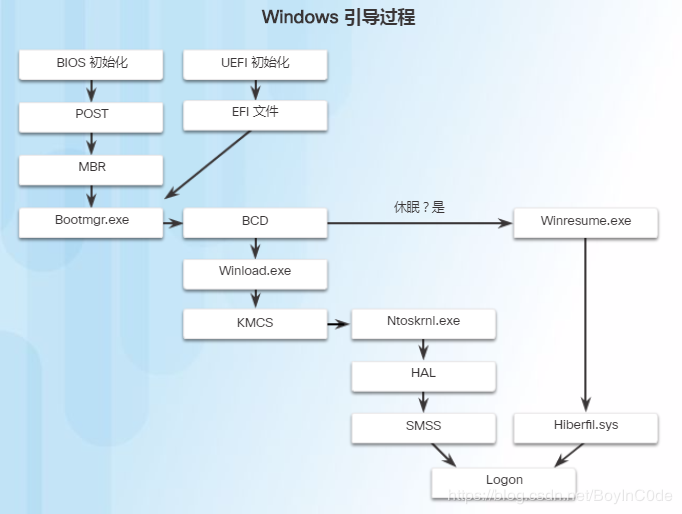
Windows引导过程：



许多操作发生在按计算机电源按钮和Windows完全加载之间，如上图所示。

知识积累：

FirmWare（固件）是固化在硬件中的软件，开机过程中，系统会先读取其内部的硬件设备初始化信息，使操作系统能够正确识别硬件，并为其他软件的运行提供最基本的依据，像硬盘、光驱等硬件都有自己的Firmware。而BIOS是一组固化到计算机内主板上一个ROM芯片上的程序，它保存着计算机最重要的基本输入输出的程序、系统设置信息、开机后自检程序和系统自启动程序。

固件就是写入EPROM（可擦写可编程只读存储器ReadOnlyMemory）或EEPROM（电可擦可编程只读存储器）中的程序。

固件是指设备内部保存的设备“驱动程序”，通过固件，操作系统才能按照标准的设备驱动实现特定机器的运行动作。

固件是担任着一个系统最基础最底层工作的软件。而在硬件设备中，固件就是硬件设备的灵魂，固件就决定着硬件设备的功能及性能。

有两种类型的计算机固件：基本输入输出系统（BIOS）和统一扩展固件接口（UEFI）。BIOS固件创建于二十世纪八十年代早期，现在的工作方式与当初创建时一样。随着计算机的演进，BIOS固件越来越难以支持用户要求的所有新功能。UEFI设计用于取代BIOS并支持新功能。

在BIOS固件中，此过程从BIOS初始化阶段开始。在此过程中，对硬件设备进行初始化，执行电源自检（POST）,确保所有设备都在通信。当发现系统磁盘时，POST终止。POST中的最后指令是查找主引导记录（MBR）。

MBR包含一个负责查找和加载操作系统的小程序。BIOS执行此代码，操作系统开始加载。

与BIOS固件相反，UEFI对引导过程有很高可观性。UEFI通过加载EFI程序文件引导，EFI程序文件作为.efi文件存储 在称为EFI系统分区（ESP）的特殊磁盘分区中。

注：使用UEFI的计算机在固件中存储引导代码。这有助于在引导时增加计算机的安全性，因为计算机直接进入受保护模式。

知识积累：

从80386开始，CPU有三种工作模式：实模式、保护模式和虚拟8086模式。80286开始的CPU引入保护模式，实际上，实模式概念是在保护模式推出之后为了区别保护模式之前的8086CPU工作模式才有的，在8086时代CPU工作模式只有一种，自然没有实模式之说。实模式有着先天的缺陷，但出于向上兼容的考虑，现代CPU仍然保持着对16位操纵模式的兼容，依照设计的规格，所有的x86CPU都是在实模式下开机，来确保传统操作系统的向前兼容性。

所谓的工作模式，是指CPU的寻址方式、寄存器大小、指令用法和内存布局等。

无论固件是BIOS还是UEFI，找到有效的Windows安装后，都会运行Bootmgr.exe文件。Bootmgr.exe可以将系统从实模式切换为保护模式，使所有系统内存都可以使用。

BootMgr.exe读取引导配置数据库（BCD）。BCD包含启动计算机所需的任何额外代码，并指示计算机是从休眠中恢复，还是冷启动。如果计算机从休眠中恢复，引导过程使用Winresume.exe继续。则允许计算机读取Hiberfil.sys文件，其中包含计算机进入休眠时的状态。

如果计算机是冷启动引导，则加载winload.exe文件。Winload.exe文件在注册表中创建硬件配置记录。**注册表**是计算机拥有的所有设置、选项、硬件和软件的记录。Winload.exe还使用内核模式代码签名（KMCS）确保所有驱动程序都有数字签名。这可确保驱动程序在计算机启动时安全加载。

检查驱动程序后，winload.exe运行Ntoskrnl.exe，启动Windows内核，设置HAL。最后，会话管理器子系统（SMSS）读取注册表，创建用户环境，启动Winlogon服务，并且在每个用户登录时准备它们的桌面。