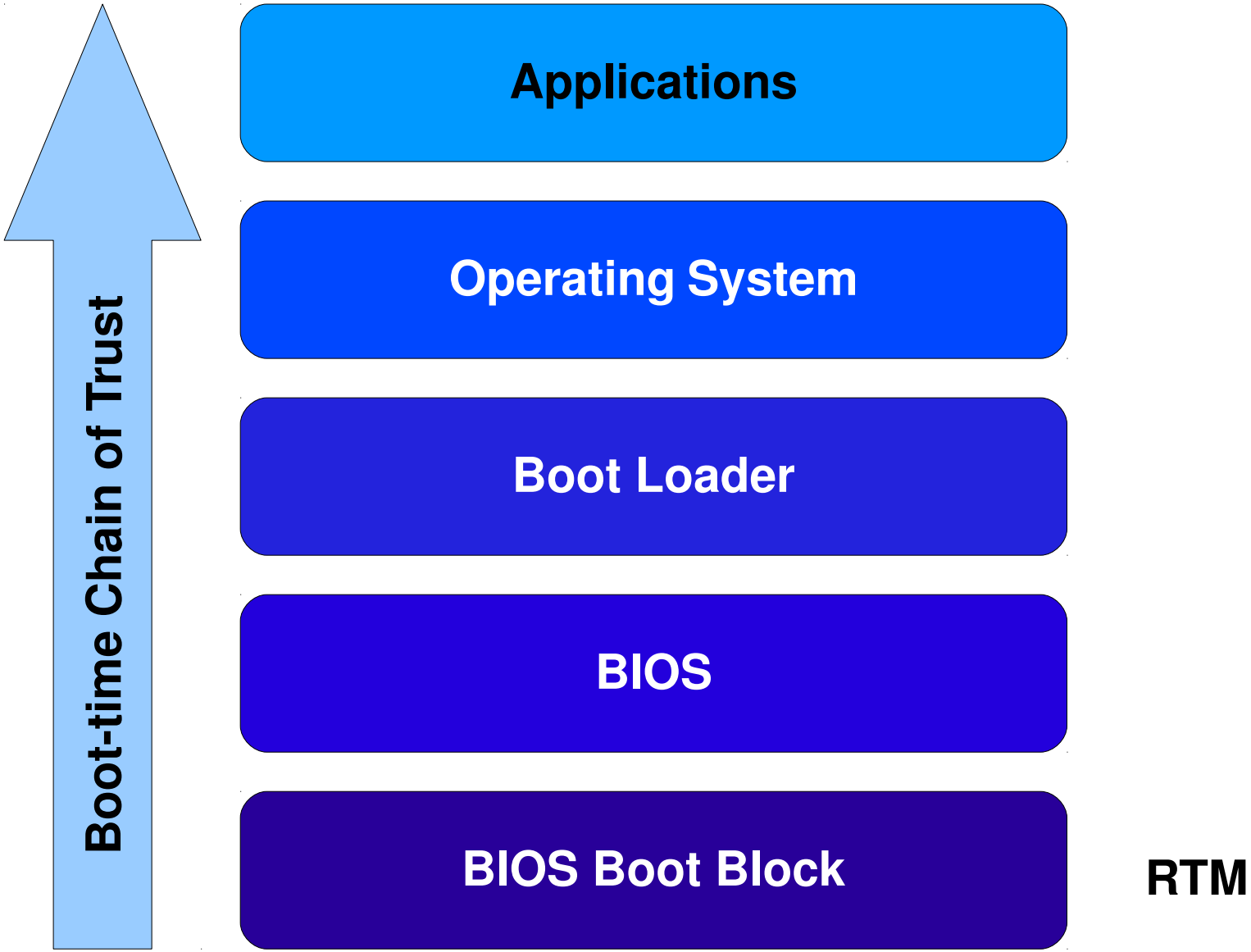
Boot-time Chain of Trust
Applications
Operating System
Boot Loader
BIOS
BIOS Boot Block
RTM