SpaceChain OS 白皮书

1.1 共同的语言

一个组织需要相互沟通的语言。这个语言需要统一 ,满足所有的场景对于沟通的需求。有了语言，人类的智慧才开始累积，相互之间的交流效果指数级上升。

有了共同的语言，人类开始聚集，学习，贸易。

共同的语言，如同一个强力的粘合剂，把所有的联盟成员结合在一起。成员的技术积累因为有了平台，开始可以互相交流，代码彼此都可以复用。专用设备变成资源池，信息在池子里流通，统一进出。

1.2 为什么我们需要操作系统

1.2.1 航天器操作系统需求

航天领域设备种类比较繁多，不同的设备运行了众多种类的操作系统。而这些众多的操作系统，就像不同语言的书。不同的是，移植操作系统的应用复杂程度远高于翻译一篇文档。

所以，我们需要有一款操作系统，来满足尽可能多的场景的需求，就像英语一样。

SpaceChain OS 首先满足绝大多数设备的技术需求。火箭的飞行控制，需要惯性导航，导航过程中的积分运算，对于实时性要求严格，这时候，必须有一款高效的实时操作系统。而如果我们希望实现火箭的返回和降落，那么，对于发动机角度和动力需要极其精确复杂的控制，我们也需要一套大型操作系统才能保证稳定运行。众多的星载、箭载、空间站设备则需要一款通用操作系统，用来处理传感器数据，显示人机界面，进行交互，并存储数据。航天领域使用的操作系统种类繁多，目前已经

得到应用的操作种类繁多，按照实时性来区分，需要两种类型操作系统。

1.2.2 用于卫星、火箭等各类航天器以及其搭载设备的实时操作系统

操作系统需要硬实时性。

- 实时操作系统，用于需要实时性控制的场景。通常包括：卫星姿态控制、星务计算机、雷达、设备监控显示、设备控制、点火系统、发动机控制系统、生命维持系统等。
- 目前，航天器上使用比较多的实时操作系统或者小型嵌入式系统有：INTEGRITY、VxWorks、SpaceOS、 Reworks、FreeRTOS、RTEMS、SylixOS，μC/OS II。

1.2.3 用于载荷等设备的通用操作系统

- 通用操作系统，用来满足航天器机载设备的需求，这类设备运行可能不需要硬实时性。在对于可靠性、稳定性的有要求的同时，更多的需求体现在易用性以及开发成本之间达到平衡。
- 目前操作系统使用比较多的包括:Linux、SylixOS、Windows 等。

通用操作系统需要满足大多数情况下的要求：

- 兼容性强，运行平台覆盖设备种类多。才能尽量所有平台采用同一操作系统，以避免过多操作系统平台带来的维护困难以及代码复用难的问题。
- 扩展性强，升级能力强。在硬件更换或升级的情况下能尽量保持 APP 不变。
- 较低的开发成本，避免开发者因成本问题而无法参与其中。
- 较高的透明度，解决不同组织对于代码信任的问题。

1.2.4 用于第三方中间件、软件的需求。

上层软件、中间件的开发通常会基于一套 API，SpaceChain OS 需要支持这套 API 和编程接口：

- 降低开发成本，降低学习成本。
- 保证原有程序尽可能少的改动就可以运行在新的平台上。提高延续性，降低迁移成本。

1.2.5 满足教育需求。

在 Space Chain 希望达成的共识机制中，新生工程师的力量是非常重要的部分。Space Chain 拥有一个宏大的教育计划和目标，以培养更多的优秀工程师，爱好者。

操作系统需要能满足对于教育行业的需求。教育有三点要求，低成本、开放、高延续性。

1.2.6 安全

信息安全，业务安全是两个重要的维度，必不可少。

信息安全：通信数据链路的安全、卫星开放的运算资源不被劫持，都是操作系统要带来的特性。

开放的卫星面临比传统卫星更多的攻击，而数据的安全也越发重要。

业务安全：航天飞行器成本高昂，必须最大限度的保证可靠性安全性，安全性。业务安全细分又有两个维度：1，业务本身运行的可靠性，稳定性。2，遭遇失败后的异常恢复机制。

操作系统需要满足这两点要求。

1.2.7 开源

一门用来沟通的语言必须是开源并且透明的，这样，不同的爱好者、公司才能安心使用，提供代码贡献或者用于设备之上。。

1.3 SpaceChain OS 诞生

1.3.1 SpaceChain OS 来源

SpaceChain OS 的内核源自于 SylixOS。SylixOS 是一款基于 GPL 协议开源的实时操作系统，目前已经在不同的设备，包括航天，无人机，潜艇、电力等行业得到了广泛的应用，代码成熟完善，可靠。SylixOS 同时是一款兼容性极强的操作系统，方便我们扩展，并且可以随时用到尽可能多的设备上。

