

AI 大（语言）模型时代下的 操作系统发展思考

报告人：武延军

中国科学院软件研究所

2024-08-20 @ 杭州

AI大(语言)模型正在成为操作系统领域热点话题

AI as the new Operating System

AI is a new paradigm for software execution, user experience, and system management



PATRICK MCGUINNESS
OCT 09, 2023

清华张亚勤：大模型将是AI时代的操作系统，产业机会将比PC时代增长100倍

2023-11-08 18:31 来源: 搜狐科技 发布于: 北京市



大模型时代，智能化操作系统面临的机遇与挑战

openEuler | 2023-10-25 | openEuler

AI OS时代来了！国产操作系统换道超车，颠覆人机交互范式

人工智能 手机通信 智东西 智东西头条 2024/01/11

Evolution of Operating Systems - The New Networked AI Era

AUG 29, 2023 / 5 MIN READ

Tech.china.com.cn

赵明：用AI重构操作系统

2024年01月12日11:03 中国网科技

Hatchworks AI | What We Do | Why Hatchworks | About Us | Resources | Our Work

HOW AI AS AN OPERATING SYSTEM IS SHAPING OUR DIGITAL FUTURE

Melissa Malec June 6, 2024

Updated: June 6, 2024

AI-Powered Operating System — A Race to Global Dominance

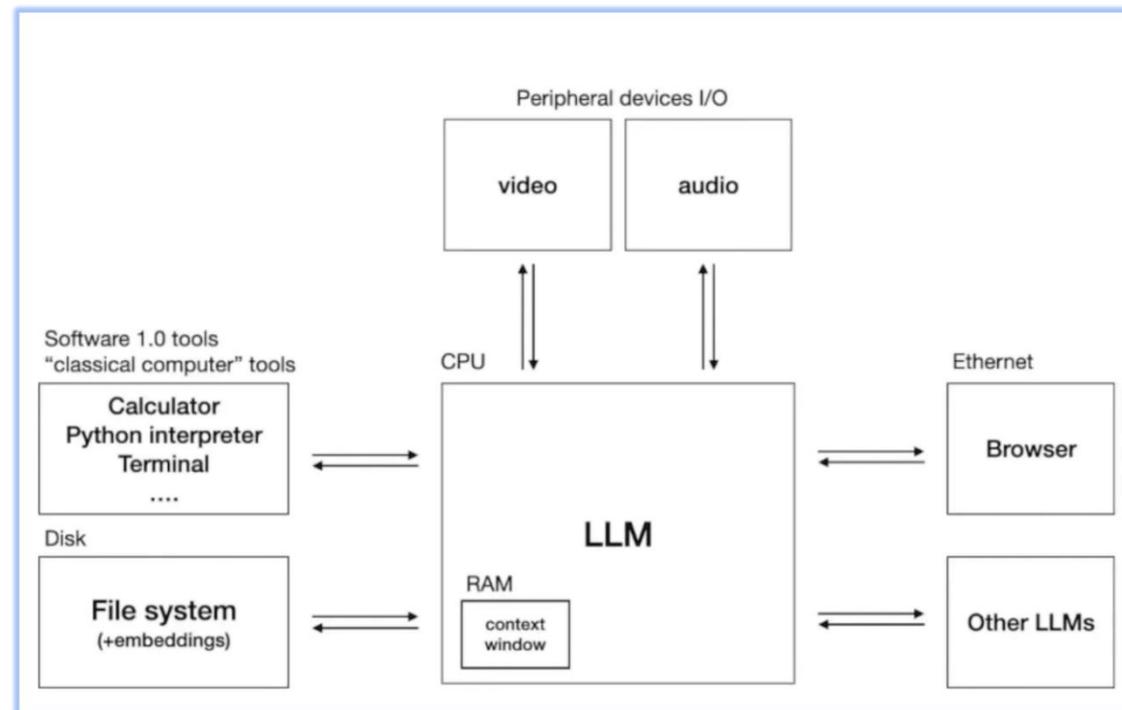


Ayush Ojha · Follow
12 min read · Dec 27, 2023

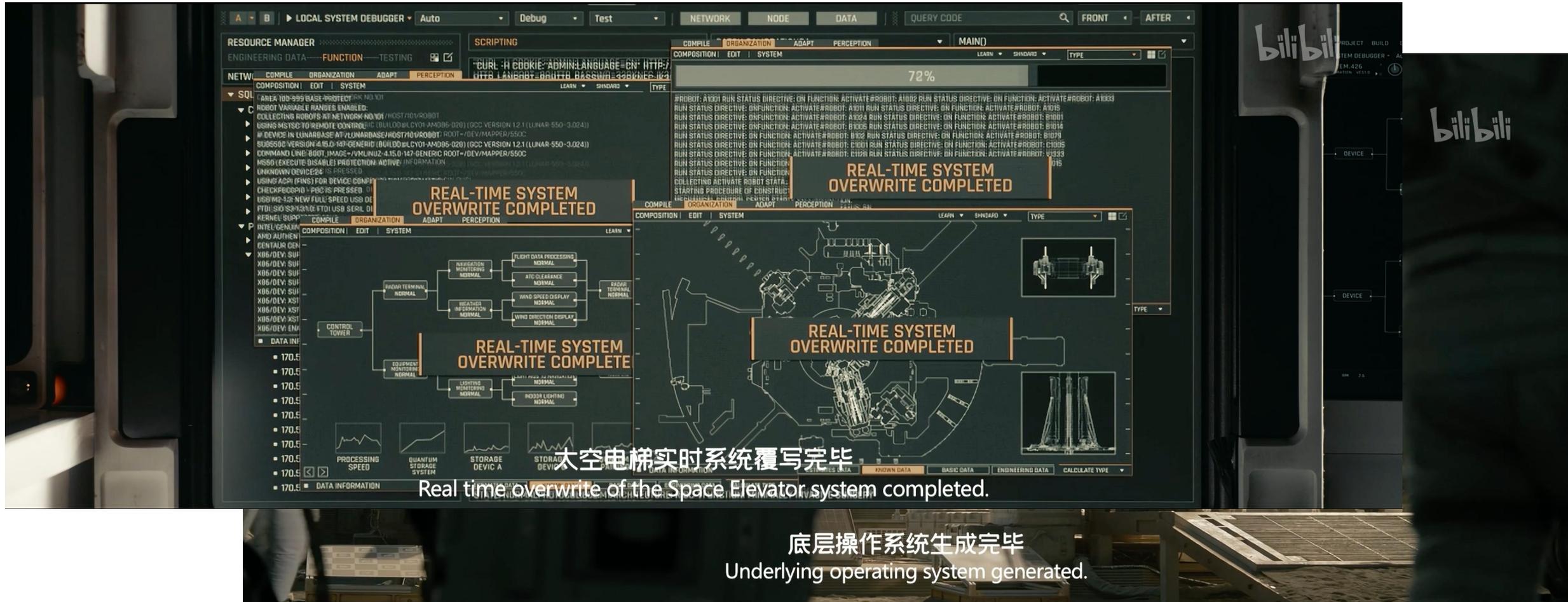
传统操作系统 VS “LLM OS”



VS



“操作系统” 在大众媒介中的概念泛化



太空电梯实时系统覆写完毕

Real time overwrite of the Space Elevator system completed.

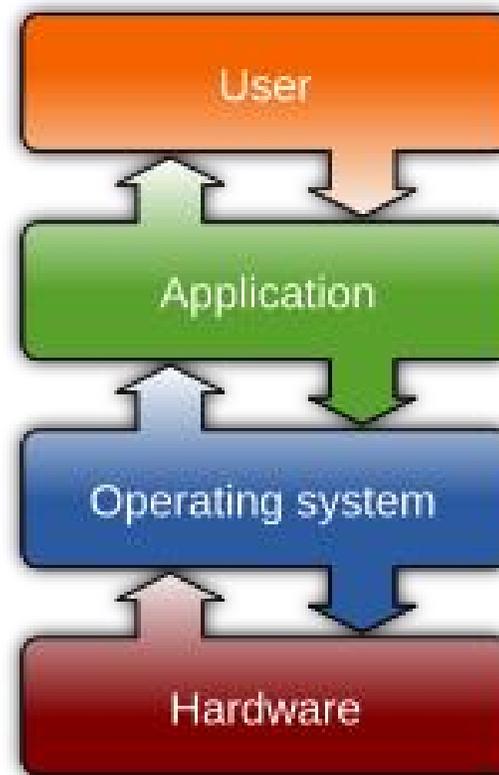
底层操作系统生成完毕

Underlying operating system generated.

