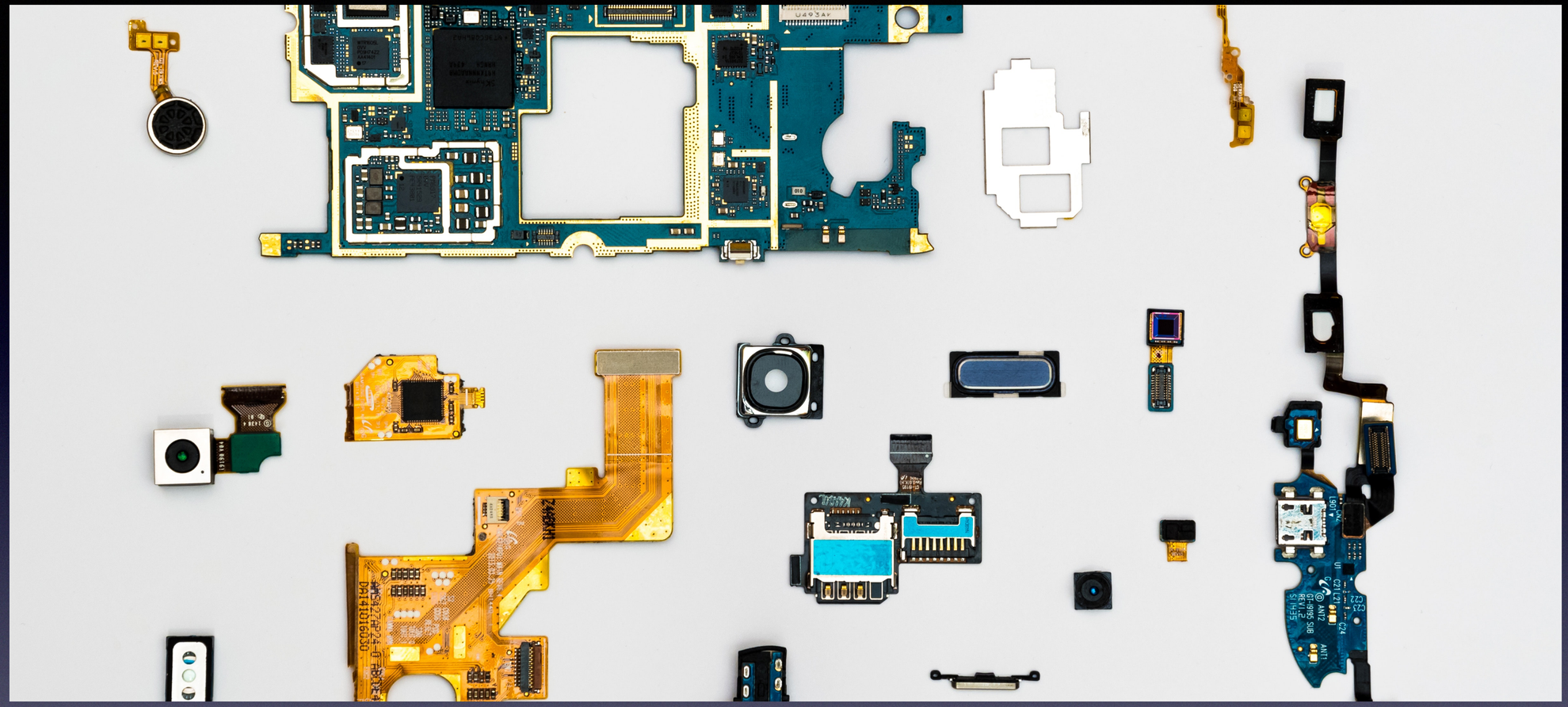
for
Mere Mortals

About Us

- Stephano Cetola
  - TianoCore Community Manager
  - Open Source Firmware (& Hardware) Advocate
- Alexander Graf
  - KVM and QEMU developer for SUSE
  - Founding member of SUSE ARM team