太空链基金会努力推广 SpaceChain OS 应用到不同的航天器，包括卫星、卫星地面系统、空间站、太空飞船、太空探测器等。实现资源的整合以及优化利用。

1.3.2 多平台的支持

SpaceChain OS 支持 6 大硬件平台，包括 ARM、DSP、SPARC、X86、MIPS、RISC-V。基本覆盖几乎所有能见到的处理器架构，其中包括目前航天使用较多的 PowerPC 以及 SPARC、MIPS，同时，对于航天领域，尤其是低轨已经崭露头角的处理器 ARM 和极具潜力的 RISC-V。

1.3.3 图形、多媒体的支持

SpaceChain OS 支持完善的 QT、Micro windows、mu C/GUI 等图形框架。完善的图形界面支持可以满足浏览器，图形显示、触控等交互和显示的需求。

SpaceChain OS 具备强大的多媒体功能，包括 QT MultiMedia、FFMPEG、VoIP、xAudio、xCamera 等。实现了完整的音视频编解码、基于 Internet 的传输，7.1 声道音频混合、视频采集，格式转换等。

1.3.4 API 及扩展能力

SpaceChain OS 应用编程接口符合 IEEE、ISO、IEC 等多种编程接口规范，目前支持四套 API，包括：POSIX 1003.1b，VxWorks V6.8（90%），GJB7714-2012，Sylix API。

强大的扩展能力使得 SpaceChain OS 在满足航天苛刻的应用环境的同时，也可以便捷地将其安全稳定的特点应用于其他领域和场景，比如地面设备、手持终端、雷达、测控站等。这些场景可能不需要实时性，甚至也不需要高可靠性。使用跨平台的应用可以极大的节省开发和学习成本。

目前，SpaceChain OS 已经支持的第三方中间件包含但不限于如下：OpenSSL、Python、unixODBC、GoAhead、FastDB、SQLite、Lua、QGIS、uGFX，OpenMP 4.0、OpenBLAS。通过支持这些中间件，Space China OS 支持加密，脚本语言，以及各类现场总线，标准等。

具体信息请参考 OS 入门手册和功能说明。

SpaceChain OS 升级能力强大。SpaceChain OS 支持动态加载，支持 APP 和操作系统单独开发，支持一键上传、部署应用，支持应用和 OS 自身在线升级等多种升级方式。以满足一个开放卫星平台得需求。通过分离 APP 和 OS，为实现了航天器运行资源的分离和共享提供支持。工程师、爱好者的应用通过沙盒安全的运行在操作系统上，地址资源独立。

1.3.5 开源

SpaceChain OS 之所以可以实现大规模的知识共享，源代码、APP 复用，最大限度保证开发成果的复用性、可延续性，一个前提就是 OS 必须开源透明。

SpaceChain OS 是一套开源的操作系统 ,包括 SylixOS kernel、第三方中间件、卫星应用、QTUM 以及其他中间件或者应用程序，所有的源代码公开。可以访问 SylixOS.com,spacechain.com 免费获得。

知识的分享不能是封闭的，Space Chain 选择了开源的 SpaceChain OS 以及开源指令集 RISC-V 作为开发教育计划的基础。Space Chain 会提供太空运算能力给到教育计划，参与者上传其 APP 就可以直接太空环境得到验证和应用。