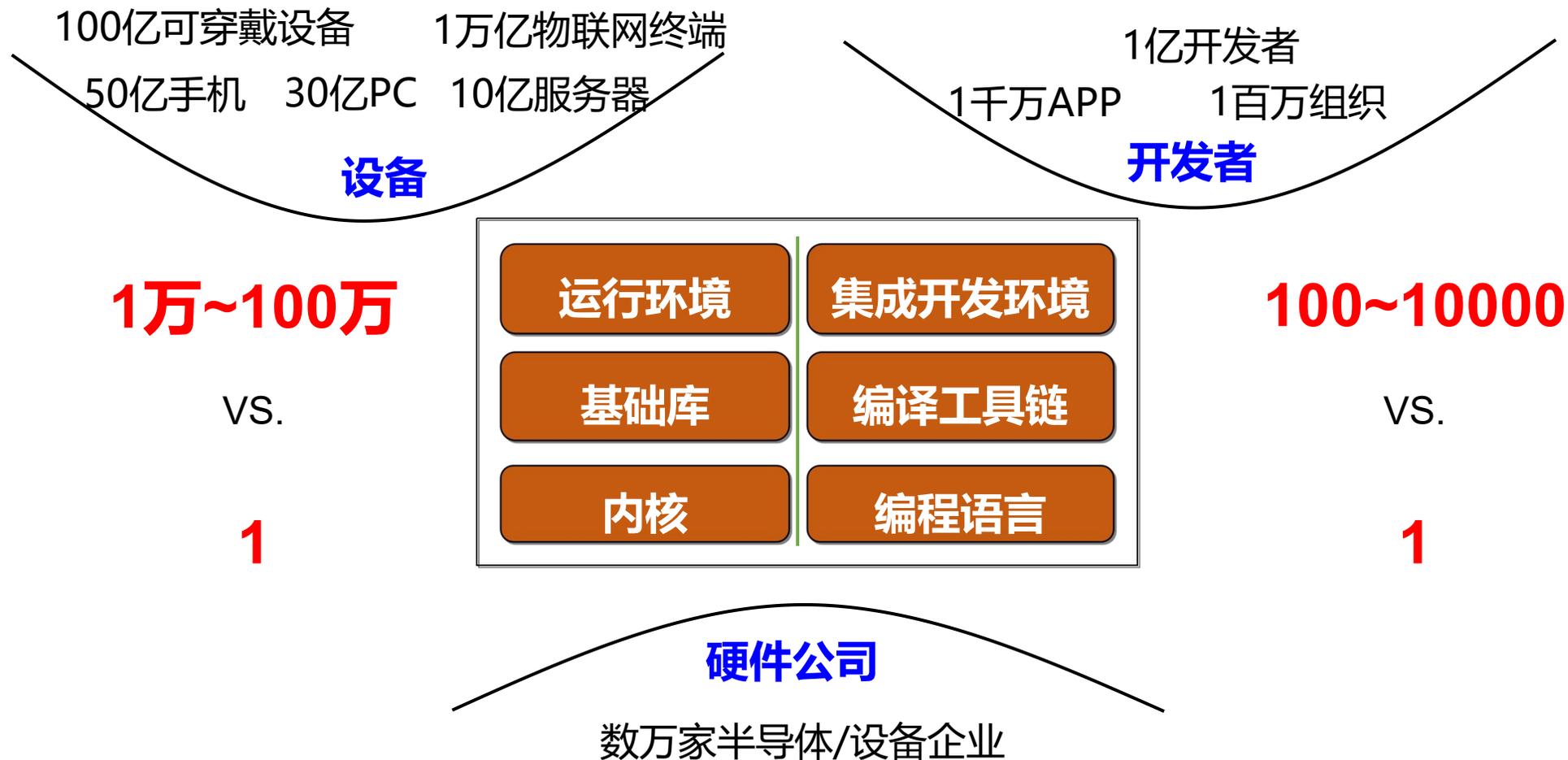
《流浪地球2》剧照

操作系统的定义和分类

- 定义：操作系统是这样一种系统软件，它管理计算机硬件和软件资源，进行**抽象**，为计算机程序提供服务。
- 常见的分类：
 - 嵌入式操作系统 / 实时系统
 - **单机系统 / 桌面 / 移动终端操作系统**
 - 集群操作系统 / 分布式操作系统

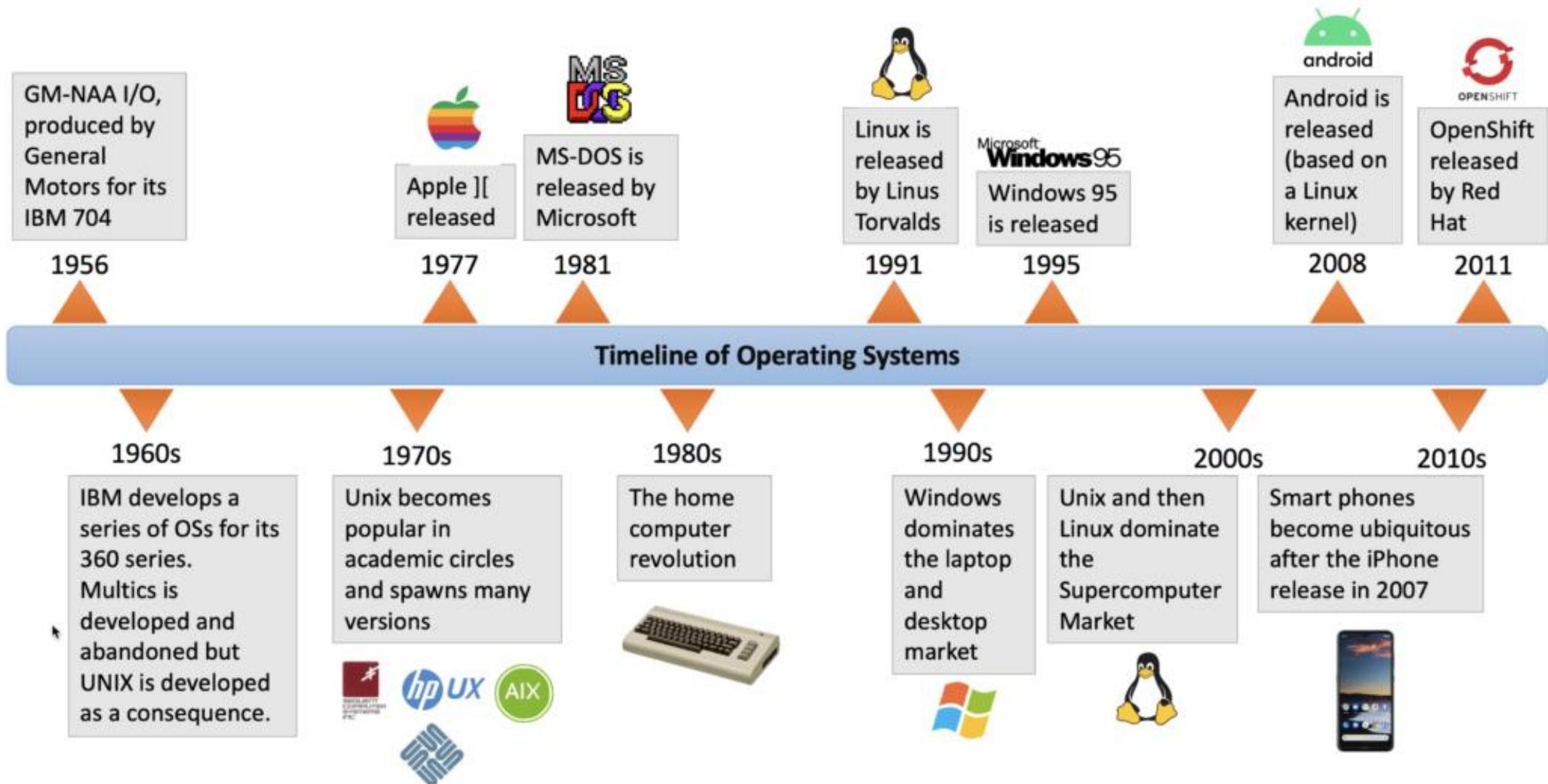


操作系统是IT生态的“粘合剂”和“倍增器”