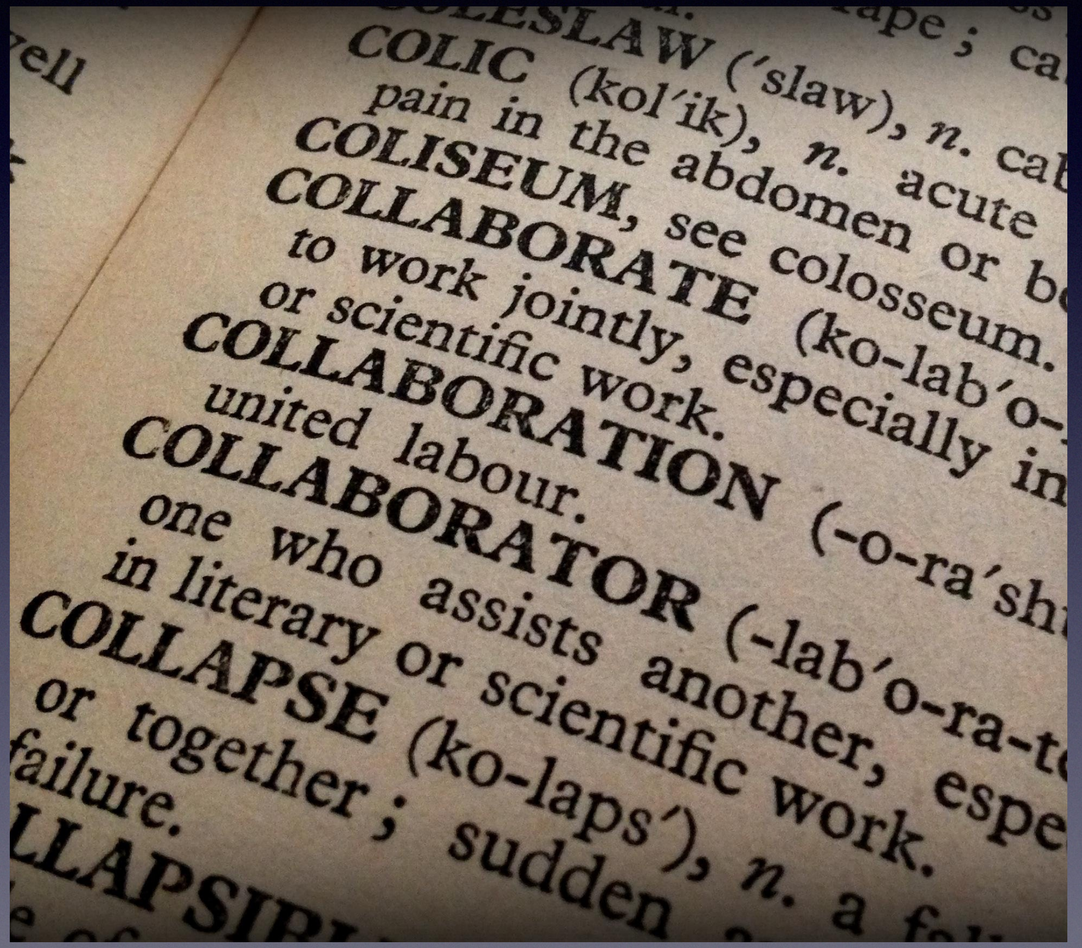


What is UEFI?

“This Unified Extensible Firmware Interface (hereafter known as UEFI) Specification describes an interface between the operating system (OS) and the platform firmware.”
-- UEFI Specification 2.7A, August 2017

What is Defined?

- Platform Initialization
- Boot & Runtime Interfaces
- Advanced Configuration & Power Interface (ACPI)
- UEFI Shell

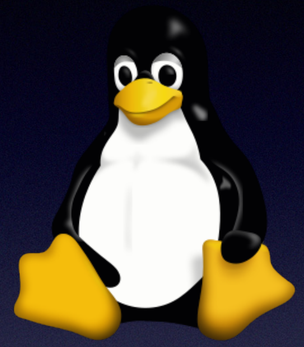


What is the Point?