开放的源代码，也是合作方彼此信任合作的基础。

从技术角度，开源的操作系统也最适用于嵌入式开发和协作。可以带来如下好处：

- 方便开发、故障定位。
- 提高系统可靠性，降低技术风险。
- 适用于嵌入式定制、裁剪、技术透明度高。

1.3.6 安全

a) 业务业务

SpaceChain OS 提供形式化验证模型、掉电安全文件系统、SIL 认证。

- 形式化验证模型。SpaceChain OS 对于核心代码采用形式化验证模式的方式进行开发。系统代码（包含源代码与汇编代码）基于高阶逻辑证明工具 Isabelle/HOL 表述语言建立操作系统抽象规范，采用人机交互式的定理证明方法，对可执行规范与抽象规范、C 语言实现与可执行规范两个层面的精化关系进行证明。
- 掉电安全文件系统。嵌入式设备面临运行风险多余桌面设备，比如随时可能的断电。在这个时候，SpaceChain OS 采用 TPsFs 文件系统，保证了在任何极端情况下文件系统、数据结构不损坏。这项创举避免了多项问题，包括在线升级失败，断电重启后系统失效等多种可能。
- 功能安全认证。功能安全（Functional Safety）的要求是无论零部件或者安全相关控制系统发生的失效是硬件随机失效还是系统失效，都需要使受控设备可靠地进入和维持安全状态，避免对人员或者环境产生危害。Space Chain 会在稍晚更新达到 SIL3 级水平，符合 IEC61508 标准的安全操作系统内核。
- 安全沙盒和并行虚拟化。Space Chain 正在开发并行虚拟化技术，提供符合 ARINC653 要求，但是性能更好的安全沙盒。超脱于传统的进程地址空间隔离，这项基于 L4 的微内核，实现了多安全分区沙盒隔离，是支持并行化的多安全分区。多分区支持多核并行加速，允许分区之间快速通讯，支持实时调度。

b) 信息安全：

开放意味着透明，但是不代表信息泄露和危险。

航天、卫星系统应用多样，既有实时性要求高的控制类应用，也有实时性要求不高的辅助性应用，不同应用的安全等级差异很大。。

- SpaceChain OS 内建网络安全模块、防火墙，网络风暴屏蔽系统、提供流量控制、负载均衡等功能。
- SpaceChain OS 支持可信计算，通过硬件以及软件双重的方式确保其上运行的设备、软件相互可信。非法设备、软件不能加入网络，也无法欺骗可信设备或软件并在之上运行。
- SpaceChain OS 利用传统安全沙盒的虚拟化能力，采用数据隔离、信息流控制、资源控制及故障隔离等方法，形成逻辑上的多个不同安全等级的计算分区，使每个逻辑分区拥有独立的资源，并能够对资源配额、信息流以及故障实现隔离处理，实现操作系统在保持实时性前提下多层次安全要求与实时性之间的有效平衡
- SpaceChain OS 提供基于区块链技术的沙盒，确保应用之间的数据相互独立，任何开发者都可以有一个安全的环境来运行他们的应用程序，就像 iOS 手机操作系统一样。APP 的错误或失败不会影响到其他的 APP，更不会影响到 OS 的运行和底层硬件的安全。区块链技术的应用也能保证数据传输过程中的加密，保证存储数据不被非法篡改。

1.3.7 其他

深度学习。SpaceChain OS 支持深度学习，针对于嵌入式设备的特点，支持训练和应用分开的模式，保持同样效果的情况下，缩小应用设备的计算规模，降低成本。对于深度学习应用，SpaceChain OS 可以实现硬件隔离和网络建模。目前，正在进行技术验证阶段。

1.4 开发和应用

1.4.1 区块链平台

Qtum 量子链是实现了在 PoS 和 UTXO 下的智能合约平台，并推动去中心化应用（Dapp）在移动端的普及。由于采用了 PoS 机制，使得在嵌入式设备上就能实现完整功能的全节点。

SpaceChain OS 已经支持了 QTUM，实现区块链沙盒功能，并且发布 EVM 虚拟机。详情可以访问 GitHub 获取代码和相关说明文档。

我们也在继续工作，以便支持企业以太坊，以便更大幅度扩展应用范围。

通过对于以上平台的支持，我们可以讲区块链运行在小规模的嵌入式系统中。这类嵌入式设备可能一个板卡只有数十美元，通过降低成本，大规模的部署区块链变得可能。

1.4.2 设计方案、案例和适用场景

目前，SpaceChain OS 提供了大量完整的设计方案和案例，包括 Sparc，PowerPC,Cortex-R5，Zynq 等，详细介绍如下。

- PowerPC

  目前应用在航天上的 PowerPC 处理器有国微电子的 SM750 处理器和 NXP 公司的 P1022 处理器。

  SM750 是国微电子的一款高性能 32 位超标量低功耗微处理器，采用 PowerPC 精简指令集，且功能兼容 Motorola 公司的 MPC750 芯片，主频：266MHz，有抗辐射、超宽温的宇航级版本芯片。

  P1022 是 NXP 公司的一款基于 E500 核心的双核处理器，主频：1GHz，性能较高，可以应用在数据处理、科学计算等性能要求较高的应用场合。目前国微电子的 SM750 处理器已经完全适配完成，因 SM750 是一款主处理器，外设只能通过桥芯片或 FPGA 扩展，所以外设一般较