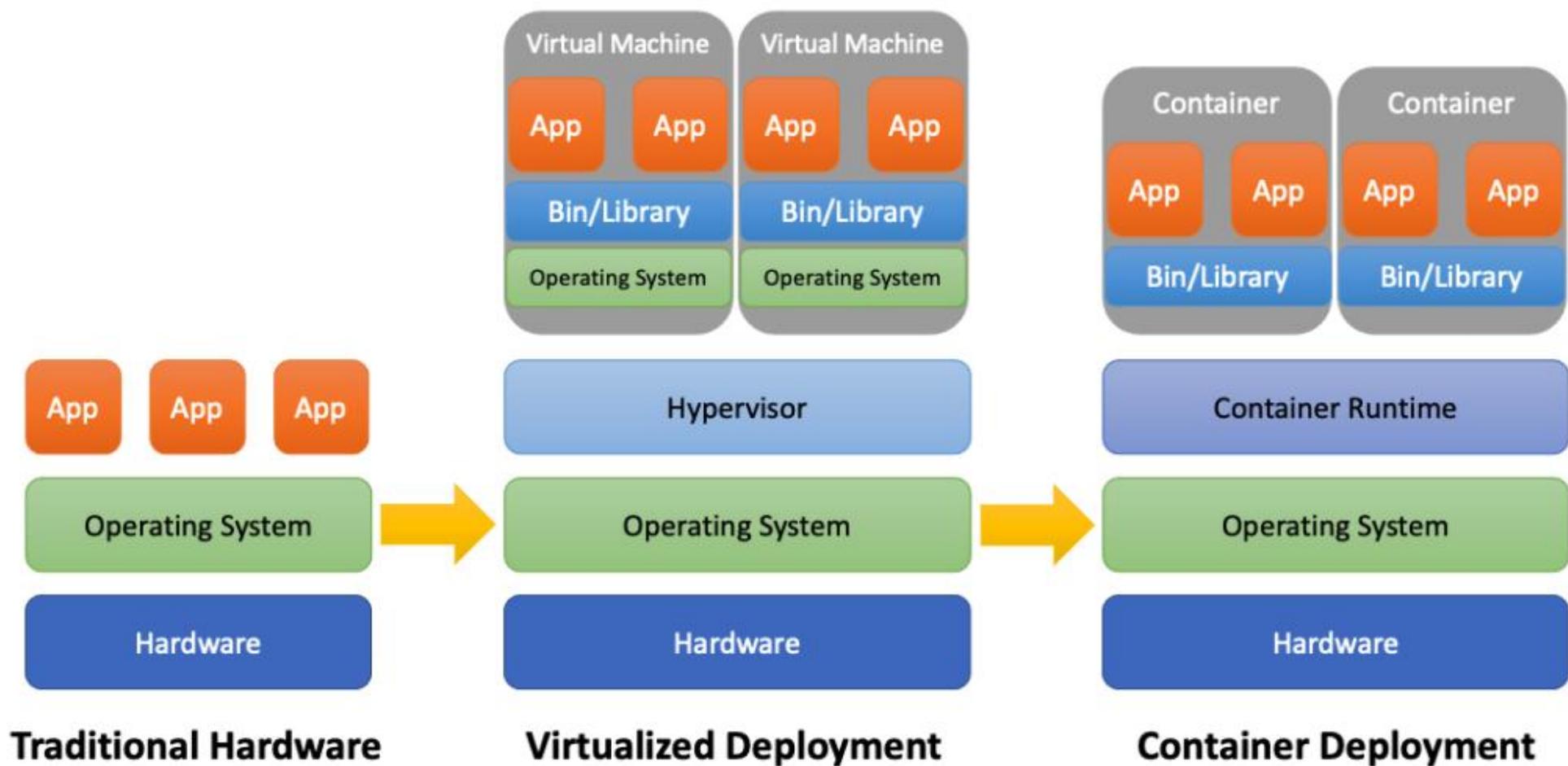


* 以上数字均为粗略估算的概数

单机操作系统的发展历程



从集群到云计算到云原生



过去几十年操作系统的变革：硬件技术演进

- CPU处理器速度成倍提升
 - 专用图形显示设备 (GPU)
- 存储空间更大, 大数据成为可能
- 电路体积减少, 嵌入更多场景
- 交互形式引发的操作系统革新
 - 按钮+穿孔卡 → 键盘+鼠标 → 高分辨率触摸屏
 - **LLM 使得对话式界面 (CUI) 更有前景**
 - 更远未来: 神经直接连接?