Hardware Init to Payload Handoff

- Reset Vector
- Memory Initialization
- Boot Media Initialization
- Initialize Silicon Features

  (USB, Network, PCIe, UART, …)



- Standards Driven Interfaces
- Signed Capsule Update
  Linux Vender Firmware Service (LVFS)
- HTTP/HTTPS Boot
- Graphics Output Protocol (GOP)

coreboot & Slim Bootloader

- Minimal initialization
- Quickly handoff to a payload

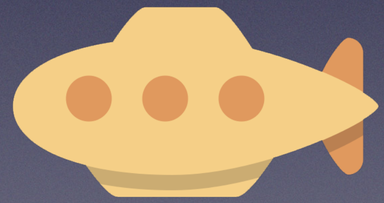
  (Bootloaders & OS's)
- Boot the OS you care about

https://github.com/coreboot/coreboot
https://github.com/slimbootloader/slimbootloader

UEFI Implementation Examples

- Full Hardware Initialization
- Provide Boot-time Services
- Allow Firmware to be updated easily

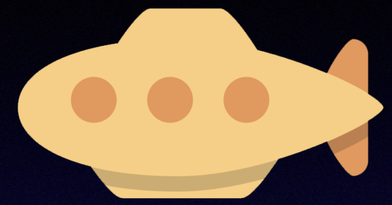
tianocore



https://github.com/tianocore/edk2
https://github.com/u-boot/u-boot

UEFI Implementation Examples

tianocore



- Open Source Since 2004
- PI & UEFI Implementations
- Numerous Platforms (Emulation)
- UEFI Shell

- Open Source from Day 1
- "UEFI Lite" Implemented
- Large Selection of Hardware
- UEFI Shell

EFI Development Kit (EDK II)

- Build your own scalable UEFI implementation
- Open source firmware code
- Multiple corporations working together
- Growing community involvement
- Work from master repo or stable release
- Fully validated UEFI Development Kit (UDK)
- Stable tags created every three months

