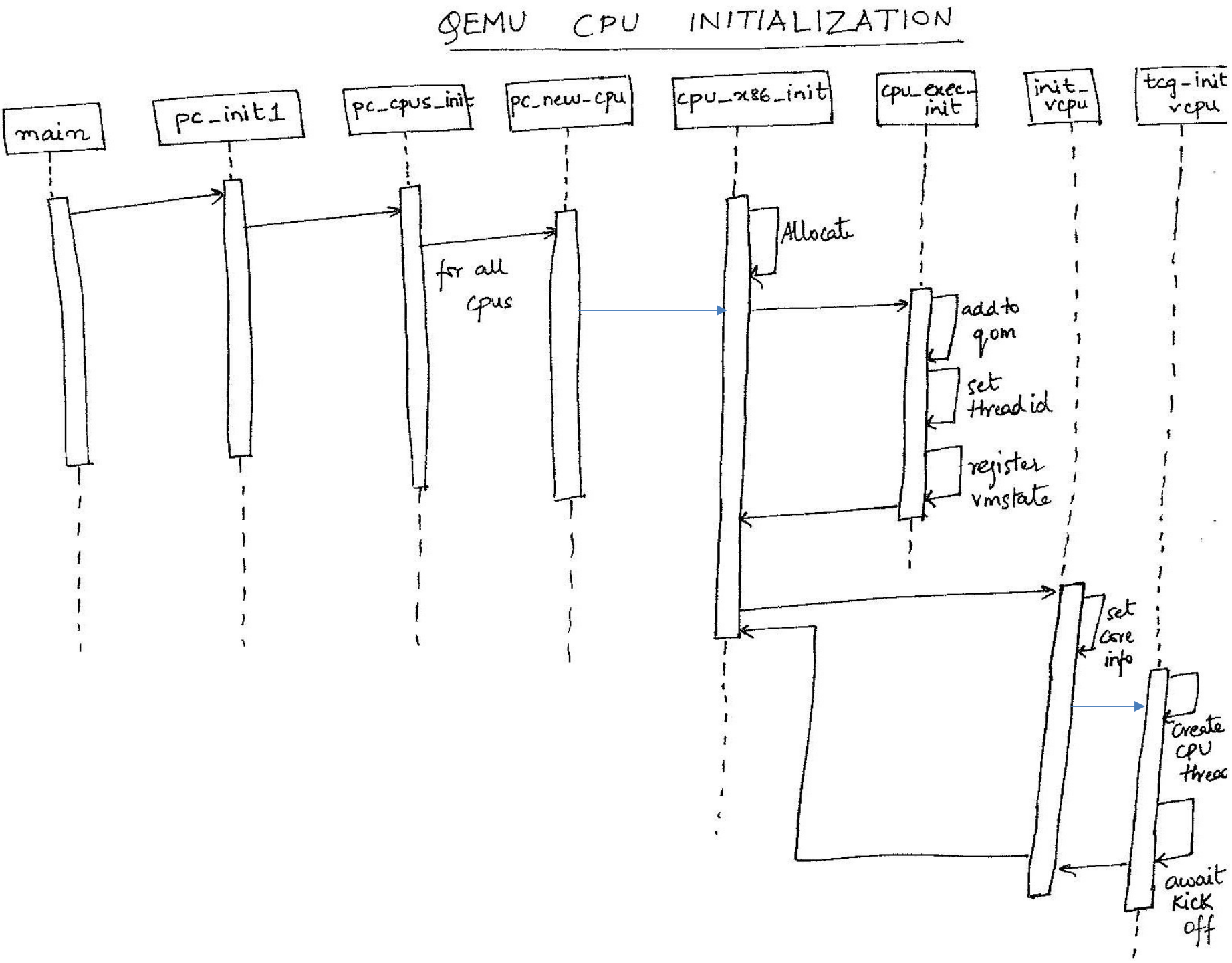
Translation Blocks

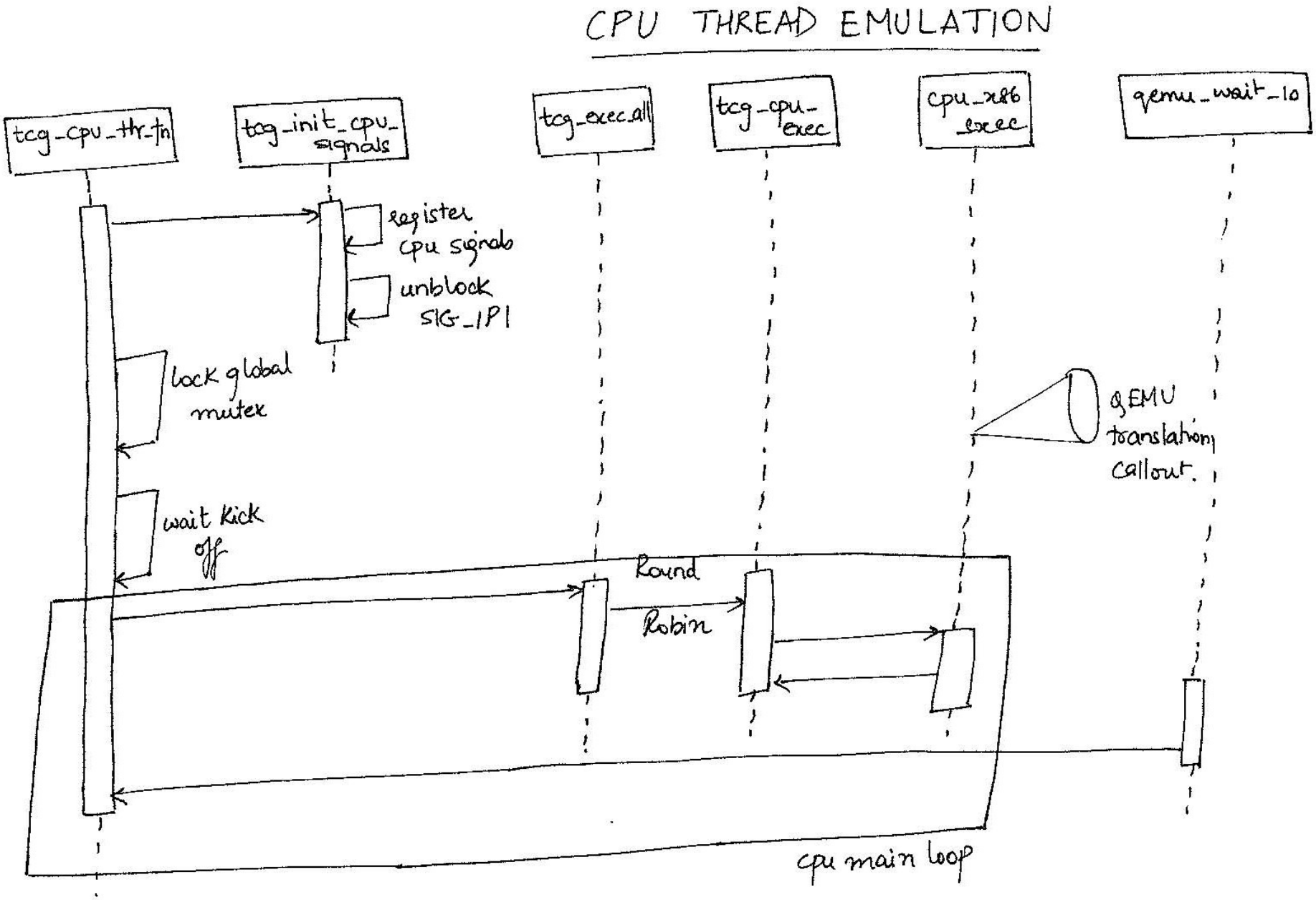


TB Chaining



QEMU ARCHITECTURE


QEMU CPU INITIALIZATION
main
pc_init1
pc_cpus_init
pc_new_cpu
cpu_x86_init
cpu_exec_init
init_vcpu
tcg_init_vcpu
Allocate
for all cpus
add to qom
set thread id
register vmstate
set core info
create CPU thread
await kick off


CPU THREAD EMULATION
tcg_cpu_thr_fn
tcg_init_cpu_signals
tcg_exec_all
tcg_cpu_exec
cpu_x86_exec
qemu_wait_io
register cpu signals
unblock SIG_IPI
lock global mutex
wait Kick off
QEMU translation callout.
Round Robin
cpu main loop

Thank you