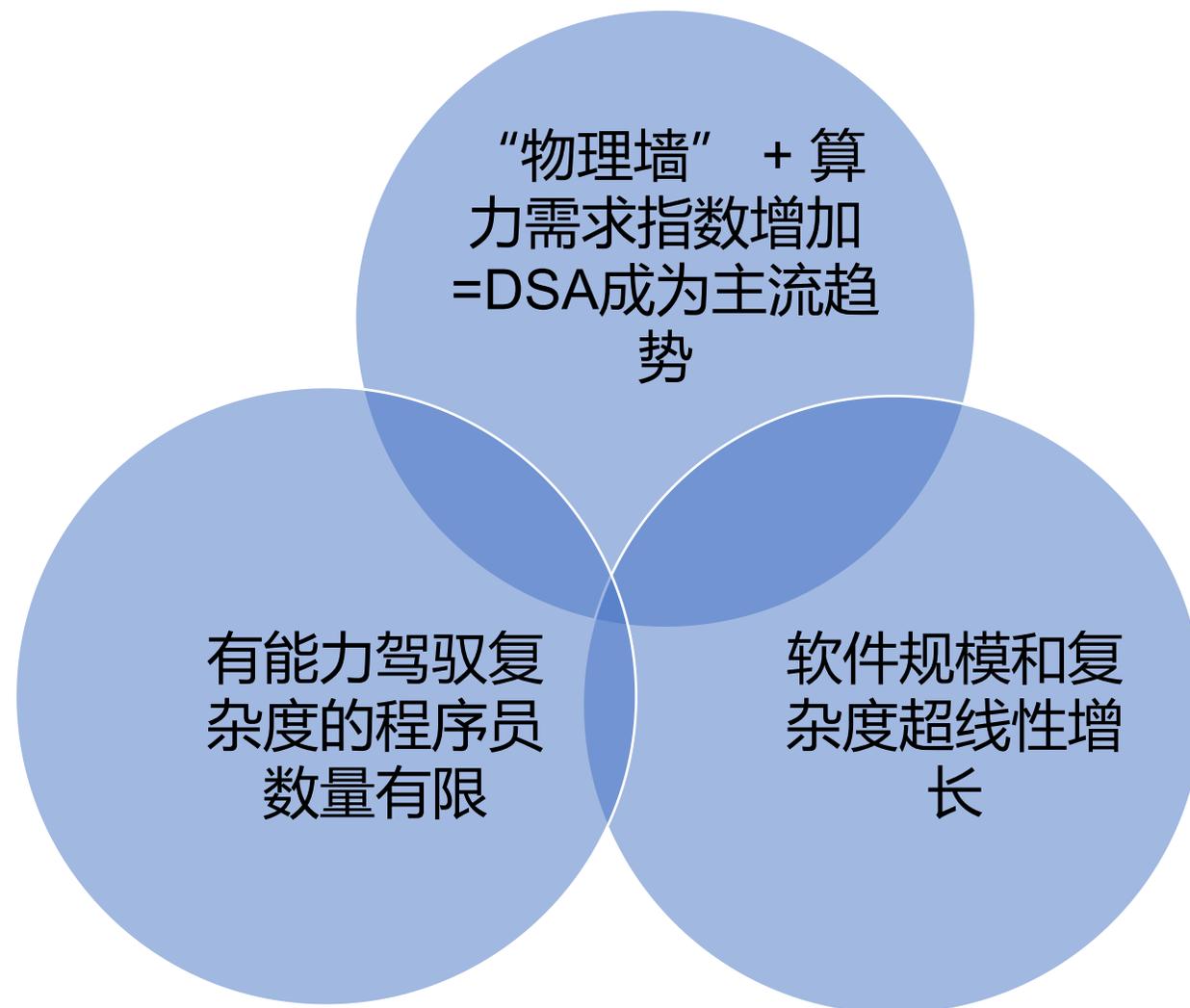


仿古的PDP11设备。背后是个树莓派

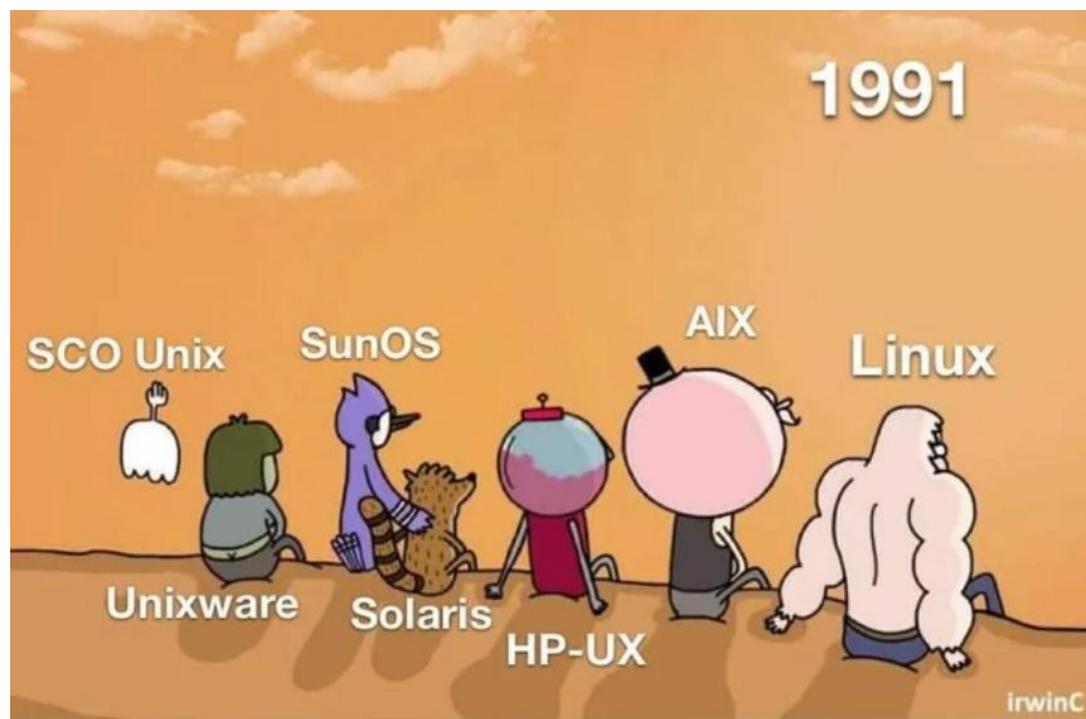
过去几十年操作系统的变革：数据和算力规模跃升

- 如何用最低成本**响应处理海量并发请求**：Linux集群
- 如何提高数十万普通Linux服务器的利用率：**云计算/租赁**
- 如何**安全**的进行云计算：硬件虚拟化技术（VT）
- 如何**更安全**的保证数据：硬件支持的机密计算（TEE、SGX）
- 如何方便地运维数千个相互依赖的服务：容器化、CI/CD等
- 如何更快的进行网络数据处理：DPDK、EBPF等
- 如何在云端更快、成本更低的为AI应用提供算力：GPGPU、TPU、FPGA等
- 如何在本地更好的加速AI推理：异构架构、NPU、RISC-V等

过去二十年信息产业的宏观趋势



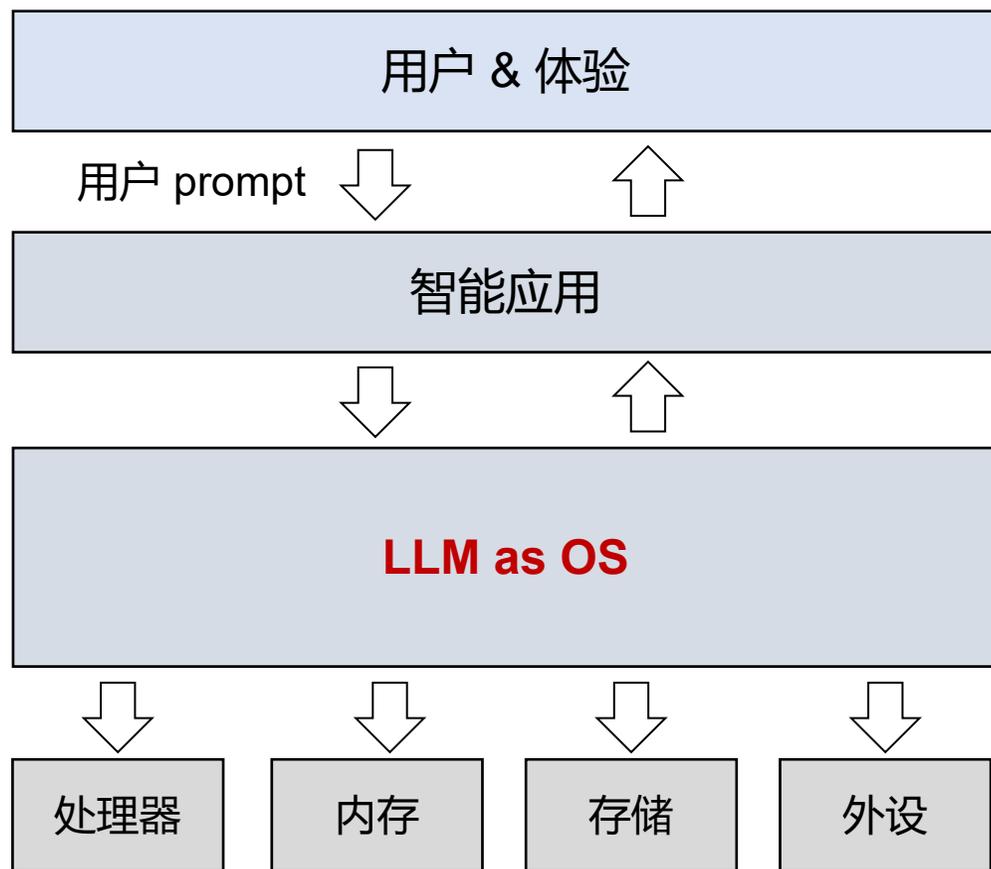
程序员数量有限：开源成为主流，能否聚集足够开发者是生死分界线



https://www.reddit.com/r/ProgrammerHumor/comments/m6zo7v/you_will_not_be_forgotten/