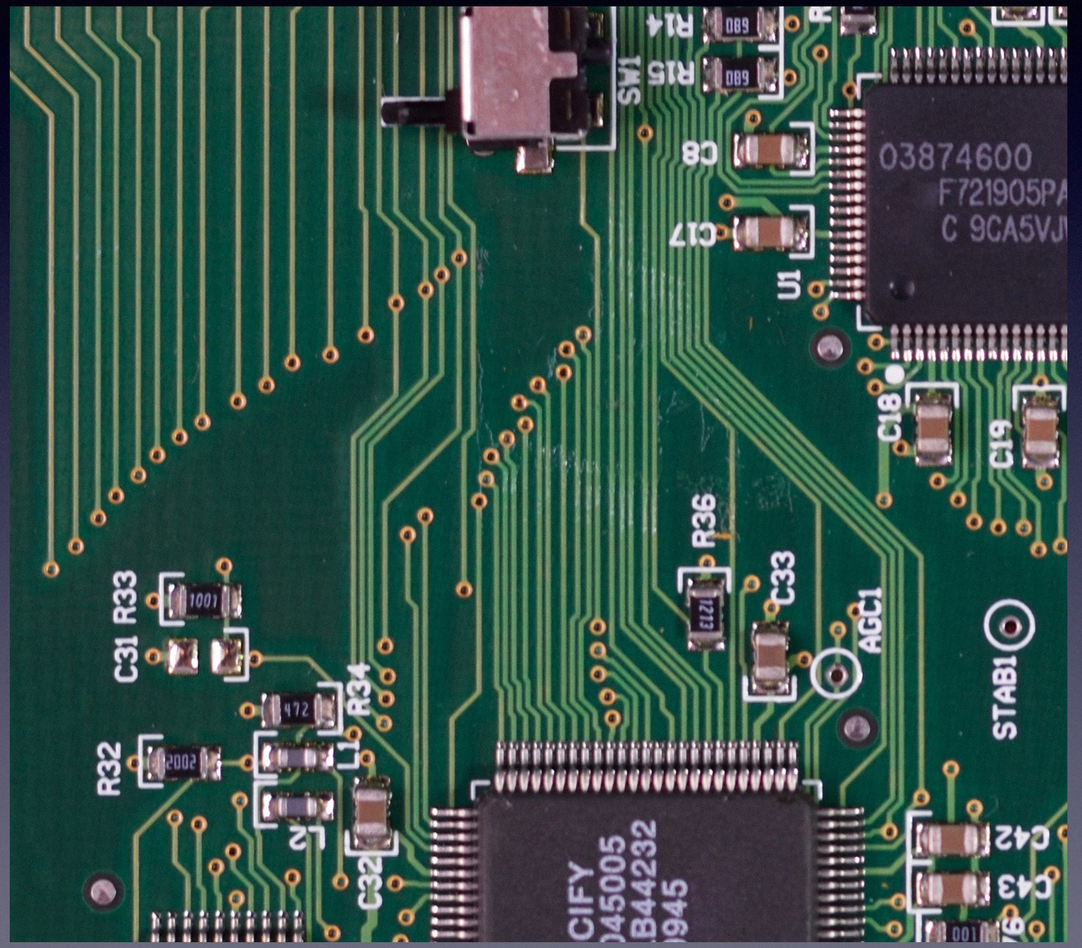
https://github.com/tianocore/edk2

tianocore Community

- Monthly Community Meetings
- https://www.tianocore.org/community-meeting
- Improving our mailing list with Groups.io
- Working on building a community continuous integration (CI) environment

edk2-platforms repo

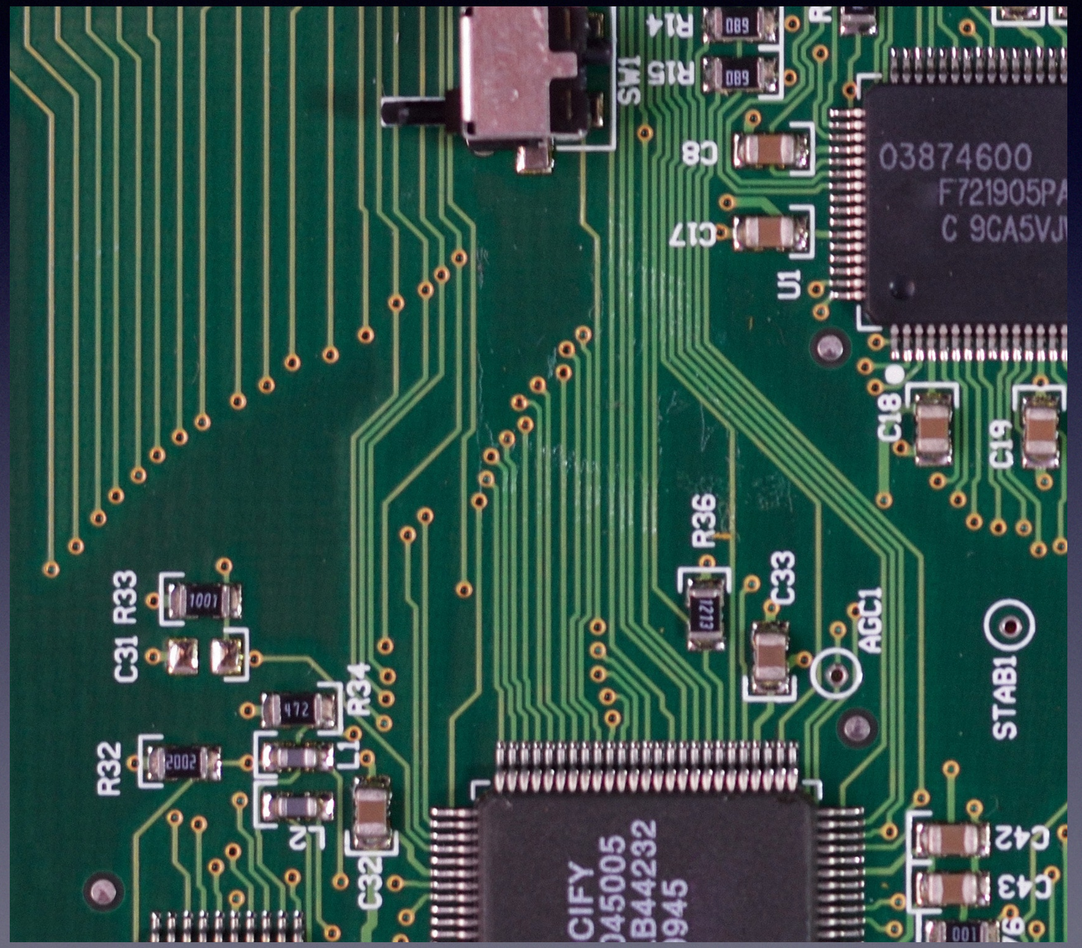
- Platforms actively maintained against edk2
- Default branch (master) contains platforms actively validated against edk2/master
- **stable**- branches track UDK releases
- **devel**- branches host works in progress