少并且有针对性，所以 SpaceChain OS 对其做了很多针对性和优化的工作，比如安全 bootloader、关键数据三选一表决、远程升级、掉电安全写平衡 flash 文件系统等等。

- Cortex-R5

ARM 公司在经典处理器 ARM11 以后的产品改用 Cortex 命名，并分成 A、R 和 M 三类，旨在为各种不同的市场提供服务。Cortex 系列属于 ARMv7 架构，这是到 2010 年为止 ARM 公司最新的指令集架构。ARMv7 架构定义了三大分工明确的系列："A"系列面向尖端的基于虚拟内存的操作系统和用户应用；"R"系列针对实时系统；"M"系列对微控制器。Cortex-R 实时处理器为要求可靠性、高可用性、容错功能、可维护性和实时响应的嵌入式系统提供高性能计算解决方案。

Cortex™-R5 能适用于航天，主要是因为其有如下两个特色安全功能：针对具有 ECC 位的高速缓存和/或 TCM 内存的可选单位错误更正和双位错误检测。处理器将自动更正单位软错误。还可在所有外部接口上实施 ECC 保护。一种双处理器配置，适用于以锁步方式实现冗余 Cortex-R5 CPU 而获得可靠的容错/故障检测系统的，或者是独立运行的双核，每个内核都使用自己的总线接口、中断等执行自己的程序。

目前应用在航天上的 Cortex-R 处理器有 TI 公司的 TMS570LS3137 处理器和 TMS570LC43x 处理器。目前 SpaceChain OS 已经完成了上面两款处理器的适配工作，并且支持上面的两个特色安全功能，保证了卫星计算机硬件系统在受到高能粒子的冲击时，能有一定的纠错和容错的能力。主要应用在低轨小卫星的主任务计算机上。

- Sparc

SpaceChain OS 和九天微星合作，在卫星主任务计算机上，使用 Sparc VC8 和 SpaceChain OS，相比较传统的 OS 和软件，SpaceChain OS 的加入带来了诸多新功能，包括：

a) 应用软件 OTA 解决方案，对于在轨微星，可以通过 OTA 的方式更新应用软件。这种更新方式对于未来扩展应用带来了极大的便利性。

b) 系统软件完整性解决方案。定制化的 Bootloader，可以实现在微星操作系统或软件启动前，检查 OS 和软件的完整性，此举旨在提升系统可靠性。

c) 多冗余备份。传统的航天备份，不管是热备份还是冷备份都是多硬件方案，成本较高，同时，浪费空间和能源。创新的软件多冗余备份机制，可以部署多套软件或者操作系统在同一卫星硬件平台上，其中一套软件遇到故障或者需要切换任务的情况下，可以手动或者自动切换到另外一套软件。此举旨在提高系统可靠性并且为未来新功能的加入提供底层技术支持。

- ARM+FPGA（ZYNQ7000 系列）

Zynq 是成熟并得到验证的方案，广泛应用于电力、轨道交通、卫星、无人机等行业。其 FPGA+ARM 的异构方案为诸多平台提供了小型化的可能性。在功耗敏感，但是又偶尔需要高性能计算能力的场合，Zynq 成为了一种绝佳的载荷设备。

SpaceChain OS 支持全部的 Zynq7000 外设，包括 QSPI、USB3.0、HDMI、SD、ETHERNET、DMA 等。

1.4.3 如何使用 SpaceChain OS

爱好者可以访问 Space Chain 官网和 SpaceChain OS Github 下载代码、文档、和开发工具。

所有的更新都会第一时间在以上平台公布，如果有更多疑问，欢迎通过社区或者发邮件至 info@spacechain.com 来获取最新信息和加入讨论。

1.4.4 后续计划

SpaceChain OS 于 2017 年 11 月开始架构设计，并同期开始操作系统的开发工作，同步执行测

试流程和卫星星务业务规划与操作系统的配合。在后续发展过程中，SpaceChain OS 不会开发独立分支，内核仍然会和 SylixOS 保持一致。我们的工作重点在于

- 继续开发更多新的中间件和功能库。对于航天和区块链通用技术进行开发和测试。
- 进行载荷试验。以便验证新功能的可靠性稳定性。
- 补充更多使用文档、工具和说明。最大程度降低使用门槛。
- 推广 SpaceChain OS 的应用领域和范围。

我们期待您的支持，期待您加入 SpaceChain OS 爱好者行列。