软件规模和复杂度超线性增长：LLM as OS 视角

视角1：LLM as OS



#1 大量概念（实时、可抢占、IPC、系统调用等）将被重新定义

#2 所有应用都需要重写

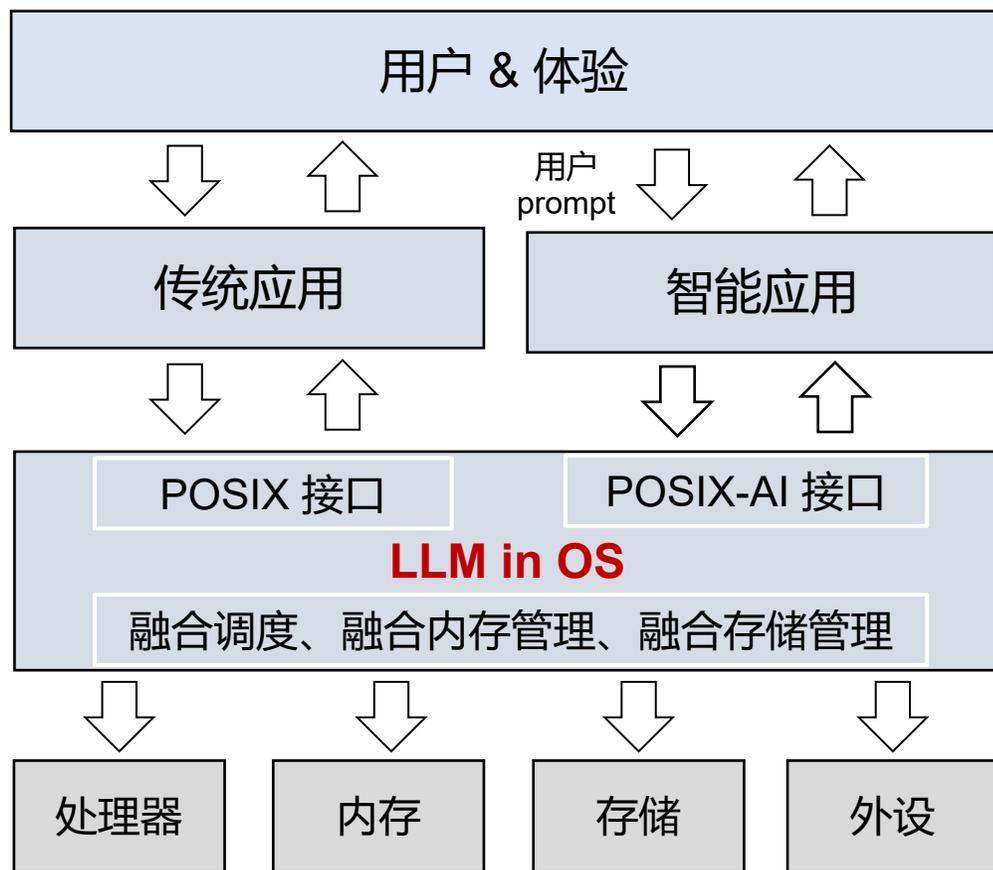
#3 超级应用（类似微信、ChatGPT等）与OS的边界需要重新界定

LLM as OS 视角：仍然存在各种局限

- 基础原理是统计学上的函数拟合，**无法总结出自然定律**
 - 无法用于需要强逻辑推断场景
- 拟合参数已经**远超人类理解极限**，**无法验证**准确性和鲁棒性
 - 输入上的细微修改有可能引起输出未期待的的巨大变化（衍生出新的安全攻击新门类）
- 错误复现难度和**可调试性**有待确认，**可修复性**待确认
 - 修复后回归测试的工程量和难度未知
- Next-Token 模式在操作系统中**使用场景**有限
 - 目前关于AI模型用于操作系统的观点多数是从用户交互角度出发
- 算力需求高（云端 vs 本地）
 - 与物理世界交互的操作系统场景有着极高的实时性和功能安全性要求

软件规模和复杂度超线性增长：LLM in OS 视角

视角2：LLM in OS



#1 操作系统的大量硬编码参数将被模型推理替代（例如通过 Kconfig / eBPF等）。

#2 新的POSIX API将诞生，以适应智能应用的编程范式。

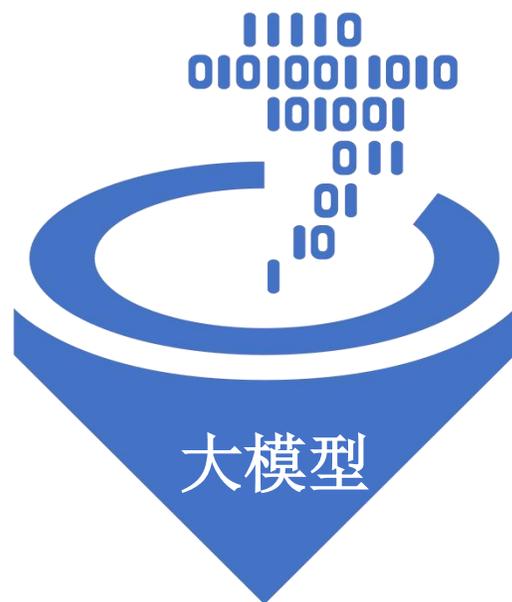
#3 实时与非实时场景共存，将带来更复杂的调度、内存、存储管理策略。

LLM in OS 视角：可以帮助操作系统变得更先进

- 手机语音助手：已经在特定交互场景取得巨大成功
- 作为辅助操作系统开发者的「外脑」
 - **“人无法阅读上亿行Linux内核代码变更历史；但是AI可以。”**
- 操作系统用户的行为感知、预测与优化
 - **“人无法长时间统计应用启动规律和资源消耗区间；但是AI可以。”**
- 操作系统层面的程序异常行为检测
 - **“人无法阅读上亿行日志文件；但是AI可以。”**
- 异构架构下的算力分配和调度
 - **“人无法精确异构计算能效比；但是AI可以。”**

LLM in OS 视角：现有应用将被大范围整合

问题： Windows约有**3500万应用**， Android/iOS各拥有超过**500万APP**，长尾应用日活率低，维护成本居高不下



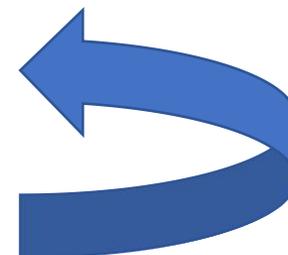
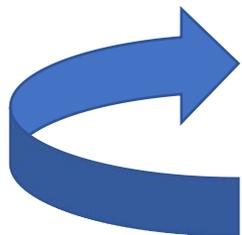
方案： 通过大语言模型，实现对APP的大范围筛选整合

DSA成为主流：RISC-V 成为“希望之星”

- RISC-V 或许有希望成为未来指令集 (ISA) 的国际统一标准架构
 - 这么多AI芯片软件栈未来一定会收缩聚焦统一
 - 这么多AI加速卡未来一定会收缩到同一个开放架构

IBM System/360的四个型号

Model	M30	M40	M50	M65
Datapath width	8 bits	16 bits	32 bits	64 bits
Control store size	4k x 50	4k x 52	2.75k x 85	2.75k x 87
Clock rate (ROM cycle time)	1.3 MHz (750 ns)	1.6 MHz (625 ns)	2 MHz (500 ns)	5 MHz (200 ns)
Memory capacity	8-64 KiB	16-256 KiB	64-512 KiB	128-1,024 KiB
Performance (commercial)	29,000 IPS	75,000 IPS	169,000 IPS	567,000 IPS
Performance (scientific)	10,200 IPS	40,000 IPS	133,000 IPS	563,000 IPS
Price (1964 \$)	\$192,000	\$216,000	\$460,000	\$1,080,000
Price (2018 \$)	\$1,560,000	\$1,760,000	\$3,720,000	\$8,720,000



硬件



Wilkes
指令和微程序

让便宜的 8 位数据路径计算机与高速的 64 位计算机共用一套 ISA

指令集出现的初衷



Brooks
IBM/360 操作系统

软件

一个设计良好的指令集带来的好处

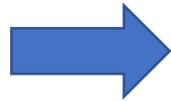
- #1 解耦软硬件，使二者可以异步并行开发**
- #2 支持多种处理器微架构（异构多样算力）**
- #3 支持多种操作系统（多种应用场景）**

然而，对于操作系统，理想与现状出现了差异

理想



One ISA to Rule Them All



现状



Too Many ISAs to Serve

例如悲惨的Linux内核:

```
[yanjun@localhost arch]$ ls  
alpha  arm    csky   ia64   loongarch  microblaze  nios2  parisc  riscv  sh    um    xtensa  
arc    arm64  hexagon  kconfig  m68k      mips        openrisc  powerpc  s390  sparc  x86
```

Linux 内核需要支持 **24** 种指令集架构

后果：代码中含有指令集相关的大量 #ifdef

➤ Discipline Matters: Refactoring of Preprocessor Directives in the #ifdef Hell (TSE '2018)

通过6种#ifdef滥用模型，对63个C项目代码重构，其中内核涉及优化代码近千行

TABLE 1: Application possibilities in 63 C projects.