https://github.com/tianocore/edk2-platforms

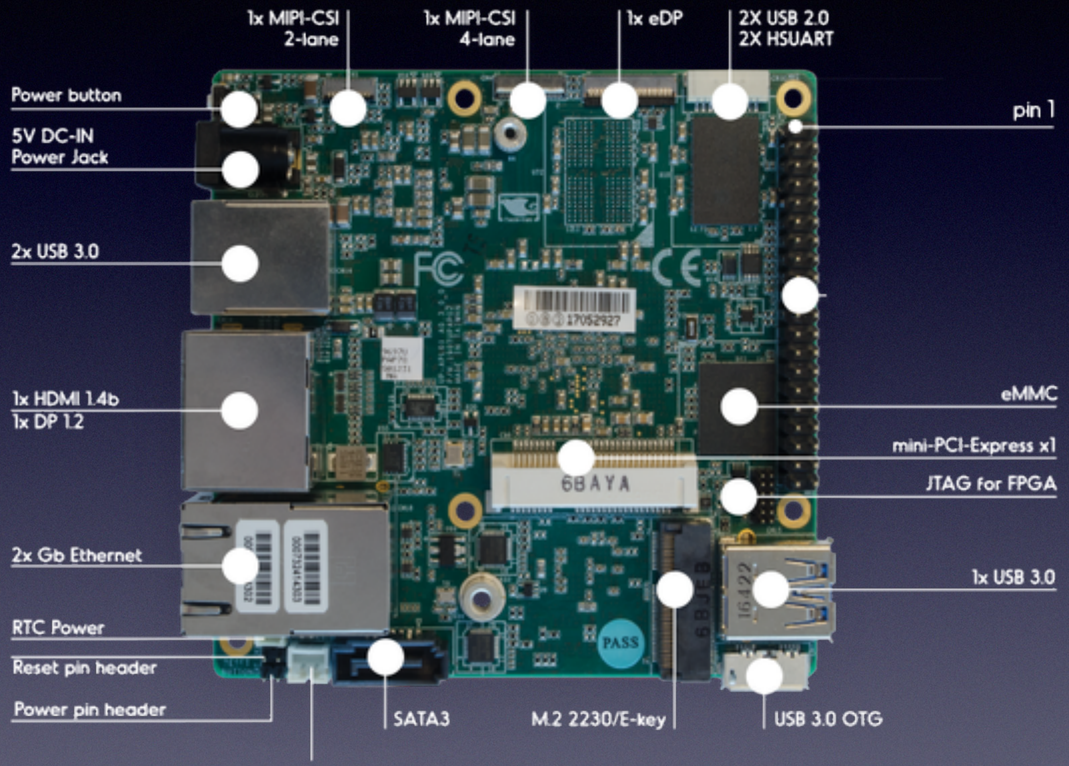
EDK2-Platforms In Progress

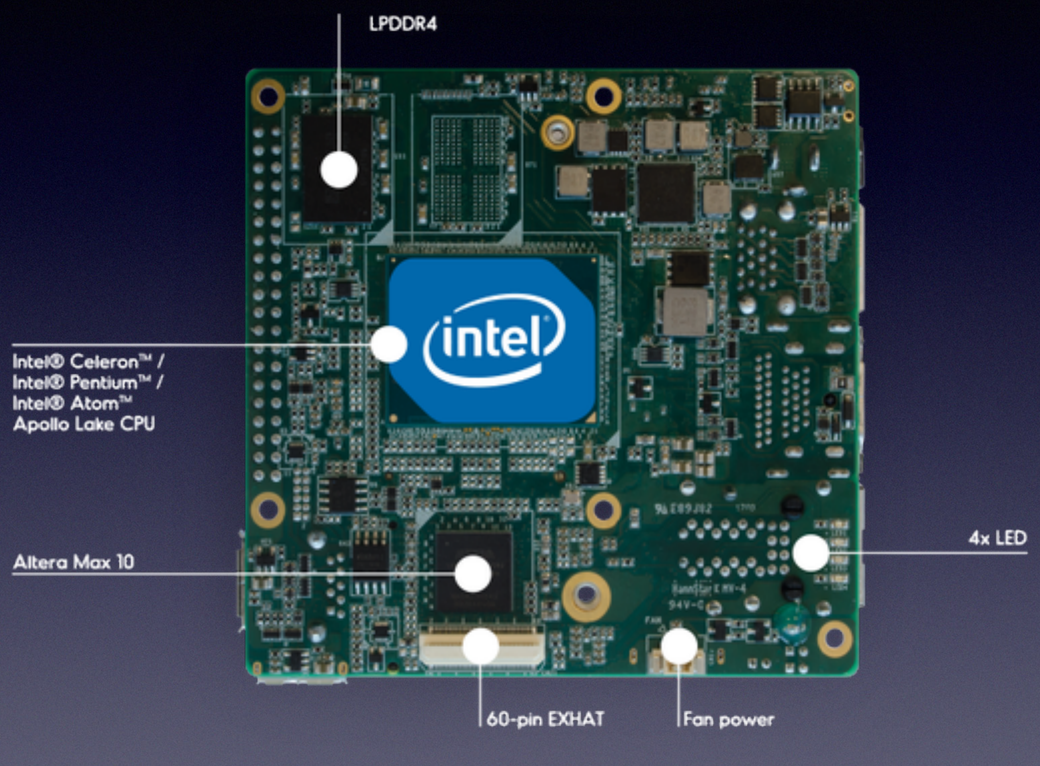
- BeagleBone Black
- Aaeon Up² Board
- Marvell MACCHIATObin
- MinnowBoard Max / Turbot



https://github.com/tianocore/tianocore.github.io/wiki/EDK-II-Platforms

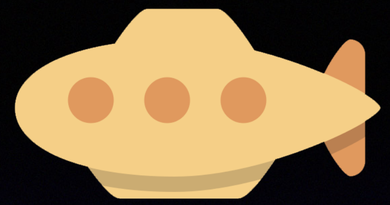
Example: Aaeon Up2 Board



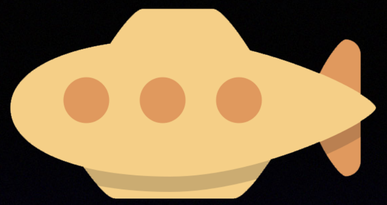


https://github.com/tianocore/tianocore.github.io/wiki/IntelAtomProcessorE3900