Project	Version	LOC	Domain	R1	R2	R3	R4	R5	R6
Angband	4.0.4	79 370	game	0	0	1	1	0	1
Amxmodx	1.8.3	262 186	server administration tool	0	21	7	12	84	6
Asfmapready	3.2.1	244 817	command line tools	0	0	3	0	0	0
Bash	4.2	96 153	command language interpreter	2	5	26	12	6	7
Berkeley DB	4.7.25	170 570	database system	5	18	6	1	9	16
Bison	2.0	20 379	parser generator	0	0	0	0	0	0
Busybox	1.23.1	182 555	common UNIX utilities	20	15	6	20	4	19
Cherokee	1.2.101	56 832	Web server	0	7	1	2	23	0
Clamav	0.97.6	342 636	antivirus software	9	9	4	4	17	12
Collectd	5.5.0	94 105	system administration tool	0	5	2	0	1	3
Curl	7.46.0	95 646	data transferring tool	5	19	2	8	38	7
Cvs	1.11.17	71 128	version control system	4	23	7	14	26	6
Dmd	2.069.2	94 687	language interpreter	2	37	12	9	2	15
Emacs	24.4	277 263	text editor	20	41	9	24	34	14
Ethersex	0.1.2	61 611	processor firmware	5	11	30	11	5	3
Freeradius	3.0.10	101 242	radius server	0	19	1	4	21	44
Gawk	3.1.4	39 499	interpreter	0	11	4	7	32	5
Gcc	4.9.2	2927 120	compiler	51	371	32	172	121	114
Glibc	2.20	638 002	C library	29	53	16	76	71	38
Gnumeric	1.12.20	277 068	spreadsheet program	4	0	1	1	0	5
Gnuplot	4.6.1	83 260	plotting tool	2	6	4	15	42	7
Irssi	0.8.15	49 085	chat client	0	0	3	1	4	0
Kerberos	1.14	280 532	network authentication protocol	0	10	4	3	3	4
Kindb	1.0	61 486	database system	0	0	7	0	2	0
Hexchat	2.10.2	56 764	chat client	0	0	5	2	2	5
Libdsmcc	0.5	1814	DVB library	0	0	0	0	0	0
Libpng	1.5.14	32 432	PNG library	5	12	9	5	23	1
Libsoup	2.41.1	36 844	SOUP library	0	0	0	0	0	0
Libssh	0.5.3	25 451	SSH library	0	0	0	0	1	1
Libxml2	2.9.0	207 996	XML library	1	27	6	5	57	8
Linux	3.18.5	9 771 439	operating system kernel	129	60	40	71	277	518
M4	1.4.17	9623	macro expander	0	3	4	5	15	2
Machinokit	0.1	197 887	machine control platform	0	5	3	1	3	4

```
#ifdef CONFIG_X86_64
void arch_release_task_struct(struct task_struct *tsk)
{
    if (fpu_state_size_dynamic())
        fpstate_free(&tsk->thread.fpu);
}
#endif
```

预处理宏定义的滥用，会对代码可读性、维护性、自动化分析等造成极大影响

RISC-V的核心愿景之一是成为指令集开放标准

RISC-V is a free and open ISA enabling a new era of processor innovation through open **standard** collaboration.

The RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the **next 50 years** of computing design and innovation.



操作系统的理想之一：通过一种 ISA 支持异构多样算力

支持异构算力 ≠ 支持多种ISA

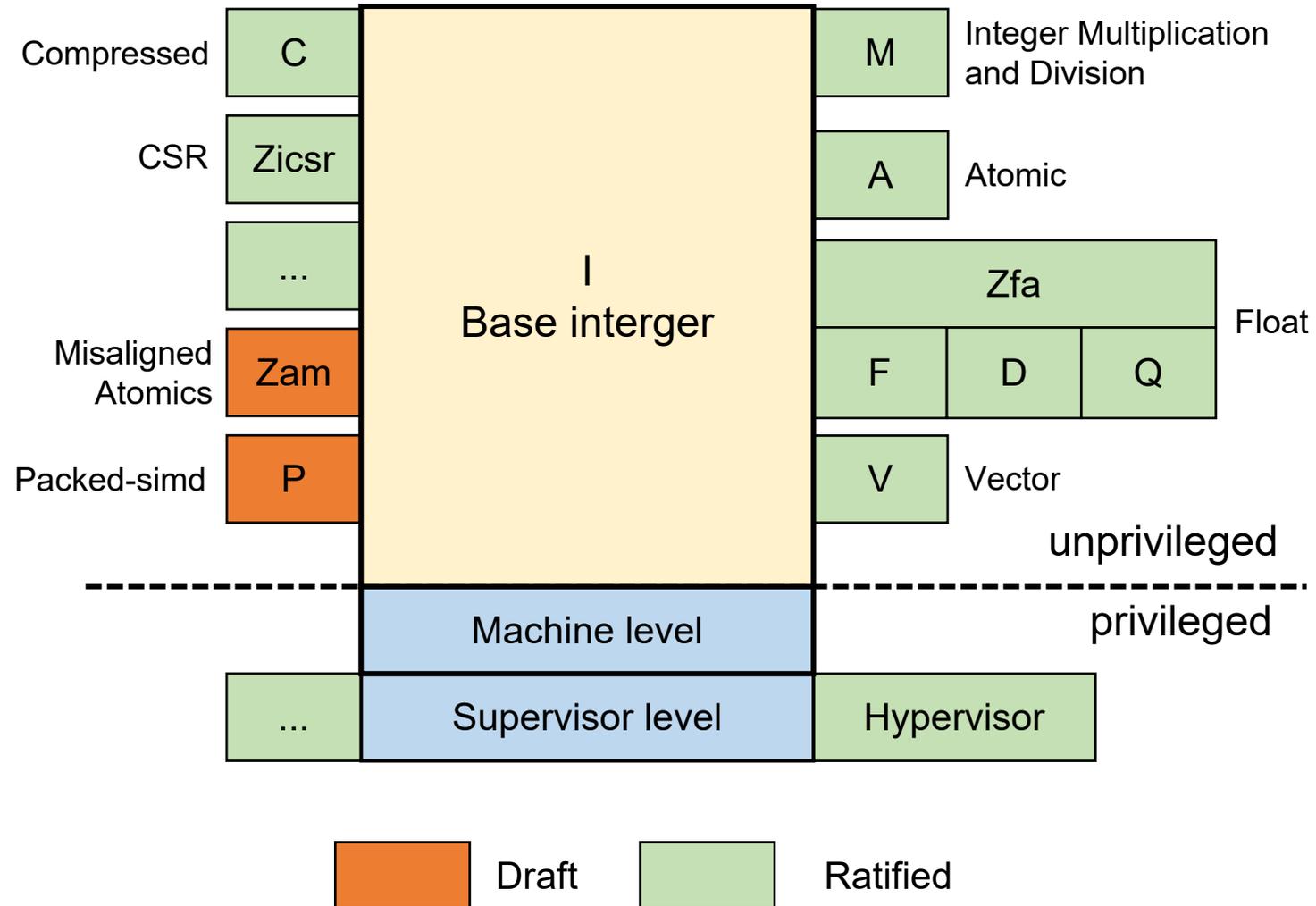
RISC-V已经提供了足够的多样性

RISC-V指令集 = 基础指令集 + 标准扩展指令集 + 用户自定义扩展指令集

多样性1
(V/P/K...)

多样性2
(安全扩展、张量扩展...)