https://github.com/tianocore/edk2-platforms/tree/devel-IntelAtomProcessorE3900



License	GPL
Size	100s kb
Market	Embedded, Integrated
Coding Style	Linux
Payload Interface	“UEFI Lite”, Direct Linux, U-Boot API



tianocore

License	GPL	BSD + CLA
Size	100s kb	low MBs
Market	Embedded, Integrated	Mixed Closed+Open (IHV)
Coding Style	Linux	CamelCase
Payload Interface	“UEFI Lite”, Direct Linux, U-Boot API	UEFI, PEI

tianocore

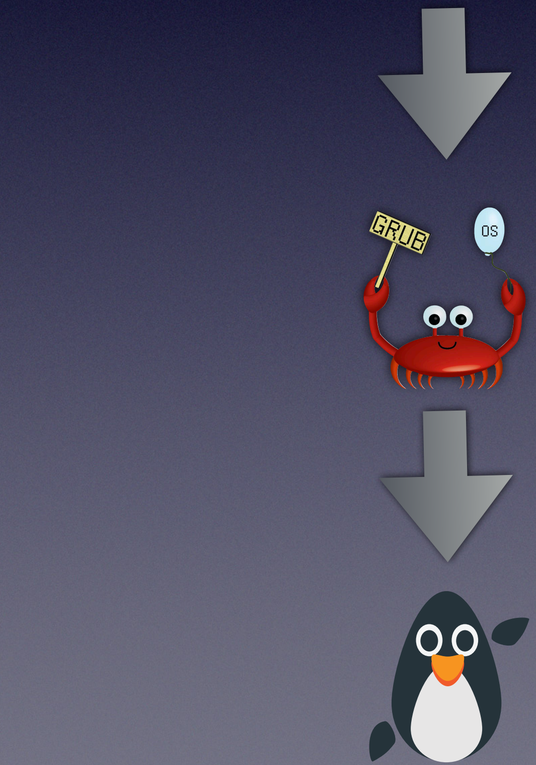
“UEFI Lite”