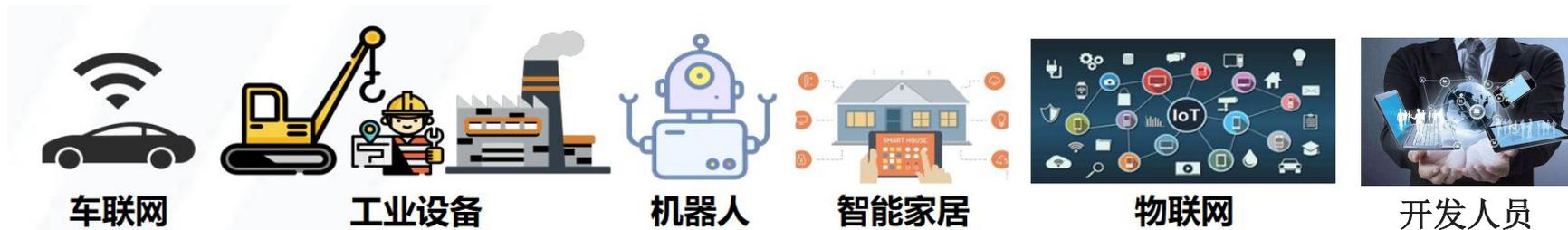
RISC-V 可扩展性带来的多样性



操作系统的理想之二：通过一种 ISA 屏蔽多种架构

千行百业的应用场景

应用场景



生态细腰：开源开放，共建共享



基础软件开发人员

CPU厂商开发人员



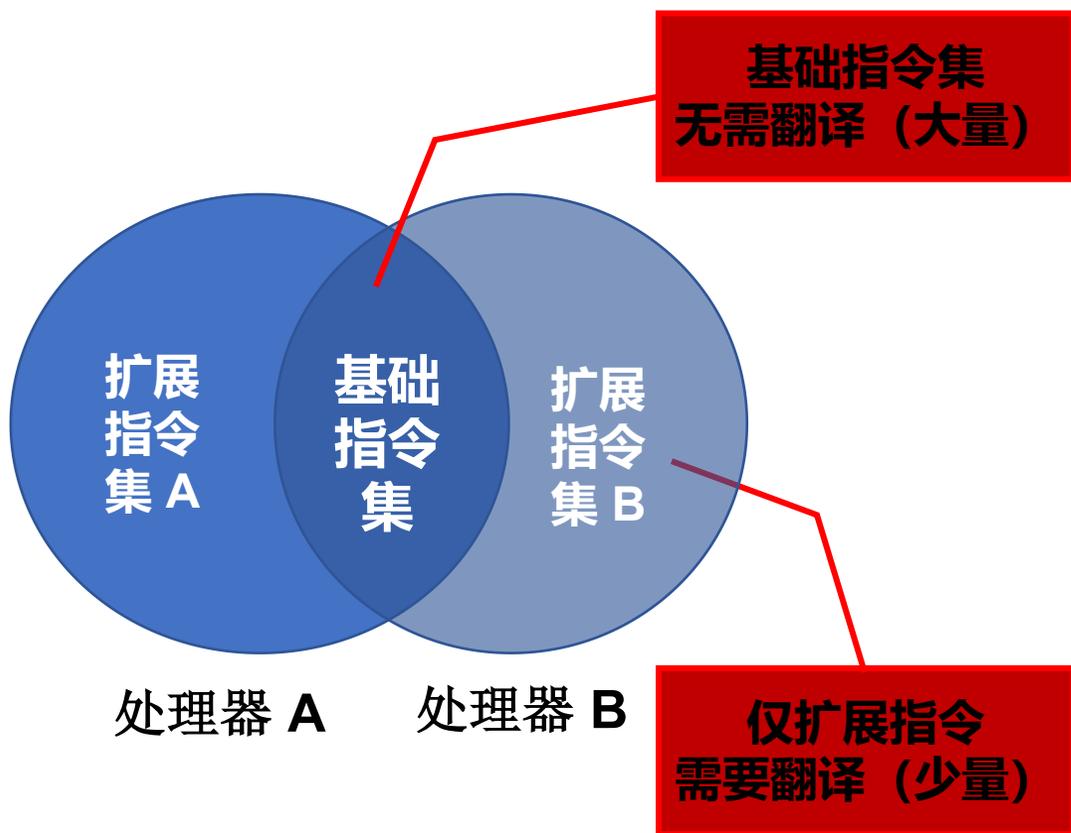
处理器芯片



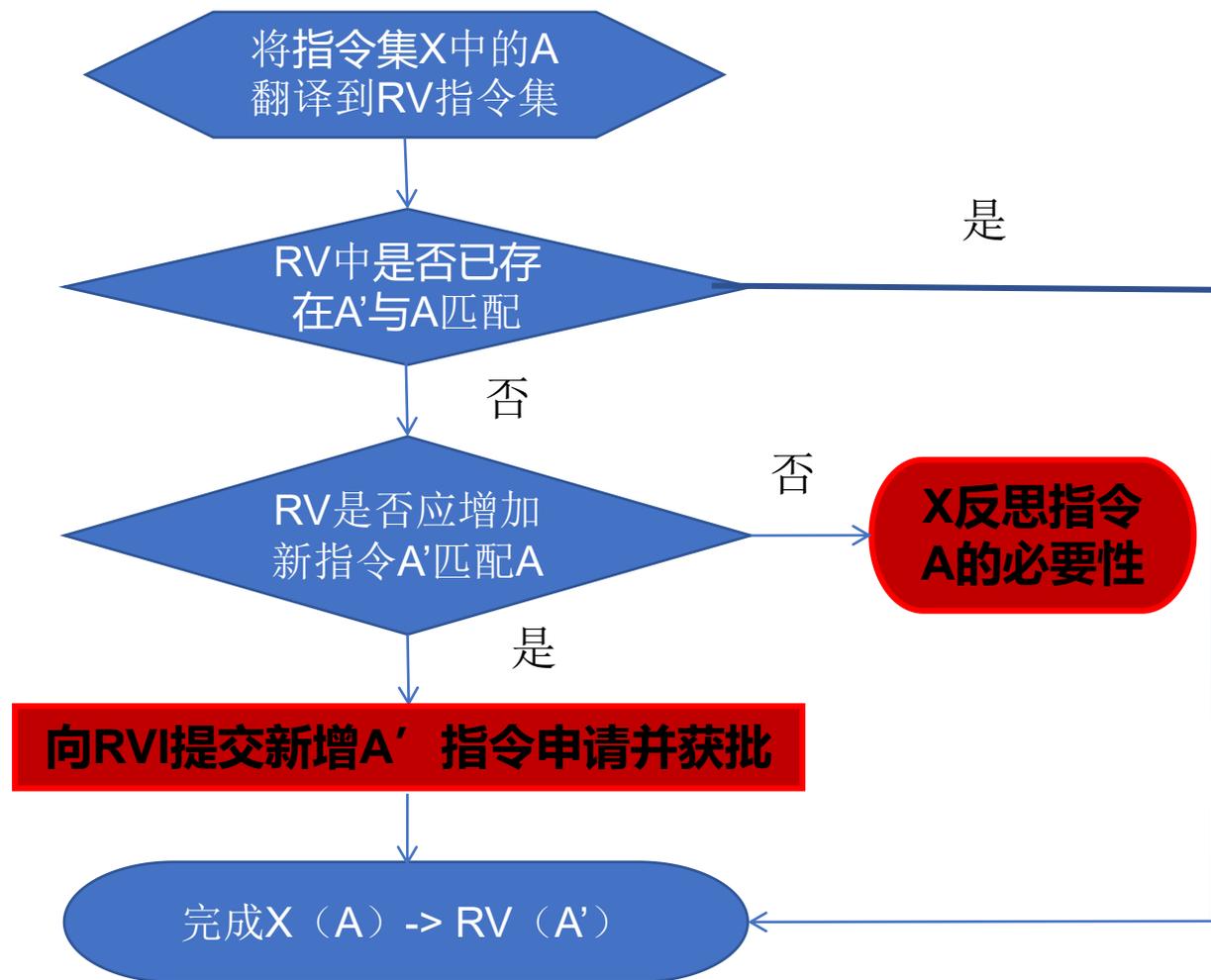
成千上万的异构芯片

RISC-V 开放性带来软件在不同架构之间迁移的便利性

RISC-V 处理器之间的迁移



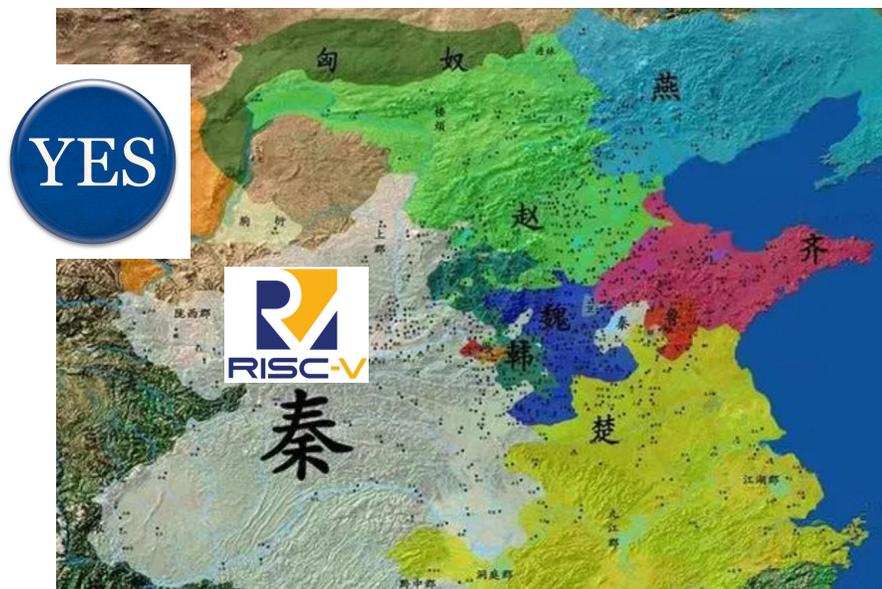
其他指令集架构 X 向 RISC-V 的迁移



“三分天下” V.S. “一统江湖”

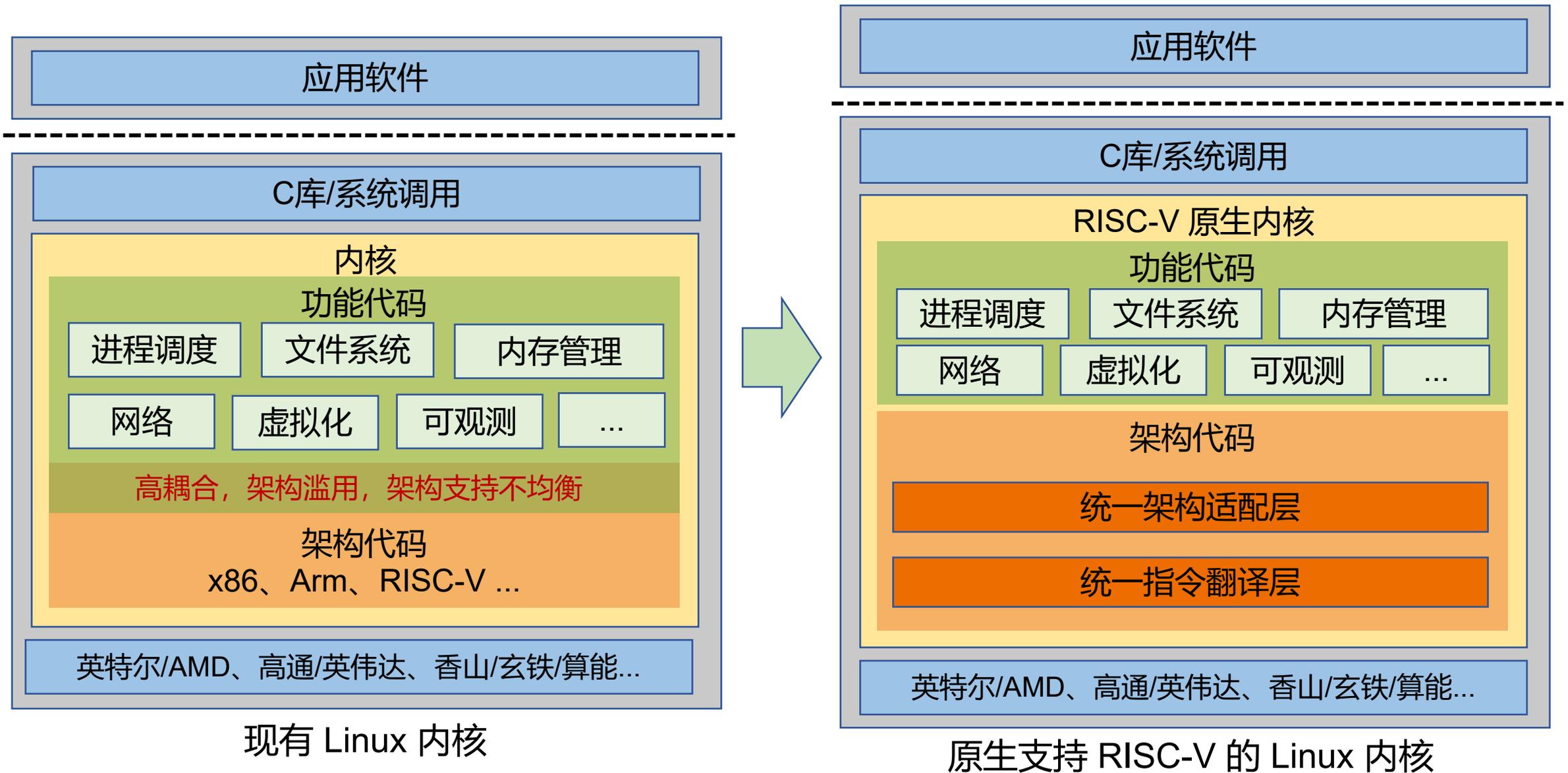
RISC-V未来只是与X86/ARM三分天下么?

“书同文、车同轨”才是RISC-V的理想



以此为目标，从现在开始，重构基础软件栈

RISC-V 平行宇宙：原生支持 RISC-V 的操作系统架构



One World, One ISA



Ref

- https://en.wikipedia.org/wiki/Operating_system
- [1hr Talk] Intro to Large Language Models https://www.youtube.com/watch?v=zjkBMFhNj_g and [slides]
- AIOS: LLM Agent Operating System <https://arxiv.org/html/2403.16971v2>
- 大模型时代，智能化操作系统面临的机遇与挑战 <https://www.openeuler.org/zh/news/openEuler/20231027-1024/20231027-1024.html>
- 清华张亚勤：大模型将是AI时代的操作系统，产业机会将比PC时代增长100倍 https://www.sohu.com/a/734708000_115565