UEFI

tianocore

“UEFI Lite”

UEFI

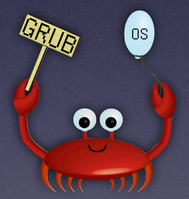


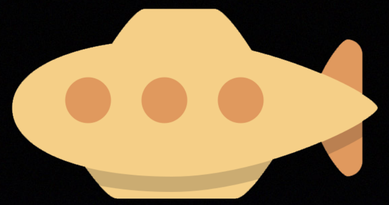
tianocore

“UEFI Lite”

UEFI

Interface





tianocore

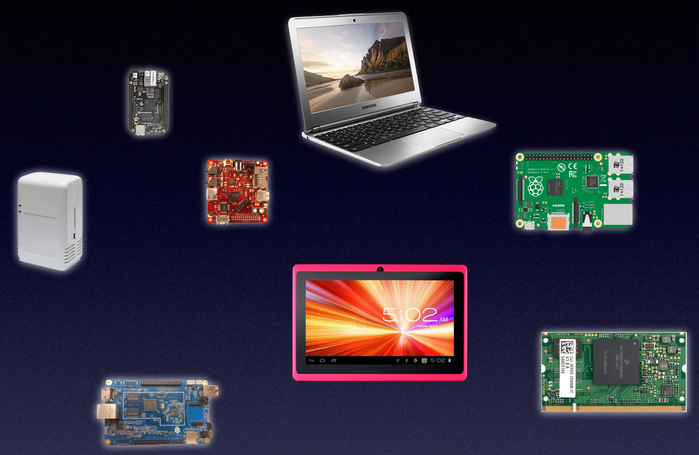
“UEFI Lite”

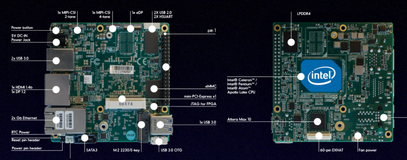
UEFI

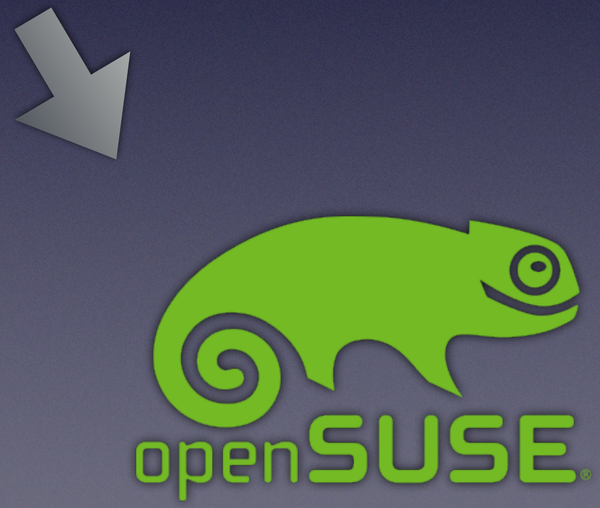
Interface

openSUSE

tianocore

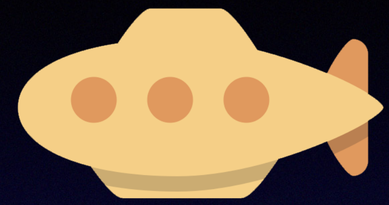






Contributions Welcome

tianocore



https://www.tianocore.org/contrib/

edk2-devel@lists.01.org

@stephano

stephano.cetola@intel.com

https://www.denx.de/wiki/U-Boot/Patches

u-boot@lists.denx.de