- 大模型元年，人类文明的操作系统正在大更新 <https://m.huxiu.com/article/2622268.html>
- The History of the Operating System – From paper tape to Red Hat OpenShift <https://www.orb-data.com/the-history-of-the-operating-system-from-paper-tape-to-openshift/>
- 张亚勤：AI大模型时代 <https://air.tsinghua.edu.cn/info/1007/2015.htm>
- 对话陈卫：为什么AI大模型时代更需要计算机理论研究？ <https://www.msra.cn/zh-cn/news/people-stories/wei-chen>
- AI OS时代来了！国产操作系统换道超车，颠覆人机交互范式 <https://zhidx.com/p/410020.html>
- 下接万卡集群、上连AI原生应用，操作系统的进化超出你的想象 <https://www.jiqizhixin.com/articles/2024-04-19-15>
- 大模型的「狂飙时代」，以开源之力推动「新Linux底层操作系统」 <https://cloud.tencent.com/developer/article/2249121>
- 腾讯发布大模型时代的AI十大趋势：走进“机器外脑”时代 <https://36kr.com/p/2849152770230912>
- LLM OS <https://x.com/karpathy/status/1723140519554105733>
- HOW AI AS AN OPERATING SYSTEM IS SHAPING OUR DIGITAL FUTURE <https://hatchworks.com/blog/gen-ai/ai-driven-operating-systems/>
- What is a conversational interface? <https://www.zendesk.com/blog/conversational-interface/>

谢谢

报告人：武延军

中国科学院软件研究所

2024-08-20 @ 杭州